Attacks on anonymous communication systems

Presented by Adam Varga
...but the real attraction was to create a context where people who were sure they should hate each other were forced to collaborate. – Paul Syverson on why they created onion routing
Overview

- Why we need anonymous communication systems
- Terminology
- Historical overview
- Other anonymity networks
- TOR
- Attacks on TOR
Why we need anonymous comm. systems

- Freedom of speech – China, Iran etc.
- Commercial reasons – Plane tickets, customised websites for competitors
- Privacy – hide otherwise compromising interests (sexual orientation, religious beliefs, medical records)
- And of course - Crime
Anonymity loves company

- There is often a tradeoff bw. usability and privacy
- Anonymity set size matters
- No organization can create anonymity systems itself
- Partitioning attack
  - User behaviour
  - Superfluous options
  - Type I remailers – padding size
Terminology

- Anonymity: is defined as the state of being not identifiable within a set of subjects, the anonymity set.

- Unlinkability: ensures that a user may make multiple uses of resources or services without others being able to link these uses together.

- Unobservability: the state of items of interest (IOIs) being indistinguishable from any IOI (of the same type) at all. E.g. you cannot tell if a sender is sending.

- Pseudonimity: Being pseudonymous is the state of using a pseudonym as ID.
Historical overview

- Anon.penet.fi
- Anonymizer, Safeweb
- Remailers and Nym servers
Johann Helsingius, 1993
Table of correspondence between pseudonyms and real email addresses
Copyright infringement 1996, Church of Spiritual Technology, Religious Technology Center and New Era Publications International Spa
Service closed in August, 1996
Ironically the revealed pseudonym pointed to another remailer system
# Anonymizer and Safeweb

<table>
<thead>
<tr>
<th>Anonymizer</th>
<th>Both</th>
<th>SafeWeb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous web proxies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filters out dynamic content</td>
<td>Wrap dynamic content</td>
<td></td>
</tr>
<tr>
<td>Passive attacker can easily identify traffic based on size</td>
<td>Uses SSL</td>
<td></td>
</tr>
</tbody>
</table>
Type I „Cypherpunk” and Type II remailers

- **Type I**
  - Codebase posted to Cypherpunks mailing list
  - 1996
  - Encode message with servers PGP key
  - Reply blocks supported, encoded with remailers public key

- **Type II**
  - Mixmaster
  - Mix network
  - Only forward path
Type III remailers, and Nym servers

- Type III (Mixminion)
  - Mix network architecture
  - Uniform sized chunks
  - SURBS – Single Use Reply Blocks

- Nym server
  - Pseudonymous remailer
  - Assign a pseudonym to a user
  - Keeps a database on how to return the mail
JAP

- Java Anon Proxy or JonDonym
- University of Dresden & Univ. of Regensburg
- Free/Commercial versions
- Cascade mixes
- 2003 German court order – log users connecting to specific sites
- Countermeasure – Mixes from multiple countries
- http://ip-check.info/?lang=en
I2P - Invisible Internet Project

- Initial release in 2003, most of the developers known only by pseudonyms
- Designed and optimized for hidden services, which are much faster than in Tor
- Fully distributed and self-organizing
- Peers are selected by continuously profiling and ranking performance, rather than trusting claimed capacity
- Floodfill peers ("directory servers") are varying and untrusted, rather than hardcoded
I2P

- Unidirectional tunnels instead of bidirectional circuits, doubling the number of nodes a peer has to compromise to get the same information.

- Protection against detecting client activity, even when an attacker is participating in the tunnel, as tunnels are used for more than simply passing end to end messages (e.g. netDb, tunnel management, tunnel testing)

- Tunnels in I2P are short lived, decreasing the number of samples that an attacker can use to mount an active attack with, unlike circuits in Tor, which are typically long lived.

- Essentially all peers participate in routing for others

- The bandwidth overhead of being a full peer is low, while in Tor, while client nodes don't require much bandwidth, they don't fully participate in the mixnet.
I2P

- Packet switched instead of circuit switched
- Implicit transparent load balancing of messages across multiple peers, rather than a single path
- Resilience vs. failures by running multiple tunnels in parallel, plus rotating tunnels
- Integrated automatic update mechanism
- Both TCP and UDP transports
- Java
Freenet

- Ian Clarke, March 2000
- Peer-to-peer censorship resistant platform
- Decentralized distributed data store
  - Users have to allocate space for the chunks
- Darknet/opennet mode
- Network can forget
Tor - index

- General overview
- Attacker model
- How Tor works
- Hidden services
- Interesting hidden services
- Silk Road – case study
- Censorship resistance
- Related projects
- The Bad Apple attack
- The NSA attack
Tor – General overview

- The Onion Router
- Overlay anonymity network
  - Access the public internet without revealing IP address
  - Access hidden services without knowing the target IP
- Free to use
  - Originally researched in the U.S. Naval Research Laboratory
- Relays TCP traffic
Tor – Attacker model

- No protection against global adversary (who can see both end of the network)
- Adversary who can:
  - Observe some fraction of network traffic
  - Delete, replay, modify, generate network traffic
  - Operate onion routers of his own
  - Can compromise some fraction of the onion routers
  - Can compromise some directory servers
Tor – Design goals and non-goals

- Goals:
  - Deployability (cheap to run, liability burden, implementation)
  - Usability (platforms, familiar apps, settings)
  - Flexibility
  - Simple design (complex is dangerous)

- Non goals:
  - Not peer-to-peer
  - Not secure against end-to-end attacks
  - No protocol normalization
  - Not steganographic
Tor - Features

- Fixed size cells
- Perfect forward secrecy
- Separation of protocol cleaning from anonymity
- No mixing, padding, traffic shaping
- Multiple TCP streams in one circuit
Tor - Features

- Leaky pipe topology
- Congestion control
- Directory servers
- Variable exit policies
- End-to-end integrity checking
Tor – Cells

- 512 bytes
- Header
  - Circuit ID
  - Command
- Payload
  - Relay header (Stream ID, Digest, Len, CMD) + Data or Data
Tor - Constructing a circuit

Alice (link is TLS–encrypted) OR 1 (link is TLS–encrypted) OR 2 (unencrypted) website

- Create c1, E(g^x1)
- Created c1, g^y1, H(K1)
- Relay c1{Extend, OR2, E(g^x2)}
- Relay c1{Extended, g^y2, H(K2)}
- Relay c1{{Begin <website>:80}}
- Relay c1{{Connected}}
- Relay c1{{Data, "HTTP GET..."}}
- Relay c1{{Data, (response)}}

- Create c2, E(g^x2)
- Created c2, g^y2, H(K2)
- Relay c2{Begin <website>:80}
- Relay c2{Connected}
- Relay c2{Data, "HTTP GET..."}
- Relay c2{Data, (response)}

Legend:
E(x)—RSA encryption
{X}—AES encryption
cN—a circID

(TCP handshake) "HTTP GET..." (response)
Tor – Integrity checking

- Tor uses TLS on its links -> external adversaries cannot modify data
- No integrity check between each hop -> Cell size would depend on the length of the circuit, or maximized at the longest
- Integrity check only at the edges of each stream
  - SHA-1, add every relay cell they create, include first 4 bytes in message
Tor – Hidden services

- AKA responder anonymity
- Users can access services without knowing the service’s IP address
- Design goals:
  - Access control (avoid floods)
  - Robustness (long term pseudonymous id)
  - Smear-resistance
  - Application-transparency
Tor – Hidden services

- Server - Introduction points – advertised (DHT)
- Alice - Rendezvous point
- Extra level of indirection -> can filter requests
Creating and connecting to a Location hidden service
Top changes in Tor since the 2004 design paper 1.

- Node discovery and the directory protocol
  - Directory protocol v2 - Tor 0.2.0.3-alpha (Jul 2007)
  - Directory servers themselves compute a consensus document, and all of them sign it.
  - Microdescriptors – only the necessary information is in the router descriptor list
  - Tunneling directory connections over TOR

- Security improvements for hidden services
  - Tor 0.2.0.10-alpha, Nov 2007
  - Hidden services publish to a set of nodes whose identity keys are closest to a hash of the service's identity, the current date, and a replica number
Top changes in Tor since the 2004 design paper 2.

- Improved authorization model for hidden services
  - Optionally, a client must know a shared key, and use this key to decrypt the part of a hidden service descriptor containing the introduction points. It later must use information in that encrypted part to authenticate to any introduction point it uses, and later to the hidden service itself.

- Faster first-hop circuit establishment with CREATE_FAST
  - No additional Diffie-Hellman exchange at first hop
Top changes in Tor since the 2004 design paper 3.

Cell queueing and scheduling
- Tor 0.2.2.7-alpha (Jan 2010)
- Favor the circuits on each connection that had been quiet recently, so that a circuit with small, infrequent amounts of cells will get better latency than a circuit being used for a bulk transfer

Guard nodes
- Tor 0.1.1.11-alpha (10 Jan 2006)
- The Tor client picks a few Tor nodes as its "guards", and uses one of them as the first hop for all circuits
Top changes in Tor since the 2004 design paper 4.

- Bridges, censorship resistance, and pluggable transports
  - Bridges – special Tor nodes which are not published in the directory
  - Tor has gradually changed its TLS handshake to better imitate web browsers
  - Tor pluggable transports – external plugins to shape traffic
Censorship resistance

- Bridges
  - https://bridges.torproject.org/
  - Gmail, Ymail - bridges@bridges.torproject.org, get bridges
- The problem: DPI
- Solution: Obfuscated proxy
  - HTTP, SkypeVideo etc.

![Diagram showing obfsproxy client and obfsproxy server with a censor between them. Tor Client and Tor Bridge are connected to the obfsproxy client and server respectively.]
Interesting

- Iran – liberation numbers – primes - DH
- Political events- censorship arises
  - China
  - Thailand
- Syria – record all of the outgoing communications
- Iran DPI – cannot recognize TOR
  - Block the whole TLS traffic
Top changes in Tor since the 2004 design paper 5.

- Changes and complexities in path selection algorithms
  - Avoiding duplicate families in a single circuit
  - Bandwidth authorities 0.2.1.17-rc
  - Weighting node selection by bandwidth 0.2.2.10-alpha

- Stream isolation
  - Different circuit for different clients, SOCKS connections with different authentication credentials, or different SOCKS port on the Tor client 0.2.3.3-alpha
Top changes in Tor since the 2004 design paper 6.

- Controller protocol
- Rise and fall of .exit
- Link protocol TLS, renegotiation
  - Tor 0.2.3.6-alpha
  - Redesign TLS negotiation to resemble HTTPS
  - Dummy certificates
  - Dummy cipher suites
The Hidden Wiki

http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page

Mirror:

https://zgktlwi4fecvo6ri.onion.to/wiki/index.php/Main_Page
Silk Road

- Online black market, the „Amazon of drugs”
- Escrow service
- Run by the administrator named Dread Pirate Roberts
- TOR hidden service - silkroadvb5piz3r.onion
- Launched in February 2011.
- Bitcoin as payment method
- Carnegie Mellon – CyLab measurement, Crawling
  - Estimated revenue: 92,000 US dollars per month
  - Trade volume 1.2 million US dollars per month
- FBI shut it down on October 2, 2013.
browsing stimulants

sort by: best selling

1.0g RAW FLAKE Cocaine, 80%-86% PURITY, UK Only
vendor: AllOnRock 2.0
ships from: United Kingdom

SPEED / 1gr Amphetamine paste
vendor: schoften
ships from: Netherlands

1g Pure Uncut High Quality Cocaine
vendor: Jack_Frost
ships from: United States

.10g Washed Fishscale Cocaine
vendor: buypld
ships from: United States

1g PSEUDO SPEED- CRUSHED ROCK – VACMYLER SEALED - AUSTRALIA ONLY
vendor: chemiclabrothers
ships from: Australia

B0.207573
add to cart

B0.015963
add to cart

B0.118010
add to cart

B0.011801
add to cart

B0.160987
add to cart
### Silk Road Anonymous Market

**Forgeries**
- Digital
- Physical
- Apparel
- Art
- Biotic materials
- Books
- Cannabis
- Collectibles
- Computer equipment
- Custom Orders
- Digital goods
- Dissociatives
- Drug paraphernalia
- Drugs
- Ecstasy
- Electronics
- Erotica
- Hardware
- Herbs & Supplements
- Jewelry
- Lab Supplies
- Lottery tickets
- Medical
- Money
- Opioids
- Other
- Packaging
- Physical goods
- Precursors
- Prescription
- Psychedelics
- Services
- Stimulants
- Writing

### Browsing Forgeries

<table>
<thead>
<tr>
<th>Product Description</th>
<th>Vendor</th>
<th>Price</th>
<th>Add to Cart</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoldenLotus Hardcore Collection</td>
<td>couponking</td>
<td>$0.077985</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>Fake Passport 1:1 (like real) New version</td>
<td>ThreeKings</td>
<td>$2.678926</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>Custom PSHQ UK Passport And Utility Scan, Any Name, Details</td>
<td>PerfectScans</td>
<td>$0.232655</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>Custom PSHQ USA Passport And Utility Scan, Any Name, Details</td>
<td>PerfectScans</td>
<td>$0.232655</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>Illinois Driver's License [Holoi+UV+Scannable+Microprint]</td>
<td>MisterReplicator</td>
<td>$0.161169</td>
<td>Add to Cart</td>
</tr>
</tbody>
</table>
Silk road – how did they find Dread Pirate Roberts? 1.

- DPR used Bitcoin tumbler, so transactions were obfuscated.
- Find the first mention of the Silk Road!
- Earliest post ever mention Silk Road on shroomery.org by user altoid:
  - I came across this website called Silk Road. It’s a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I’m thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it.
Silk road – How did they find DPR? 2.

- Post directed readers to visit silkroad420.wordpress.com
- A subpoena to WordPress Revealed that the blog had been set up on January 23, only four days before the Altoid post
- Further research revealed, that altoid posted on Bitcoin Talk, looking for a bitcoin expert, directing all inquiries to "rossulbricht at gmail dot com,"
- FEDs connected other accounts – Google+, Youtube, StackOverflow
Silk road – How did they find DPR? 3.

- Meanwhile FBI probably hacked the site, and revealed its real IP address, contacted the hosting provider, and cloned the site
- Homeland security - Fake passport incident
- Got arrested in San Francisco Public Library – logged into Silk Road as DPR
- Hitman incidents
The new Silk road

- [http://silkroad6ownowfk.onion](http://silkroad6ownowfk.onion)
- After a 2 weeks hiatus, it reopened
- Currently inactive because of site redesign
  - One other black market was closed by the FBI, another one stole their vendors BitCoins
  - DPR announced that they redesign the site to be able to handle the increased traffic
Related projects

- Tor Browser
- Tails
- Torbirdy
  - TorButton for Thunderbird
- Tor2Web
  - Trade anonymity for usability
- TorCloud
  - EC2
Attacks published in the original paper - passive

- Observing user traffic patterns
- Observing user content (Privoxy)
- Option distinguishability
- End-to-end timing correlation (self owned OR)
- End-to-end size correlation (leaky pipe)
- Website fingerprinting
Attacks published in the original paper - active

- Key compromise
- Iterated compromise
- Run a recipient
- Run an onion proxy
- DoS non-observed nodes
- Run a hostile OR
- Introduce timing into messages
- Replace content of unauthenticated protocols
- Smear attacks
- Distribute hostile code
Attacks published in the original paper - directory

- Destroy directory servers
- Subvert a directory server
- Subvert a majority of directory servers
- Encourage directory servers dissent
- Trick the directory servers into listing a hostile OR
- Convince the directories that a malfunctioning OR is working
Attacks published in the original paper – rendezvous p.

- Make many introduction requests
- Attack an introduction point
- Compromise an introduction request
- Compromise a rendezvous point
Assumption: attacker controls an exit node

Reveal IP:
- Flash injection – connect to external IP
- Javascript injection – send local IP -> not effective bco. NAT (192.168.0.1)

Timing pattern injection:
- HTML Meta refresh tag
- Users leave page open long enough so the pattern can be spotted by an entry node controlled by the attacker
One bad apple spoils the bunch

- Attack against TOR, presented in 2010
- Attacker model
  - Exit node
  - Torrent peer
- Centralised tracker, DHT
- Connect multiple circuits - Peer ID
NSA attack on TOR 1.

- Not the protocol, instead the TOR Browser Bundle
  - Preconfigured Firefox to use the TOR network
- Turbulence, Turmoil and Tumult – powerful data analysis systems, monitors Internet traffic
  - The usage of TOR can be easily identified
    - Exit nodes are known
- Quantum servers- part of Turmoil, placed at key locations on the Internet backbone, can respond faster
  - “Man-on-the-side” attack
NSA attack on TOR 2.

- FoxAcid – Servers on the public Internet
  - Attacks only trigger if called with special URLs – FoxAcid tags
    - http://baseball22.2ndhalfplays.com/nested/attrs/bins/1/define/forms952_z1zzz.html
  - Different URL for each type of attack

- Specific example: EgotisticalGiraffe exploit – type confusion vulnerability E4X XML extension for Javascript - Firefox 11.0 -- 16.0.2 affected

- Aim is to infect the target’s computer, reveal his identity, and track later activities
How to use TOR

- Use the Tor Browser
- Don't enable or install browser plugins
- Use HTTPS versions of websites
- Don't open documents downloaded through Tor while online
- Use bridges and/or find company
Conclusions
Thank you. Are there any questions?
Opt- The threats to your security

- Insecure modes of operation
- Optional security (may allow cookies)
- Badly labeled off switches (social tricks)
- Inconvenient (written down passwords)
- False sense of security (encrypted ZIP arch.)
- Bad mental models (lock icon)
References

- http://www.i2p2.de/how_networkcomparisons
- https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html
- http://anon.inf.tu-dresden.de/index_en.html
- http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf
- https://blog.torproject.org/blog/top-changes-tor-2004-design-paper-part-1