Lecture 32 – Anonymity

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017

Security News

- DOJ once again advocating crypto backdoors
- “Hack the Pentagon” bug bounty and vulnerability disclosure program results in thousands of bug fixes
- Chrome disabling iframe redirects, opening new tabs with redirects, and masking links (e.g as play button or close ad)

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 the same as secrecy/confidentiality
  - Confidentiality is about message contents,
    - (what was said)

    Anonymity is about identities
    - (who said it and to whom)

Understanding Anonymity

- "without a name"

- Who wants anonymity?

- Threats to anonymity?

- How to get anonymity?

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

How to get Anonymity

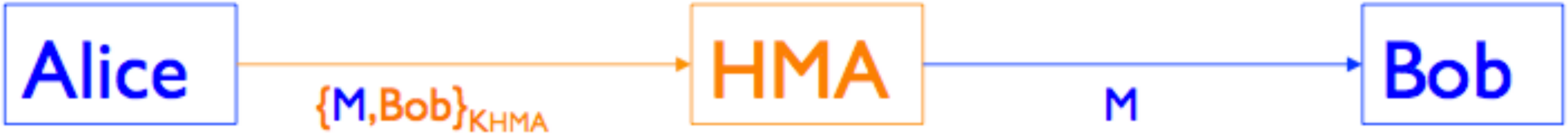
- Internet anonymity is hard*
  - Difficult if not impossible to achieve on your own
  - Right there in every packet is the source and destination IP address
  - * But it’s easy for bad guys. Why?
- How do we do it?
- State of the art technique: Ask someone else to send it for you
  - Ok, it’s a bit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

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.

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.

Metadata

Everything except the contents of your communications.

- If
- When
- How much
- Who
- What (this is actually the data)

“... analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content.” - Prof. Edward W. Felten, Computer Science and Public Affairs, Princeton; Chief Technologist of FTC

Encryption Tools: PGP

- GnuPG, free software
  - Pretty Good Privacy (PGP), Phil Zimmerman ('91)
  - GnuPG (GPG) is a free software recreation
  - 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?

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

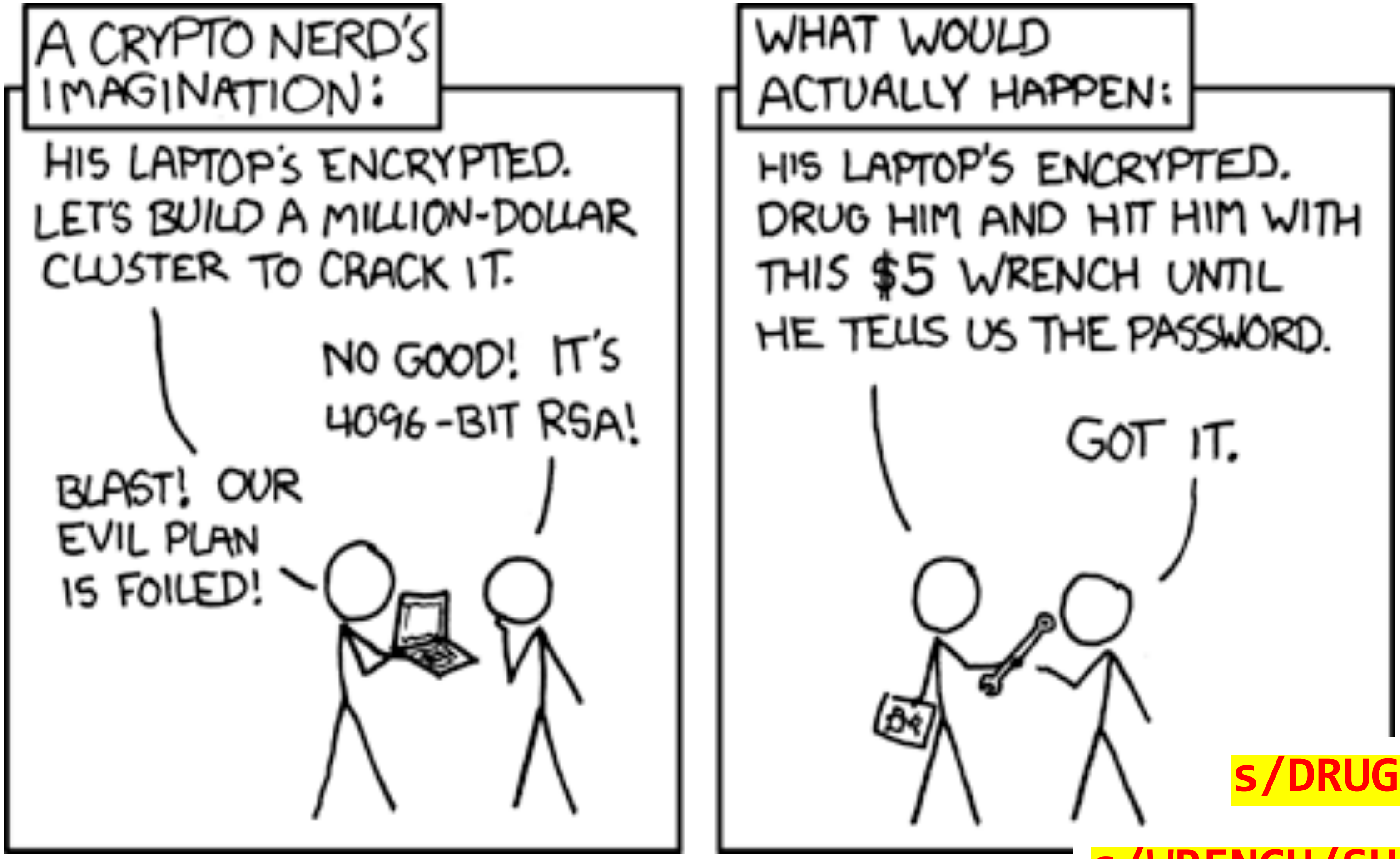
Fingerprints

- 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
  - Key servers: store public keys, look up by name/email address, verify with fingerprint
- What if you don't personally know Bob?
  - Web of Trust (WoT), “friend of a friend”
  - Bob introduces Alice to Caro by signing Alice’s key

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
- The software created lots of incriminating records
  - Key material that decrypts data sent over the public Internet
  - Signatures with proofs of who said what
- Alice better watch what she says
  - Her privacy depends on Bob’s actions

Drawbacks of (Just) Encryption II


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

s/DRUG/JAIL

s/WRENCH/SUBPOENA

Casual Conversations

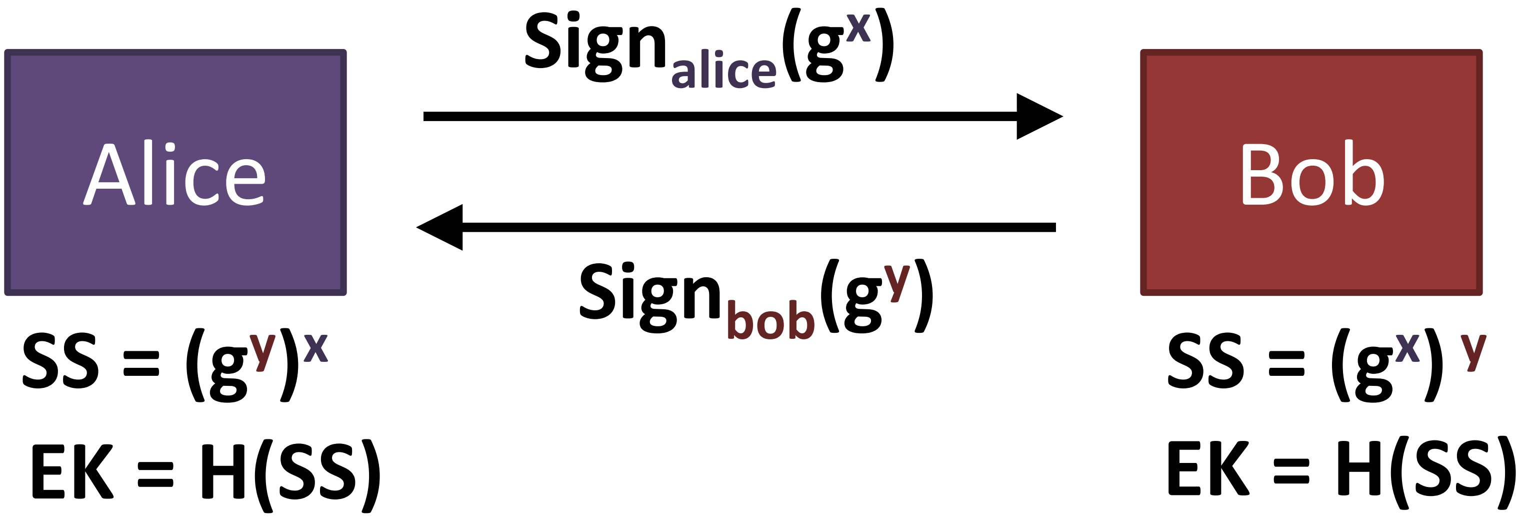
- Alice and Bob talk in a room
- No one else can hear
  - Unless being recorded
- No one else knows what they say
  - Unless Alice or Bob tell them
- No one can prove what was said
  - Not even Alice or Bob
- These conversations are “off-the-record”

Desirable communication properties

- Forward secrecy:
  - Even if your key material is compromised, past messages should be safe
- Deniability: be able to *plausibly* 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

Off-the-Record (OTR) Messaging

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



$\mathbf{Sign_{alice}(g^x)}$

Alice

Bob

$\mathbf{Sign_{bob}(g^y)}$

$\mathbf{SS = (g^y)^x}$

$\mathbf{EK = H(SS)}$

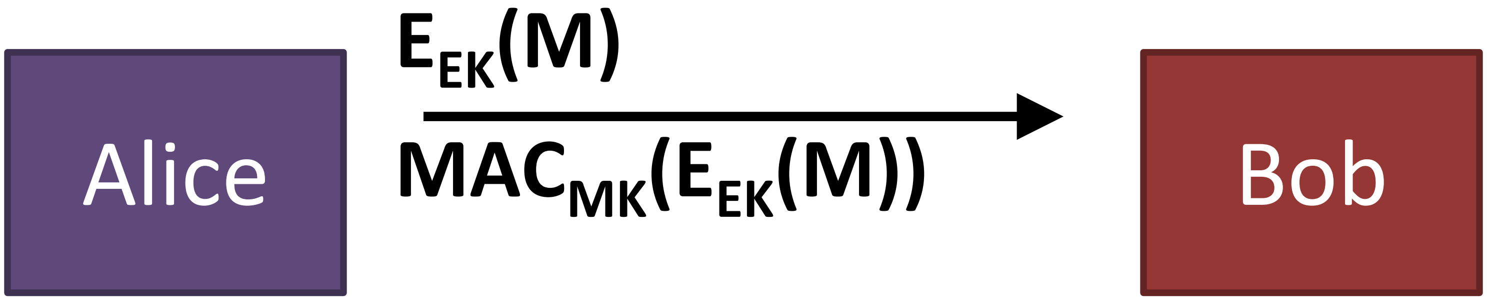
$\mathbf{SS = (g^x)^y}$

$\mathbf{EK = H(SS)}$

Off-the-Record (OTR) Messaging

2. Then use secret-key encryption on message M

... And authenticate using a MAC



Alice

$\mathbf{E_{EK}(M)}$

$\mathbf{MAC_{MK}(E_{EK}(M))}$

Bob

$SS = (g^y)^x$

$EK = H(SS)$

$\mathbf{MK = H(EK)}$

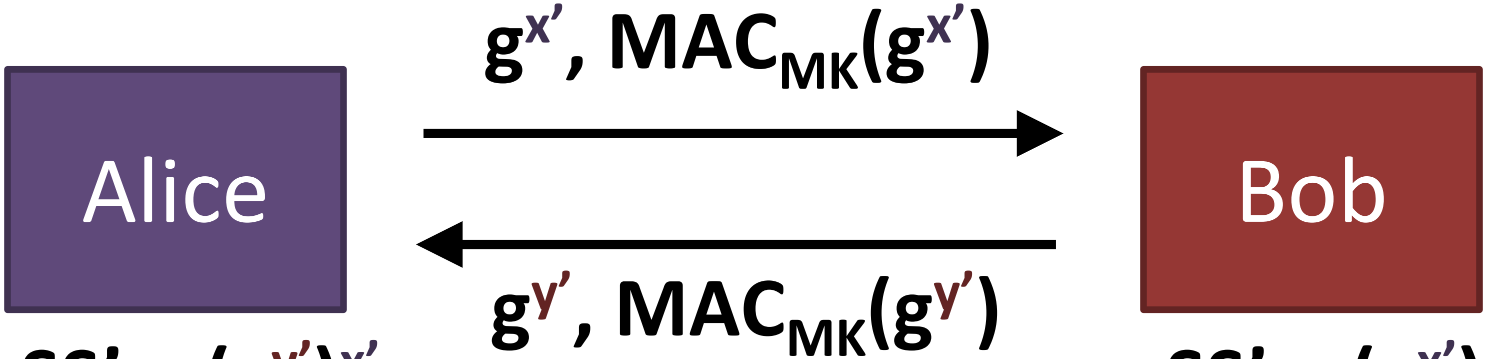
$SS = (g^x)^y$

$EK = H(SS)$

$\mathbf{MK = H(EK)}$

Off-the-Record (OTR) Messaging

3. Re-key using Diffie-Hellman


$g^{x'}, \mathrm{MAC}_{MK}(g^{x'})$
Alice
Bob
$g^{y'}, \mathrm{MAC}_{MK}(g^{y'})$

$SS' = (g^{y'})^{x'}$

$EK' = H(SS')$

$MK' = H(EK')$

$MK = H(EK)$

$SS' = (g^{x'})^{y'}$

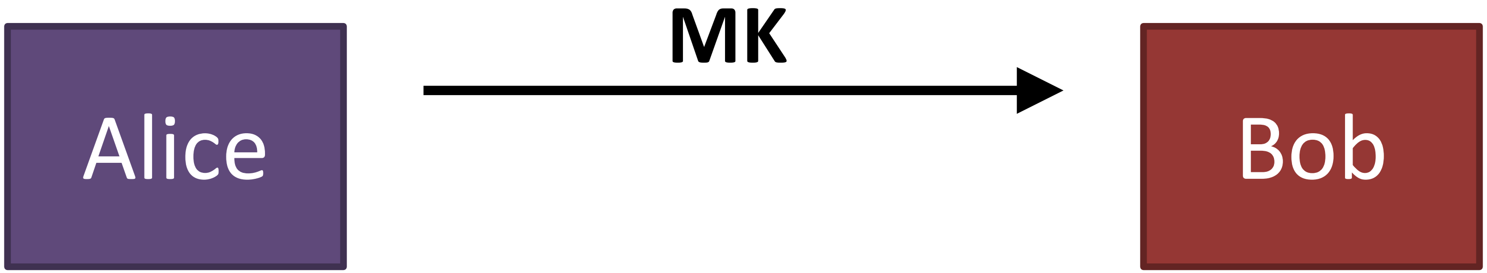
$EK' = H(SS')$

$MK' = H(EK')$

$MK = H(EK)$

Off-the-Record (OTR) Messaging

4. Publish old MK



$SS' = (g^{y'})^{x'}$

EK' = H(SS')

MK' = H(EK')

~~MK = H(EK)~~

$SS' = (g^{x'})^{y'}$

EK' = H(SS')

MK' = H(EK')

~~MK = H(EK)~~

Off-the-Record (OTR) Messaging

- Note this is suited to interactive communication, not so much email
- But, OTR provides
  - message confidentiality
  - authentication
  - perfect forward secrecy
  - Deniability
    - Caveat: we do not have examples of “deniability” serving its purpose in practice

Signal and the "Double Ratchet"

The protocol behind Signal app (iphone,android)

Trevor Perrin and Moxie Marlinspike

- Forward secrecy

Today's messages are secret, even if key compromised tomorrow

- Future secrecy

Tomorrow's messages are secret, even if key compromised today

- Deniability

No permanent/transferable evidence of what was said

- Usability Tolerates out-of-order message delivery

https://whispersystems.org/docs/specifications/doubleratchet/

Plausibly Deniable Storage

Goal: Encrypt data stored on your hard drive

Problem: Can be compelled to decrypt it!

Idea: have a “decoy” volume with benign information on it

Example: VeraCrypt

[Does this solve the problem? Caveats?]

Recap Privacy/Anonymity

Metadata: Everything except the contents of your communications.

- If
- When
- How much
- Who

- What (this is actually the data)

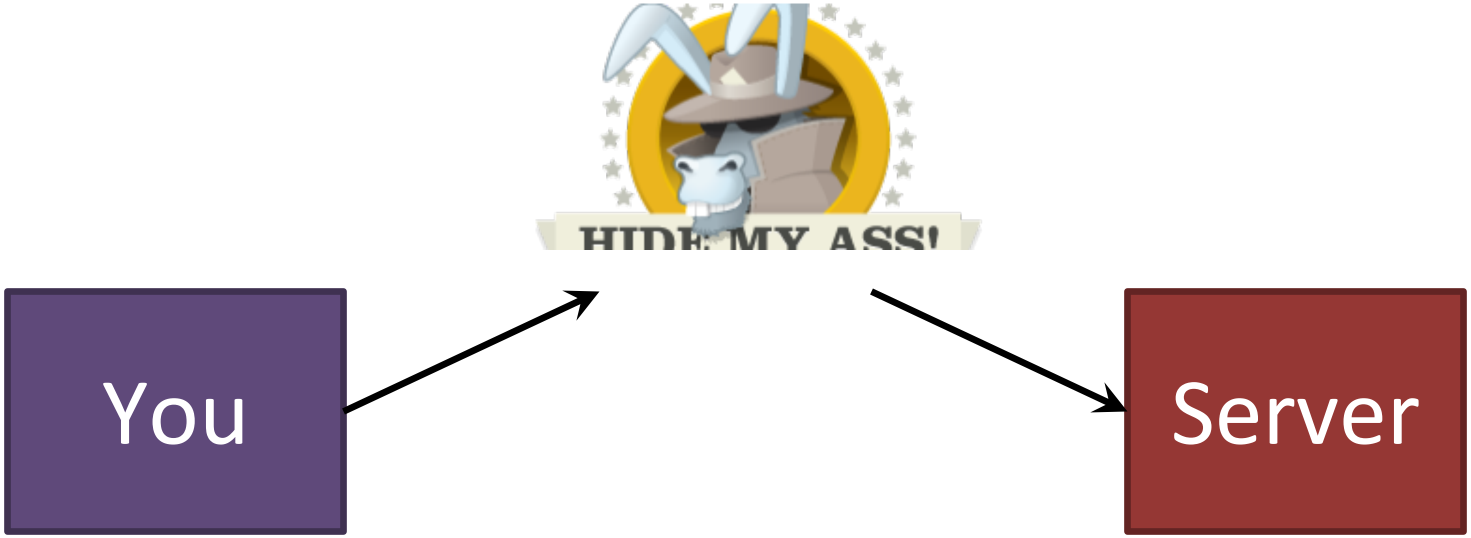
Signal and OTR

Anonymity for browsing?

You

Server

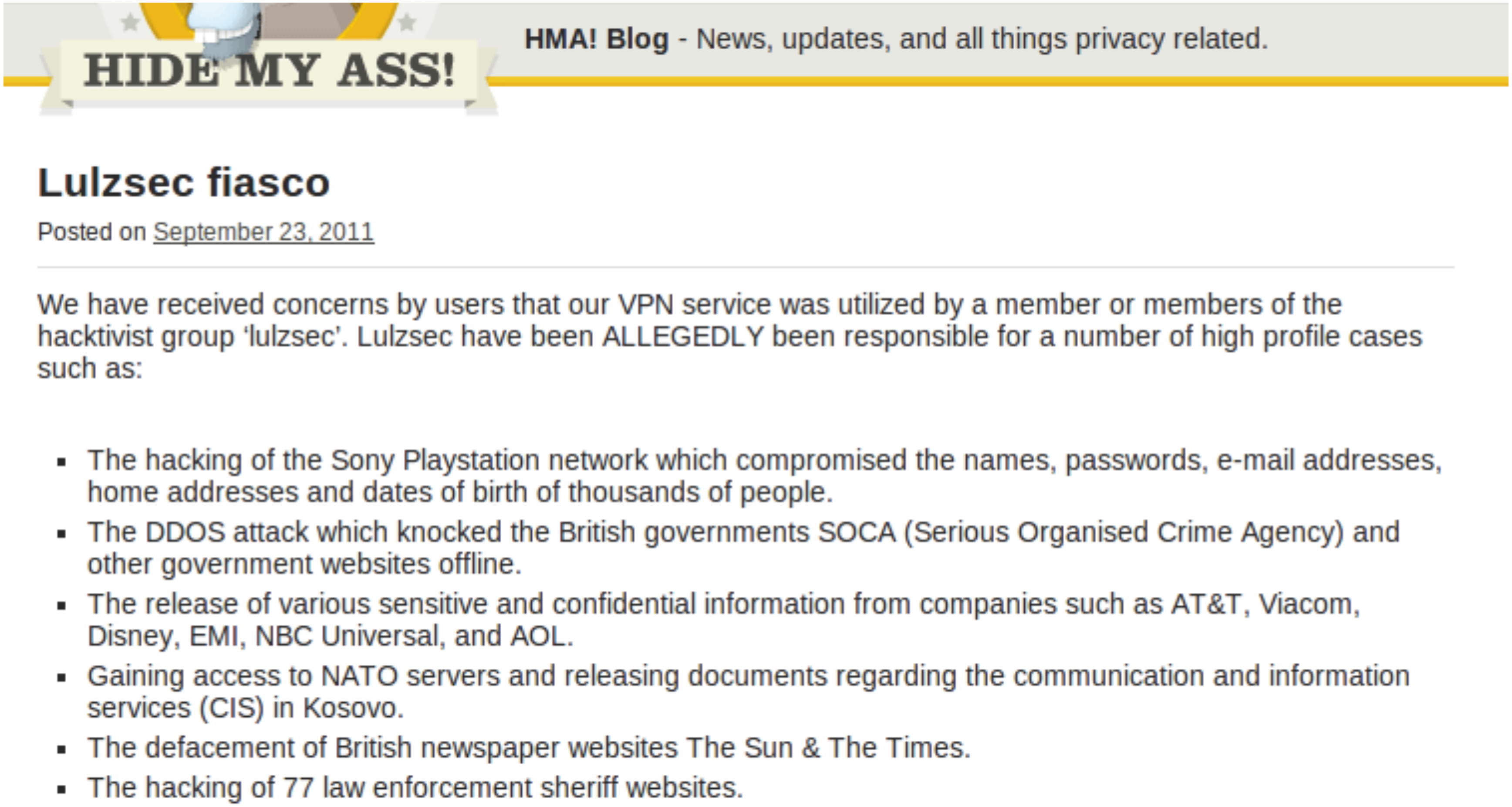
Naive approach .... VPNs



You

Server

VPNs



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

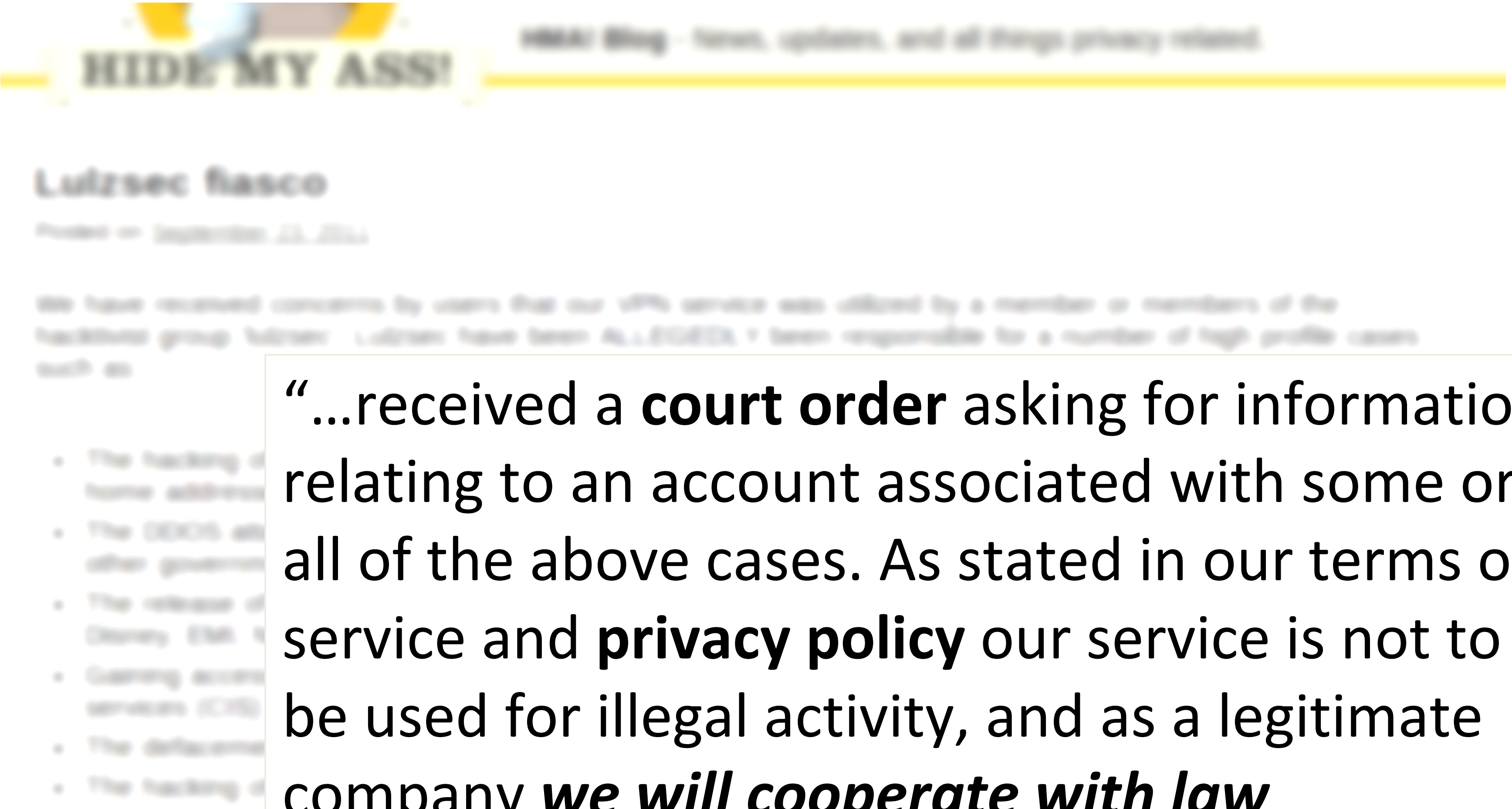
Lulzsec fiasco

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.

VPNs



HIDE MY ASS!

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:

"…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***"

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

Tor overview

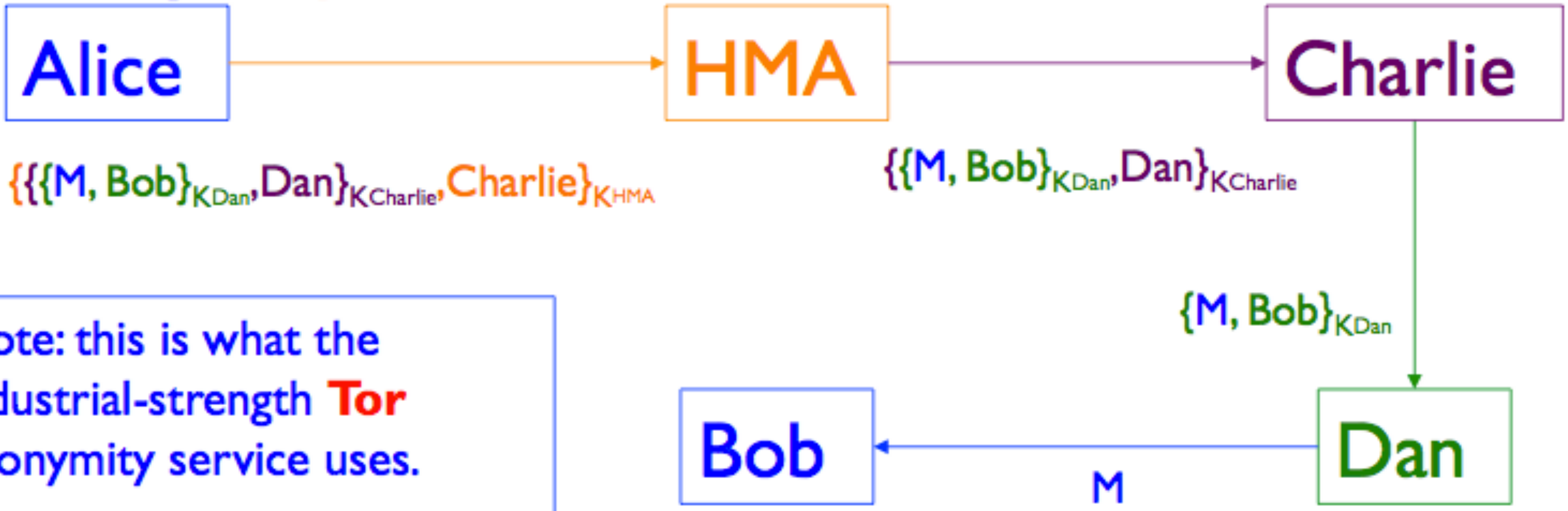
- Works at the transport layer
- Allows you to make TCP connections without revealing your IP address
- Popular for web connections
- Tor network made up of volunteer-run nodes, or onion routers, located all over the world

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

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

Onion Routing


Alice
HMA
Charlie
Dan
Bob
$\{\{\{M, Bob\}_{KDan}, Dan\}_{KCharlie}, Charlie\}_{KHMA}$
$\{\{M, Bob\}_{KDan}, Dan\}_{KCharlie}$
$\{M, Bob\}_{KDan}$
M

Note: this is what the industrial-strength Tor anonymity service uses.

(It also provides bidirectional communication)

Key concept: No one relay knows both you and the destination!

Tor

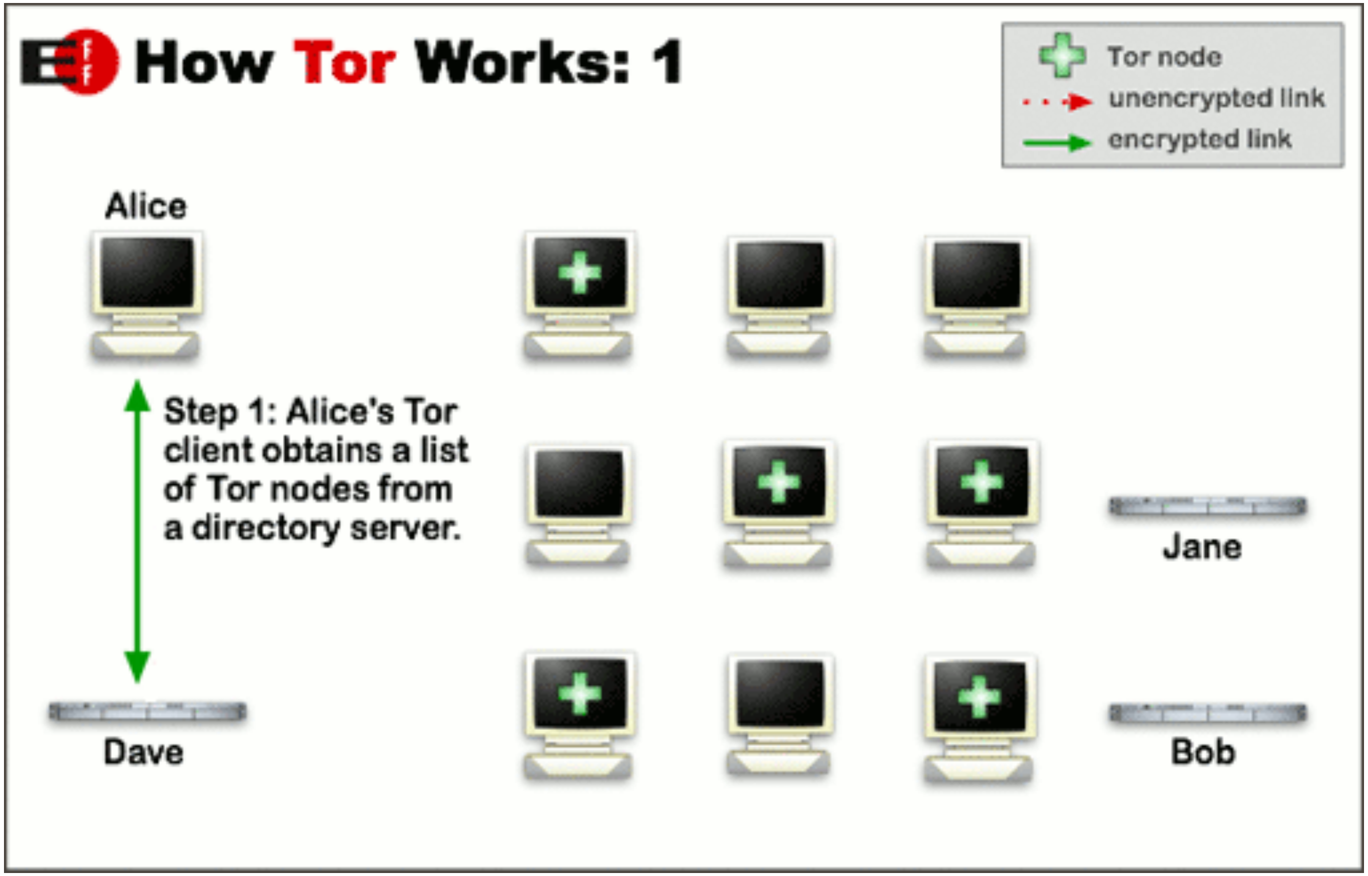
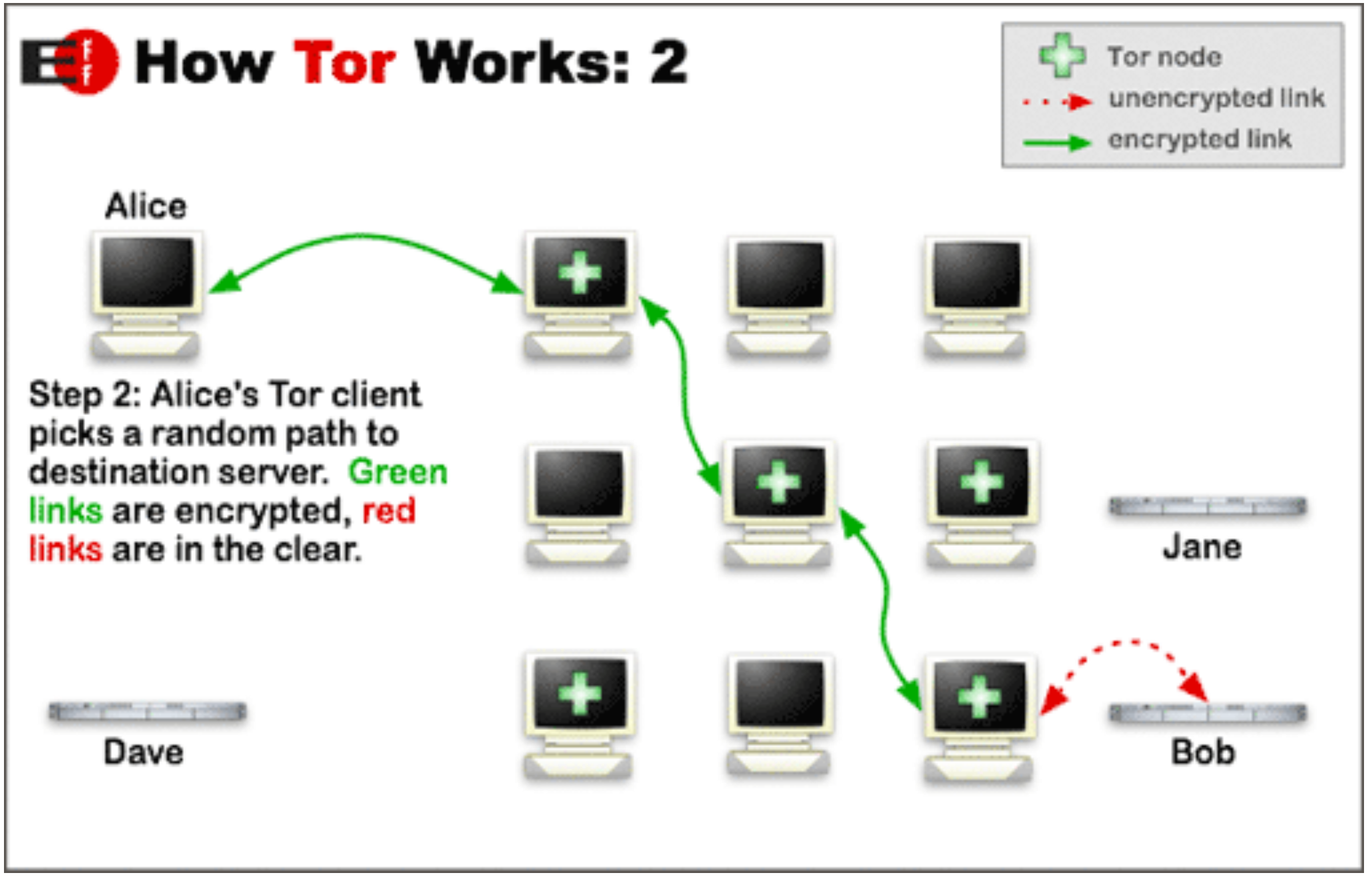

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

Image credit:
Tor Project

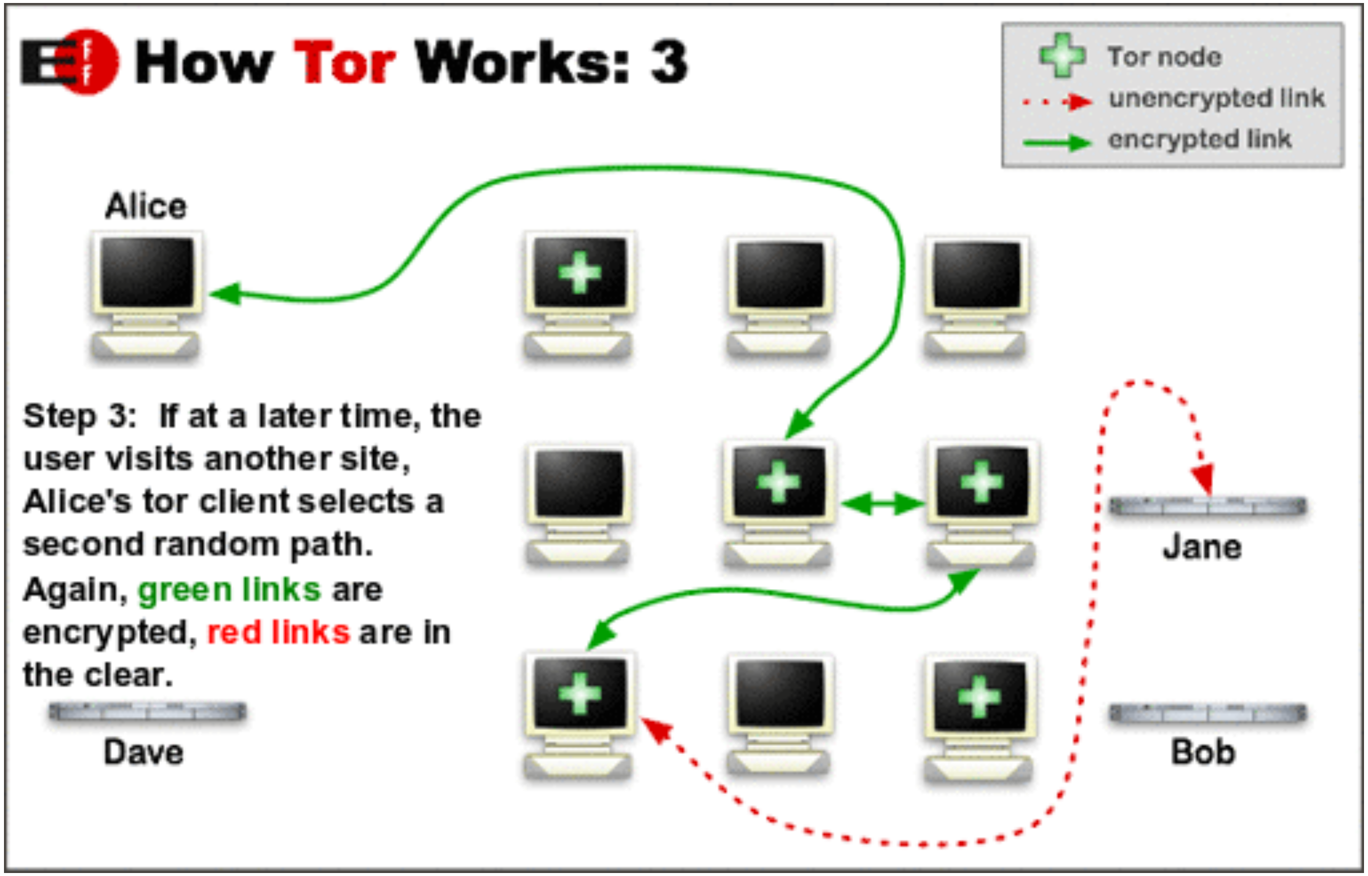
Tor



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

Image credit:
Tor Project

Tor



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

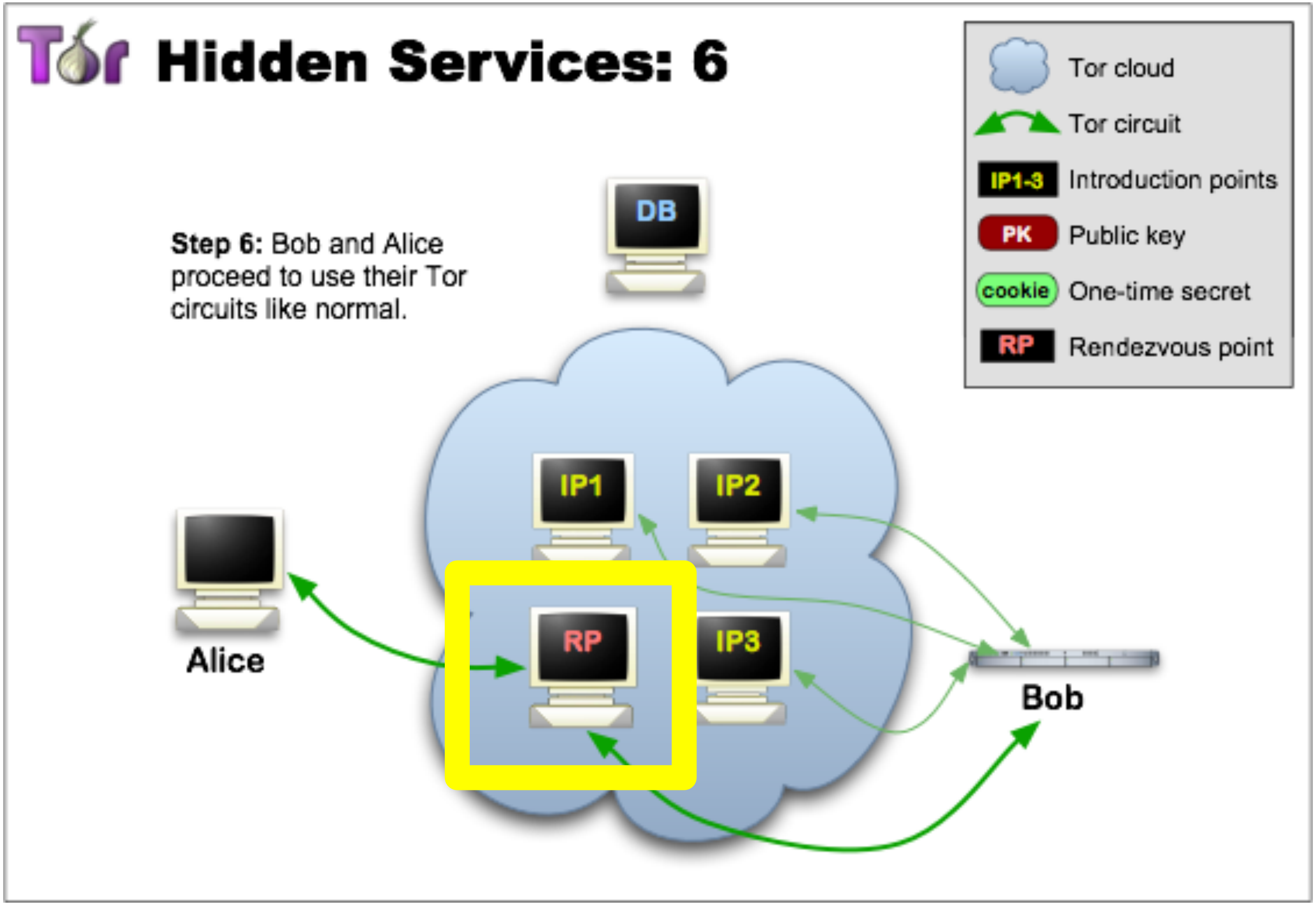
Image credit:
Tor Project

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)

Tor Hidden Services



Step 6: Bob and Alice proceed to use their Tor circuits like normal.

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.

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: ~6,500)
- 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

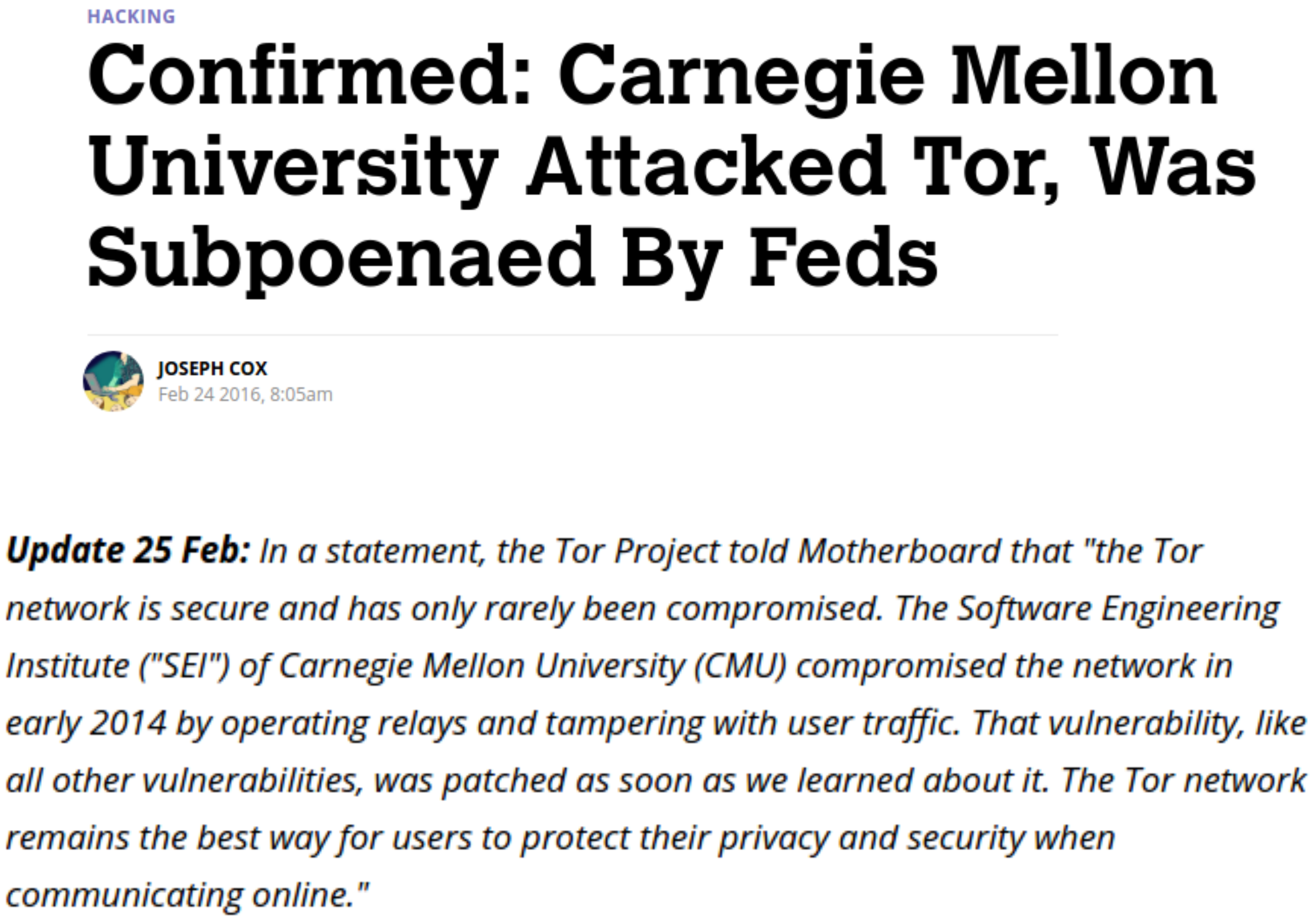
https://metrics.torproject.org/networksize.html

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?

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



HACKING

Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds

JOSEPH COX
Feb 24 2016, 8:05am

***Update 25 Feb:** In a statement, the Tor Project told Motherboard that "the Tor network is secure and has only rarely been compromised. The Software Engineering Institute ("SEI") of Carnegie Mellon University (CMU) compromised the network in early 2014 by operating relays and tampering with user traffic. That vulnerability, like all other vulnerabilities, was patched as soon as we learned about it. The Tor network remains the best way for users to protect their privacy and security when communicating online."*

Metadata

- If
- When
- How much
- Who
- What

Metadata

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

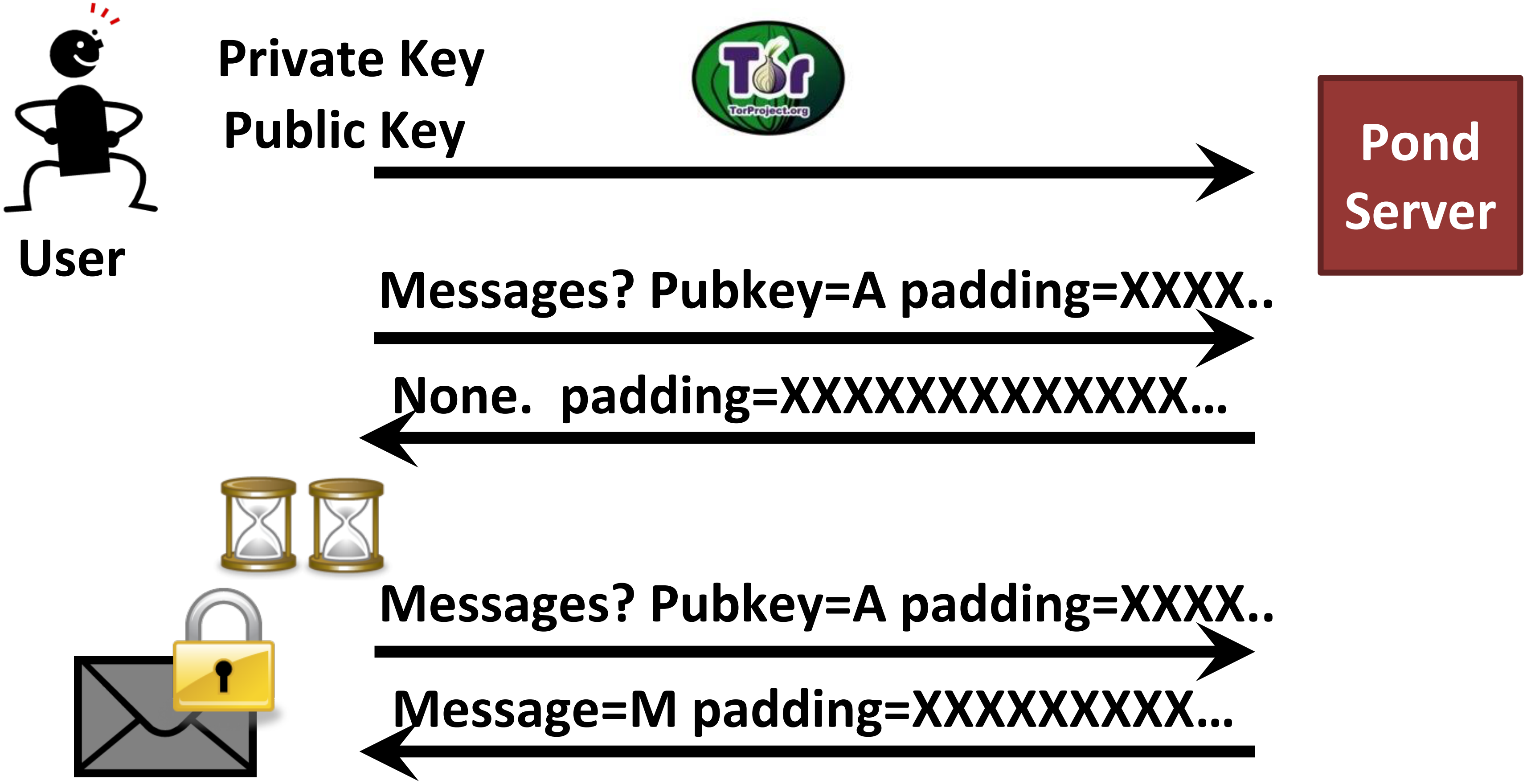
Metadata

- If
- When
- How much
- Who ← Tor TorProject.org
- What ← TLS/PGP/OTR/Signal

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

Pond



User

Private Key

Public Key

Pond Server

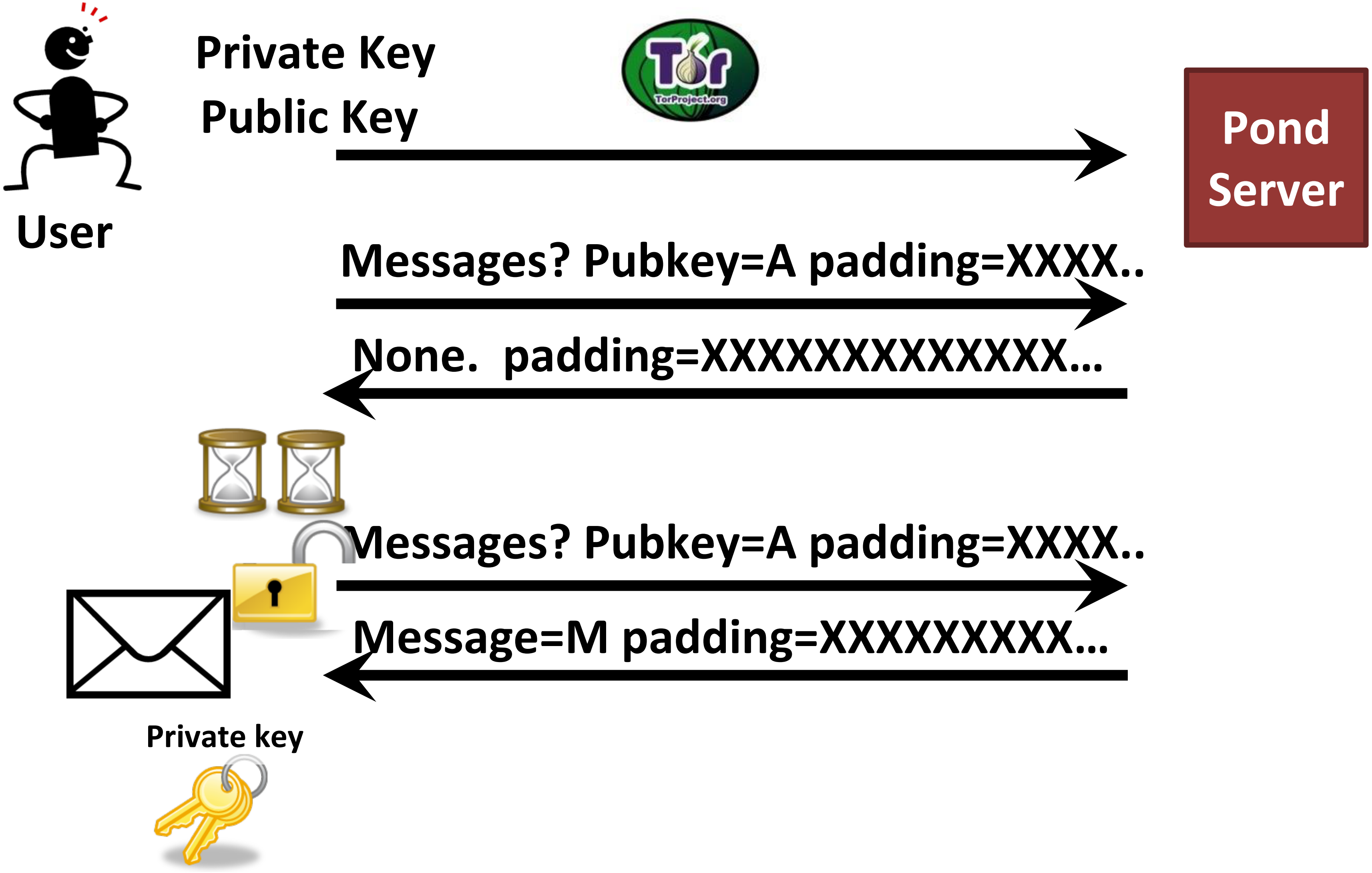
Messages? Pubkey=A padding=XXXX..

None. padding=XXXXXXXXXXXXXX…

Messages? Pubkey=A padding=XXXX..

Message=M padding=XXXXXXXXXX…

Pond



User

Private Key

Public Key

Pond Server

Messages? Pubkey=A padding=XXXX..

None. padding=XXXXXXXXXXXXXX…

Messages? Pubkey=A padding=XXXX..

Message=M padding=XXXXXXXXXX…

Private key

Metadata summary

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

“Anonymity loves company”

https://www.freehaven.net/doc/wupss04/usability.pdf

- Better anonymity in a system with a large number of users
- May need to trade off some strength of security in order to have a more usable system ⇒ more users!

  What are the ideal tradeoff point?
- Using privacy-enhancing tools provides better privacy for others.
- Practice now helps if/when you need it later!

Extra...

Optional exercises. Play with the following:

- Tor Browser bundle
- Signal
- 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...