Exploiting hidden services to setup anonymous communication infrastructures

21 October 2006
Luxembourg

Fabio Pietrosanti
naif at s0ftpj.org
My goals

- Explain anonymity concept and different networks
- Explain the potential of exploiting anonymous networks in a different way
- Present the Laissez Faire Island Project and get interests and contributors
- Discuss on how to support the growth of anonymous communication systems with an a-commerce market
What’s this talk not about?

• Not go deeper in the technical details of anonymous protocols
• Do not make any promotion of commercial tools
Me

- Underground: member of the s0ftpj group, sikurezza.org italian mailing list, e-privacy and winston smith anonymous communities, and some advisories made for PIX firewalls
- Work: CTO of a swiss privacy provider
- Personally: love for anonymity research!
You

- Who does personally require anonymity?
- Who have ever used TOR?
Agenda

- Anonymity
- Anonymity use and abuse
- Anonymous Networks
- TOR - The Onion Router
- Anonymous Backbone Concept
- Laissez Faire Island Project
- LFI MAIL: unconventional approach to anonymous email
Anonymity
What’s anonymity

• Anonymity is a state of not being identifiable within a set of subjects

• Big difference between anonymity and confidentiality:
  • Identity protection
  • Location protection
  • Deniability of actions (w.r.t. identity)
What to protect?

The sender/receiver anonymity issues

- Who you are
- Where you are located
- Whom you communicate with
- Where the recipient/server is located

Most of anon nets protects only the sender!

Good anonymity requires mutual protection
Anonymity requires cooperation

- No organization would ever be able to stay anonymous by itself.
- You can only get confidentiality yourself.
- Anonymous network requires cooperation
Agenda

- Anonymity
- Anonymity use and abuse
- Anonymous Networks
- TOR - The Onion Router
- Anonymous Backbone Concept
- Laissez Faire Island Project
- LFI MAIL: unconventional approach to anonymous email
Anonymity use and abuse
Personal use

- Discussion of sensible issues
- sexual attitude
- religious belief / vision
- political inquiries
- Avoid tracking and profiling by isp’s / corporate / governments / google!
Corporate use

- Business Intelligence activity
- Stop competitive analysis (r&d, procurement)
- Legal discussions
- Communications from non democratic countries and war places
- Journalist communications
- Prevent price & information discrimination
Government use

- Diplomatic communications
- Where is the ambassador staying?
- Anonymous requests by citizen to law enforcers
- Criminal investigation
  - Oh... FBI is looking at my website!!
- Stuff in the public interest...
Security Research

USAGE

- Security Researchers caught at security conferences
  - Dmitry Sklyarov @ Defcon
  - Stephen Rombom @ Hope
- 20 September 2006: Tron @ Toorcon 8
  - First conference over TOR!
- Ventrilo (2k/s voice streaming) + VNC (5-10k/s video streaming) = Alan Bradley & Kevin Flynns talked securely away from the USA/DMCA risks
Abuse (why limits?!?)

- Do only terrorists need anonymity?
- Hotmail & drafts methods!
- Hey... also mafia, pedopornograph, cyber vandals use TOR!
- So we should declare illegal internet, airplanes, child, knifes because it can be abused?
- Adversaries are much less skilled than what we ever thought!
Agenda

- Anonymity
- Anonymity use and abuse
- Anonymous Networks
  - TOR - The Onion Router
  - Anonymous Backbone Concept
  - Laissez Faire Island Project
  - LFI MAIL: unconventional approach to anonymous email
Anonymous networks
There’s too much garbage!

- There are tons of anonymous technologies out there:
  - Few projects got success
  - Few projects grow
- Limitations are mainly related with:
  - Risk context to be managed
  - Deployment & usability
High latency

• Good for store & forward action -> Email

• Anonymous Remailers:
  • CypherPunk type I: old technology, old network)
  • Mixmaster type II: around 35 servers, very stable networks
  • Mixminion type III: experimental networks by freeheaven
  • Nym servers: old school -> anon.penet.fi / nym.alias.net

• Those networks are not email systems: need true, traceable email systems
Low latency

- Good for interactive action -> Web Browsing / Chat
- Onion Routing -> The Onion Router (c)
  - The biggest anonymous network ever known
- I2P (java)
  - Free mixnet
  - Fully distributed (p2p)
  - Variable latency through I2P API
- FreeNET (java)
  - P2P storage for mutual anonymous content publishing and access. Still too slow
Misc anon networks

- AnoNET
- Crowds
- Invisible IRC
- WASTE
- Entropy
- Mute
- GNUnet
- Winny
- Mnet
- Infrastructure for resilient internet systems
- Rodi

- Marabunta
- Morphmix
- Tarzan
- AntsP2P
- ....
Agenda

- Anonymity
- Anonymity use and abuse
- Anonymous Networks
- **TOR - The Onion Router**
- Anonymous Backbone Concept
- Laissez Faire Island Project
- LFI MAIL: unconventional approach to anonymous email
The Onion Router
Who did make it?

- USA Department of Defense
- Electronic Frontier Foundation
Goals

• Deployability for supporters and users
• Flexibility of the protocols
• Usability for the users
• Simple design of architecture

• Directory Servers - RendezVous Servers - Users - Tor Servers (Middleman / Exit node)
NOT Goals

- Not peer to peer
- Not secure against end-to-end attacks
- No protocol normalization (Use privoxy!)
- It’s filterable
  - Block http request for /tor/* (dir server)
- It’s identifiable (TOR-bl, public list of nodes)
TOR network expansion

last 24 months growth of tor routers
http://www.noreply.org/tor-running-routers/totalLong.html
TOR network bandwidth

last 24 months grow of tor bandwidth
Vidalia

- [http://vidalia-project.net](http://vidalia-project.net)
- Status - Stop/Start - Map - Logos - Configuration - Help - Translations - Monitor
TOR typical use

- Protect only the identity & location of the sender accessing internet services
A look at exit nodes traffic

- Most http, messaging, pop3
- A lot of porn and googling!
- Automated web attacks
- Cinema like telnet! ;)
- EVERY EXIT NODE CAN INTERCEPT NON ENCRYPTED TRAFFIC!
- Paranoid but dumb: https://tor.unixgu.ru/
Agenda

• Anonymity
• Anonymity use and abuse
• Anonymous Networks
• Anonymous Backbone Concept
• Laissez Faire Island Project
• LFI MAIL: unconventional approach to anonymous email
Anonymous internet backbone
Changing the rules

- Consider the Internet as a generic transport media
- TOR as an anonymous backbone
  - do you know MPLS?
- Mutual anonymous protection
- High performance anonymity
- No more 3 trusted third party!!!
No more 3 trusted party

- Protect the identity & location of the sender AND of the receiver (server) by accessing hidden services.
Onion LAND

- Hidden services are tcp redirects from the running tor client
- Hidden services can be exposed behind NAT
- Latency:
  - New connection: 80ms - 5 seconds
  - Established connection: 700ms - 2 seconds
- .onion TLD for each registered service
- No restriction policy as for Exit Node!
Usability issue

- Make the .onion hostname easier
- Hidden wiki http://6sxoyfb3h2nvok2d.onion
- FreeNODE irc irc://mejokbp2brhw4omd.onion
- Application level Internet redirection (not a good way!)
- 2nd level TOR rendez vous services
- Easy hidden url
service limits

• High bandwidth services (video)
• Frequent connections (p2p file sharing)
• Low latency services (telephony)
  • Ok for Push To Talk
• Serious troubles with full duplex!
Anonymous services

- Develop an anonymous society
- Start doing business with anonymous tools!
- Promote Free and NON-Free anon services:
  - Email hosting
  - Server (physical or virtual) hosting: rayservers, me (free vps)
  - Internet reverse proxy services (easy migration)
    - es: http://serifos.eecs.harvard.edu/proxy/http://6sxoyfb3h2nvok2d.onion
  - Payment provider (egold exchanger, prepaid visa cards)
Thinking anon business

- There are many business to be build around anonymous networks!
- Main issues: availability (b2b) & payment (b2c)
- Investing % of the income in the network would really improve availability
- Anonymous VPNs
- Anonymous Messaging
Anonymous VPNs (1)

- VPNs are not so private (identity & location)
  High risk context VPNs are useful in business and personal use
- The anonymous backbone is a nat proof transport media
- Good for email, instant messaging, file services (better webdav with keepalive!) and http resources
Anonymous VPNs (2)

- Example use: Journalism, Public safety, NAT bypass, non-democratic country branch
Anonymous VPNs (3)

- Place privacy enforcement on the firewalls!
Anonymous Messaging

- Email messaging with anonymous network works really definitely well but...
- No hidden diffused email messaging services
  - xrek (62 users) [http://4nc7xi5usjq6z7bc.onion/](http://4nc7xi5usjq6z7bc.onion/)
  - Tormail down ([onion.theme1.com](http://onion.theme1.com))
- TOR block outgoing SMTP (for spam)!!!
Agenda

• Anonymity
• Anonymity use and abuse
• Anonymous Networks
• TOR - The Onion Router
• Anonymous Backbone Concept
• Laissez Faire Island Project
• LFI MAIL: unconventional approach to anonymous email
Laissez Faire Island Project
Do you remember Laissez Faire City?

In ’95 a group of cyber/economist fanatic created a new sovereign international cyber city

Developed a privacy infrastructure to allow individual to operate in the freedom of cyberspace outside the confines of the traditional nation-state

Declaration of the independence of CyberSpace

http://homes.eff.org/~barlow/Declaration-Final.html

A mix between crypto-anarchism and anarcho-capitalism
Laissez Faire City

- Mailvault - [www.mailvault.com](http://www.mailvault.com) - YodelBank -
- DMT - Digital Monetary Trust
  - DMT ALTA - Asset Lodgement Trust Accounts
  - DMT LESE - Laissez-Faire Electronic Stock Exchange
- ICA - International Contract Registration
- CEP - Common Economic Protocol
  - [http://cep.metropipe.net/](http://cep.metropipe.net/)
Laissez Faire Island

• Laissez Faire Island aims to become a small piece of land in the sea of anonymity

• We want to create and stimulate the creation of anonymous social environments

• TOR gives us the chance to do that!

• Laissez Faire Island is a baby!

• We need a logo!
Laissez Faire Island

• Laissez Faire Island require infrastructures!
• Several islands are required to born before service network can be really effective!

• We provide free virtual private server for anonymous services!
• Get one and setup free a service!
LFI Architecture (1)

- How to implement a Laissez Faire Island?
  - Be 100% sure that no one would be able to discover where it is!
  - Be 100% sure that incoming traffic follow a different path respect to outgoing traffic
  - Differentiate services and traffic routing!
  - Use virtualization technology (XEN)
LFI Architecture (2)

- Carefully select TOR-IN / TOR-OUT
LFI Architecture (3)

- TOR CVS simplify the setup
  - TransPort 9040 + iptables/iproute2
- DNS servers
  - tor-dns-proxy.py (dugsong)
  - dns-proxy-tor (http://p56soo2ibjxx23xo.onion/)
- Iptables / iproute2 for network policy/redir
- Dynamic firewall script for tor-only traffic
- Dmcrypt-luks for disk encryption
We want your island!

- Setup your island!
- Came with us!
- Build a redundant and solid Anonymous Infrastructure!
- Availability & distribution are key features!
Agenda

- Anonymity
- Anonymity use and abuse
- Anonymous Networks
- TOR - The Onion Router
- Anonymous Backbone Concept
- Laissez Faire Island Project
- **LFI MAIL:** unconventional approach to anonymous email
Laissez Faire Island
Email Platform
An old need

• Before spam, people thought anonymous email was a good idea:
LFI MAIL GOAL

• Provide anon email services through a network of redundant servers located in many islands of the sea of anonymity

• Escape from the net: stay in the islands!

• internal communication (simple)

• external outbound communication (complex!)

• external inbound communication (very complex!)
Escape from TOR

- TOR exit nodes block outgoing SMTP but...
- SMTPS (465/tcp) is allowed!
- 19/35 Mixmaster anonymous remailer nodes support SMTPS!
- http://www.noreply.org/tls/
- We mix the best we can get from different anonymous networks!
LFI MAIL: anonymix!

External outbound communications made easy & more paranoid!
LFI MAIL sw

- An email system quick to be setup) (www.kolab.org)
- Mixmaster & smtp2mix
- Horde Webmail (+mod_security +mod_chroot)
- Simple signup system
- Upcoming: automatic encryption (anubis)
Still no internet inbound

• Having a unique inbound internet-to-TOR gateway would expose the system to interception

• Inbound connection would require an high number of information nodes around the world giving their IP

• Idea! Ask TOR-ops/Mixmaster-ops to redirect 25/TCP port to the network of islands!

• DNS MX Record: 900 results around the world!
future useful ideas

- Old school shell server
- Conference streaming platform
- Proxy middleware to avoid tor exit issues
- Free “Exit Node” pcap dump for all!
- TOR development
  - Hidden Service Round Robin
  - Easy 2nd level rendez vous services
Questions?

- Contribute and share your passion!
- wiki http://vbp22opdeypalsic.onion
- naif@vbp22opdeypalsic.onion (beta LFI mail)
- Internet: naif@s0ftpj.org
- Get TOR! http://vidalia-project.org