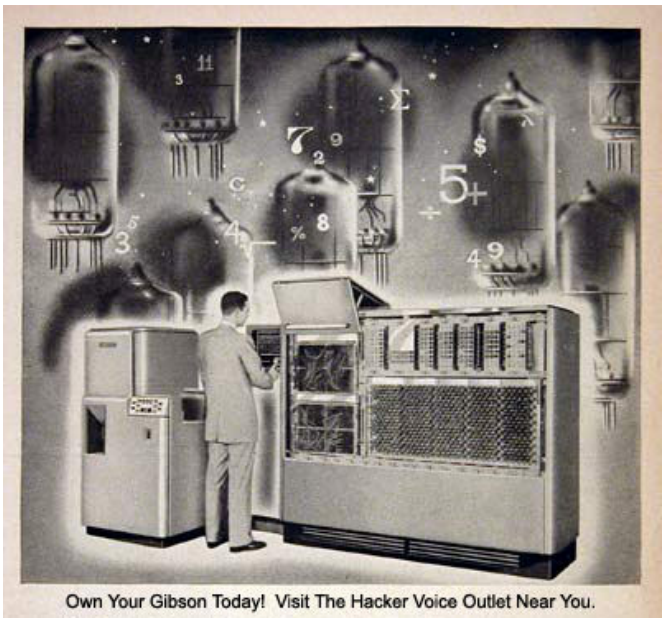
THE HACKERS VOICE

TELECOMMS DIGEST

A ROUGH GUIDE TO NUMBER STATIONS
BTS LINE TEST NUMBER MAPPED
PHREAKING AROUND WITH ASTERISK
CAFFEINATED BEVERAGES
WHO ARE THEY WATCHING?
SOCIAL ENGINEERING
AND MUCH MORE!

DIGESTIVE CONTENT



Own Your Gibson Today! Visit The Hacker Voice Outlet Near You.

The Hackers Voice Telecomms Digest Team

Editors:	Blue_Chimp, Demonix.
Staff Writers:	Blue_Chimp, Naxxtor, Belial, 10nix, Demonix & Hyper
Contributors:	UltraViolet, eDgE, and Sam.
DTP:	Demonix.
Cover Graphics:	Demonix.
Printing:	THV. A limited number of printed versions of this digest is made available on release please contact the HVR team for further details.
Thanks:	To everyone who has input into this issue, especially the people who have submitted an article and gave feedback on the beta releases.
Back Page:	Demonix.

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.

The Hackers Voice projects include a Radio Show, Forums, an IRC server and much more. Please visit our site and join in with the community:

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

Article Submissions. Photos & Letters

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**

Disclaimer

The views expressed by the contributors are not necessarily those of the publishers. Every care (well some) is taken to ensure that the content of the digest are accurate but we are not able to accept responsibility for errors. The publisher and contributors will not be responsible for any police or military action that occurs to you if you use the information provided for illegal activity. If you go to Jail for some reason do not blame us when you drop the soap.

CONNECTIONS

It has been almost two decades since the dawn of modern computing. We have seen many technological advances to our lives and the silicone solid state microprocessor has revolutionized our worlds. At the forefront of this revolution were unique individuals who can only be described as explorers of the modern age. They dedicated their lives to bringing something so complex, bulky, expensive and specialized into the homes of the every family.

The true meaning of this modern age is the advance of our most powerful organ, the human brain. We above all species seek to communicate with our fellow sapiens. This drive has brought us to develop and improve on technology that joins towns, cities, countries and continents. Every person born today is, from a very young age, taught to use and master this technology. We alone live in an age when children do not know a time before what is the most amazing technological advance in human history, borne from the need to communicate, in the dangerous and life threatening time of the Cold War. The Internet.

It is a true living creature that lives, grows and dies, made by man, and fed is massive amounts of data on a daily basis. Almost every single person in the western and developed world uses the Internet for one means or another. Peoples lives are recorded - their events - birthdays, marriages, deaths – rises and falls.

Everything we want to share is logged, stored and distributed. We can reach and talk to people in real time instantly who are across the other side of the world! It's amazing how from such a simple plan and idea that a massive network of interconnected, routed, computers has developed.

This tool can make you an instant celebrity; it can bring you closer to friends and loved ones. It can also help to manage and organize your life better. The Internet truly brings a large degree of freedom to human kind. It’s something so cold and mechanical, but paradoxically so very natural and human.

That human factor creates problems. Mainly due to the side effects of this true and free information exchange, and power enabling source of mass communication. As we have known throughout history that the biggest enemy to dictatorships is a free minded educated population. This problem brings a very interesting twist to our unique masterpiece. For who owns access to the Internet can sell it to others and control it. This means that for those who fear their governments retribution for their peoples speaking their minds are again being quashed by the higher powers eroding their freedoms of communication. It is only due to the nature of the beast is such that who owns connections to it controls the flow of information.

So are we facing a backfire of our dream? Has our openness to share and communicate brought us to a vulnerable and uncertain state?

If information is truly power, then should our scientists and greatest creative minds be our leaders? However the contrary is true.

If we are seeing a stall in the expansion of the Internet and a tightening of its freedoms is it possible that we are on the step of a controlled and censored Internet stairway?

Ever since the globalisation of the computer it can be noted that what was done to give it birth, and the skills to tinker and experiment, has been bought out by businesses and governments, and replaced with adverts and shiny slogans. Somewhere along the line of the process - something went horribly wrong.

But if this is the case then what can now be done? What kind of power do we have, as individuals?

Well we still have the ability to improve technology, we can adapt and develop, we can communicate, and we still are able to communicate freely with one and another. This magazine, for example, is an expression of the right to distribute information and thoughts freely: so you should be able to do the same.

We have to take back the Internet for ourselves. We need to be able to regain the true meaning of freedom of information and remove politicians, governess, finance ministries and corporations from violating the Internet. Maybe the realization is that people have been given a powerful tool - but they never truly understand to how best use it. It seems as if the computer has been "dumbed down". We need to re-educate the youth. The only way we can do this is if we shed the detrimental negative associations with the word "hacker".

We are the few who still express that same desire for knowledge and development of technology. We understand how the Internet works - better than the average person. It's not a great surprise how many people really don't understand the concept of the Internet and computers. But they use it almost every day. In fact, this technology means that they may not even have an job, or an industry, without it.

I feel that it is our duty to use our skills and technology to free information: educate others and fight anyone who wishes to censor it. Within this magazine is but a small snap shot of our journey through understanding how the world around us works. It is therefore our duty to bring this information to you and give you the right to distribute and improve on this. The concept of learning, understanding and teaching should be revived and empowered. We can do this and we will do this.

For however long it takes, information wants to be free and we will deliver it to our fellow man.

I hope you will enjoy this first issue of our magazine and I invite you to join us on our journey. You can contribute, regardless of your skill level. Take the first step to reach out and use the power of the Internet to communicate with other like minded individuals...

Belial

Belial.

ROUGH GUIDE TO NUMBER STATIONS

Part #01
By Demonix

- Introduction
Half way through 2006 I started to investigate the phenomena known as Number Stations and its time for me to share what I've found in a series of articles which I will be releasing via The Hackers Voice. When I first started to look into Number Stations I found that there were no decent guides for "Noobs" and most information threw the reader right in at the deep end. Hopefully my guide will give you a foot up into the murky world of Number Stations and give you the knowledge to start to look deeper!

As a side thought, remember that I am not an expert on the subject, rather I'm someone who's has a deep interest in it and wishes to share what he has found. If you have anything to add/expand upon what I have written please get in touch, even if it is to correct me. I'll use the feedback in the other articles and of course you'll get a shout out.

I decided to split the guide into a number of questions which I would have liked answered when I first started to look into the subject, so let's get on with things…

- What are Number Stations?
They are Shortwave Radio (3Khz to 30,000Khz) transmissions that seem to appear at random and have no specific origin. The transmissions normally involve voices repeating strings of numbers or letters. On further investigation a fair few Number Stations are not random at all and in fact transmit on a regular basis through out the year. It is good to note there are some Number Stations that do not involve voices; we will go into the different types further on in the article.

- Who is transmitting?!
No one really knows, but we can speculate on who or what is behind the transmissions which include Spies, Drug Dealers and Armies. Some claim that the stations are closely linked with espionage activity. There are a few rouge HAM radio operators which enjoy a laugh at others expense too.

It is possible to track the signals but most of the people interested in Number Station do not have the equipment required to carry out the work involved. A couple of more experienced HAM radio operators have allegedly managed to track down the source of a few Number Stations but I'm yet to see any proof of the tracking method and from what I can see they have just claimed it was from an Army base.

Naxxtor's Comment: "*The main reason it's hard to track down is because the shortwave transmitters are in the Megawatts, and the signal is so strong it will go through the planet*".

- How are the Messages transmitted?
Basically any High Frequency transmitter can be used to setup a Number Station but how far the signal goes is another matter. As well as the transmitter power (normally seen measured in watts) you need to take into consideration things like season, weather conditions, local RF noise (my own PC seems to cause a lot of interference for example), and sunspots cycles. These conditions are important as they affect a phenomena known as radio propagation.

Radio propagation is where radio signals "bounce" around the Earth using the ionosphere (that's the upper most bit of the atmosphere) allowing the signal to travel long distances. Bad weather, local interference etc causes the signal to degrade and sound faint/crackly.
With this in mind when you hear a Number Station the chances are that it is not based on the other side of the planet… unless of course the Number Station owner has some very highly powered equipment!

- **What is being transmitted?**

At present we do not really know what is being transmitted but there are a few groups on the internet who are logging and monitoring the transmissions in hope of one day decoding the messages. It's suggested that the strings of numbers/letters are encoded messages which to decode requires the use of a "One Way Pad".

Finding a Number Station broadcast without a schedule can be a bit hit and miss too so I suggest that you try find one on the internet before trying to search. One schedule we can recommend is the one maintained by the Enigma 2000 group. Details about this group can be found at the end of this article.

Transmissions in Europe are normally in English, Spanish, German, Chinese or Russian languages and consist of many strings of 4 or 5 digit groups of numbers. Sometimes the messages start and end with special strings of numbers or even music or a tone. In the US Number Station voices are generally in Spanish but there are ones that use English.

Some Number Stations use a Phonetic Alphabet to transmit the messages. There are many different ones in use and the most popular in use today is the NATO Phonetic Alphabet which dates back to around 1955:

NATO Phonetic Alphabet				
A - Alpha	F - Foxtrot	K - Kilo	P - Papa	U - Uniform
B - Bravo	G - Golf	L - Lima	Q - Quebec	V - Victor
C - Charlie	H - Hotel	M - Mike	R - Romeo	W - Whiskey
D - Delta	I - India*	N - November	S - Sierra	X - X-ray
E - Echo	J - Juliet	O - Oscar	T - Tango	Y - Yankee
NOTE: * Indigo is used by the UK Police				Z - Zulu

The NATO Phonetic Alphabet is approved by the International Civil Aviation Organization, and the International Telecommunication Union. It's good to note that there are variants of this alphabet in use all over the world too and during World War I and II a few different alphabet systems were in use. If you are interested in looking into these systems we suggest that you do a couple of searches on the Internet.

Mon 14th May 2007, 12:30 on 7918Khz

```
YHF 3m m g120 t

KIBRB YAQWY ZWGDW EBRYG LTCXW CELXP RHGGF ZSNWM KAMXB KGNAN

WSEWK THPYG HQNBF ETSQF OOWDQ KGBEJ NNXAR NXYKJ DADZU IEUVP

RDUAD IJRWO QKBLH IKTNU GVJUU PUREP NMCQR IITQZ IHTQA AIZSQ

FGQFO SSVJK KBGGW HZCGK SHJFH ULGWO KJLOZ FAGQN ENZRD PFSAF

BXSWZ EISVX YULQM UIXSI MXSZX ADDYL AWLOK YTYLP URPBC XTDQT

CBCWO TEXBX MBMHO QVPYY ODNNO GBUOO MIYRQ RFCUC LXSSE ISGTO

QITTY PCHLH EVRSZ COCZN NPVMH KPICQ IASBJ OGMXR LIEAO AGBPT

YTCJP TKRGC YGLEB BMLWC JRPJM JDKLV XZAUD HZPJB SZNWN WMKPK

BXQIE FUHRL RHKKT LGWRU IEUWQ BQWMI JYIFL WPKHR ISKGD GLFVO

RABPQ BPHRF RPFUS HNKTU GKZIM LDAYH YCOKJ EIANS TARJC NZVTQ

ZKWST MWRTA NZURB CQXYM ZRJCM JVVWV BSAYG PNEYM LBHBO LRVXZ

HNFRF IKCTE VGJEM LQAED ZKZIS IMUYQ ELJLX AFOYH QVZPJ NIYBC

eom m g119 t
```

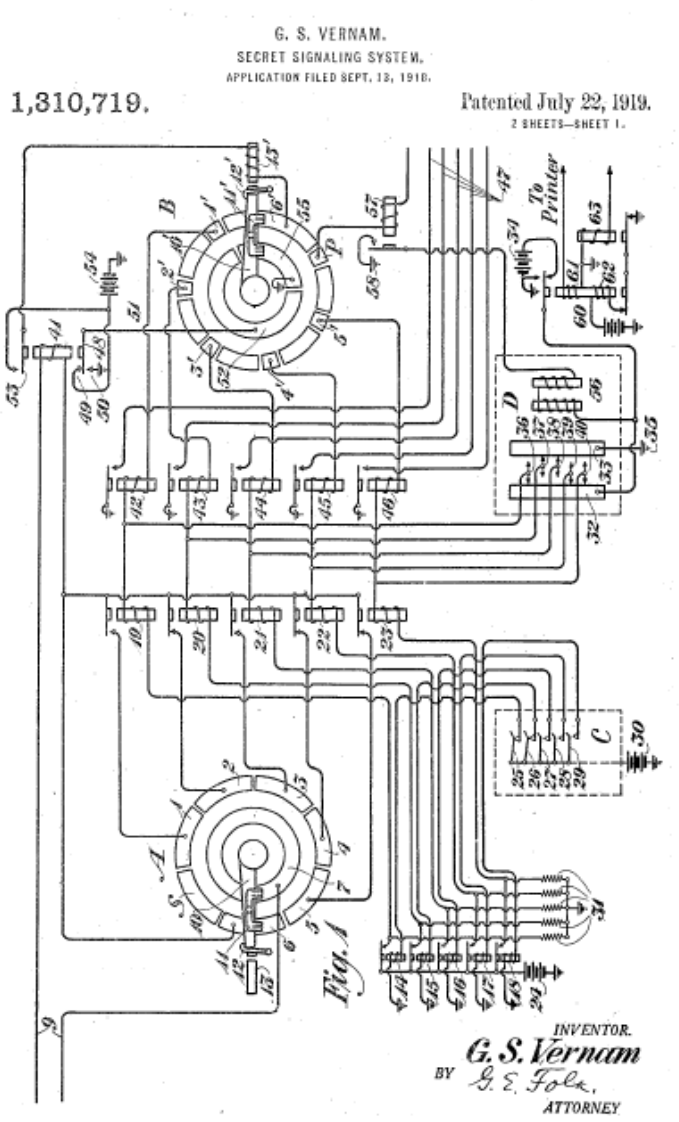
To give an example of what is transmitted we have taken one which was recorded back in May 2007 by "Alpha" which you can see on the right.

Something to think about….

Radio listener's equipped with spectrum analyzers have claimed to have found data bursts within the transmissions. Only recently we were listening to a transmission and noticed that there was a very short burst of data. We could hear this without the aid of a spectrum analyzer and we will report further on these findings in the future.

- What is a "One Way Pad/One Time Pad"?

It is an encryption system that was originally created by Gilbert Vernam (an AT&T Bell Labs engineer) and later enhanced by Joseph Mauborgne in the mid 1920's. Gilbert invented the Vernam Cipher but it was possible to break the code; Mauborgne noticed this and enhanced the system (called a One Time Pad) which seems to be in use on the Number Stations that are heard on a daily basis.


G. S. VERNAM.
SECRET SIGNALING SYSTEM.
APPLICATION FILED SEPT. 13, 1918.
1,310,719. Patented July 22, 1919.
2 SHEETS—SHEET 1.
To Printer
Fig. 1
INVENTOR.
G. S. Vernam
BY G. E. Folk,
ATTORNEY

On the left you can see a copy of Gilbert Vernam's patient for his "Secret Signaling System".

The sender and the receiver of the encoded message have the same "Pad"; The "Pad" being a book of paper which contains hundreds of sheets and each sheet having a seemingly random set of numbers/letters/ words.

A random key is used per sheet and this can be used to do a lookup to encode/decode the messages.

We will be going into more detail about One Way/One Time Pads in a future edition of the magazine but if you wish to find out more we suggest you track down the original patient information for some interesting in-depth information.

The Vernam Cipher is actually used today in computing for many applications. The most widely used is RC4 which is used in protocols such as SSL (to help protect Internet Traffic) and WEP (to help secure wireless networks for a few minutes). RC4 is not seen as a good crypto standard to use these days but is still widely used and abused!

```
55847 55844 2794 42794 00729 00729 72689 72689 3721RM 37211 20260
20260 02865 2865 70256 70256 54486 54486 52749 S2749 76810 76810
```

- What types of Number Stations Exist?

Number Station Classifications		
Type	**Medium**	**Details**
Voice Station.	Shortwave Radio.	This is the most distinct and no doubt the most monitored type of Number Station. Male/Female Voice can usually be heard in various languages.
Music/Jingles/Weird Sound Effects.	Shortwave Radio.	Some Number Stations use a jingle which signals the start of their transmission, one example of this is the fabled "Lincolnshire Poacher" Number Station.
Morse Code.	Shortwave Radio.	If you do not know Morse Code it'll be difficult to understand what is being transmitted. I found that a piece of software called UA90V CwGet was good for decoding Morse Code from .wav format.
RTTY.	Shortwave Radio.	Radio TeleTYpe. This sort of transmission sounds like a very slow modem. To receive these type of transmissions you'll need to hook up your radio to your PC or an old Tele-Printer. There are various free applications that you can download from the internet that allow this.
Military Stations.	Mixture.	The Military use all sorts of methods to transmit encoded messages but strangely they still use Voice Stations.
Telephone / VoIP Station.	Internet/Phone	The VoIP Number Stations seem to be fairly new and the only one I have heard was broadcast on 2600's Off the Hook Radio Show. Another hacking group was behind the station but its interesting to see how they got people to call a number and listen to the message and try to decode it.
Pirate Stations.	Shortwave Radio.	Perhaps a rogue HAM Radio operator with no license transmitting random stuff.
Drift Net Beacons	Shortwave Radio.	This is a new subject area for me and I'm still learning about it. If anyone has any details about a Drift Net Beacon Number Station please get in touch.
Time Signals	Shortwave Radio.	Time Signals are used to help synchronise clocks etc but it's been noted that some time signals have been appearing on strange frequencies transmitting the wrong time. Could this be a Number Station?
Other Examples	TV / Movies	TV and Movies have also used Number Stations and the most recent to memory is in the American TV series Lost. The Number Station was transmitting a series of numbers which keep cropping up though out the first few series.

- What or who is this "Lincolnshire Poacher"?

"The Lincolnshire Poacher" is a folk song which one Number Station plays just before and after a transmission. The LP Number Station appeared in around 1970 and at first the voice on the Number Station was not electronically generated (i.e. it was read out by a human).

Example Broadcast Schedule

MONDAY
1400 10426//12603//14487
1500 11545//13375//12603 or 15682
2000 11545//??//??

TUESDAY
1400 12603//14487//??
1500 10426//??//??
1600 11545//13375//??

WEDNESDAY
1300 14487//15682//16084
1400 14487//15682//16084
1500 11545//14487//16084

THURSDAY
1300 16084//??//??
1400 14487//15682//16084
1500 11545//12603//13375
1600 12603//14487//??

FRIDAY
1300 14487//15682//16084
1400 14487//15682//16084
1500 11545//12603//13375
1600 11545//13375//??

SATURDAY
1300 14487//15682//16084
1400 11545//14487//??
1500 11545//12603//13375
1600 11545//12603//13375

SUNDAY
1400 11545//14487//15682
1500 11545//12603//13375

NOTE: This schedule was taken from the Spooks Digest

Structure of the LP Broadcasts

Here is an example structure:

1. The Lincolnshire Poacher Tune is played around Twelve times.
2. A five figure header is read five times.
3. A Pause occurs then followed by the Header being read five more times. Sometimes a glockenspiel is played twice.
4. 1 to 3 is then repeated five times giving sixty responses if you write them all down.
5. Three pairs of chimes are heard.
6. 200 five figure groups of digits are read out.

"The Lincolnshire Poacher" Song

When I was bound apprentice, in famous Lincolnsheer,
Full well I served my master, for more than seven year,
Till I took up with poaching, as you shall quickly hear:
Oh! 'tis my delight of a shiny night, in the season of the year.

As me and my companions were setting of a snare,
'Twas then we seed the gamekeeper, for him we did not care,
For we can wrestle and fight, my boys, and jump o'er everywhere:
Oh! 'tis my delight of a shiny night, in the season of the year.

As me and my comrades were setting four or five,
And taking on him up again, we caught the hare alive;
We caught the hare alive, my boys, and through the woods did steer:
Oh! 'tis my delight of a shiny night, in the season of the year.

I threw him on my shoulder and then we trudged home
We took him to a neighbor's house, and sold him for a crown;
We sold him for a crown, my boys, but I did not tell you where
Oh, 'tis my delight on a shiny night in the season of the year.

Bad luck to every magistrate that lives in Lincolnsheer;
Success to every poacher that wants to sell a hare;
Bad luck to every gamekeeper that will not sell his deer:
Oh! 'tis my delight of a shiny night, in the season of the year.

Interesting Information…

- On looking about the Interweb we found that there's a cheese called the "Lincolnshire Poacher":

- The Number Station was apparently traced to RAF Akrotiri in Cyprus but there is no concrete proof available to prove this; if you look online there are a few photos or the apparent site but there's no additional detail to go with it. Perhaps there are a few locations which use the same system?

Other Interesting Information about LP…

- **The** Lincolnshire Poacher song is believed to have been created in 1776.
- Some of the UK Number Station groups do not like to talk about the LP Number Station and sometimes talking about it can generate a flame war.
- The song is used as the quick march of the RAF College Cramwell.
- The woman's voice used in the transmissions seems to be used often on Shortwave radio.
- Someone has tried to jam the LP transmissions but no or little luck.
- During a transmission is has been noted that the inflection on the voice changes between number groups.
- There is a cheese called The Lincolnshire Poacher.

- **Are you sure all Number Stations are Spies/Drug Dealers/Army?**

Some of the transmissions have been created by rouge radio HAMs (having a laugh), radio engineers carrying out tests etc. Some of these stations are solved and are well documented on the internet. There are a lot of hoax information on the internet about Number Stations too so beware what you read, it may be a complete lie!

One of the more interesting transmission types is generated by the US Army called an EAM - Emergency Action Message. The US Department Global High Frequency Network (or GHFS) uses similar methods to Number Stations to transmit messages from their aircraft and ground stations.

The GHFS uses both plain text messages (usually from Aircraft) and encoded messages from one of their many ground stations. Have a search around the internet and you'll sure to find some more detailed information about these transmissions along with some example sound clips.

- How do I listen to Number Stations?

One way to listen to the Number Stations is get hold of a decent AM Radio that has SSB support. SSB is Single Side Band modulation which allows the signal to be finely tuned. Without SSB it's almost impossible to hear the Number Stations but on AM you may be able to hear what sounds like the parents from Charlie Brown on acid or very muffled gobbledygook.

Believe it or not a similar SSB technology was used during the 1930's for sending multiple voice signals down phone lines. We will explain SSB in more detail in future digests.

One of the better AM Radios with SSB support is the Eton E5 which you can see on the right. Its SSB turning is second to none and as the radio is small it is highly portable and can be used just about anywhere. Its well worth looking online for other AM/SSB Radios and use the Eton E5 to compare with that you find.

The other nice feature of an AM/SSB radio is that you can also listen in to HAM Radio, Maritime, Aeronautical, Military, Fax, RTTY, Morse Code and some other weird broadcasts.

If you do not have a vast quantity of cash available but still wish to listen to Number Stations we suggest that you join some of the online groups or use a search engine to find some sound clips.

We will detail better frequency information in the future parts of the guide but here is a small list which may come in handy (Note these may be different in the US):

1700-1800 Khz	HAM Radio (160m)
1800-2000 Khz	Maritime Communications
2182 Khz	Maritime Distress Channel
2850 – 3150 Khz	Aeronautical
3150 – 3200 Khz	RTTY
3200 – 3400 Khz	HAM Radio (90m)
3400 – 3500 Khz	Aeronautical
3500 – 4000 Khz	HAM Radio (80m)

4000 – 4063 Khz	Military
4063 – 4438 Khz	Maritime
4125 Khz	Maritime Call Freq'
4438 – 4650 Khz	Fix/Mobile Stations
5950 – 6200 Khz	49m Broadcast
7000 – 7300 Khz	HAM Radio (40m)
10100 – 10150 Khz	HAM Radio (30m)
14000 – 14350 Khz	HAM Radio (20m)

- What Online Groups Deal With Number Stations?

These groups on the Internet are worth looking into:

Spooks Digest

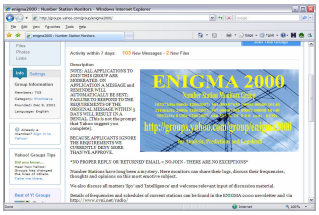
- This is a daily/weekly email digest which people post Number Station material to. Some of the posts can be confusing unless you understand the format being used. If you do join its worth while looking. To sign up pop to this web site:

http://mailman.qth.net/mailman/listinfo/spooks

Also check out the owners main Number Stations pages here:

http://www.spynumbers.com/

Enigma 2000



- One of the best resources we know of is the E2k group. To join the group you need to fill in an application form which can be found on their web site:

http://groups.yahoo.com/group/enigma2000/

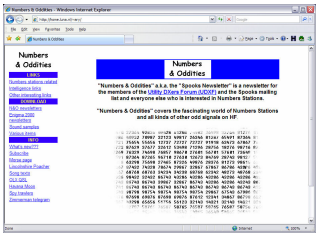
Once accepted you will receive their daily digest which contains details of recent transmissions plus some interesting chats from the members. E2k release a free magazine on a random basis which is normally a good read. The E2k group also offers other useful tools which includes the known schedules of the Number Stations they are tracking.

The Hackers Voice

It goes without saying that THV is a good place to find out more about the Number Stations and chat with people who are interested in the subject. THV have forums and an IRC channel dedicated to Phreaking and everyone is welcome along to talk and give their thoughts about the subject:

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

Numbers & Oddities Digest



This Digest covers Number Stations as well as many other weird signals that can be heard in HF. The site has archives of all their digests as well as samples of recorded signals.

The Digest is available from here:

http://home.luna.nl/~ary/

- What Else is Handy to Know?

Listening to Numbers Stations in the UK is apparently illegal under the Wireless Telegraphy Act 2006. As the stations are not meant to exist I'm not sure how someone would be prosecuted for listening and recording the transmissions without blowing the cover on something big!

- Questions?

If you have any further questions or wish to know about a certain aspect of Number Stations more in-depth please get in touch and we'll try to include the answers in future magazines.

Rough Guide to Number Stations – Part 2- Coming Soon!
We look more in depth at One Way/One Use Pads, Frequencies, More Famous Stations, Drift Nets and Time Signals.

MAPPING THE BT 17070

By Blue_Chimp

First off a little background 17070 as you may or may not know is BT's line test phone number. There are a number of options available to you on it. I took the time to map it, due to there not actually being a map I hope you enjoy and find it useful, there are a number of very interesting features.

Right so simple first step pick up your phone and dial 17070. After it reads back your telephone number (This Circuit is defined as 0207 60* ***4), You are then presented with a number of options in numerical order as shown on the right:

1. Ringback Test.
2. Quiet Line.
3. Fast Test.
4. Fast Clense.
5. Clear Down.

So starting with #1 its quite simple you press 1 it tells you to clear down (BT talk for hang up), It will then call you with the message "Ringback Test Completed, Thank you for using BT's linetest facilities, goodbye) Also on CID enabled lines the callback test comes back as 08003289393

Next up is #2 'Quiet Line' which really does exactly what it says on the tin, it keeps the line open and stays quiet. It doesn't respond to any DTMF (I tried all on the standard telephone keypad) it also says "Silent Line" every 1 or 2 minutes I was not sitting there with a stopwatch!

Right this is where it gets interesting #3 'Fast Test' right upon dialing 3 you will be greeted with; "Press 1 if you have been authorized to use this system" at your own risk press 1. Then you will be greeted with "For the new and enhanced test's including copper line and digital press 1" again, at your own risk press 1. You will then greeted by a new sub-menu of 5 options:

1. Copper Line Test.
2. Digital Test.
3. Results.
4. Cable Pair ID.
5. DSL test including DSL Net Check, DSL frames jump, CAMS switching.
6. Local Loop Unbundling Options.

All of the above require a valid mobile phone number (probably an engineer's number) followed by what BT term 'Square' (it often confuses a lot of new phreaks) Square is BT term for #, simple!

Right so leaving behind Fast Test behind, We have #4 Fast Cleanse. We have 5 Main options in numerical order:

1. For Cabinet.
2. For Pillar.
3. For Distribution Point.
4. Record Spare Terminations.
5. Record Pair Terminations.
6. Clear Down.

For sub-option 1 you are asked to enter a cabinet number followed by square (#), I dialed 456 then followed it with # (the Cab number is usually found on the side stenciled in white paint it's a 3 digit number as far as I know). I was then presented with the following options #1 for 'E' side number #2 for 'D' side number

The next one oddly enough is #2 the 'Pillar' option upon dialing this I was asked to enter pillar number I again dialed 456 followed by # I was then given the following options #1 for 'D' Side #2 for 'E' Side

Option 3 'Distribution Point. I was asked to enter the 'DP' number followed by Square (#) I again dialed 456. I was then given then option "'Press 1' for Cable Pair number followed By square, For non-numeric press star (*)"

Option 4 is 'Record Spare Terminations. Again I was greeted with 'Please Enter '1' for Cabinet, '2' for Pillar, 3 For Distribution Point, all of these ask for ask for a Number I again dialed the usual 456 followed by # then I was given '1' for 'E' side '2' for 'D' side

Last but not least is option #5 'Record Pair Terminations' press '1' for cab '2' for pillar '3' for Distribution I was then asked for a pair number (which can be found in the Cab box).

Conclusion:
As you can see there is a hell of a lot of options for 17070, I also understand some options may not be available on certain exchanges or some may have more options. Also the most interesting out of all of these seems to be the fast test options, if you have successfully dialed into any of these options, I am very interested to hear what came of it, please let me know I will give full credit to you (I personally hate plagiarism). If you have anything corrections, or anything in addition to add, please contact me at, blue@bobsbasement.co.uk

Shouts: Muftak, Metatron, BOfH, SHAGGSTaRR, the rest of HVnet and H-Sc check them out at www.hackscotland.com

COMMUNICATIONS

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

letters@hackervoice.co.uk

"The UK Hacker Scene" – A Letter from eDgE…

I think the UK hacking scene is moving too slowly. We're miles behind the US and many other countries like Germany because we don't communicate enough as a hacker community and this keeps us as an ineffective group of people. If we met up, or had regular IRC conversations, we could collaborate for big projects and UK hackers could have a voice.

Not just about electronic hacking or computer systems but also the freedom of speech that has been the legacy for hackers in the US. I found it hard enough to get into the hacker community but for new geeks it must be almost impossible.

N00bs are the new generation of hackers and we need to help them become good hackers, intelligent hackers, NOT script kiddies. Comparing the UK to the US again, we are lazy. Americans travel miles across the US just to meet up with other hackers while us in the UK don't even email each other. This is why we are not developing fast enough; because we don't work together.

I don't want to go on about the UK hacking community but I hope you understand how important it is to create and develop a strong force of computer experts in the UK.

eDgE

THV Magazine Replies….
This letter was sent to us be eDgE many moons ago and THV have surely helped with the UK hacking scene since then… but we would like to reply to it anyway as it makes sense…

Please STFU you Emo Noob!

PART #1

BY

```
 _ ___ _
/ |/ _ \ _ __ (_)_ __
| | | | | '_ \| \ \/ /
| | |_| | | | | |> <
|_|\___/|_| |_|_/_/\_\
```

INTRODUCTION:
Welcome. Today I will be presenting international phreaking with the Asterisk Open Source PBX system, and free services. We will compile Asterisk from source, configure it to connect to Free World Dialup and Voip User, and then design a custom dial plan using the Asterisk Extension Language to make and receive calls (including provisioning US and UK phone numbers), route forwarding, establish encrypted connections, set up a conference calling server and a voice mail server on the laptop, and explore Caller ID spoofing, Backspoofing, and call forwarding manipulation in the US, and UK. Then we will briefly explore exploiting the weaknesses in the SIP protocol, and initiate passive digital wiretaps of a conversation using Wireshark. First a bit of a glossary on the terminology.

GLOSSARY:
Asterisk will be represented by * here-on in.

VoIP=Voice Over IP. (sorry)

PSTN=Plain Standard Telephone Network. This is the 'normal' telephone network that in the UK is run by the Dalek... I mean British Telecom.

ADA=Analog Digital Adapter. This allows you to use standard telephones with VoIP servers.

SIP=Session Initiation Protocol. This is the ipso-facto industry standard for VoIP. It is used by most major VoIP providers including Vonage, and initiated voice conversations over port 5060 then carries on packet communication over RTP. It is a rock soild Open source standard, and as it becomes adopted more the NAT transversal issues typically associated with it are being overcome using STUN servers.

IAX=Inter-Asterisk Exchange protocol. This is an open source protocol developed by Digium (the developer of *) for use with *. It offers many advantages over the SIP protocol, including seamless NAT transversal, and fixed bandwidth trunking. It also includes a little documented feature of 128bit AES encryption using MD5 authentication.

Skype=A bullshit proprietary VoIP service that uses a P2P connection system to route computer to computer calls, and offers incoming and outgoing PSTN termination for a fee. The protocol is closed source, and so there is little development of applications using Skype's network outside of Skype itself. Skype is the anti-thesis of *, and for the life of me I have no idea why it has become so popular aside from its ease of configuration and use. It is known for buggy software, dropped calls, and general suckyness. I will be happy to debate this after the presentation.

FWD=Free World Dialup. This is a free service that offers many of the same features of Skype, and many that Skype does not offer. The major difference is that FWD uses the Open Source SIP protocol, and allows the connecting client to choose its codec. It is fully compatible with * as well as any SIP softphone or ADA. FWD also offers free IAX termination. It offers free calls to toll-free numbers in 5 different countries including the US, and UK, and peering with over 50 different VoIP providers. There is also a little known quirk using * that allows you to set outgoing Caller ID fields for free. For this tutorial we will be acquiring two separate FWD #'s.

CID Spoofing=Changing the outgoing Caller ID presentation flags to mask the origin of a call.

Backspoofing=Using CID spoofing to pull CNAM (Customer Name) information.

-And Now For The Show!

But first a word about TrixBox. TrixBox is a CentOS based distro that comes with asterisk, and many other toys for asterisk included. It is solid, reliable and easy, so why not use it right? Well, it is a viable option, however, you will be limited in the ways that it can be configured. I always opt for flexibility over ease of use. Also using the vanilla * allows me the ability to continue to learn how * works, and the flexibility to make it work how I want it to. If you are new to linux, and * then trixbox may be a great place for you to start. If you are interested in rolling up your sleeves, and getting a bit dirty, then please read on.

INSTALLATION:
Firstly we will be installing * from source. There are Binary Packages available for many Distributions, but in order to use a recent version of the PBX it is much better to compile it from source.. I have already taken the liberty of installing all of the dependencies for *, so we will be compiling libpri, zaptel drivers (necessary even though we do not have digium hardware, we will need the zaptel-dummy driver for its timer to use conference calling).

OK, lets get started. Just do a standard:

./configure
make
make install

for zaptel, then libpri, then asterisk. On my laptop I have compiled the newest version of asterisk-1.2, but on the HVR PBX I am running the newest version of asterisk-1.4. I recommend 1.4, but am running 1.2 on my laptop because I have compiled some custom modules for * that demand 1.2. Both work, but 1.4 has the newest cool stuff. Anyway, if you are going to use 1.4 also make sure to : make samples. This will give you the sample configurations that are pretty well documented, though full documentation can be found on www.voip-info.org.

Please note that you can use a pre-compiled binary for your distribution, but chances are it will be a rather old version of *, and as development of the PBX happens quickly I find that it is best to use the most current versions.

After you have compiled * go ahead and run the command:

sudo su
asterisk -vvvvvc

* is run as root, so always make sure you have root access when running the server, the CLI, or editing the configs. This will start * and the CLI (command line interface) with a verbosity of 5. If all apears to be going well and you are dropped to the CLI> command prompt, then type:

stop now

This will stop * and bring you back to your prompt. Now lets cd to /etc/asterisk and issue an ls. These are the guts of *, the config files. You are now ready to make * your own.

CONFIGURATION:
There are 5 configuration files we will be using: sip.conf. iax.conf extensions.conf voicemail.conf, and meetme.conf. We will be writing extensions.conf from scratch. all the others we will be modifying to suit our needs. We will be starting with sip.conf. It is the configuration file that defines all of the SIP interactions. This includes both the Voip provider's servers, and the clients that will connect to * for service. We will be configuring one client, and connections to the FWD servers, and the Voip User servers. As we go I will explain the configuration options. I will also be providing the specs on the codecs available, and the pros and cons of each.

SIP.CONF
OK, lets open up sip.conf in your favorite editor (I like Nano), and take a look see. It's not as confusing as it may seem, lets just take it easy to start. The first thing we are going to need is to have a client to connect to the * server. Let's go all the way to the bottom of the conf and make up a sip client. We'll add these lines:

(The comments after the ; tags are just that, comments, and unnecessary for the conf to work, they are just my explanations)

```
[100] ;this will be the sip client designation we will use when dialing this phone in extensions.conf
type=peer
host=dynamic ;this indicates that the client can connect from any IP address
username=100
secret=MAKEaPASSWORD
qualify=yes ;this is not necessary, but with this tag when you issue the "sip show peers" command in the CLI it ;will give you the latency, and I like that.
port=5060 ;this is the standard port for SIP
nat=yes ;or no, depending on wether the client is behind a NAT firewall
dtmfmode=rfc2833 ;this is the dtmf signalling protocol to use. I also use inband on lines that i want to dial ;using a tone dialer
disallow=all ;this refers to codecs. This allows me to choose which codecs I want to connect using
allow=ulaw ;G.711u (see chart below)
allow=alaw ;G.711a (" " )
allow=gsm
context=local ;this is the context that will handle calls made to this client. So a client outside of the local ;context will not be able to dial this client's extension directly.
canreinvite=yes
callerid="10nix" <100> ;Anything in the "" tags is the Caller ID name, and in the <> is the #. You can set these ;either to the internal extension (as was done here), to one of your incomming #, or any other # for that matter.
```

OK, now we have the client configuration for our first sip client, but wait! We need a client! Here we have many options, ranging from free softphones, to ATA's (they allow you to use normal phones with VoIP, to costly, but really cool, IP phones. The choice is yours, but for now lets go with a free soft phone. We will be using thew Xten Xlite softphone offered by Counterpath. It is a sip softphone, and is freely available to download from: .
In addition to this there are Windows, Mac OS, and Linux versions of the phone available.

These instructions are for the linux version, other versions may vary:
After downloading the softphone lets go ahead and get it configured. Open up the menu button, and go to System Settings -> SIP Proxy.

Click on the first entry, and set it up like this:

```
Enabled: Yes
Display Name: (What you set as Caller ID in the sip.conf, same format, but with no "" on the Caller ID name.
Username: 100
Authorization User: 100
Password: (The password you cose in sip.conf)
Domain/Realm: IP of the * server, if on the same machine, use the local loopback 127.0.0.1
SIP Proxy: same as above
Out Bound Proxy: same as above
Send Internal IP: Default
Register: Default
```

The rest just leave the same. Now hit back twice and X out of the menu.
Now go to the command line on the * box, and type:

asterisk

This starts the * server as a deamon, and backgrounds it. To connect to the CLI issue the command:

asterisk -r

Now at the CLI>, issue the command

set verbose 8 (or: core set verbose 8 : for asterisk-1.4)
Now restart the xlite softphone. You should see the REGISTER happen in the CLI. Thats really cool, but without a dial plan, its kind of useless, but before we go on, we are going to configure sip.conf for making and receiving calls using FWD. I configure my systems for both SIP and IAX connectivity to FWD for redundancy.

The sip.conf for FWD looks a bit like this:

In the [general] section of sip.conf look for the portion that has the registers in it, and insert the FWD registration line:

```
register => ${FWD #}:${FWDpassword}@fwd.pulver.com

[fwd-gw]
context=fromiax ;we will be configuring FWD with IAX as well, and this is the context we will be dropping ;incomming FWD calls to
port=5060
type=peer
secret=${YOUR_FWD_PASSWORD}
username=${YOUR_FWD_#}
auth=md5,plaintext
host=fwd.pulver.com
disallow=all
allow=ulaw ;again this is a matter of preference and bandwidth. See chart below.
dtmfmode=rfc2833
canreinvite=no
insecure=very

qualify=yes
nat=yes
```

IAX.CONF
We will then move on to the iax.conf. This is the same sort of configuration as sip.rconf for IAX. We will be setting up an encrypted client, and a connection with the FWD IAX server. Again, the configuration options will be explained as they are set.

Before we set up an iax registration for FWD, log into the FWD web interface for your account, and make sure that you have iax enabled. At this point it is very simple to configure * for IAX FWD. Open up the iax.conf file with your favorite editor. Before we get into registrations, and configurations for clients and providers, we are going to tweak some general options. First off, we need to adjust our codec's for bandwidth. There are two ways to do this. The first is with the bandwidth= low,medium,high field in iax.conf. I prefer to comment that out entirely, and set the default codec's by hand. This is achieved in the general section of the iax.;conf in the same manner that we chose the codec's when configuring a sip peer in the sip.conf, i.e. with the allow= and disallow= options. Next we will scroll down to the IAX registration section, and have * register through IAX with FWD. We just add the line:

register => ${ FWD_#}:${FWD_PASSWORD}@iax2.fwdnet.net

Now scroll down some more, and make sure that the following portion is uncommented, and the context is changed to reflect where we are going to handle incoming calls from FWD:

```
[iaxfwd]
type=user
context=fromiax
auth=rsa
inkeys=freeworlddialup
```

That was easy enough, now lets set up a couple of encrypted lines so that they can talk to each other securely. Scroll down to the end of iax.conf, and add the lines:

```
[1007]
type=friend
host=dynamic
username=encrypt1
auth=md5
secret=VERY_SECURE_PASSWORD
trunk=no
notransfer=no
encryption=aes128
disallow=all
allow=ulaw
context=encrypt

[2007]
type=friend
host=dynamic
username=encrypt2
auth=md5
secret=VERY_SECURE_PASSWORD_2
trunk=no
notransfer=no
encryption=aes128
disallow=all
allow=ulaw
context=encrypt
```

A couple of quick things to note:
-You must use md5 authentication (auth=md5) otherwise the peers will not be encrypted, even though it will indicate that they are with the iax2 show peers command in the CLI.
-Please note the context=encrypt option. This will tell us where to configure the dialplan for these lines.

EXTENSIONS.CONF

extensions.conf is where the dialplan itself is set. We will be setting up the call functions mentioned in the introduction, and exploring some of the functions in the dialplan. Later on we will be looking at the extensions.conf of a production environment (albeit a sloppy one) to see some of the more advanced functions. It is important to not that * has the ability to call AGI's from the dialplan including php and perl scripts. Additionally * can make system calls directly from the dialplan. The ringback function we will be looking at is an excellent example of this.

So we've come this far with little or no problems, but we still can't dial anything, or use anything we've configured. We need a dialplan, and fast. As we've gone on and configured up a bunch of peers and friends and such we have indicated that we are using a bunch of different contexts (local,fromiax,encrypt). To begin with we are going to put the example extensions.conf file that is included with the distro somewhere safe so we can refer to it if we want, and maybe borrow from it a bit when we need.

Make sure that we are still in the /etc/asterisk folder, and type the following commands:

mv extensions.conf extensions.conf.example
then
nano extensions.conf

I much prefer to set up extensions.conf from scratch to eliminate everything that im not going to be using, and to be able to find whatever portions of it that I need quickly. Also there is usually a section in extensions.conf for macro functions. I find these to be very useful for production environments with many users, but unnecessary for a small setup like I use for phreaking. For our purposes we will not be delving into macro functions, but feel free to explore this further as you get more familiar with *.

So lets get started on our extensions.conf. We will start at the best place, the beginning.

This is the portion where we will be setting up options that will apply to all other contexts:

```
[general]
static=no
writeprotect=no
clearglobalvars=no
```

Easy enough, now let's start with our contexts. These are defined by [ ], and are the guts of the dialplan. We will begin by setting up incoming calls from FWD because as of now it is the only service provider that we are using. We will be using the fictitious 123456 and 654321 #s for FWD, when configuring your own, replace 123456 with your own FWD #s.

A breif note on syntax: All extensions are defined by the exten => tag, followed by a comma, the priority, a comma, and the dialplan application to execute.

```
[fromiax] ;Remember this from iax.conf and sip.conf context= ?
exten => 123456,1,Answer ;Always answer an extension first unless you have a reason not to answer the call.
exten => 123456,2,AGI(cid.agi)
exten => 123456,3,System(echo NUMBER: ${CALLERID(NUM)} >> /var/lib/asterisk/custom-log/ast.log)
exten => 123456,4,System(echo NAME: ${CALLERID(NAME)} >> /var/lib/asterisk/custom-log/ast.log)
exten => 123456,5,Dial(SIP/100,20,rt)
exten => 123456,6,VoiceMail,u100
exten => 123456,7,VoiceMail,b100
exten => 123456,8,Hangup
```

OK, this is going to take a bit of explaining. Ok, first off it answers the call. Priority 2 tries to replace the Caller ID name by doing a reverse lookup on the #, and failing that, trying to pull the location of the NPA-NXX (In the US). Priority 3 stores the Caller ID number as the variable ${CALLERIDNUM}, and priority 4 sets the Caller ID name as the variable ${CALLERIDNAME}. Now remember when I mentioned that * could pass system commands directly from the dialplan, well that is what we are going to do next. Priority 5 writes the CID number in the text file /var/lib/asterisk/custom-log/ast.log, and priority 6 does the same for the CID name. Now would actually be a great time to create that file:

```
mkdir /var/lib/asterisk/custom-log/
touch /var/lib/asterisk/custom-log/ast.log
```

Priority 7 then adds a nice little line to separate the entries. The PBX automatically does this in the cdr with other information that can be parsed in many different ways, but I like to create this separate file to set up a real time Called ID display in a bash shell using the cat command. To set that up, just open up a new shell, and issue the command:

```
cat /var/lib/asterisk/custom-log/ast.log
```

BAMB! instant Caller ID display!

Priority 8 then dials the SIP extension 100, tries it for 20 seconds passing a ring tone, and then allows the extension to transfer the call when answered. If in 20 seconds the call is not answered Priority 9 forwards the call to voicemailbox 100 with the unavailable message, and in the event that the line is already in use, priority 10 sends it to voicemail with the busy message. Finally priority 11 makes sure that after all that goes down that the incoming portion is hung up once it is routed properly.

```
[local]
;This is where we will set up dialplan options for the sip client that we set up before.
;[default] for asterisk-1.4
;This will set up toll free calling in 5 different countries:
;for the UK and US you dial the # like you would in that country
;for the others, it is the country code followed by the #
;
;United States Toll-Free
exten => _1800NXXXXXX,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)
exten => _1888NXXXXXX,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)
exten => _1877NXXXXXX,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)
exten => _1866NXXXXXX,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)

;United Kingdom Toll-Free
exten => _0800.,1,Dial(SIP/fwd-gw/*44${EXTEN:2},60,t)
exten => _0500.,1,Dial(SIP/fwd-gw/*44${EXTEN:2},60,t)
exten => _0808.,1,Dial(SIP/fwd-gw/*44${EXTEN:2},60,t)

;Netherlands Toll-Free
exten => _31800.,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)

;Norway Toll-Free
exten => _47800.,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)
;Germany Toll-Free
exten => _49800.,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)
exten => _49130X.,1,Dial(SIP/fwd-gw/*${EXTEN:1},60,t)

;and now to dial other FWD #'s, dial *393 (*FWD) then the #:
exten => _*393.,1,Dial(SIP/fwd-gw/${EXTEN:4},60,rt)
```

It is important to note that the Caller ID presented in the sip.conf will get passed to the # that you are dialing. Now let's set up some fun extensions:

```
exten => *1,1,VoiceMailMain ;access the voicemail server
exten => *2,1,Meetme ;access the Conference Bridge

;play your music on hold
exten => *3,1,Answer
exten => *3,2,SetMusicOnHold,default
exten => *3,3,Musiconhold
exten => *3,4,Hangup

;dictations, stores sound files in /var/lib/asterisk/dictations (make sure that folder exists)
exten => *4,1,Dictate(/var/lib/asterisk/dictations)
;dial 1 to toggle record and playback modes
;dial 0 for help
;dial * pause/unpause
;dial # to enter a new filename
;
;PLAYBACK MODE OPTIONS
;dial 2 to toggle fast playback (speed 1x, 2x, 3x, 4x)
;dial 7 to seek backwards a few frames
;dial 8 to seek forwards a few frames
;
;RECORDING OPTIONS
;dial 8 to erase the whole file and start again
```

VOICEMAIL.CONF
voicemail.conf is a simple configuration for the voicemail server. It serves as a good example of a highly efficient configuration for a fully functional program.

We're going to add a mailbox for our softphone:

Scroll to the mailbox portion of the conf ([default]), and add the line:

100 => 1337,10nix,10nix@hackervoice.co.uk

that's mailbox 100 => Password,Name,Email-Address (must have SMTP on server to email messages)

MEETME.CONF
meetme.conf runs along the same lines as voicemail.conf, but for the conference calling application.
We'll setup an example conference like this:

conf => 1337,1337,31337

that's conf => conference number,pin,admin-pin

Part Two of Phreaking Around With Asterisk can be found on Page 28

JOYBUBBLES R.I.P

If we look back to the 1970's we'd see a young Phone Phreaker known as Josef Engressia playing with the phone systems. His interest the in the phone system and how it worked has helped form the phreaking community over the years and given inspiration to many famous (and of course non-famous!) phreakers out there. Unfortunately Joybubbles died at his Minneapolis home on August 8, 2007. Rest in Peace JoyBubbles!

Some Interesting Facts about JoyBubbles…

- ☎ He changed his name from Josef Engressia to JoyBubbles in 1991.
- ☎ Josef was born on the 25th May 1949. He was blind all his life.
- ☎ He could whistle 2600Hz (Human Blue Box!) which allowed him to get free long distance phone calls.
- ☎ He setup a weekly story telephone line called "*Stories & Stuff*" and the Telephone Numbers are +1 206-FEELING (+1 206 333-5464), +1 612-813-1212, and +1 773-572-3109). Mp3's of the stories can also be found here: http://blakeops.com/storiesandstuff/
- ☎ He wrote Telephiles for Playback Magazine.
- ☎ Joybubbles.com will be setup sometime in the future and will contain dedicated information about his life.
- ☎ Apparently had an IQ of 172.

PHREAKING BLOODY ADVERTS!

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.

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

---

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 Telecomms 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**

Announcements

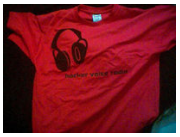
Hacker Voice Radio - HVR is an online radio show set up as a vocal forum for all the UK hackers and phreaks to come together, work together and a place to share information. HVR is hosted by either Be|ia| or Naxxtor; frequent co-hosts are 10nix, _hyper_, Vesalius and Blue_Chimp - Tuesday, Wednesday and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



Hacker Voice TV 2 DVD: You, too, can own a piece of hackerdom history in the form of the limited edition Episode 2 DVD, which not only contains the Episode itself, but also loads of extra features too! Including, but not limited to, an exclusive video episode of Hacker Voice Radio, outtakes and Hacker Cooking!

If you are interested in any Hacker Voice merchandise send an email to **gear@hackervoice.co.uk** for further information.

Personal Messages

WrongOne: A voice a voice, to ring out in the night.....a voice for justice and a voice of fright.

Omega-1: Anyone know what is going on with this site? http://www.geocities.com/ glenwills01/ it seems to have hidden information on it,

THV Team: Anyone know what the hell WrongOne is talking about?!

Internet Relay Chat

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

Phone Numbers

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

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

Miscellaneous

The Encoder: Vs lbh pna ernq guvf lbh'ir cnffrq gur svefg unpxre grfg. cng lbhefrys ba gur onpx naq lbh abj pna pnyy lbhefrys n A00o unpxre!

UV: Rmlyc3RseSB3ZWxsIGRv bmUgaW4gZGVjcnB5dGluZyB 0aGlzIHNpbXBsZSBiYXNlNjQ gbWVzc2FnZSEgIFdlIGVuY29 1cmFnZSB5b3UgYWxsIHRvIG ZvcndhcmQgeW91ciBlbmNyc Hl0ZWQgbWVzc2FnZXMgZm9 yIG90aGVycyB0byBjcmFjay4gI FNlbmQgdGhlbSBhbG9uZyB0 byBUSFYgdGVhbSBmb3IgaW 5jbHVzaW9uIGluIGZ1dHVyZS BkaWdlc3RzLg==

CULTURE: CAFFEINATED BEVERAGES--TEA

By Naxxtor

Caffeine – a drug which nearly every one of us has at least encountered, if not depends upon. There are many avenues through which it can enter our system, be it through beverages, energy food, mints, and medicine or in tablet form, the most common being through beverages such as tea or coffee. This series of articles will delve into the core aspects of a number of these beverages and the science and practicalities which they involve. The first, then, is about tea.

As a Japanese proverb says, "If man has no tea in him, he is incapable of understanding truth and beauty." I probably wouldn't go quite that far, but tea is certainly a historic drink which isn't going away any time soon. It also contains caffeine, which makes it an excellent mainstay for the British hacker who needs to stay alert with minimum cost.

The process or preparing tea is quite simple in procedure, but rather more complex in its science. There is only one way to make tea, and if you did it any different you wouldn't be drinking tea. Even ice tea is prepared in the same way, except it is chilled after the brewing is complete.

To put us on the same level, I'll briefly summarise the general preparation of tea:

1. Place leaves into a vessel.
2. Pour boiling water into vessel.
3. .Wait for a brewing period.
4. Pour the contents of the vessel (minus leaves) into a mug, and add other ingredients as desired.

A little abstract, but that is what defines the creation of tea. That isn't to say that it is an inflexible procedure – the leaves may be loose or in a bag, the tea may be brewed in the mug itself, the length of the brewing period can be varied.

Here's a simple tip for someone who wishes to get maximum caffeine from their tea. Assuming you are using a high volume teabag (a pyramid bag, for example), taking into account the differences between brands, you should brew the tea using briskly boiling water (poured no more than 10 seconds after the kettle has boiled) and leave the bag in the mug for no more than 32 seconds.

During that time you should swirl the water to aid diffusion, but do not squeeze the bag out. If you do, that will squeeze the nasty stuff out of the leaves and reduce the caffeine concentration (the solubility of the water will decrease with the addition of these products, such as salts which are more soluble than caffeine).

The resulting beverage is palatable and has high caffeine content, and in order to get maximum diffusion into your bloodstream you should drink it at around 60C; but a good temperature to drink at is around 65C if you can stand it. If you don't have a thermometer to hand, worry not. My briefly conducted) research shows that with a cylindrical mug with a 5mm wall made from a normal ceramic, going for 95C to 65C takes around 4 minutes. Take off the brewing time and you've got 32 seconds brewing, 3:28 minutes waiting.

Obviously, adding cold milk makes a considerable difference to this. Your average shot of milk at 12C or less will speed this time up to around about 2 minutes cooling time, providing you mix thoroughly.

If you're in the construction profession, you may consider adding copious amounts of sugar and semi-skimmed milk. That's your own preference, of course.

A number of kinds of teas are available, the most common being the high-caffeine, fast-brewing sort which is the mainstay of the general public. Although nobody has yet been prosecuted for treason for refusing this kind of tea, it is only a matter of time. There are also other herbal teas, which in my opinion are rather overrated and require more effort than it's really worth – with one notable exception… Camomile tea

Camomile tea is a remarkably good relaxant, providing it is brewed correctly. If you have been trying to work 25 hours a day for a week and have ended up going to sleep at around lunchtime, this may be the solution. At the appropriate time (say, 10pm) brew a nice strong cup of Camomile tea.

You may just find it knocks you back enough to put you to sleep on time. Then again, you just may end up in bed with your laptop writing articles for some hacker magazine.

The debate about when it is most appropriate to drink tea is one which shouldn't be dwelled upon too much, however it is reasonable to say that breakfast, elevensies, lunch and teatime are all acceptable times to have a cuppa. They are also most practical as you can make the drink en-masse and avoid boiling the kettle more times than required throughout the day, and so saving energy.

Speaking of energy, it appears that the powers that, uhh, power ... can monitor the success of television programs by the power consumption of our tea brewing devices. It can also cause problems. Imagine 600,000 people turning on 1kW kettles simultaneously as they shuffle into the kitchen at the ad break for Coronation Street. This problem is so bad that the National Grid has a team of statisticians whose job it is to predict when and where the British masses will put the kettle on for a cup of tea, and tell the engineers to account for it. There is even a name for it in the industry – a “TV Pickup”. You can watch these happen yourself.

See if you can predict when a pickup might be, and check with the real time data at the National Grid website (www.nationalgrid.com).

And with that, I'm going to go have a nice cup of Tetleys.

Links:
http://www.nationalgrid.com/
http://www.tetley.co.uk/
http://www.pgmoment.co.uk/
http://engr.oregonstate.edu/momentum/k12/oct04/

Additional Photos: Demonix
Sorry Naxxtor but I prefer PG!

WHO ARE THEY REALLY WATCHING?

By Belial

"The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinised." - **George Orwell's "1984"**

Close circuit television cameras have for a long time become a large part of every day urban life in the UK.

London has some of the most complex CCTV networks in the world. It is stated that an average day for a Londoner could result in them being captured on CCTV 300 times. The congestion charging zone and the square mile security WIFI camera zones, also with a planed increase to double the number of CCTV cameras around London in anticipation for 2012 - I put it to you, who are they really watching?

What Purpose Do Most Of These Cameras Serve?

In this article I will not argue about how effective CCTV can be in fighting crime. I will not go into the details of law, legislation. My main point of interest is with all these cameras monitoring the UK 24/7, 356 days a year - what's all this surveillance used for?

What purpose do these cameras serve? My belief is that with such a dense network of surveillance cameras covering London, also with nearly over thousands of automated congestion charging cameras in central London, who has the time to monitor each one?

Assuming that each one is in full working order and each one is being recorded, the amount of data collected by each camera could be incredibly large. As you can only get a certain degree of compression on VHS and even DVD before the image becomes un-comprehendible. Is the government spending that much money on DVDs every day? Hundreds and hundreds of gigs every minute? The government has recently rolled out new WIFI digital surveillance cameras.

All the cameras are linked up by encrypted wireless 802.11 links. They span the square mile and most of Westminster. These will add to the number of screens and number of DVDs that need to be used for recording.

How can it be humanly possible for all this data to be checked? Well it simply is not. All of the data cannot be checked however it is used for reference. So the cameras do not effectively prevent crime. Just record it for later viewing.

Why add onto an ever increasing problem? The more cameras watching, the more data can be collected. This is the point where the conspiracy starts...

Constant surveillance of London can produce very valuable data of the habits of people. Now with the advance of facial recognition and automated camera systems, you can map people's movements across a CCTV network. We can see that the CCTV system is predominantly ineffective as a crime deterrent. Most of the cameras are not even switched on or fully working. Some are not even watching what they should be. In central London we see many mobile temporary surveillance vans placed in location to monitor people and crowds. Other vans are used for congestion charging. I have seen vans

with up to 5 cameras placed on top

With all this in mind. It could be stated that this data is not being used for just a pure public safety sense. They could be used to collected analytical data about the movements and habits of people. This data can then in turn be sold to corporations or bodies that have a invested interest in the acquisition of this data.

Who's Watching YOU?

I fear that there will be no stopping to the number of state owned cameras I fear that citizens will have no right or control over these cameras. Any control we have now will quickly be taken away with changes to legislation in favor of some blind, maliciously motivated, anti-terror joke of a bill.

"CCTV does not have a deterrent effect on violent alcohol influenced street brawls according to research conducted by University Hospital of Cardiff, published in Injury Prevention journal which compares actual emergency hospital admissions with unreliable police violence statistics."

I can safely say that we are very quickly running into a 1984-esque world. Our shopping, living, working habits are monitored closely.

Every individual is being used as a tool. Our pockets are being harvested by extraordinarily rich corporations that use real time statistical data to improve their ability to market products to an already confused and hyperactive market.

Let's fight back before it's too late!

Resources:
"The Independent newspaper (Tuesday 12th January 2004) has devoted its headline and leading articles to CCTV Surveillance, claiming that over 4,285,000 i.e. about 20% of the world's CCTV cameras are used in the UK."

http://news.independent.co.uk/uk/this_britain/story.jsp?story=480364
http://news.bbc.co.uk/2/hi/uk_news/3339133.stm
http://ip.bmjjournals.com/

Links:
http://mysociety.blogs.com/mysociety/2003/10/cctv_map.html
http://www.spy.org.uk
http://www.online-literature.com/orwell/1984/

GOOGLE CHIPS

Welcome to the very first Google Chips! If your wondering what the hell a Google Chip is take a look at some definitions:

Google: A Well Used Search Engine. **Chip:** A Crack or Flaw caused by the removal of a small piece.

So basically Google Chips are search examples that can potentially be used to exploit a system or just find out more information – more than you would expect to see in fact! If you have found a Google Chip and would like the details published please get in touch with us on the forums!

Cisco VPN 3000 Concentrator Chip by Hyper.

Google Search: http://www.google.co.uk/search?hl=en&q...earch&meta=
Search: intitle:"inc. vpn 3000 concentrator"

The output and a quick search online for the default Username/Passwords will give you some interesting results.

Online Security Camera Search by Various People.

Google Search: http://www.google.com/search?hl=en&q=inurl...ndexframe.shtml
Search: inurl:indexframe.shtml
Alt#1: inurl:"MultiCameraFrame?Mode="
Alt#2: inurl:":1024/main.cgi"

Searching for online security cams is quite fun and if your lucky you might find one with the controls fully open so you can pan and zoom the camera image. There are loads of different methods for searching for the camera's and we've only included are few examples. If you find any others get in touch and we'll print them in the nice issue.

UNEXPECTED HACK?

Photo by Sam from IRC

PART #2

BY

```
 _ ___ _
/ |/ _ \ _ __ (_)_ __
| | | | | '_ \| \ \/ /
| | |_| | | | | |> <
|_|\___/|_| |_|_/_/\_\
```

USAGES OF ASTERISK

Ok, so now we've got our own PBX running on a laptop, that's really cool, but lets see what we can do with it. For our purposes, we will be mostly controlling the PBX through the extensions.conf. Take note as we go along to the syntax. Just like anything else, its all about the details, but once understanding of the frameworks is achieved, it becomes trivial to control call flow, and processing.

- Called ID Processing, and Spoofing:

As was mentioned before * allows you to set outgoing CID, just like any other PRI. This allows for CID spoofing. This single handedly got me into * in the first place. Let's look at some of the different ways to accommodate CID spoofing in the Dial Plan. For a while now there have been AGI scripts floating around that prompt you for the inputs, and set the fields accordingly. These work just fine, but for this phreak they are too cumbersome, and in-efficient. When designing call functions for * I often times have to hack together burdensome, and lengthy bits to achieve functionality. This is either to bypass using for pay services that would be easier, or because I am simply limited in my knowledge, am not aware of a 'better' way. CID spoofing is not one of these times. I use a very simple method the uses two lines in the dial plan:

- US national dialing with CID spoofing

```
exten => _*33NXXNXXXXXXNXXNXXXXXX,1,Set(CALLERID(all)=${EXTEN:13})
exten => _*33NXXNXXXXXXNXXNXXXXXX,2,Dial(SIP/telasip-gw/${EXTEN:3:10},60,rt)
```

OK, that was three lines, but the comment line is hardly necessary. As for an explanation, _*33 tells the server to process anything that starts with *33 and has 20 digits following it using this extension. So say *338004444444202456 1414 is dialed. priority one takes out the first 13 digits and sets all CallerID fields as 202-456-1414 (the switchboard to the White House). Priority 2 then places the call through the SIP provider telasip, eliminating thew first 3 digits (*33) and the last 10. So it would call 800-444-4444 (MCI ANNAC). MCI would then say "our system indicates you are calling from area code 202 456-1414... Please note that it is a common miconception that CID can only be spoofed through IAX. TelaSIP is just one provider that allows it using the sendrpid=yes option in sip.conf. In contrast to this for UK CID spoofing I use an IAX provider. It looks like this:

- UK national dialing with CID spoofing

```
exten => _*44.,1,Set(CALLERID(all)=0${EXTEN:13})
exten => _*44.,2,Dial( IAX2/${accountname}@voiptalk/${EXTEN:1},rt)
```

This does the same thing as the above example. the . after _*44 is a wildcard, and tries to process any number of digits after the *44. There is a better way to do this; I just have not figured it out yet.

Suppose you want to spoof your Caller ID, and then record the phone call as well; that is not a problem:

```
exten => _*444X.,1,SetVar(CALLFILENAME=${EXTEN:1}-${TIMESTAMP})
exten => _*444X.,2,MixMonitor(${CALLFILENAME},wav)
exten => _*444X.,3,Set(CALLERID(all)=0${EXTEN:13})
exten => _*444X.,4,Dial(IAX2/84471531@voiptalk/${EXTEN:2},rt)
exten => _*444X.,5,StopMonitor()
exten => _*444X.,6,Hangup
```

This will set the Caller ID, make the call, and record it in /var/lib/asterisk/sounds as ${NUMBER CALLED}-${TIME_CALLED}

Now to round out our CID roundup let me introduce to you Backspoofing: according to an article in this Summer's 2600 magazine by Natas, backspoofing is "calling yourself with spoofed Caller ID for the purpose getting the CNAM (Caller ID Name) associated with a particular number. Now it is my understanding that BT does not maintain a CNAM database, and so Caller ID name is a feature that is unavailable in the UK. I have some primative workarounds. One is to call a perl script through an agi to look up the number on google. This does not usually work, and since the UK does not have any free reverse lookup directories for now it seems that backspoofing in the UK proves ellusive. None the less, here is an example of how it would look in an extensions.conf:

- Backspoofing

```
exten => _*22.,1,Set(CALLERID(all)=${EXTEN:3})
exten => _*22.,2,Dial(SIP/telasip-gw/${inbound #},20,r)
exten => _*22.,3,Hangup
```

Well that wraps that up, but before we move on from Caller ID, there are a couple of things that I would like to mention. FWD allows passing outbound CID. This means that even without FWDout credits, you can spoof CID to 5 different countries using the standard (and free) FWD service.

Moving on. We have set up a couple of Services on * (A conference Bridge and Voicemail). Lets check them out. These services, though necessary, and really cool, are alas, standard fare. Lets play a bit. The extensions.conf file allows us the flexibility to implement dialplan functions on a whims.

For instance, one day someone asked me: "say, could you make a DTMF Readback on the PBX"? I thought about it, and about 3 minutes later, it was up and running. See the box on the right on how this was done…

```
exten => 403,1,Answer
exten => 403,n,Wait(1)
exten => 403,n,Playback(please-enter-your&number)
exten => 403,n,Read(dtmfinput,then-press-pound,,,,)
exten => 403,n,SayDigits(${dtmfinput})
exten => 403,n,Playback(thanks-for-using)
exten => 403,n,Wait(1)
exten => 403,n,Hangup
```

Then I made sure that the line that accesses this extension has dtmfmode=inband in the sip.conf. This allows * to register dtmf signalling using the sound rather than rfc2833.

Lets look at some other cool things we can do:

Automated Name and Number Announcement Circuit:

```
exten => 404,1,Answer
exten => 404,2,SayDigits(${CALLERID(NUM)})
exten => 404,3,SayAlpha(${CALLERID(NAME)})
exten => 404,4,Hangup
```

Record Custom Prompts in a Native Codec:

```
exten => 1111,1,Answer
exten => 1111,2,Wait(2)
exten => 1111,3,Record(Custom-Prompt%d:ulaw)
exten => 1111,4,Wait(2)
exten => 1111,5,Playback(${RECORDED_FILE})
exten => 1111,6,Wait(2)
exten => 1111,7,Hangup
```

The sound file will be saved in /var/lib/asterisk/sounds with the name Custom-Prompt0, Custom-Prompt1, etc.

- Test Text To Speech Software:

Festival Test

```
exten => 2222,1,Answer
exten => 2222,2,Festival('London Twenty Six Hundred Scares Me With How Leet They Are, All My Base Belong To Them')
exten => 2222,3,Hangup
```

Talking Time!!! (Hah! Take that BT, we can do that too!!)

```
exten => 3333,1,Answer
exten => 3333,2,SayUnixTime(GMT,ABdYRS)
exten => 3333,3,Hangup
```

Think That's Phun? Now lets get into some of the really phun stuff...

Check this out, you can pass system calls in the dialplan, allowing us to do virtually anything directly from the dial plan! Here is a sample bit that allows for a caller to dial a number, and never get connected to it. Why in the hell would anyone want to do that you ask? Well, while the phone is ringing away, the PBX goes ahead and grabs the Caller ID of the incoming call. It then waits 5 seconds (presumably long enough for the savvy caller to hang-up) and calls them back, and hell, while we're at it, why not change the Caller ID of the call to something interesting, lets say... the FBI.

This example is for the US, but in a moment I'll show you a version working in the UK.

```
exten => 841425,1,Ringing
exten => 841425,2,Congestion
exten => 841425,3,Hangup
exten => h,1,System(echo channel: SIP/telasip-gw/${CALLERID(NUM)} > /tmp/${CALLERID(NUM)}.call)
exten => h,2,System(echo callerid: 3104776565 >> /tmp/${CALLERID(NUM)}.call)
exten => h,3,System(echo extension: s >> /tmp/${CALLERID(NUM)}.call)
exten => h,4,System(sleep 5)
exten => h,5,System(cp /tmp/${CALLERID(NUM)}.call /var/spool/asterisk/outgoing)
exten => h,6,Hangup
```

- AUDIO CODECS

For the audio codecs commonly used in VoIP we suggest you look at the following web site:
www.cs.columbia.edu/~hgs/audio/codecs.html

-ARTICLE REFRENCES

www.voip-info.org :: All that is VoIP.
www.asterisk.org :: Asterisk project page.
www.hackervoice.co.uk :: Reppin my peeps yo.

- SHOUTS

To Belial, Naxxtor, Skoby, Strom Carlson, Mo0, Voltagex, Felix, and all the HVR IRC crew!

SOCIAL ENGINEERING

By Hyper

So what a Social Engineer?

A social engineer uses the art of extracting little snippets of information from a number of sources to put together a picture and a way in. He can form relationships with his targets and speak to them again and again leaving a permanent hole which can be used again and again. So rather than paint a vague picture I will offer an example of a simple job. ON A MAJOR TARGET!

I sat in a Cafe in central London eating a bacon sandwich opposite was a guy who for legal reasons I'll call Simon Wills. I knew his name was Simon Wills as it said it on his work ID that was around his neck. I also noticed that the company had a customised necklace that holds his pass with the company name on it.

Key Information

- Social engineering is the art of deception.

- It has the ability to exploiting the weakest part of any system.

- You can be running windows, Solaris, Linux or Apple Mac in fact ANY operating system.

- You can spend thousands and thousands on high end firewalls. But as a security engineer if you don't educate your staff, you have wasted every penny.

- A Social Engineer can exploit any system; it can exploit physical security as well as offer a means to exploit technical security.

- Social engineering exploits the human element in the equation. It exploits the human emotion of wanting to help.

So I now know where he works and I know his full name, plus I reckon it must be close to the cafe where we are sitting right now. Low and behold it's across the street. What can I do with this little bit of information?

Now I know that these rather large financial customers have nice canteens that are heavily subsidised by the firm. The only reason that I can think of that this guy wasn't eating in there was because he wanted cafe food which happens to us all :) So I thought whilst sitting eating my Sandwich "fuck it" I want to have my lunch in the 1istinvestment Bank's (I've changed that name too) canteen next week. I want to taste success myself ;)

So here are the processes I took:

1. I call reception and I ask for the extension number of Paul Wills:

Hyper: Hi can you give the extension number of Paul Wills please, I'm sorry I can't remember which dept. he works in.
Receptionist1: Oh Hello there sir, Paul Wills is in research, his extension is 412223
Hyper: Oh that's great; does he have a direct line?
Receptionist1: Yeah sure, its 0207 111 1111
Hyper: That's great.
Receptionist1: Would you like to be put straight through
Hyper: Oh no thanks, I'm driving at the moment ill call him back once I get off the road. Thanks for your help though.

2. I write all this information down on my notepad. And then I call back:

Hyper: Hi there, this is Paul Wills from research. Who am I speaking to?
Receptionist2: Hi Paul this is Julia
Hyper: I need to have a client enter the building next Thursday; I've not done this before so I have no idea which system to use.
Julia: Oh its okay, you need to raise a Seibel ticket.
Hyper: Oh okay how do I do that?
Julia: You call 0800 111 111 and they will raise the ticket for you, its easy to do.
Hyper: Well I'm not onsite at the moment. I'm calling you form my mobile, does that matter?
Julia: No you can them anywhere from the UK. If it's outside the UK it's another number.
Hyper: That's great, so which one are you then?
Julia: what do you mean?
Hyper: Sorry which receptionist. He he
Julia: Oh I'm the one in dark hair I always sit on the far left.

Hyper: Oh I know who you. Anyhow it's nice to finally talk to you. I always seem to scurry past you without saying hello.
Julia: Well next time make sure you say Hi.
Hyper: I will! And thanks for your help Julia.
Julia: Thanks have a good afternoon.

3. I then call the 0800 number.

Hyper: Hi I need to raise a Siebel request please
Seibel: You mean a Seibel ticket
Hyper: Yes that's it
Seibel: Okay what's you employee number?
(Shit I didn't expect that)
Hyper: Damn I don't know it off by heart. Ill have to call you back. Is that okay?
Seibel: (sigh) yes of course sir (Hang up)

4. Damn, now I should have known that companies like these all use employee numbers for everything. Now in this case you can use a number of methods to get this but the easiest is to just ask the employee. So I call my mate Paul on his direct line. Now this is the first time I have spoken to Paul, I was hoping I wouldn't have to.

Hyper: Hi Paul, This is Jon from finance.
Paul: Hi Jon
Hyper: I have a change request under you name and as you don't often make them can I just check its you.
Paul: Sure fire away
Hyper: Fine what's your employee number?
Paul: 1121478

(Shit! He rolled it off like a robot, which means I should have as well but ill continue)

5. I make my excuses, "oh it's not you" and "it's been a mistake someone must have pressed the wrong key that happens sometimes". I hang up.

6. So armed with my new info, I raise my ticket. But I'm now told that I have to accompany myself at all times. I must escort myself in and out of the building and I must never leave myself alone for the duration on the visit. Double shit.

7. So now Thursday is fast approaching, and I'm wrecking my brain for what to do. Just before entering the building I ring my pal Julia in reception explains who I am and she is all to please to hear my voice. I explain that I'm running late and could she call inform security that Joe Boggs is coming Seibel ticket 10101010 is arriving in around five minutes. Could they have someone take him down the canteen and Ill meet him there in around 15mins. Oh and please make sure they really apologise on my behalf.

8. I walk in the building now I'm suited and booted and my heart is in my throat. I walk up to security, they are expecting me they check my ID and hand over an guest pass (Now this is the worst bit as I have to use my real identify, they need a passport, I don't own any fake ones I'm not a criminal) plus they give me a little sticker for my jacket. They shower me in apologies and one of the guys takes me down stairs to the basement to where the canteen is located.

9. Now at the bank you need a pass to buy food. You credit your work pass with money and then you can spend it as you wish. I get the security guard to allow me to put a couple of pounds on his card and I buy my self a meal. The guard leaves me to it. I sit at a table with loads of different staff. I take a mental note of all their names on there passes. I finish my meal have a cup of tea and head off into the sunset.

Now I managed to enter a major investment bank in the city and have lunch in there restaurant without ever being invited. I social engineered a number of people into giving lots of little bits of information. Including there call raising centre and the security for the building. Plus the target himself. And it all began from an employee with work pass round his neck.

That's social engineering, I used simple techniques to gain the information I needed to enter a high security building. I will be writing regular articles of information on Social Engineering, and other little hacks for everyone to read and learn, and hopefully making your companies information a whole lot safer.

HIDING YOUR TRACKS WITH TOR

By Naxxtor

As many of you already know, Tor is a (reasonably) new method of making anonymous connections over the Internet. For those who are unfamiliar with the Tor network, the basic workings are as follows:

A Tor node is a machine on the Internet which is running the Tor executable, which listens to Tor traffic on a specific port. For this example, we will call our connecting Tor node Alice (as per convention). When a Alice wishes to make a connection to a server on the Internet, it will first contact a Tor directory server (another Tor node), which we will call Dave. Dave will share all of the other Tor nodes which it knows of to the first Tor node. Alice will then in turn ask each of the newly discovered nodes for their directories, and build up a large list of Tor nodes on the network.

Once a suitable collection of nodes has been built, Alice will try to create a 'circuit'.
This circuit will allow Alice to send packets to any node in her directory, and have it forward to other Tor nodes until it reaches a final Tor node, called the exit node. This exit node will then send those packets on to the intended destination. Equally, packets being received by the Tor node will also be passed back to the circuit, and they will work their way through a different route before finally reaching Alice.

The beauty of the system is that no one Tor node can tell you both where the packets were coming from AND where they're going to. This means that if an attacking party subpoena's a Tor node, then they will not know both the destination and the source.

In fact, in order to conclusively prove where the destination and source nodes were, you would need to subpoena every single Tor node in the circuit at the time- and since a circuit often contains 20 or more computers running on a wide variety of networks (home, commercial, military, educational...), this is hardly practical.

The developers of Tor bundle a couple of programs with their distributions these days.
The Windows distribution contains Tor, TorCP (a GUI to control Tor) and Privoxy.
For Linux/BSD/Mac they include Tor and Privoxy, unless you choose to download these separately. Privoxy is a vital part to Tor, as it prevents DNS leakage.

DNS leaks punch a nasty hole in your anonynimity when using Tor. If you think about it for a moment - if you're going to resolve a hostname to an IP (which will often be the case), what's the point of routing your traffic through the Tor network when you're publically asking to resolve the hostname of the system you're trying to connect to? Privoxy is a HTTP proxy, which prevents this problem my ensuring that Tor is used to resolve hostnames. It also works as a filtering proxy to kill ads and cookies. Nifty eh?

There are umpteen tutorials on how to set up Tor for normal web browsing. I suggest you go read one specific to your system at http://tor.eff.org/. Being the conscientious hacker you are, you don't want to get an email from your ISP saying you've broken their ToS by abusing someone's server. So you're probably going to want to secure a few other applications too.

Again, there are tutorials on how to secure a huge number of applications on the Tor website, but for the sake of convenience I'll show you how to configure SSH on Backtrack, and PuTTy on Windows, to use Tor.

BACKTRACK

I'm going to be using the connect.c method, because it's simple and it worked for me. If that gives you a head start, then go for it. First, you'll need to be connected to the Internet somehow. If you're going to be using Tor I think that's a fair assumption.

Make a directory in /root/ called connect:

```
mkdir connect
cd to it ...
cd connect
Download connect.c
wget http://www.taiyo.co.jp/~gotoh/ssh/connect.c

NOTE: If that gives you a 404 or some other error, then Google for it. Once it's downloaded, you need to compile it:
gcc connect.c -o connect
Then copy it into place:
cp connect /usr/bin/
cp connect /usr/local/bin/
```

Now connect is installed. I guess if you were so inclined you could include this binary using a Slax module, but I'll leave that as an exercise for the reader. Next you need to add a few lines to your ssh config file. For the sake of brevity, I'll assume that you're only going to be connecting to external hosts while you're using this config file (if you need to connect to an internal host, just rename the file to something else).

```
echo "Host *" >> ~/.ssh/config
echo "ProxyCommand /usr/local/bin/connect -4 -S 127.0.0.1:9050 %h %p" >> ~/.ssh/config
```

Almost done! Now, you just need to run Tor (open a console, type tor, or tor & if you want to background it), and then connect away. If you need to resolve a hostname, then use this command: tor-resolve some.host.name.com

Then copy paste the IP to your SSH command. Tor will complain about how it's only getting an IP and that's not very good because it might mean DNS leakage, but since we resolved it using Tor that isn't the case.

WINDOWS

This is as simple as it gets:

```
Open up PuTTy
Go to the Proxy tab under Connection.
Select SOCKS v5, type the address localhost port 9050.
Done!
```

Now, bear in mind this will be REALLY slow. I'm talking treacle syrup slow. BUT it does mean that you can clean up your logs without worrying about leaving any traces of your real IP behind. My advice would be to simply use it to upload and run a script which does the log cleaning for you.

Normal disclaimer applies - don't use the information to do anything too naughty. And if you do, don't blame me.

Links:

Torifying software HOWTO: http://wiki.noreply.org/noreply/TheOnionRouter/TorifyHOWTO
BackTrack: http://www.remote-exploit.org/index.php/BackTrack
PuTTy: http://www.chiark.greenend.org.uk/~sgtatham/putty/

THE RANDOM DATA DUMP

This Issues Random Data Dump concentrates on who the Core HackerVoice team are and a plug for someone called Gary…

Belial
The "smooth talker" of Hacker Voice Radio. Belial is one of the main hosts of the radio show, and has been present for every episode. Belial is a dedicated member of HVR and started hacking at a very early age. Phreaking through out his teens and developing applications for personal use. All this while juggling work rest and play, Belial brings a fresh and balanced look on UK hacking/phreaking.

Hyper
Hyper-ventilation Hyper-active Hyper-manic Hyper-alcoholic, What ever you call this guy. You cant say anything bad about him. Hyper is one of our most recent but heavily dedicated members of the hackers voice. However not so public he has contributed very generously. He hopes to appear more often on the radio show.

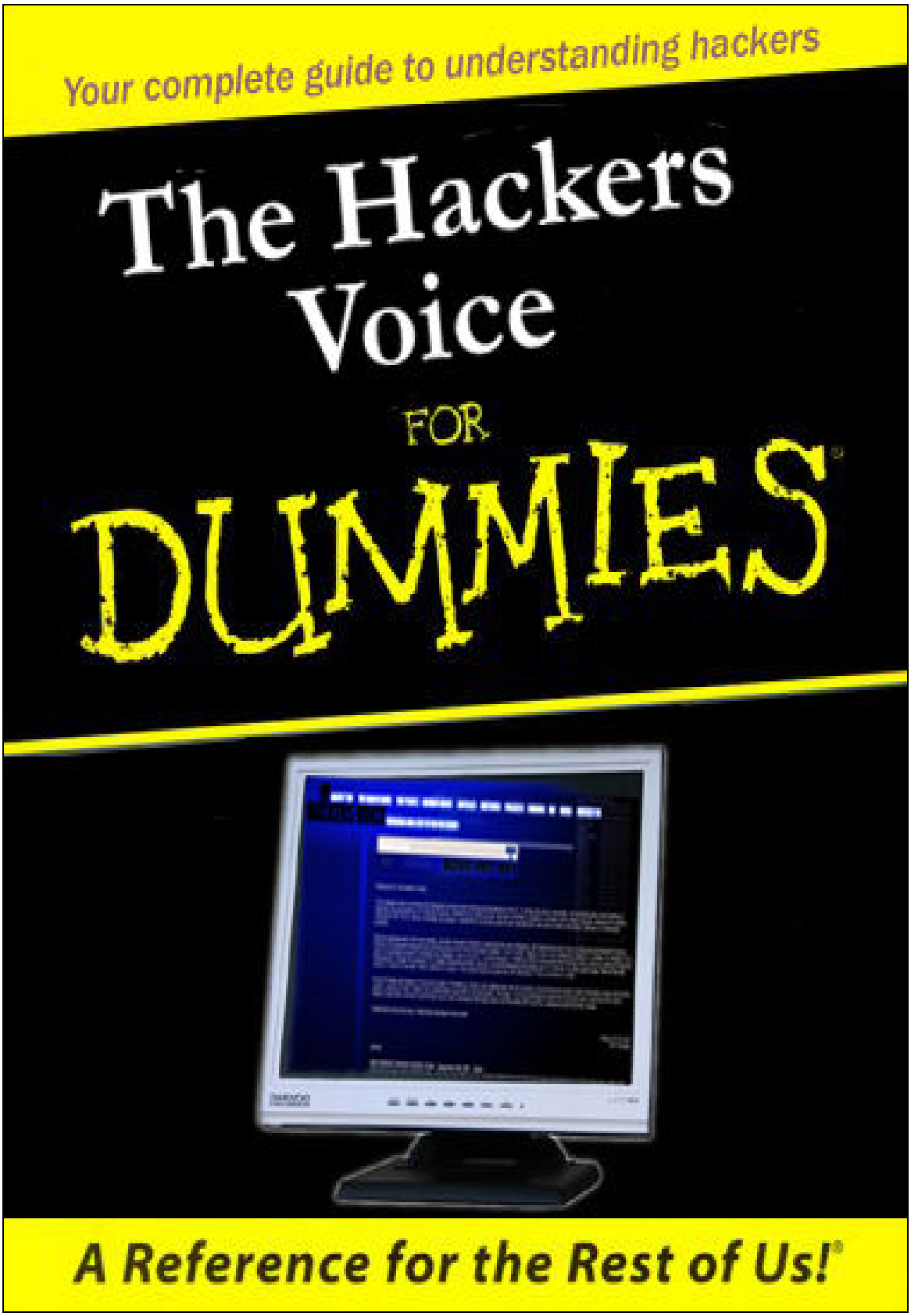
Naxxtor
Naxxtor is a man of many names and too many qualifications. He has an interest in multimedia and was last observed trying to recreate the 1972 Dr Who theme tune using C. He makes the world turn backwards using Perl and Ruby, running on Linux, Windows or *BSD, and does so whilst listening to chiptunes. He has a hatred for SuSE and a love for Gentoo, and feels mildly indifferent about Ubuntu.

Naxxtor also does post production for HVTV, and is a Londoner - at least half of the time.

DarkNature
DarkNature joined the Hacker Voice team in April 2006 after becoming a regular phone-in guest on the radio show. Likes include messing about with computers, programming, coffee and smoking cigarettes. Dislikes include TV, the nanny state and "elective stupidity" (ignorance is NOT cool). DarkNature's current projects include Operation PhishNet - a project to reduce the incidence of phishing on the web by making people more aware of the dangers and ways to deal with phishing attacks. "Hacking is not just about breaking into stuff and if I wanted a bunch of credit cards numbers I'd get a bunch of credit cards."

10nix
10nix[(eye-on-ix) -noun. Name of American Boy. Name of someone who's docs have been dropped more than once.] 10nixis the ad hoc US representative to HVR. He is self described as "The Token American", but it is in jest. 10nix lives in Florida, US currently, and is from the state of New York. He develops Winix, emulated linux off of a CD-ROM drive (emulation and all) that runs on Windows. Though thoroughly un-accomplished, he does seem to know a surprising bit about many topics. Likes include Linux, making an ass of himself, and his soldering iron. Dislikes include Windows, making an ass of himself, and the US (ironic). He is always ready to lend a helping hand, and appreciates the opportunity to be a part of something greater than himself.

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 magazines content we'll include it. Remember the more random and interesting the better chance it will appear in the next magazine! Submit your pages to **articles@hackervoice.co.uk**


Your complete guide to understanding hackers
The Hackers Voice
FOR
DUMMIES
A Reference for the Rest of Us!