

Anonymity and Anticensorship



EECS 388: Introduction to Computer Security
March 18, 2015

1

Why Privacy?

- Privacy is not equivalent to secrecy
- Necessary to ensure civil liberties:
 - Free speech, free association, autonomy, freedom from censorship and constant surveillance
- "Nothing to Hide Argument"
 - Dangers of constructing a Kafkaesque world
 - Optional reading: '*I've Got Nothing to Hide*' and *Other Misunderstandings of Privacy*, Daniel J. Solove

2

Nymity Spectrum

- **Verinymity**
 - credit card #s, driver's license, address
- **Pseudonymity**
 - pen names, many blogs
- **Linkable anonymity**
 - loyalty cards, prepaid mobile phone
- **Unlinkable anonymity**
 - paying in cash, Tor

3

Understanding Anonymity

- "without a name"
- Who wants it
- How to get it
- Threats to it

4

Anonymity

- Anonymity: Concealing your identity
- In the context of the Internet, we may want anonymous communications
 - **Communications where the identity of the source and/or destination are concealed**
- Not to be confused with confidentiality
 - Confidentiality is about contents, anonymity is about identities

5

Anonymity

- Internet anonymity is *hard**
 - Difficult if not impossible to achieve on your own
 - Right there in every packet is the source and destination IP address
 - * But it's easy for bad guys. Why?
- You generally need help
- State of the art technique: **Ask someone else to send it for you**
 - Ok, it's a bit more sophisticated than that...

6

Proxies

- Proxy: Intermediary that relays our traffic
- Trusted 3rd party, e.g. ... hidemyass.com
 - You set up an encrypted VPN to their site
 - All of your traffic goes through them
- Why easy for bad guys? Compromised machines as proxies.

7

Alice wants to send a message M to Bob ...

- Bob doesn't know M is from Alice, and
- Eve can't determine that Alice is indeed communicating with Bob.



- HMA accepts messages encrypted for it. Extracts destination and forwards.

8

Anonymity motivation



Surveillance under:

- The Patriot Act
- Section 215
- National Security Letters (NSLs)
- FISA Amendment Act

9

★ ★ ★ ★ ★ SURVEILLANCE UNDER THE PATRIOT ACT ★ ★ ★ ★ ★

Hastily passed 45 days after 9/11 in the name of national security...

The Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records, and track the activity of innocent Americans on the Internet. While most Americans think it was created to catch terrorists, the Patriot Act actually turns regular citizens into suspects.

National Security Letters (NSLs)

are issued by FBI agents, without a judge's approval, to obtain personal information...

FBI

Between 2003 and 2006, the FBI issued **192,499 NSLs** Which led to **1 terror-related conviction**

"I want to deliver a warning... when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."

Senator Ron Wyden (D-OR), May 26, 2011

SOURCE 1 SOURCE 2 SOURCE 3

Diagram illustrating the scope of National Security Letters (NSLs):

- NSL is at the top level.
- Phone Records and Computer Records are connected to NSL.
- Credit History and Banking History are connected to Computer Records.

A magnifying glass icon is shown over the "192,499 NSLs" text.

Text at the bottom right: "The conviction would have occurred even without the Patriot Act." (SOURCE 3)

Image credit: ACLU

Surveillance under the PATRIOT Act

Abuse of Privacy:
The Patriot Act does not require information obtained by NSLs to be destroyed – even if the information is determined to concern innocent Americans.

At least **34,000** law enforcement and intelligence agents have access to phone records collected through NSLs.

In response to **9 NSLs**, **11,100** Americans' telephone account records were turned over to the FBI.
SOURCE: 4

The Patriot Act prohibits Americans who receive NSLs from telling anyone. These "gag order" provisions have been held unconstitutional in several legal cases.

Image credit: ACLU

Surveillance under the PATRIOT Act

Between 2003 and 2005, the FBI made **53 reported criminal referrals to prosecutors** as a result of **143,074 NSLs**.

143,074 NSLs

53 REPORTED CRIMINAL REFERRALS:

Category	Count
MONEY LAUNDERING	17
IMMIGRATION	17
FRAUD	19
TERRORISM	0

SOURCE: 5

Image credit: ACLU

Surveillance under the PATRIOT Act

"Sneak & Peek" Searches:

The Patriot Act allows federal law enforcement agencies to delay giving notice when they conduct secret searches of Americans' homes and offices—a fundamental change to Fourth Amendment privacy protections and search warrants. This means that government agents can enter a house, apartment or office with a search warrant when the occupant is away, search through his/her property and take photographs—in some cases seizing property and electronic communications—and not tell the owner until later.

Of the **3,970 Sneak & Peeks** in 2010:

76%	drug-related
24%	other
<1%	terror-related

SOURCE: 6

TO LEARN MORE, VISIT ACLU.ORG/PATRIOT
[FACEBOOK.COM/ACLU.NATIONWIDE](https://www.facebook.com/ACLU.NATIONWIDE) [TWITTER.COM/ACLU](https://twitter.com/ACLU)

Source:
 1. <http://wyden.senate.gov/newsroom/press/release/?id=34edddcb-2541-42f5-81d-19224030d91e>
 2. <http://www.justice.gov/oig/special/10903b/final.pdf>
 3. http://thescienceofsecurity.org/blog/CT%20since%209-11_by_Breakthrough.pdf
 4. <http://www.justice.gov/oig/special/10703b/final.pdf>
 5. <http://www.aclusa.org/legislation/ctbstatute.pdf>
 6. Report of the Director of the Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions for fiscal year 2010, on file with the Administrative Office of the United States Courts.

Image credit: ACLU

Google Transparency Report

National Security Letters (NSLs)

Reporting Period	National Security Letters	Users/Accounts
January to June 2014	0–999	0–999
July to December 2013	0–999	1000–1999
January to June 2013	0–999	0–999
July to December 2012	0–999	0–999
January to June 2012	0–999	1000–1999
July to December 2011	0–999	0–999
January to June 2011	0–999	0–999
July to December 2010	0–999	1000–1999
January to June 2010	0–999	1000–1999
July to December 2009	0–999	0–999
January to June 2009	0–999	0–999

14

Google Foreign Intelligence Surveillance Act (FISA) Requests

Non-content FISA requests

Reporting Period	Number of requests	Users/Accounts
<i>Data subject to six month reporting delay</i>		
January to June 2014	0–999	0–999
July to December 2013	0–999	0–999
January to June 2013	0–999	0–999
July to December 2012	0–999	0–999
January to June 2012	0–999	0–999
July to December 2011	0–999	0–999
January to June 2011	0–999	0–999
July to December 2010	0–999	0–999
January to June 2010	0–999	0–999
July to December 2009	0–999	0–999
January to June 2009	0–999	0–999

15

Google FISA Requests

Content requests

Reporting Period	Number of requests	Users/Accounts
<i>Data subject to six month reporting delay</i>		
January to June 2014	0–999	15000–15999
July to December 2013	0–999	9000–9999
January to June 2013	0–999	12000–12999
July to December 2012	0–999	8000–8999
January to June 2012	0–999	9000–9999
July to December 2011	0–999	7000–7999
January to June 2011	0–999	5000–5999
July to December 2010	0–999	3000–3999
January to June 2010	0–999	3000–3999
July to December 2009	0–999	2000–2999
January to June 2009	0–999	2000–2999

16

XKEYSCORE

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

What Can Be Stored?

XKEYSCORE

- Anything you wish to extract
 - Choose your metadata
 - Customizable storage times
 - Ex: HTTP Parser

```
GET /search?hl=en&q=islamabad&meta= HTTP/1.0
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-application/msword, application/x-shockwave-flash, */*
Referer: http://www.google.com.pk/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.google.com.pk
```

No username/strong selector

Connection: keep-alive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

17

XKEYSCORE

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Document Tracking

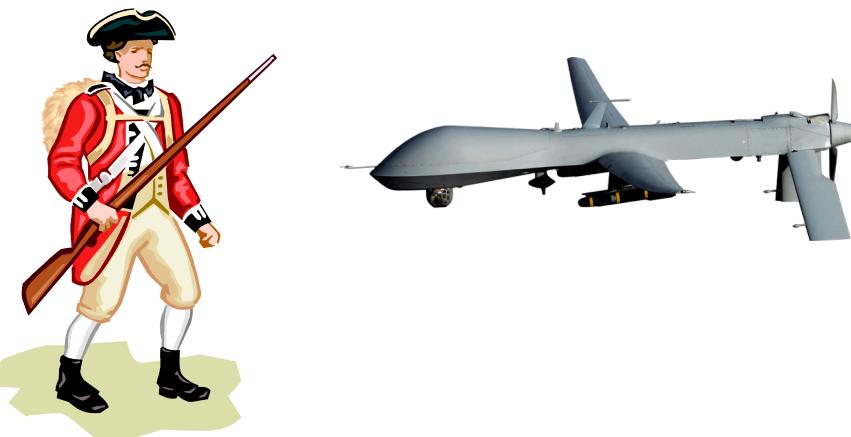
XKEYSCORE

- I have a Jihadist document that has been passed around through numerous people, who wrote this and where were they?

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

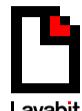
18

Technology as a defense



19

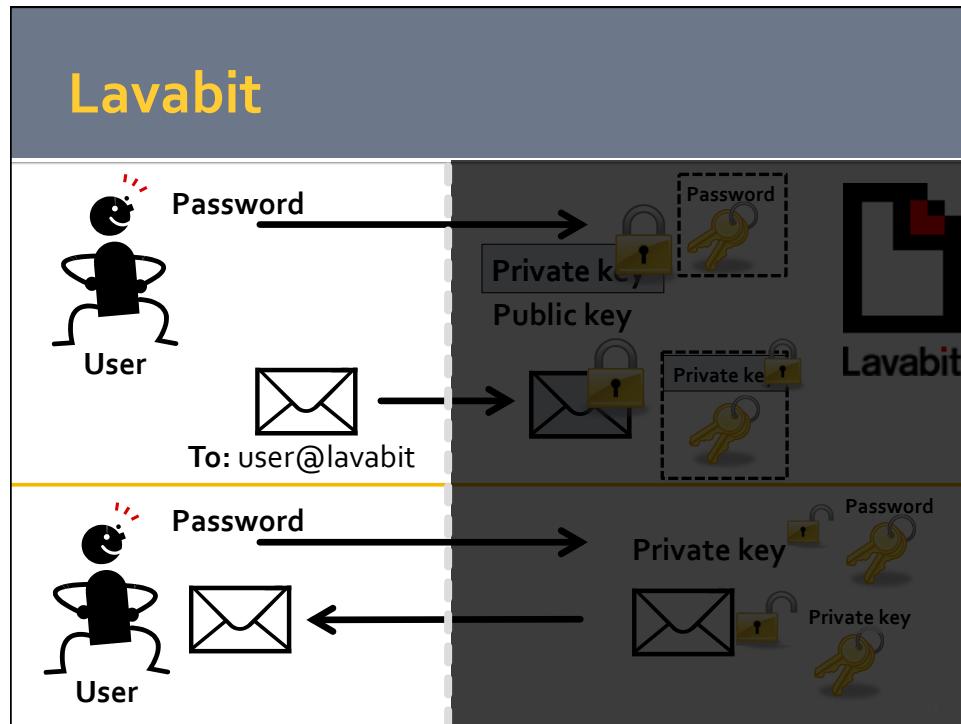
Poor example: Lavabit



My Fellow Users,

I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

20



Encryption Tools: PGP

- GnuPG, free software
 - Pretty Good Privacy (PGP), Phil Zimmerman ('91)
 - Lets you hide email content via encryption
- Basic idea:
 - Hybrid encryption to conceal messages
 - Digital signatures on messages (hash-then-sign)

PGP cont'd

- Each user has:
 - A public encryption key, paired with a private decryption key
 - A private signature key, paired with a public verification key
- How does sending/receiving work?
- How do you find out someone's public key?

23

Sending and receiving

To send a message:

- Sign with your signature key
- Encrypt message and signature with recipient's public encryption key

To receive a message:

- Decrypt with your private key to get message and signature
- Use sender's public verification key to check sig

24

Fingerprints

- How do you obtain Bob's public key?
 - Get it from Bob's website? (⊕)
 - Get it from Bob's website, verify using out-of-band communication
 - Keys are unwieldy → **fingerprints**
 - A fingerprint is a cryptographic hash of a key
 - What if you don't personally know Bob?
 - Web of Trust (WoT)

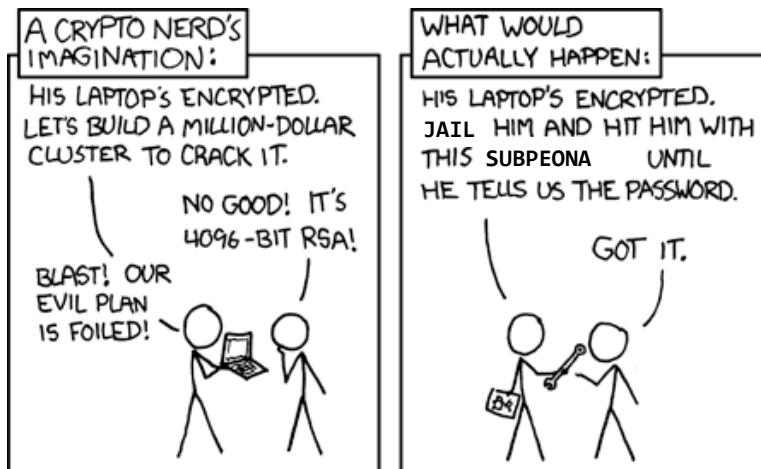
25

Drawbacks of (Just) Encryption I

- What if Bob's machine compromised?
 - His key material becomes known
 - Past messages can be decrypted and read
 - You also have **sender's signature** on messages sent, so you can prove identity of sender
- So...
 - PGP sends key material to decrypt content over public channel
 - Sender must trust recipient's ability and desire to keep her statements private

26

Drawbacks of (Just) Encryption II



27

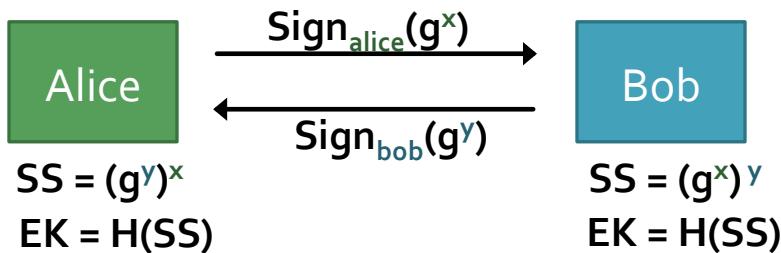
Desirable communication properties

- **Forward secrecy:**
 - Even if your key material is compromised, past messages should be safe
- **Deniability:** be able to deny having sent a message
- Mimic casual, **off-the-record** conversations
 - **Deniable authentication:** be confident of who you are talking to, but unable to prove to a third party what was said

28

Off-the-Record (OTR) Messaging

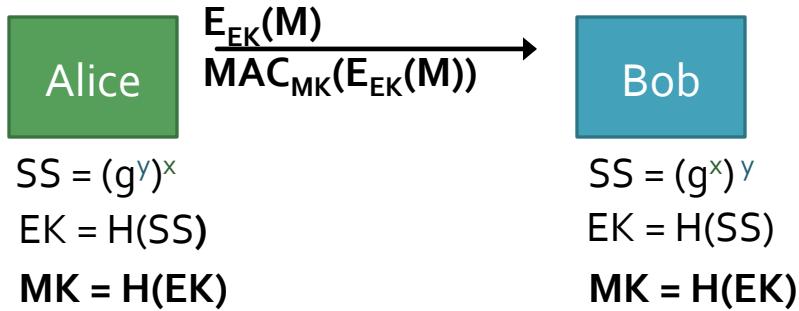
1. Use Authenticated Diffie-Hellman to establish a (short-lived) session key EK



29

OTR II

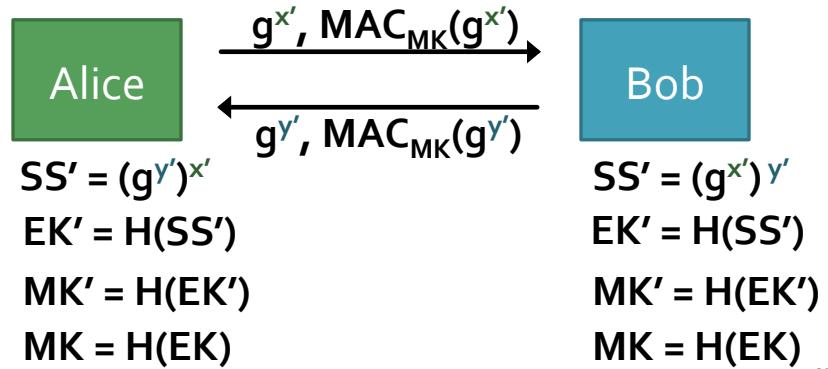
2. Then use secret-key encryption on message M
... And authenticate using a MAC



30

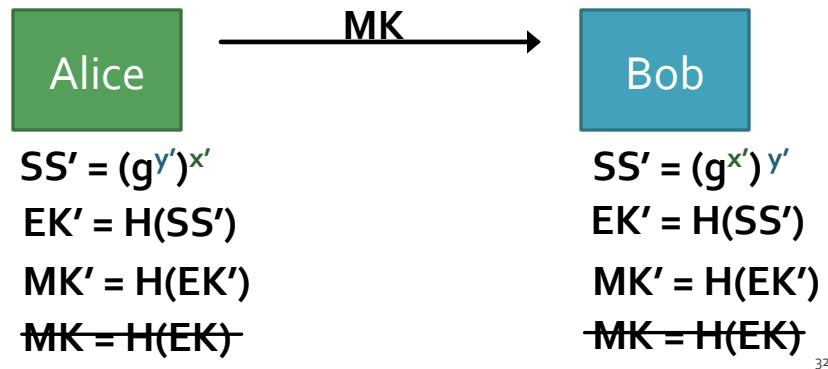
Off-the-Record

3. Re-key using Diffie-Hellman



Off-the-Record

4. Publish old MK



Off-the-record Messaging (OTR)

- Note this is suited to interactive communication, not so much email
- But, OTR provides
 - message confidentiality
 - authentication
 - perfect forward secrecy
 - deniability

33

Using OTR

- Built in to Adium and Pidgin
- But beware **defaults**
 - Logging enabled by default
 - Etiquette dictates you should disable this, so does history (e.g., Chelsea Manning)
- ☺ optional exercise: create an account on jabber.ccc.de, install OTR and verify a buddy.
You may also want to run it over [Tor](#).

34

Anonymity for browsing?

You

Server

35

Naive approach VPNs



36

VPNs



Home | Pro VPN | Web proxy | Proxy list |

HMA! Blog - News, updates, and all things privacy related.

Lulzsec fiasco
Posted on September 23, 2011

We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group 'lulzsec'. Lulzsec have been ALLEGEDLY been responsible for a number of high profile cases such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times.
- The hacking of 77 law enforcement sheriff websites.

It first came to our attention when leaked IRC chat logs were released, in these logs participants discussed about various VPN services they use, and it became apparent that some members were using our service. No action was taken after all there was no evidence to suspect wrongdoing and nothing to identify which accounts.

37

VPNs



Home | Pro VPN | Web proxy | Privacy Policy |

HMA! Blog - News, updates, and all things privacy related.

Lulzsec fiasco
Posted on September 23, 2011
We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group 'lulzsec'. Lulzsec have been ALLEGEDLY been responsible for a number of high profile cases such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times.
- The hacking of 77 law enforcement sheriff websites.

It first came to our attention when leaked IRC chat logs were released, in these logs participants discussed about various VPN services they use, and it became apparent that some members were using our service. No action was taken after all there was no evidence to suspect wrongdoing and nothing to identify which accounts.

"...received a **court order asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and **privacy policy** our service is not to be used for illegal activity, and as a legitimate company **we will cooperate with law enforcement if we receive a court order**"**

38

Better approach: Tor

- Low-latency anonymous communication system
- Hide **metadata**
 - who is communicating with whom?
 - e.g., just sending an encrypted message to The Intercept may get you in trouble
- Hide **existence** of communication
 - any encrypted message may get you in trouble

39

Tor overview

- Works at the transport layer
- Allows you to make TCP connections without revealing your IP address
- Popular for web connections
- Tor network made up of volunteer-run **nodes**, or **onion routers**, located all over the world

Basic idea: Alice wants to connect to a web server without revealing her IP address

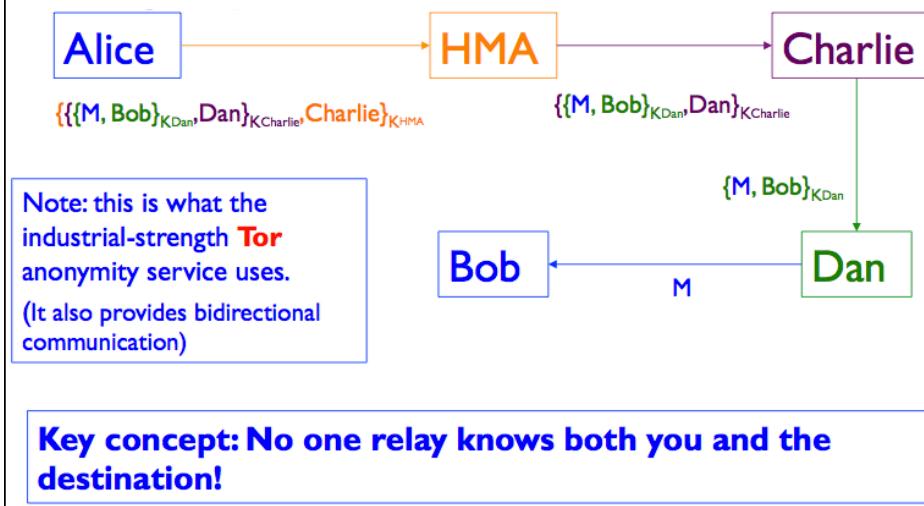
40

Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie
- **As long as any of the mixes is honest, no one can link Alice with Bob**

41

Onion Routing



Tor

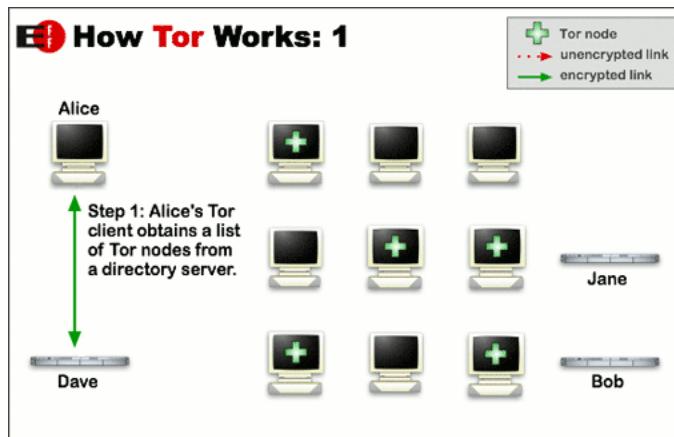


Image credit:
Tor Project

Tor

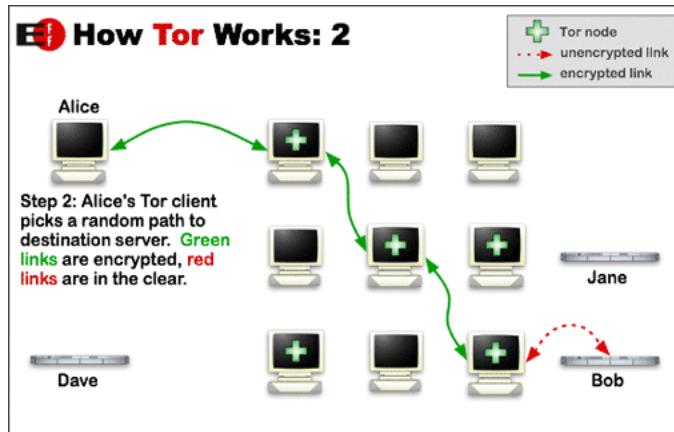


Image credit:
Tor Project

Tor

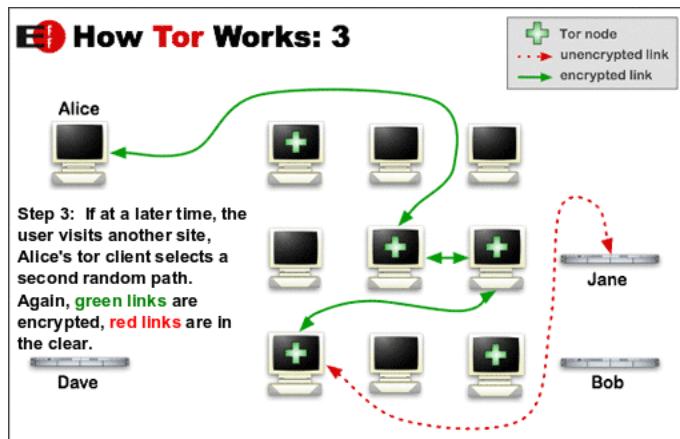


Image credit:
Tor Project

Trust in Tor

- Entry node: knows Alice is using Tor, and identity of middle node, but not destination
- Exit node: knows some Tor user is connecting to destination, but doesn't know which user
- Destination: knows a Tor user is connecting to it via the exit node

Important to note that Tor does not provide encryption between exit and destination! (e.g., use HTTPS)

46

How to get Tor

- Tor Browser bundle available (built on modified version of firefox)
- ☺ optional exercise: download and use it!
- <https://www.torproject.org/>
- ...or volunteer to be a part of the Tor network.

47

Egotistical Giraffe

- TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
- 
- (TS//SI//REL) Exploiting TOR
- 
- (TS//SI//REL) Can't distinguish OS until on box
 - That's okay
 - (TS//SI//REL) Can't distinguish Firefox version until on box
 - That's also okay
 - (TS//SI//REL) Can't distinguish 64-bit from 32-bit until on box
 - I think you see where this is going

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

48

Onion Routing Issues/Attacks?

- Performance: message bounces around a lot
- Attack: rubber-hose cryptanalysis of mix operators
 - Defense: use mix servers in different countries
- Attack: adversary operates all of the mixes
 - Defense: have lots of mix servers (Tor today: ~2,000)
- Attack: adversary observes when Alice sends and when Bob receives, links the two together
- A side channel attack – exploits timing information
 - Defenses: pad messages, introduce significant delays
 - Tor does the former, but notes that it's not enough for defense

49

Onion Routing Issues, cont.

- Issue: **traffic leakage**
- Suppose all of your HTTP/HTTPS traffic goes through Tor, but the rest of your traffic doesn't
- How might the operator of sensitive.com deanonymize your web session to their server?

50

The traffic leakage problem

- Answer: they inspect the logs of their DNS server to see who looked up sensitive.com just before your connection to their web server arrived
- Hard, general problem: anonymity often at risk when adversary can correlate separate sources of information

51

Tor Hidden Services: Overview

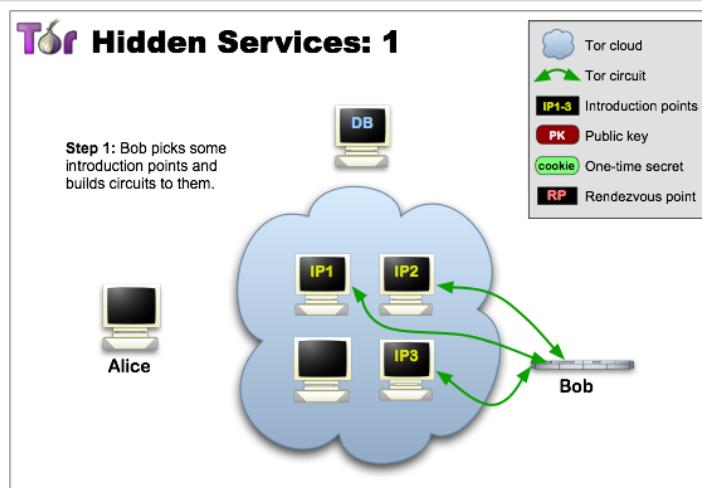


Image credit:
Tor Project

Tor Hidden Services

Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.

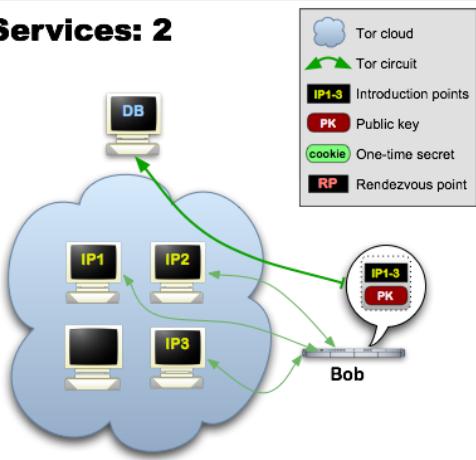


Image credit:
Tor Project

Tor Hidden Services

Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

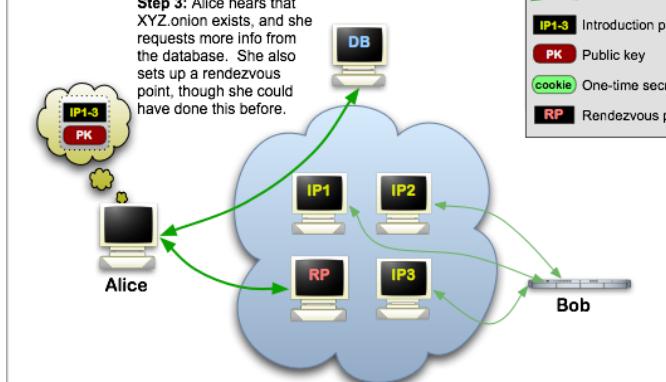


Image credit:
Tor Project

Tor Hidden Services

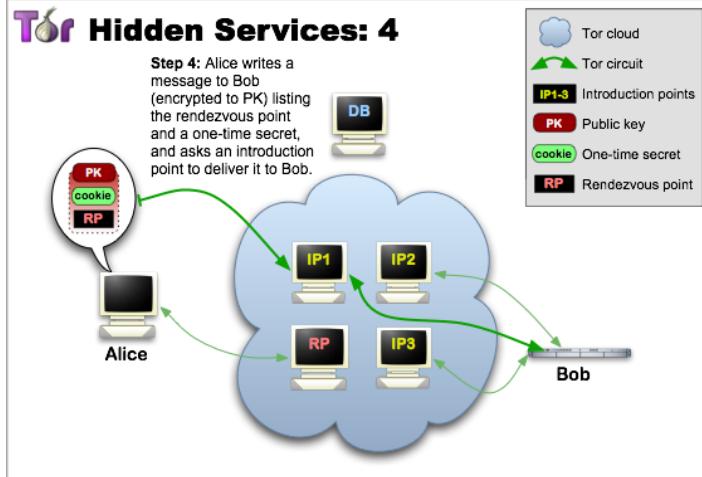


Image credit:
Tor Project

Tor Hidden Services

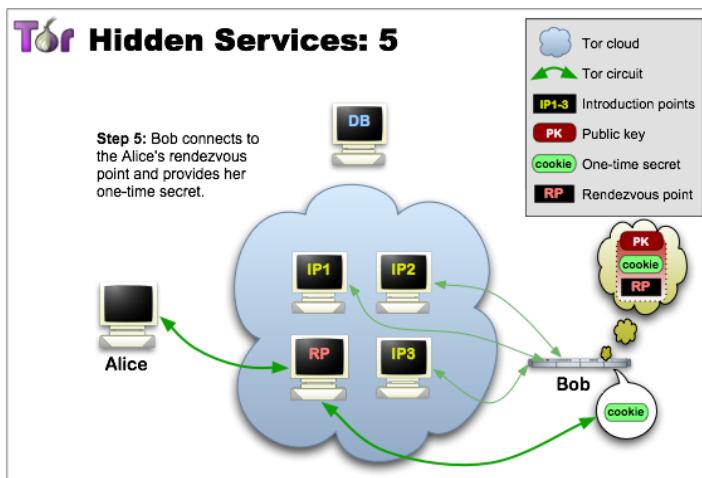


Image credit:
Tor Project

Tor Hidden Services

Tor Hidden Services: 6

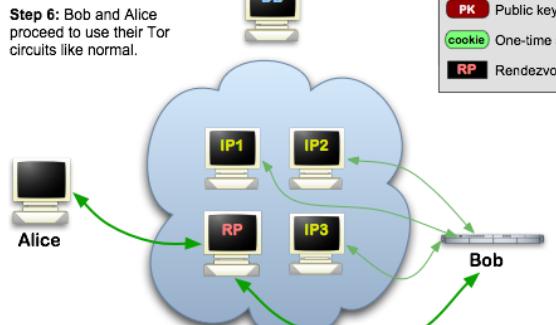


Image credit:
Tor Project

SilkRoad Marketplace



Welcome nowOpen!
messages(0) | orders(0) | account(\$0) | settings | log out
 search | (0)

Shop by category:

Drugs(752)
Cannabis(280)
Ecstasy(35)
Dissociatives(11)
Psychedelics(84)
Opioids(62)
Stimulants(53)
Other(107)
Benzos(70)
Lab Supplies(6)
Digital goods(98)
Services(48)
Money(55)
Weaponry(15)
Home & Garden(14)
Food(4)
Electronics(5)
Books(49)
Drug paraphernalia(28)
XXX(30)
Medical(3)
Computer equipment(4)
Apparel(4)
Musical instruments(2)
Tickets(1)
Forgeries(13)



News:

- Escrow hedging update
- New feature to help protect sellers
- We are hiring! Get paid for a referral, too...
- Reclaim lost coins from MyBitcoin.com
- Seller ranking and feedback overhaul
- Change your Mt. Gox password

recent feedback:

58

SilkRoad Marketplace

THIS HIDDEN SITE HAS BEEN SEIZED
by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



59

Metadata

- If
- When
- How much
- Who
- What

60

Metadata

- If
- When
- How much
- Who
- What ← TLS/PGP

61

Metadata

- If
- When
- How much
- Who ← 
- What ← TLS/PGP

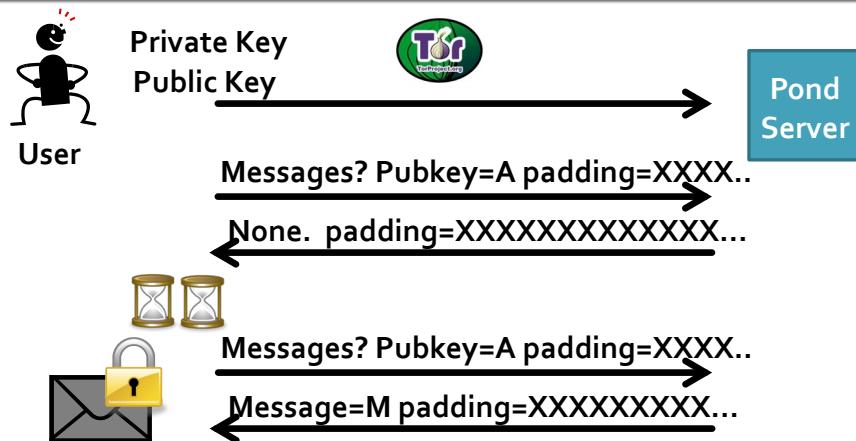
62

Pond

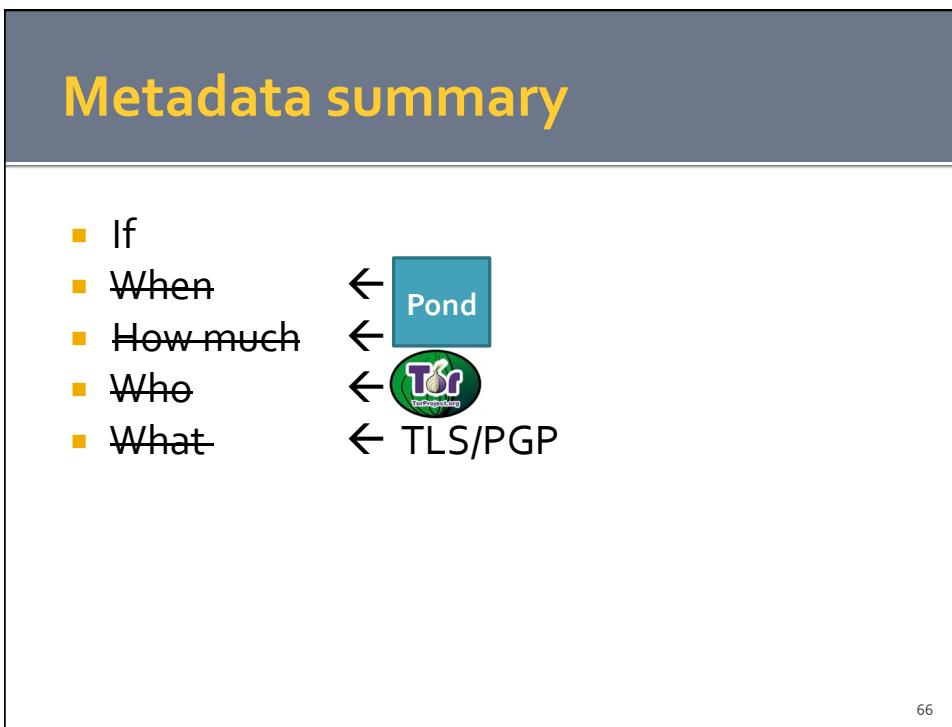
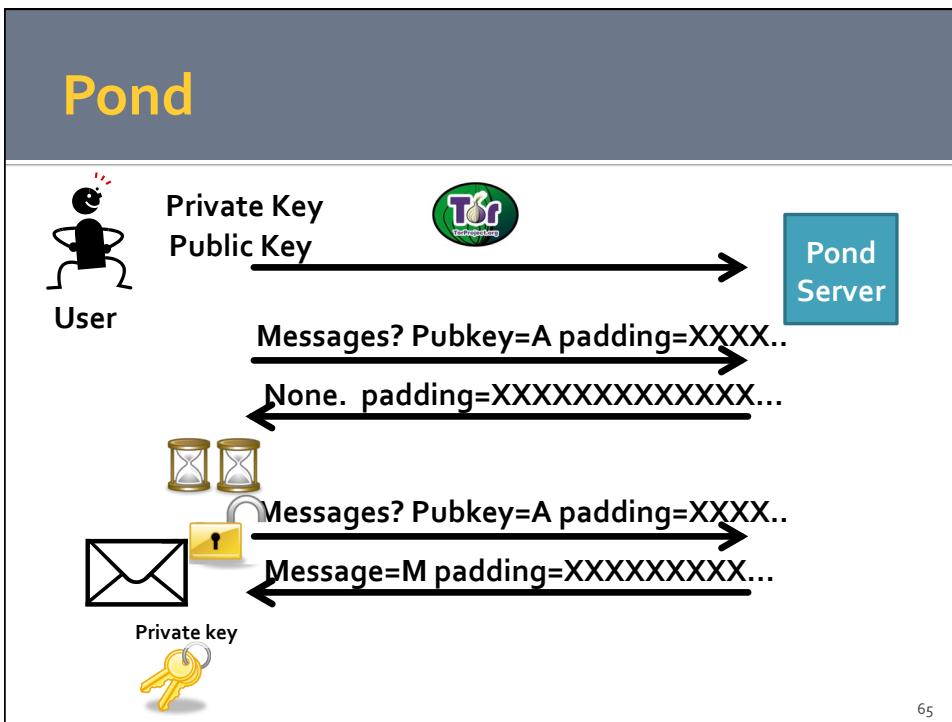
- "Pond is not email. Pond is a forward secure, asynchronous messaging system for the discerning"
- Seeks to protect against leaking traffic info against all but a global passive adversary
 - forward secure
 - no spam
 - messages expire automatically after a week

63

Pond



64



Extra...

Optional exercises. Play with the following:

- Tor Browser bundle
- GnuPG
- OTR on pidgin (or adium)
- Pond ...
 - highly recommend using the CLI for pond
 - make a contact over Pond using a human memorable secret, as in the PANDA protocol...

67

Other Tools

From WhisperSystems

<https://whispersystems.org/>)

For Android: RedPhone, TextSecure

For iOS: Signal

(compatible with RedPhone, a texting app is on the way)

68