THE TOR PROJECT :

AUTHORITY “NO CHECK” WEAKNESS

Piotr CHMIELNICKI

CONTEXT

The Tor network is an onion routed darknet used by people around the world to secure, anonymise and uncensor their communications.
More informations about the Tor Project : https://www.torproject.org.

Interesting thinks

- Many sensitives informations are transferred by this network.
- Relays are provided by volunteers, everyone can set up his own Tor relay.
- Exit nodes are used to be the most sensitive part of the network because every exit node operator is able to dump outgoing traffic.

TOR AUTORITIES

The Tor Project use authority servers that publish the list of all the tor relays.

EXIT NODE INTERCEPTION

Exit node interception is a known problem. It can be solved by using encrypted protocols. The most used are TLS and TLS based HTTPS.

AGGRESSIVE MIDDLE-MAN ATTACKS

Encryption can sometimes be defeated by some tricks :

- TLS communications can be decrypted using a middle-man attack. Off course, the certificate should not match but user can force the software to proceed anyway. A user who doesn't know many things about crypto can easily be trapped.
- HTTPS can be broken by more transparent middle-man tricks than the TLS basic middle-man attack, for example by replacing `<form action=" https://...` by `<form action=" http://...` in HTTP (not encrypted) responses. No warning will be displayed by the browser.

Theses attacks can easily be detected because they alter the relayed information.

CHECK THE RELAYS !

The sad point is that the **Tor Project authorities don't detect or won't stop aggressive middle-man attack.**

A script should perform some tests every hour on every tor exit node and report problems.

PROOF OF CONCEPT

The result of 3 days of HTTP **and HTTPS** POST dump using an aggressive middle-man attack using a modified sslstrip :

http://www.exploit-db.com/sploits/TorPOC.zip

Mirror : http://perso.epitech.eu/~chmiel_p/TorPOC.zip

sha512	60fbb49b36b271f543ffb34b87ebccf889ddad070c5e04f386f530a639b787a90826ac7c5b80b47acc22cb3e905ce710a94419b97fb06e54d7d93b8bc015b223

CONTACT

piotr.chmielnicki@epitech.eu