Lecture 30: Honeypots, Privacy

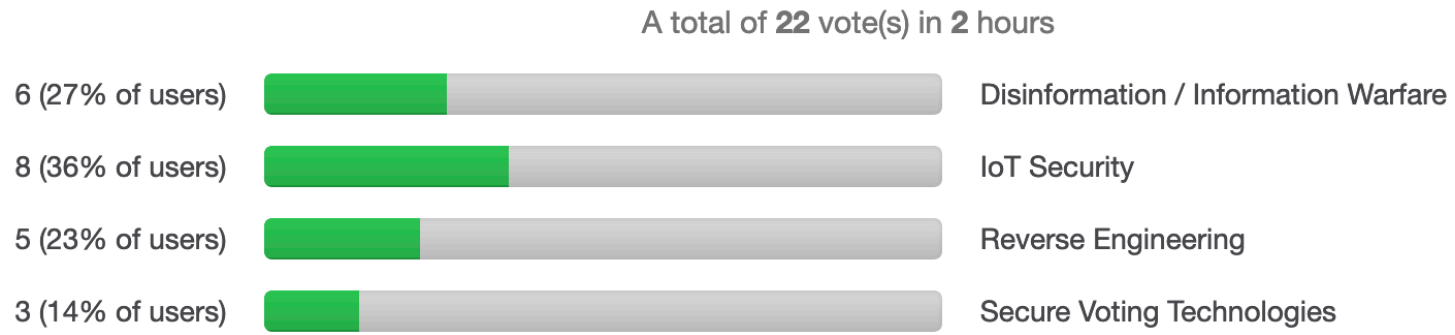
Professor Adam Bates
CS 461 / ECE 422
Fall 2019

Goals for Today

- Learning Objectives:
  - Conclude discussion of network security
  - Explore considerations for anonymity online
- Announcements, etc:
  - Final Exam *is* on Dec 13 at 7pm
  - Networking CP2: Due Nov 11
  - *MP5 Checkpoint 1 is released! Due November 18*
  - **Discussion section for MP5 today!**

Reminder: Please put away devices at the start of class

you picked 'em



1. IoT Security (experts: Deepak, Pubali)
2. Disinformation (experts: Prof. Carl Gunter)
3. Reverse Engineering

Due to travel conflicts, lectures will be interspersed throughout remainder of semester.

Using a NIDS

- Plan your incident response process well before you install the system
- Know what you're looking for
- Make the system comprehensive
- Don't overreact to alarms
- If using a rules-based system, keep up with vulnerability reports

Honeypots

Characterizing threats

- The goal is to provide timely forensic information on new Internet threats such as denial of service attacks and worms
- Why?
  - Detection
  - Signature generation
  - Mitigation or Quarantine
  - Clean-up
  - Forensics

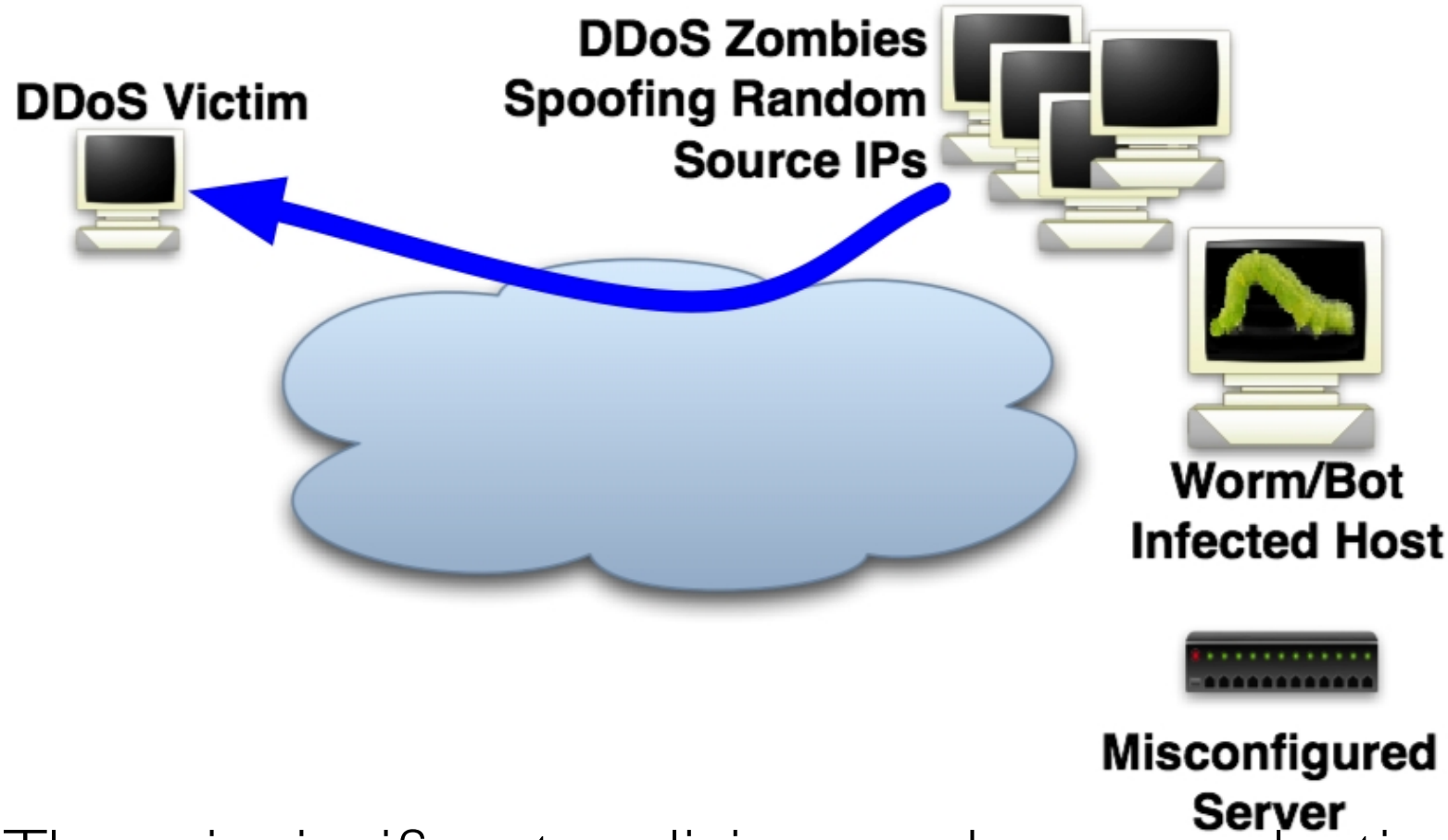
Current Network Security Solutions

- Host and Network-based Detection and Prevention
  - Operate on *production* host and network activity
  - Prevent attacks: e.g., firewalls
  - Detect attacks: e.g., signature-based IDS or anomaly detection system [Kim04, Singh03, Roesch99]
- Honeypots
  - Operate on *non-productive* hosts and networks.
  - Detect attacks: e.g. honeyd [Provos04]

Unused IP address threat detection

- Organizations do not typically use all of their allocated address space, leaving blocks of unused addresses within a network
- A unused sensor monitors an unused globally advertised address block that contains ***no active hosts***
- Many threats don't know where potential targets are, and therefore scan to find new targets. These scans are visible to the unused sensor.
  - This approach will miss anything that does not scan (e.g. email worms)

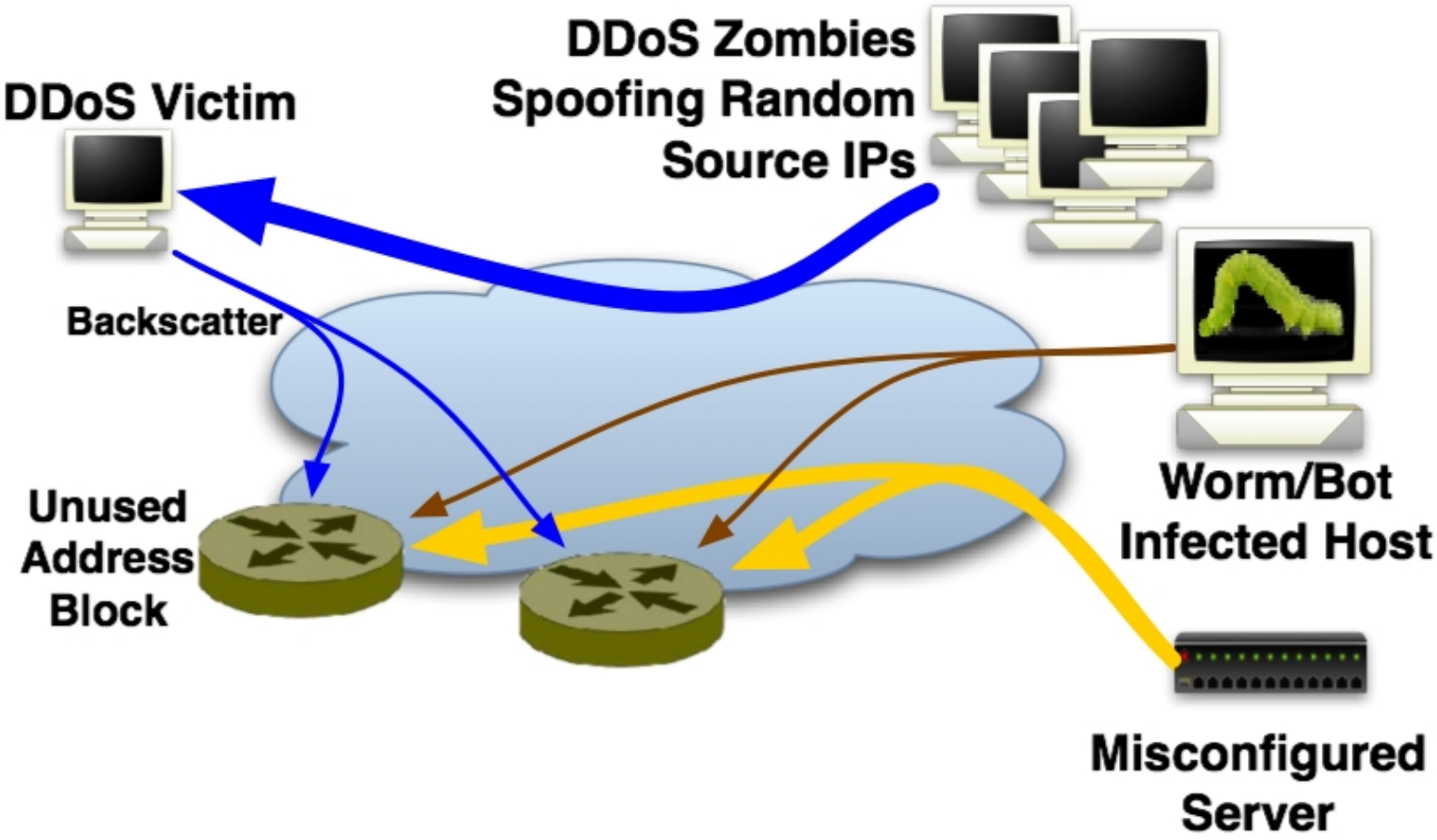
IMS Honeypot



- There is significant malicious and non-productive activity on the Internet today (e.g. DoS, worms, botnets, misconfiguration)

[Bailey et al., NDSS'05]

IMS Honeypot



- Much of this non-productive traffic is observed by unused addresses

[Bailey et al., NDSS'05]

Breadth, depth, and cost

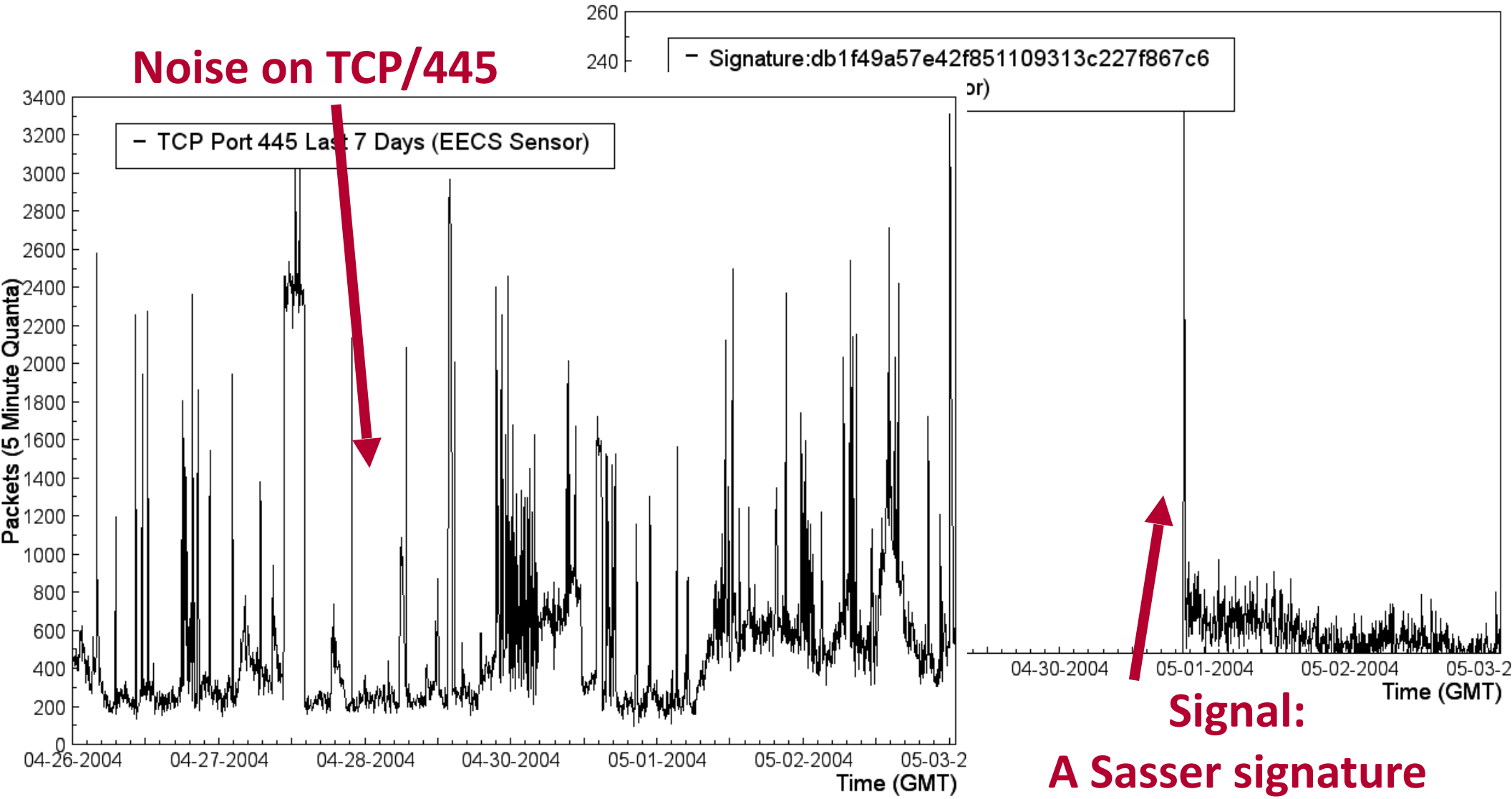
- Monitoring of unused address space defines a technique, but not a metric of utility.
- We define the utility of a threat monitoring system to be its
  - **Breadth**. This describes the scope of the monitoring system and defines its ability to quickly detect events
  - **Depth**. This describes the ability of the system to provide detailed forensic information on threats
  - **Cost**. This describes the scaling, deployment, and maintenance costs of the monitoring system

What is breadth?

Number Addresses Monitored	Scanning Rate (pps) 10	50	4,000	25,000
1	4971 days	994 days	12 days	2 days
256	466.0 hrs	93.2 hrs	1.2 hrs	0.2 hrs
65536	109.2 min	21.8 min	0.3 min	0.0 min
16777216	25.6 sec	5.1 sec	0.1 sec	0.0 sec

- Expected time to observe one or more packets from a single host scanning uniformly
- The difference in expected time to measure a CodeRedII host … 25.6 seconds verses 13.6 years
- ***Breadth defines the time to detection!***

What is depth?



Depth enables us to differentiate threats!

Understanding breadth

Measurement Class	Example Project	Breadth	Depth	
			Minimum Interaction	Example Threat
Passive	UCSD Network Telescope	/8-/5 ~16 million hosts	Capture connection attempt	Slammer, Witty
Transport	IMS	/16-/8	Response on 1 or more ports	Blaster
Virtual	Honeyd	/16-/12	Application response	Slapper
VM	Honeystat Potemkin	/21-/19	Virtualized end host behavior	Doomjuice, Dabber
Live Host	Honeynet Deepsight	/29-/26 ~64 Hosts	End host behavior	Agobot

"Future" Defenses

S-BGP Design Overview

- IPsec: secure point-to-point router communication
- Public Key Infrastructure: authorization for all S-BGP entities
- Attestations: digitally-signed authorizations
  - Address: authorization to advertise specified address blocks
  - Route: Validation of UPDATEs based on a new path attribute, using PKI certificates and attestations
- Repositories for distribution of certificates, CRLs, and address attestations
- Tools for ISPs to manage address attestations, process certificates & CRLs, etc.

Slide: Steve Kent

DNSSEC

- Basically no change to packet format
  - Goal is security of DNS data, not channel security
- New Resource Records (RRs)
  - RRSIG : signature of RR by private zone key
  - DNSKEY : public zone key
  - DS : crypto digest of child zone key
  - NSEC / NSEC3 authenticated denial of existence
- Lookup referral chain (unsigned)
- Origin attestation chain (PKI) (signed)
  - Start at pre-configured trust anchors
    - DS/DNSKEY of zone (should include root)
  - DS → DNSKEY → DS forms a link

Other

- IPv6
- SDN (We covered this! :D)

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)

Why do we need anonymity?

- Necessary to ensure civil liberties:
  - Free speech, free association, autonomy, freedom from censorship and constant surveillance
- Privacy is a human right
  - Dignity
  - Not explicit in US constitution, but relevant to 1st 4th 5th 9th amendments in bill of rights
- Surveillance is exploited for profit
  - Targeted marketing campaigns
  - Discrimination (insurance, employment)

Why do we need anonymity?

- Occasionally, anonymity is a legally-guaranteed right to ensure government transparency and accountability:

Arguments against Privacy?

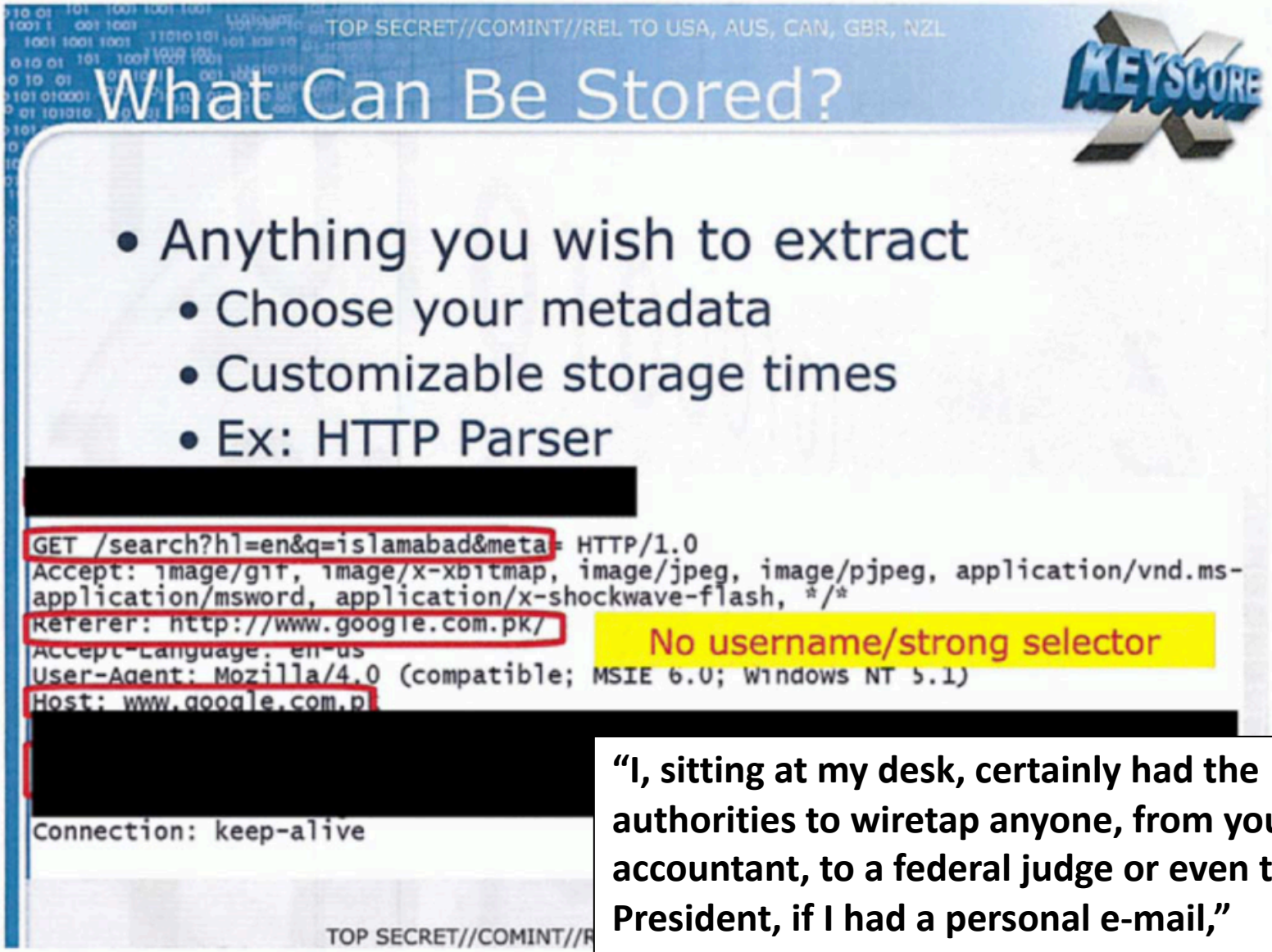
- The "Nothing to Hide" Argument
  - Dangers of constructing a Kafkaesque world
  - Optional reading: 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, Daniel J. Solove
  - Typically spoken from a view of privilege
- No one expects privacy anymore anyway
  - Kids today share their entire lives on Facebook
- Benefits from sharing (better search results?)
- Private communications abused by bad guys

N.S.A. Collection of Bulk Call Data Is Ruled Illegal

By **CHARLIE SAVAGE** and **JONATHAN WEISMAN** MAY 7, 2015

In a 97-page ruling, a three-judge panel for the United States Court of Appeals for the Second Circuit held that a provision of the U.S.A. Patriot Act, known as Section 215, cannot be legitimately interpreted to allow the bulk collection of domestic calling records.

XKEYSCORE



"I, sitting at my desk, certainly had the authorities to wiretap anyone, from you or your accountant, to a federal judge or even the President, if I had a personal e-mail,"

Technology as a defense

- Policy is not enough to protect abuse
- What technology is available to ensure our privacy?

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)

Metadata: A Caution

"... 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

- i.e., protecting the 'what' alone isn't enough
- Often, the metadata tells the whole story
- Charges, convictions, government watchlists, state assassinations, often based exclusively on metadata.

Encryption Tools: PGP

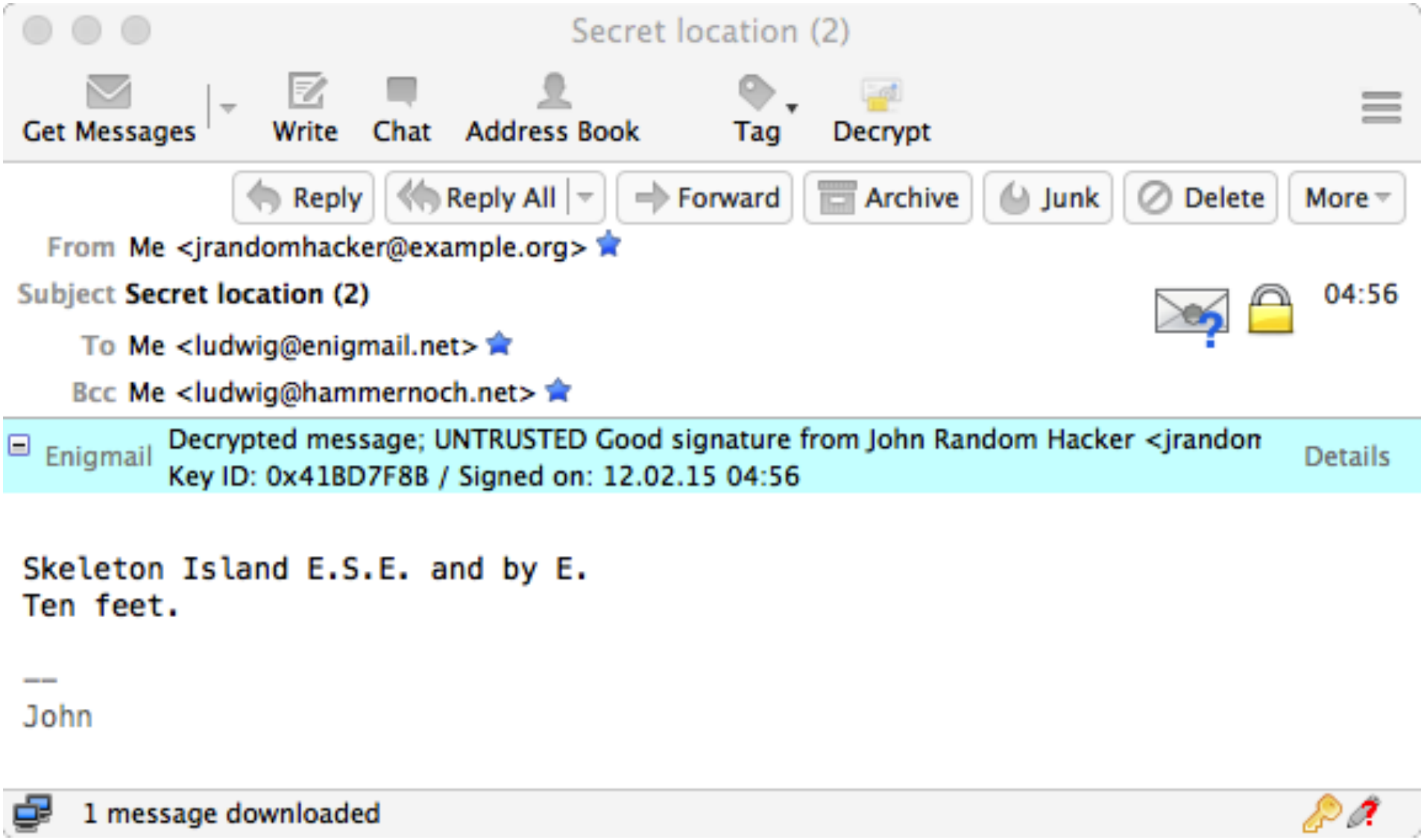
- GnuPG, free software
  - Pretty Good Privacy (PGP), Phil Zimmerman ('91)
  - GnuPG (GPG) is a free software recreation
  - Lets you hide email content via encryption
- Basic idea:
  - Hybrid encryption to conceal messages
  - Digital signatures on messages (hash-then-sign)

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

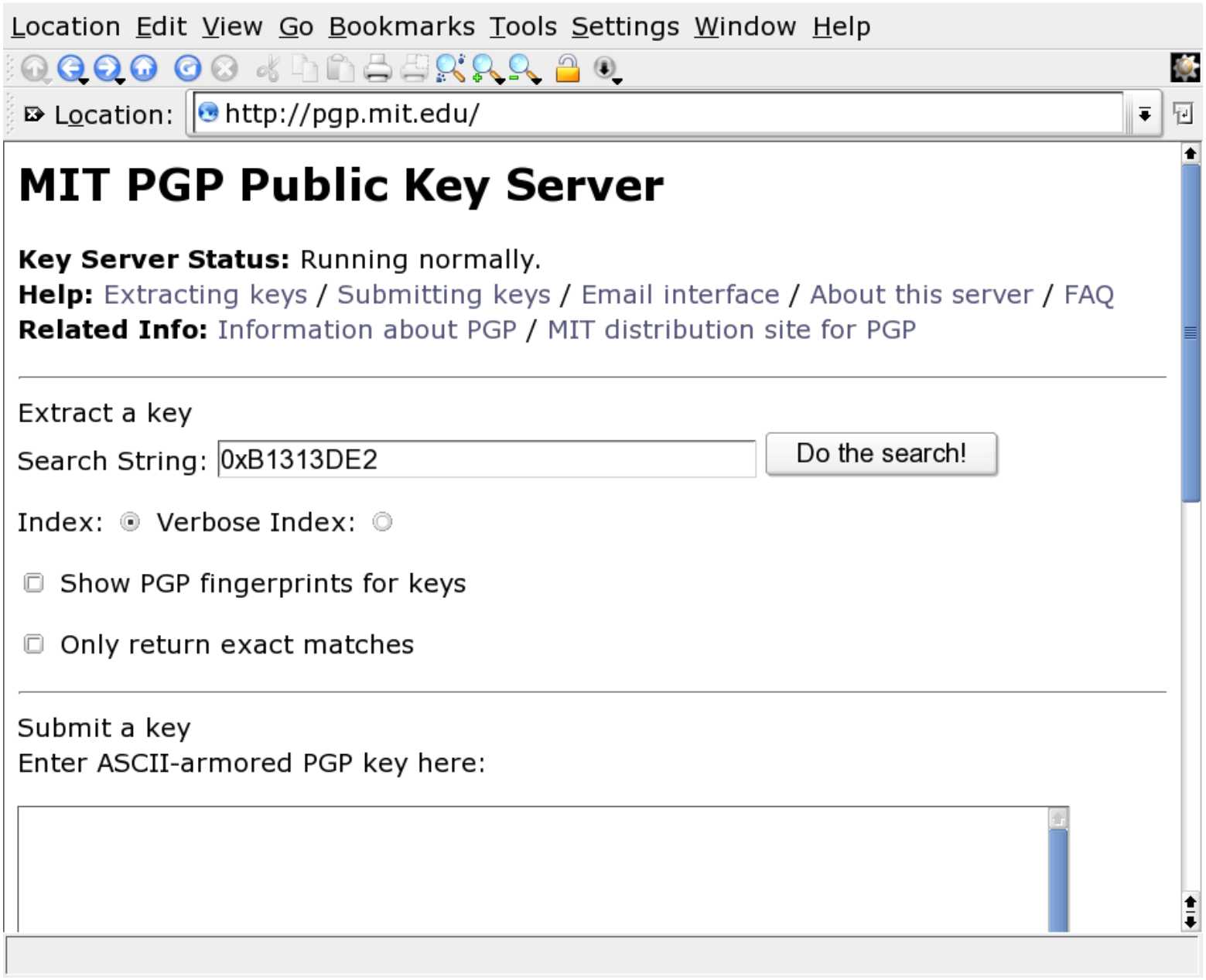
- To send a message:
  - Sign with your signature key
  - Encrypt message and signature with recipient's public encryption key
- To receive a message:
  - Decrypt with your private key to get message and signature
  - Use sender's public verification key to check sig


Secret location (2)
Get Messages
Write
Chat
Address Book
Tag
Decrypt
Reply
Reply All
Forward
Archive
Junk
Delete
More
From Me <jrandomhacker@example.org>
Subject Secret location (2)
04:56
To Me <ludwig@enigmail.net>
Bcc Me <ludwig@hammernoch.net>
Enigmail
Decrypted message; UNTRUSTED Good signature from John Random Hacker <jrandon
Key ID: 0x41BD7F8B / Signed on: 12.02.15 04:56
Details
Skeleton Island E.S.E. and by E.
Ten feet.
--
John
1 message downloaded

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

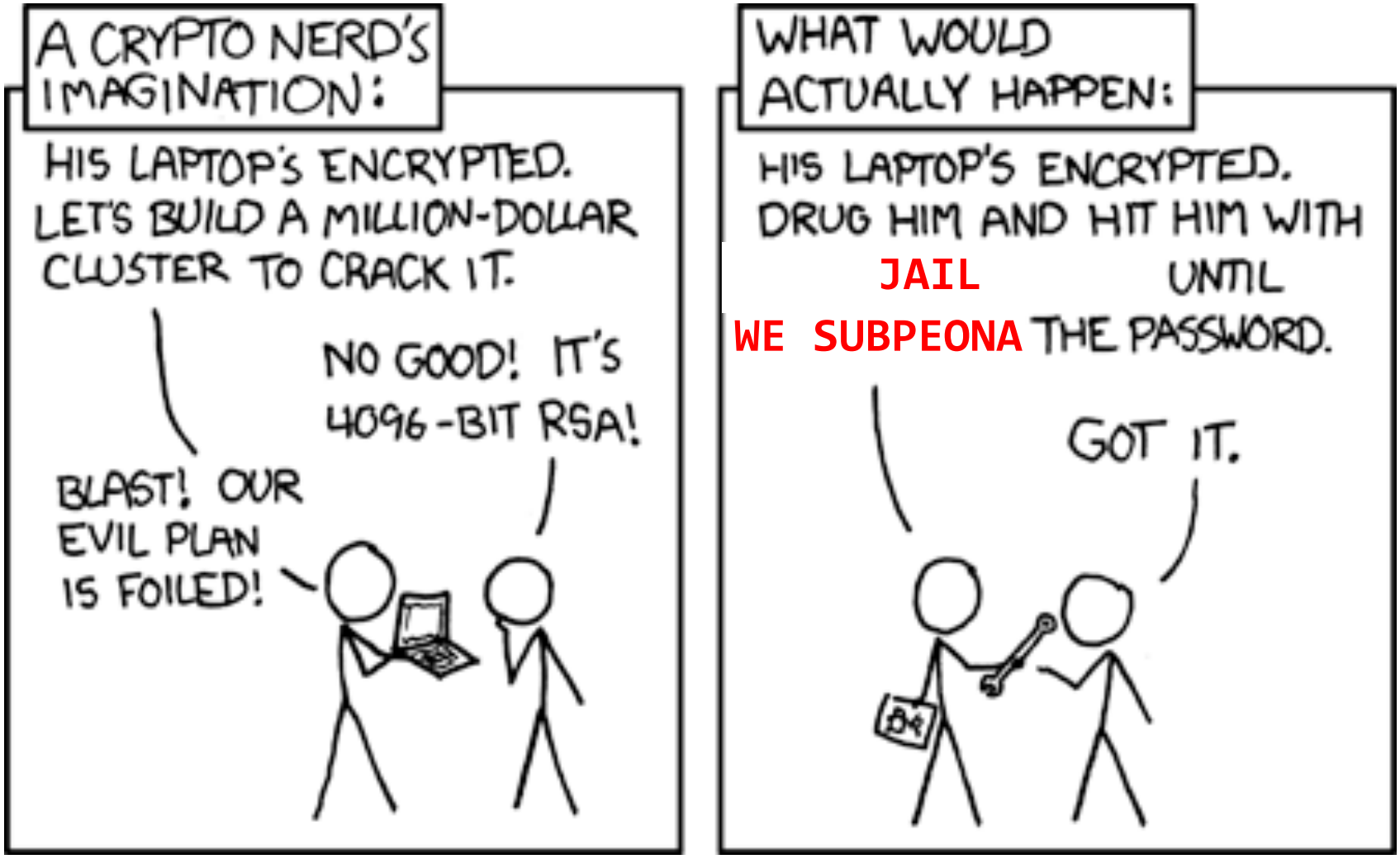
PGP Key Servers



Drawbacks of (Just) Encryption

- 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



Casual Conversations

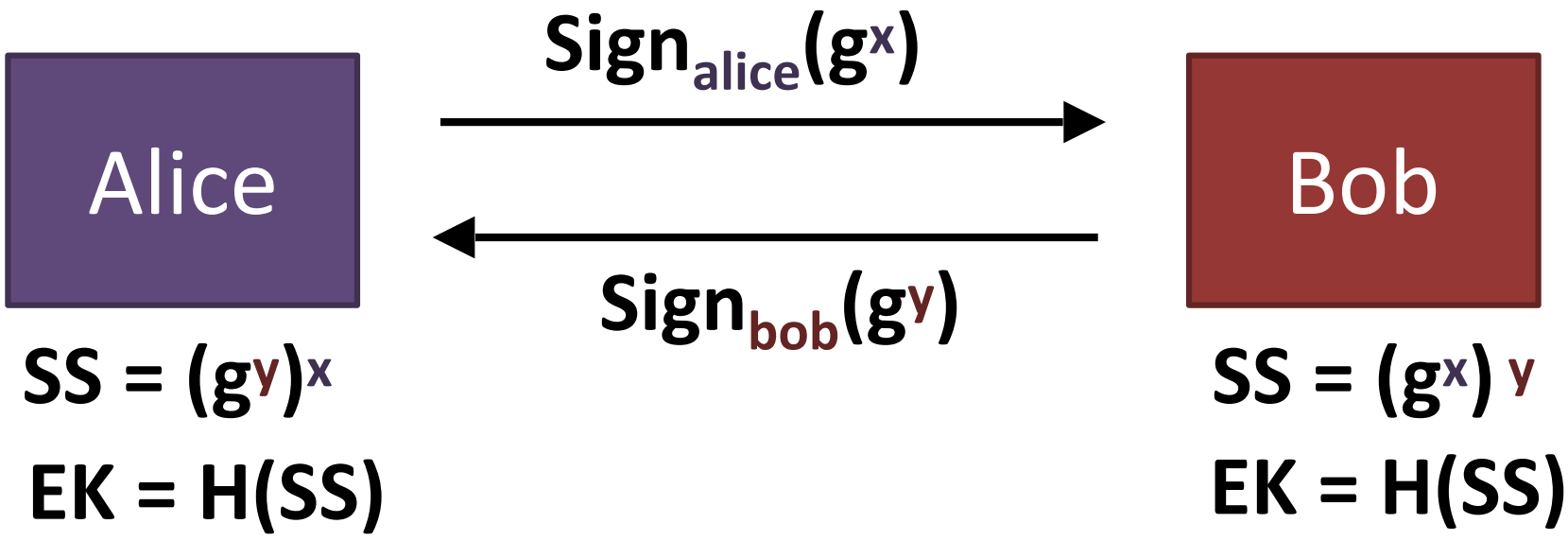
- Alice and Bob talk in a room
- No one else can hear
  - Unless being recorded
- No one else knows what they say
  - Unless Alice or Bob tell them
- No one can prove what was said
  - Not even Alice or Bob
- These conversations are “off-the-record”

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)

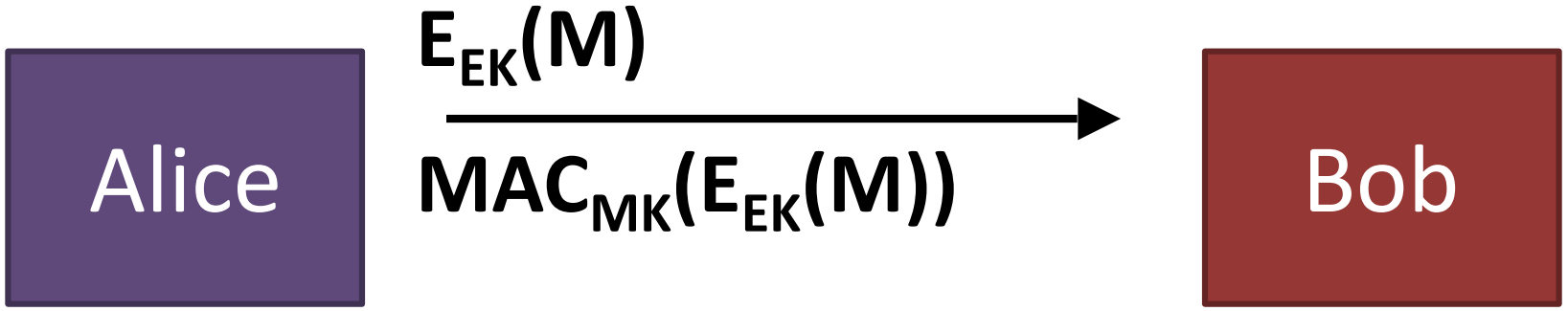
1. Use Authenticated Diffie-Hellman to establish a (short-lived) session key EK



Off-the-Record (OTR)

2. Then use secret-key encryption on message M

... And authenticate using a MAC



$SS = (g^y)^x$

$EK = H(SS)$

$MK = H(EK)$

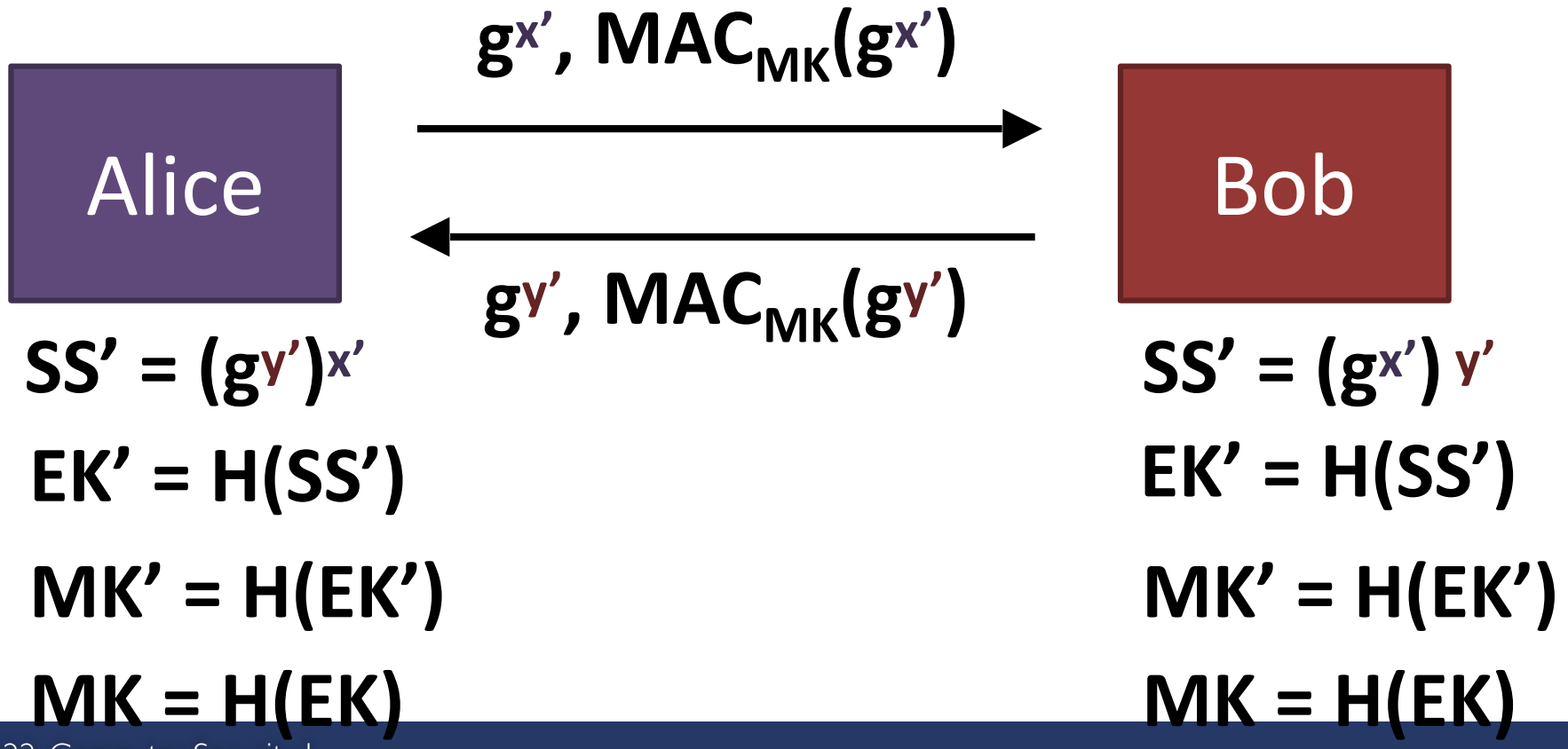
$SS = (g^x)^y$

$EK = H(SS)$

$MK = H(EK)$

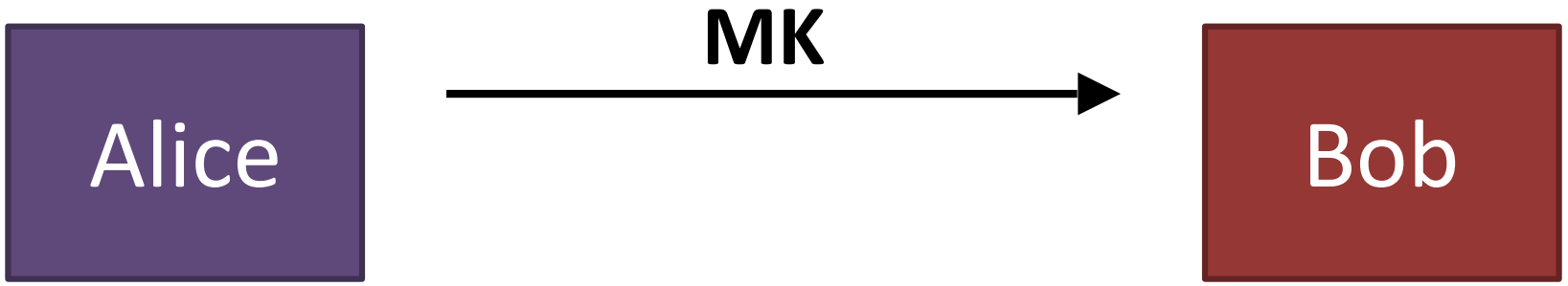
Off-the-Record (OTR)

3. Re-key using Diffie-Hellman



Off-the-Record (OTR)

4. Publish old MK (HUH????)



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)

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

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 calyxinstitute.org, install OTR and verify a buddy. You may also want to run it over Tor.

Double Ratchet Protocol

The protocol behind Signal app (iphone,android)
Trevor Perin and Moxie Marlinspike

- Forward secrecy

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

- Future secrecy (i.e., Backwards 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/

Recap Privacy/Anonymity

Metadata: Everything except the contents of your communications.

- If
- When
- How much
- Who 

- What 
Signal and OTR (this is actually the data)