S2E7 - The Onion Routing project

Nicholas Morrison nick@nanocat.net

Workshop Goals

- understand and discuss TOR and why it's called Onion Routing
- understand and discuss its uses and its limitations

Symmetric encryption

- Wikipedia: https://en.wikipedia.org/wiki/Symmetric-key_algorithm
- both sides share the same key
- that key is used for encryption and decryption
- great if both parties trust each other but nobody else

Asymmetric encryption / public key encryption

- Wikipedia: https://en.wikipedia.org/wiki/Public-key_cryptography
- A **key pair** consists of a Public Key and a Private Key
- great for allowing anyone to send you encrypted data, without you needing to share your key with them
- or vice versa
- Public Key
  - encrypt data
  - verify a signature
- Private Key
  - decrypt data
  - sign data
- If I have your Public Key, I can send you data that only you can decrypt with your Private Key.
- I can sign a blob of data with my Private Key, which you can then verify using my Public Key.
- Public Keys can be shared freely, advertised, uploaded to directory servers
- Private Keys must be kept secret

Using them both together

- Use asymmetric encryption to establish an encrypted communications channel
- Use this channel to share an ephemeral symmetric key
- Use symmetric encryption to communicate securely using the ephemeral key
- Ephemeral key can be rotated every x seconds or every x bytes (forward secrecy)

Onion Routing

- Wikipedia: https://en.wikipedia.org/wiki/Onion_routing
- Forward your data along a chain of nodes
- Only the exit node knows that it is an exit node

- Other nodes don't know if they are receiving packets from the originator or from another node
- No node can see your original packet
  - Except for the "exit node"
  - So it's very very important to always use your normal security practices! (HTTPS, SSH, SSL)

What it can do

- hide your IP address from your ISP
- hide your IP address from the server you are connecting to
- disguise your activity
- let you connect to `.onion` sites (the dark web)

What it cannot do

- provide total anonymity

The Onion Routing project

- https://torproject.org
- Started by the US Military in the 90s
- Released as open source in 2003 (CLI tools)
- The TOR Browser released a few years later (modded firefox)
- Many TOR nodes active on the internet: https://www.dan.me.uk/tornodes

Steps: setup

- You = OP = Onion Proxy
- OP finds a list of nodes from a TOR directory server (https://metrics.torproject.org/rs.html#search/flag:authority)
- OP selects some (3 by default) relay nodes, with an exit node at the end (nodes A (guard), B (relay) and C (exit))
- OP gets public keys of all nodes in the chain
- OP uses these keys and receives (3) ephermeral keys for symmetric encryption with all nodes in the chain

Steps: send a packet

- Encrypt your packet with the key of node C
- Encrypt again with the key of node B
- Encrypt again with the key of node A
- Send your packet to Node A
- Node A decrypts, and now has a packet encrypted for node B
- Node A sends this packet to node B

- Node B decrypts, and now has a packet encrypted for node C
- Node B sends this packet to node C
- Node C decrypts, and now has a packet to send to the internet
- Node C sends this packet to the server on the internet

Steps: receive a reply

- The internet server sees a connection with a source IP of the TOR exit relay
- It sends reply packets back to this IP (node C)
- Node C encrypts the packet with the ephemeral symmetric key
- Node C sends the packet to node B
- Node B encrypts the packet with its ephemeral symmetric key
- Node B sends the packet to node A
- Node A encrypts the packet with its ephemeral symmetric key
- Node A sends the packet to you
- You decrypt the packet three times, with those three ephemeral keys
- Now you have the original packet!

Being a relay

- You can choose to become a TOR Relay node yourself
  - Your computer will forward traffic to and from other TOR nodes
- You can also become a TOR Exit Relay
  - Your computer will forward traffic to the internet from TOR users
- If you just run the TOR Browser you're not a relay

Attacks

- Attackers want to deanonymise you
- Timing attacks (control all the nodes)
- User errors (oops I logged in with my username and password)
- Side channel attacks (javascript bugs, malicious ads, etc)