Protecting your Privacy with FreeBSD and Tor

Christian Brüffer
brueffer@FreeBSD.org

MeetBSD – Warsaw, Poland

November 18, 2007
Overview

- Who needs anonymity anyway?
- Anonymization concepts
- Tor
- FreeBSD
- What else to take care of?
- Demonstration
- Summary
Overview

- Who needs anonymity anyway?
- Anonymization concepts
- Tor
- FreeBSD
- What else to take of?
- Demonstration
- Summary
Who needs anonymity anyway?

- Journalists
- Informants, whistleblowers
- Dissidents (China, Myanmar...)
- Socially sensitive information (abuse, AIDS)
- Law enforcement (anonymous crime reporting, tips, surveillance...)
- Companies (research competition...)
- Military (covert operations...)

MeetBSD 2007
Who needs anonymity anyway?

- You?
  - EU data retention directive
    - connection data gets stored for 6 – 24 months
    - phone, SMS, IP, e-mail, dial-in data
    - (finally we'll be safe from all those terrorists!)
  - which interests do you have?
  - who do you talk to?
Who needs anonymity anyway?

- Criminals
  - already do illegal stuff
  - no problem doing more illegal stuff to get anonymity
    - identity theft
    - renting bot-nets
    - creating bot-nets
    - cracking one of the thousands of insecure computers in the net
Who needs anonymity anyway?

- Very different groups
- All with the same goal

anonymity needs diversity
Overview

- Who needs anonymity anyway?
- **Anonymization concepts**
- Tor
- FreeBSD
- What else to take care of?
- Demonstration
- Summary
Anonymization concepts

- Proxy

(Source: http://www.at-mix.de)
Anonymization concepts

- Proxy
  - fast
  - simple
  - single point of failure
Anonymization concepts

- Mix

(Source: http://www.tm.uka.de/itm)
Anonymization concepts

- Mix cascade

(Source: http://sarwiki.informatik.hu-berlin.de)
Anonymization concepts

• MIX cascade
  – slow
    • public key encryption
    • mixing
  – distributed trust
  – one MIX secure
    connection anonymous
Overview

- Who needs anonymity anyway?
- Anonymization concepts
- Tor
- FreeBSD
- What else to take care of?
- Demonstration
- Summary
Tor

- The Onion Router
- Open source, BSD license
- TCP-overlay network
- Provides SOCKS interface
- Available on many platforms:
  - Windows, Linux, MacOS X
  - FreeBSD, OpenBSD, NetBSD
  - Solaris, other UNIX systems
Tor

- Aims to combine positive attributes of proxies and mixes
  - speed (fast)
    - session keys
    - TCP multiplexing
  - distributed trust
- Design goals: deployability, usability, flexibility, simplicity
Tor

(Source: http://www.torproject.org)
Tor

How Tor Works: 2

Step 2: Alice’s Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.

(Source: http://www.torproject.org)
Tor

How Tor Works: 3

Step 3: If the user wants access to another site, Alice’s Tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.

(Source: http://www.torproject.org)
Tor

- Exit policies (for nodes)
  - control which TCP connections can exit your node
  - default policy blocks SMTP, NNTP and some others
  - allows the rest (HTTP, SSH...)
  - reject everything: middleman- or entry-node
Tor

• Hidden Services
  – Services with no published IP address
  – Cannot be physically found
  – Can be provided anywhere connection to Tor network is possible
  – Resist Denial of Service
  – Resist censorship
  – Addresses: duskgytldkxiuqc6.onion
Tor

(Source: http://www.torproject.org)
Tor

(Source: http://www.torproject.org)
Tor

• Legal issues
  – may be forbidden in some countries
  – crypto restrictions (Great Britain, “RIPA”)
  – special laws (Germany, “hacker paragraph”)
  – destination servers have Exit-Node IP in their logs
    • node operator has to answer if there is trouble
    • server may get ceized (happened before)
    • ...

Overview

- Who needs anonymity anyway?
- Anonymization concepts
- Tor
- **FreeBSD**
- What else to take care of?
- Demonstration
- Summary
FreeBSD

• Well suited for Tor (node) operation
• Operational security
  – Jails (jail(8))
  – Disk/swap encryption (geli(8), gbde(4))
  – audit(4)
  – mac(4) framework
• Hardware crypto(4) acceleration
• Well maintained Tor-related ports
FreeBSD

• Important ports
  – security/tor
  – security/tor-devel
  – www/privoxy
  – net-mgmt/vidalia
  – security/trans-proxy-tor
Overview

- Who needs anonymity anyway?
- Anonymization concepts
- Tor
- FreeBSD
- What else to take care of?
- Demonstration
- Summary
What else to take care of?

- **Name resolution**
  - Some applications bypass configured proxy (hi Firefox < version 1.5!)

- **Cookies, web-bugs, referrer**
  - Disable cookies/referrer or better use Privoxy

- **Connection Exit-Node <-> Destination**
  - Not encrypted! Use secure protocols

- **Services that require registration**
  - Tor cannot help you there
Overview

- Who needs anonymity anyway?
- Anonymization concepts
- Tor
- FreeBSD
- What else to take care of?
- Demonstration
- Summary
Overview

• Who needs anonymity anyway?
• Anonymization concepts
• Tor
• FreeBSD
• What else to take care of?
• Demonstration
• **Summary**
Summary

- Tor useful for stealthy net usage
- Can be used to provide resilient services
- FreeBSD a very good choice as a platform

All this very much needed in light of recent laws etc

Tor website: http://www.torproject.org
Questions?
Thank you for your attention!