Cybersecurity for Future Presidents

Lecture 1:
Where are we today?

Introductions

- Who am I?
- Who are you?
- Why are we here?

Cybersecurity for Future Presidents

Carl E. Landwehr, Ph.D.
David Voorhees, Ph.D.
Aparna Das, Ph.D

What can we teach you now that will help you make the right decisions on cybersecurity matters in 20 years, when you have risen to a position of leadership in government or industry?

Goal: At the end of the course, you should

- Understand, and be able to explain and apply basic, general concepts of computing, communications, and cybersecurity
- Understand and be able to explain relevant laws, policies, social concerns and market forces surrounding cybersecurity issues
- Be able to apply your understanding to assess critically arguments put forth in favor of alternative policy positions

Caution: This is the beta version after last year's alpha! Plans may change a little as the semester progresses.

Some recent cybersecurity-related events

Some 2015 – 2016 events

- Power grid cyber attacks: Israel (this week) Ukraine (late Dec.)
- U.S. Cyber Command announcing forthcoming cyberattack capabilities
- US – EU negotiating over privacy issues after "safe harbor" revoked
- NY, CA proposing laws to ban smartphones with unbreakable crypto
- Chrysler recalls 1.4M vehicles following hacking demonstration
- Attacks on healthcare record systems: Primera, Anthem, Carefirst
  Attacks on government record systems
  - OPM penetrations (attributed to China)
- Attacks on banks ($45M stolen after extensive reconnaissance)
- Ashley-Madison – personal distress, possible suicides
- Ransomware – stealing the right amount, payments via bitcoin
- Volkswagen "defeat device" software – malware vs. insider threat

It’s a big problem now, but what are the long-term issues?

- Can we build systems that aren’t so vulnerable?
  - If so, how to incentivize this?
  - If not, how to protect ourselves?
- What kind of privacy do we want?
- How do we provide accountability in computing and communication systems?
- How do we protect information in the long term (e.g. genetic information)?
- What’s the proper role for digital currency?
- How do we establish international norms for cyberwarfare?
- How should we vote in a digital age?

Planned Debate Topics

1. **Resolved: The U.S. government should mandate that storage technology providers include a mechanism by which protected data can be obtained under lawful court order.**

2. **Resolved: The US should adopt the E.U. "right to be forgotten" online.**

3. **Resolved: The U.S. Election Assistance Commission should promote internet voting for public elections on a model similar to Estonia.**

4. **Resolved: Commercially stored genomic data requires no further government regulatory controls.**

5. **Resolved: The U.S. Treasury Department should treat bitcoin as currency rather than as property.**

The Lecture on One Slide:

Where are we today in cybersecurity?

1. What do we mean by “cybersecurity” ?
   Key concepts that will recur

2. Recent occurrences in cyberspace

3. What does the U.S. President control?

Cybersecurity: security in cyberspace

Security

- Originally (OED) freedom from anxiety or care (se + cura)
- More recently (2011), OED added a definition:
  - Freedom from danger or threat: with reference to encryption, or telecommunications or computer systems: the state of being protected from unauthorized access; freedom from the risk of being intercepted, decoded, tapped, etc.
  - Note especially "threat" – security has to do not only with accidental, but also malicious acts

Cyber: Cybernetics: coined by Norbert Wiener, 1947

- from Greek κυβερνήτης "steersman" or "governor",
- context of feedback control, automated steering (ships, guns)

Cyberspace What is cyberspace?

- origins in sci fi of the early 1980s: Vernor Vinge *True Names*; William Gibson, *Burning Chrome*, *Neuromance*r

Cybersecurity: security in cyberspace

Privacy and Surveillance

Definitions of privacy

- Privacy as Confidentiality: Dan Geer – "ability to lie about yourself"
- Privacy as Contextual Integrity -- Helen Nissenbaum
- Privacy as Practice (socio-technical) -- Seda Gursa

Surveillance and society

- Visual surveillance:
  - Jeremy Bentham's panopticon
    - See Illinois Stateville penitentiary, eg
  - Pervasive CCTV / webcams: David Brin's Transparent Society, 1998; "Sousveillance" (from underneath)
- Surveillance in cyberspace
  - Commercial: cookies, cameras, etc.
  - Governmental: CALEA, backdoors, etc. Warranted, unwarranted

Accountability and Anonymity

Accountability:

- Ability to be called to account, take responsibility
- Butler Lampson's definition re spam
- Forensics as a form of accountability

Anonymity

- Ability not to be identified with some action
- Pseudonymity (Federalist papers, e.g.)
- Participation in experimental trials
- Re-identification

Discussion

Are accountability and anonymity antithetical? Can we have both?

What about security and privacy? Can we have one without the other?

Cybersecurity and Economics

- Information asymmetry and the market for lemons
  - Akerloff
  - Consumer can't distinguish good car (secure system) from lemon (insecure system) and so market fails to reward producer of good car (secure system) and they disappear from market
- Public goods: is cybersecurity a public good?
  - Schneider and Mulligan
  - Network security: non-rivalrous and non-excludable
- Liability and insurance

Cybersecurity and Human Behavior

- Central role of people in cybersecurity (Pogo: "We have met the enemy, and he is us!")
  - As consumers: What do we buy? How do we decide?
  - As individual users
  - As system administrators
  - As technology designers and developers
  - As hackers
  - As trolls

U.S. Government

- Federal
  - Executive: President, Departments and Agencies
  - Legislative: Congress
  - Judicial: Supreme Court and District Courts
- States
  - Governors, legislatures, courts
- Local
  - Cities, towns, etc.

What does the President control?

U.S. Government Departments with major Cybersecurity and Privacy concerns / responsibilities

- Department of Defense: protecting, international surveillance, attacking; research (NSA, DIA, DARPA, …)
- Department of Homeland Security: infrastructure protection
- Department of Justice: prosecution of cyber-crime, anti-trust, FBI
- Department of State: promulgating freedom of expression, authentication (passports)
- Department of Treasury: protection of financial systems, national and international
- Department of Commerce: international trade, standards (NIST)
- Department of Health and Human Services: medical records (HIPAA), medical devices (FDA), medical research (NIH)
- Department of Energy: nuclear weapons control, national labs (research)
- Department of Transportation: aircraft and aviation system safety, drones (FAA); automotive safety (self driving cars?)

[there are 6 more departments – can you name them? – see below]

(USDA, ED, HUD, DOL, DOI, DVA)

What does the President control?

Federal Agencies with Cybersecurity concerns/responsibilities

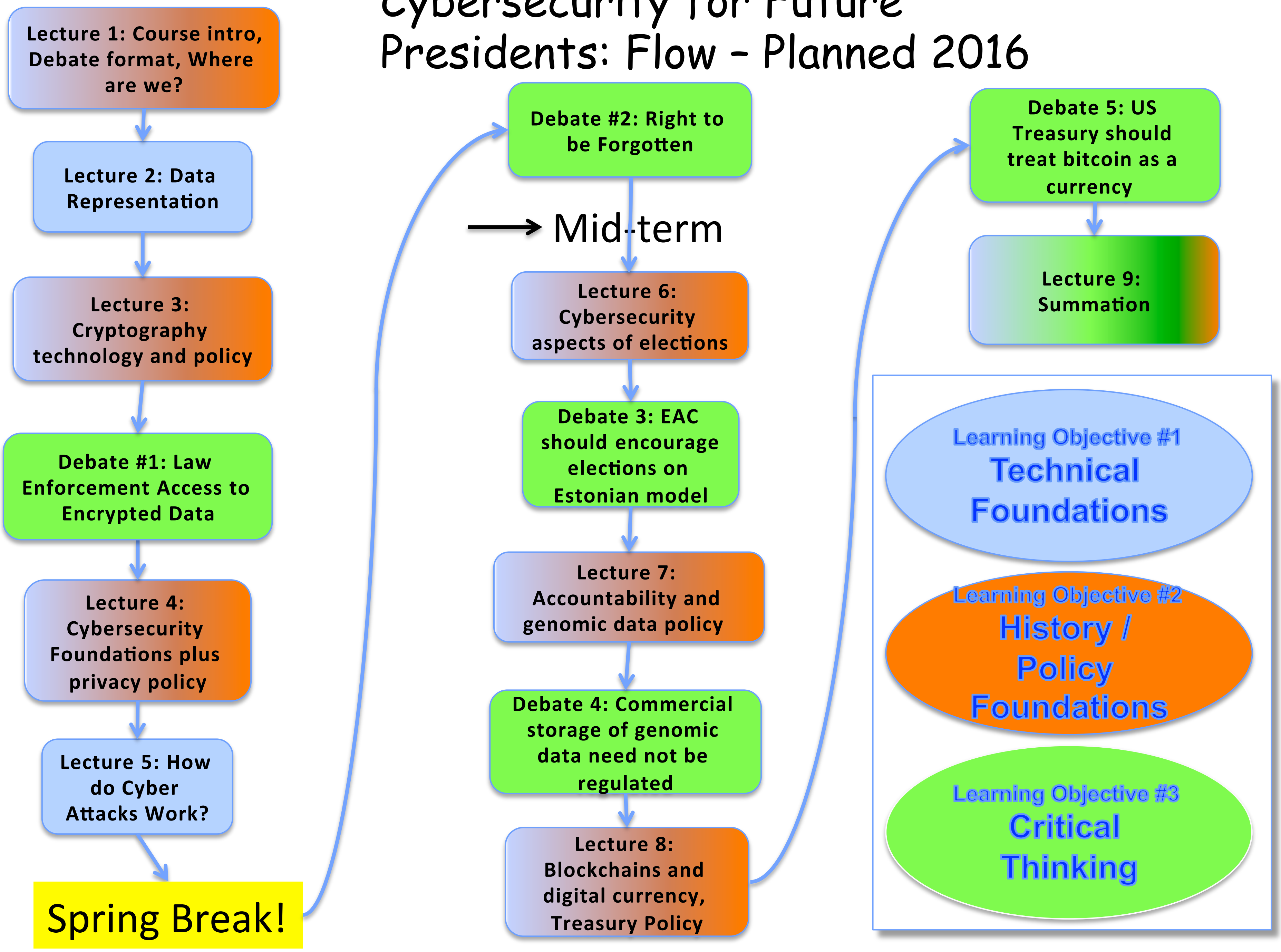
- Intelligence agencies (CIA, NRO, NGIA,…)
- Federal Trade Commission (privacy enforcement under fair business practices)
- Federal Communications Commission (regulation of communication networks, “network neutrality” a current concern)
- Securities and Exchange Commission (SEC) – securities trading
- Federal Energy Regulatory Commission (FERC – power grid)
- Nuclear Regulatory Commission (NRC) – reactor cyber security
- National Science Foundation: research, education

Wrap up

- It’s complicated!
  - But there are some underlying technical and policy issues that we can study and use to organize our understanding

- What is a future President likely to face?
  - National security issues
  - Commerce and trade issues
  - Public health and welfare issues

Cybersecurity for Future Presidents: Flow - Planned 2016



Lecture 1: Course intro, Debate format, Where are we?

Lecture 2: Data Representation

Lecture 3: Cryptography technology and policy

Debate #1: Law Enforcement Access to Encrypted Data

Lecture 4: Cybersecurity Foundations plus privacy policy

Lecture 5: How do Cyber Attacks Work?

Spring Break!

Debate #2: Right to be Forgotten

Mid-term

Lecture 6: Cybersecurity aspects of elections

Debate 3: EAC should encourage elections on Estonian model

Lecture 7: Accountability and genomic data policy

Debate 4: Commercial storage of genomic data need not be regulated

Lecture 8: Blockchains and digital currency, Treasury Policy

Debate 5: US Treasury should treat bitcoin as a currency

Lecture 9: Summation

Learning Objective #1
Technical Foundations

Learning Objective #2
History / Policy Foundations

Learning Objective #3
Critical Thinking

Requirements and Policies*

Weekly homeworks

Assigned Wednesday, lab sessions on Friday, due Tuesday (unless otherwise specified). Some of the homeworks will involve writing, some technical.

Tests: Midterm (Friday, March 18 – following spring break) and Final (May 12)

Debates: There will be 5 debates on topics that relate cybersecurity technology and public policy. Each student will argue in one debate and be a questioner in all the others. These will be spaced throughout the term.

Grades based on: Homeworks and debates 40%, Midterm 30%, Final 30%.

Classroom policy: no laptops / tablets / phones please. Too distracting!

Collaboration policy: Working together to thoroughly understand the material is encouraged, but once you have things figured out, you must part company and compose your written answers independently. That helps you to be sure that you understand the material, and it obviates questions of whether the collaboration was too close.

Meet the professor: My office hours: Noon – 3pm Wednesday. Each student please sign up for one 15 minute slot so I can understand your interests and you can meet me.

*Please see Canvas pages for details. The Canvas pages are the authority.

Textbook and supplement

The text:

Brian Kernighan, D is for Digital, 2011

- Readable, broad introduction to computing – hardware, software, communications, algorithms – for a general audience
- We will skip around a bit in it, but I recommend reading all of it
- → First assignment: READ all of Chapter 2 for next week. Bring questions!

Supplement:

- Ross Anderson, Security Engineering, 2nd Ed., 2008
  - available free online in chapters:
  - http://www.cl.cam.ac.uk/~rja14/book.html
  - Good depth on a wide range of topics. Use it if you are confused and want an alternative description of a topic

Ethics

- We may talk about vulnerabilities in systems and attacks on systems
- I want you to understand how the attacks work, because without it your ability to make good decisions will be limited
- But be aware that actually attacking systems is in general both unethical and illegal!
  - People doing responsible research into vulnerability-finding need to behave ethically and responsibly
  - There are extensive discussions about what exactly this means in practice, but in general
    - If you find a vulnerability, first notify the person/ organization who is in a position to fix it
    - Only after the fix has been distributed and installed is it appropriate to make public statements about it

Why Have Debates?

- Help you learn to think critically about topics relating to both cybersecurity and public policy
- Help you learn to express an oral argument
- Expose different viewpoints on issues of current interest
- Motivate the technical parts of the course
    - Prior to each debate, lectures and readings will cover material relevant to both technology and policy for that debate

Debate Procedures – In advance

- Two 3-person teams, one to speak in favor of the resolution (PRO), one against (CON). Toss of coin to see which side goes first.

- In advance, each side prepares a position paper (one paper per team), 2500 words (about 5 pages), with references, presenting the team's position.

- One student (or more!) from each side visits me for 15 minutes to discuss the team's plan

- Non-debaters review provided materials and draft one question for each side (this is the homework for debate weeks)

Debate Procedures – Day of the Debate

On the day of the debate (note: PRO and CON order may be interchanged based on coin toss)

<initial vote>

- PRO presents opening statement (5 min.)
- CON presents opening statement (5 min.)

<brief pause for preparation> (3 min.)

- PRO presents rebuttal (5 min.)
- CON present rebuttal (5 min.)

<brief pause> (3 min.)

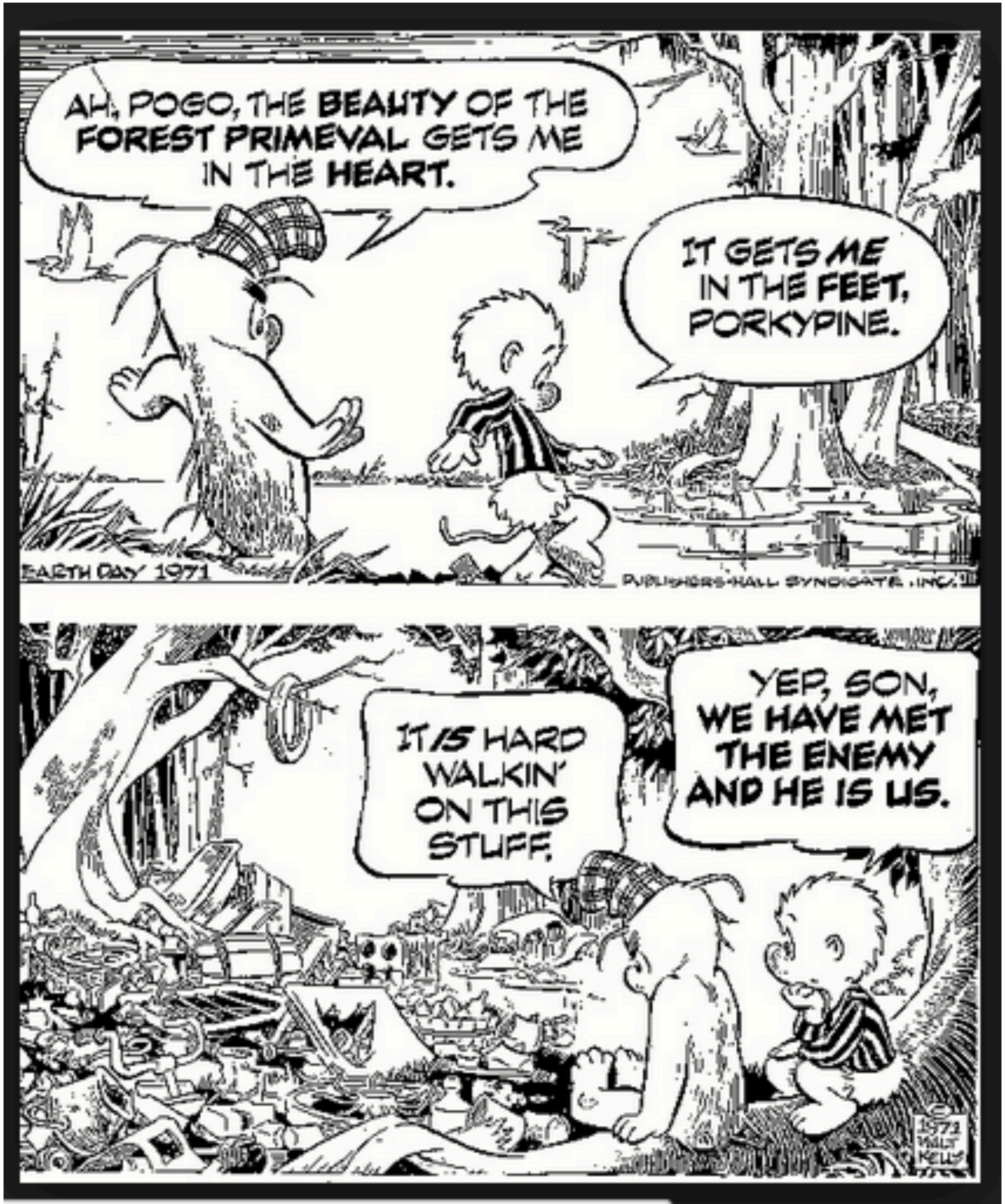
- PRO presents closing statement (5 min.)
- CON presents closing statement (5 min.)

Questions are posed to each side by moderator and/or professors (10 min.)

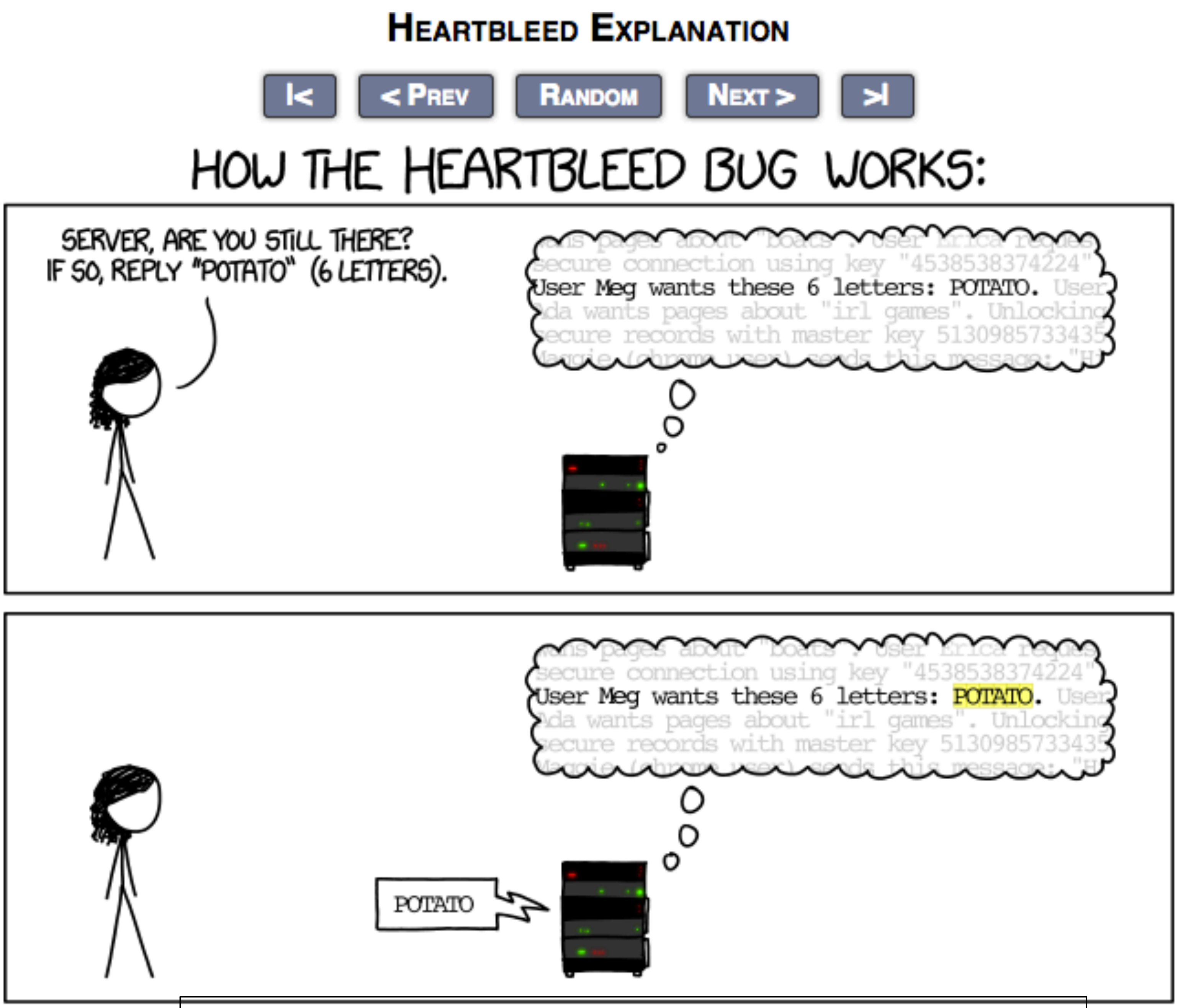
<final vote>

Backup slides and callouts

Pogo
by
Walt
Kelly

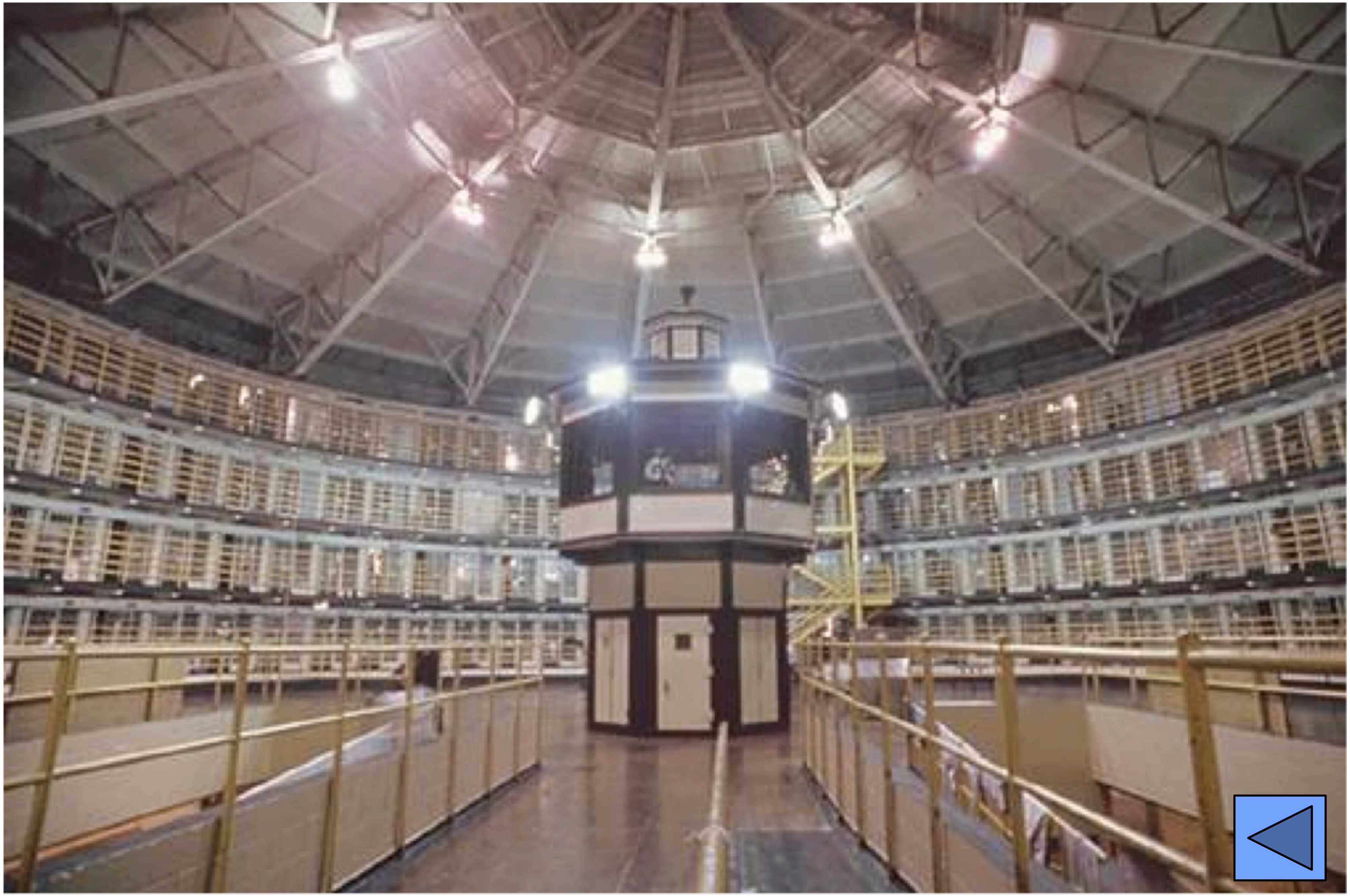

AH, POGO, THE BEAUTY OF THE FOREST PRIMEVAL GETS ME IN THE HEART.
IT GETS ME IN THE FEET, PORKYPINE.
EARTH DAY 1971
PUBLISHERS-HALL SYNDICATE, INC.
IT IS HARD WALKIN' ON THIS STUFF.
YEP, SON, WE HAVE MET THE ENEMY AND HE IS US.
©1971 WALT KELLY

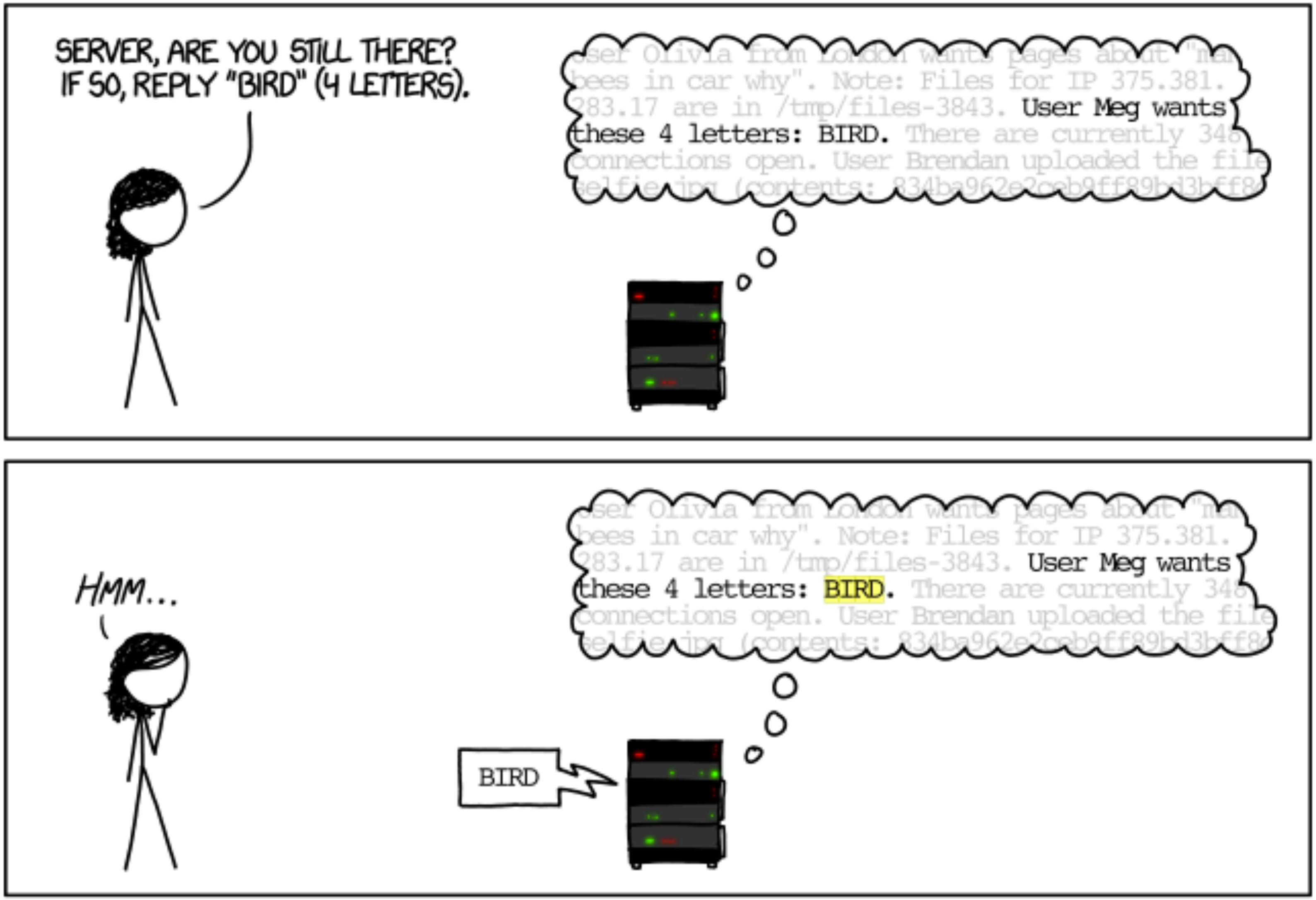
<back>


Heartbleed Explanation
|<
< Prev
Random
Next >
>|
HOW THE HEARTBLEED BUG WORKS:
SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
wants pages about "boats". User Erica reques
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
Maggie (chrome user) sends this message: "H
wants pages about "boats". User Erica reques
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
Maggie (chrome user) sends this message: "H
POTATO

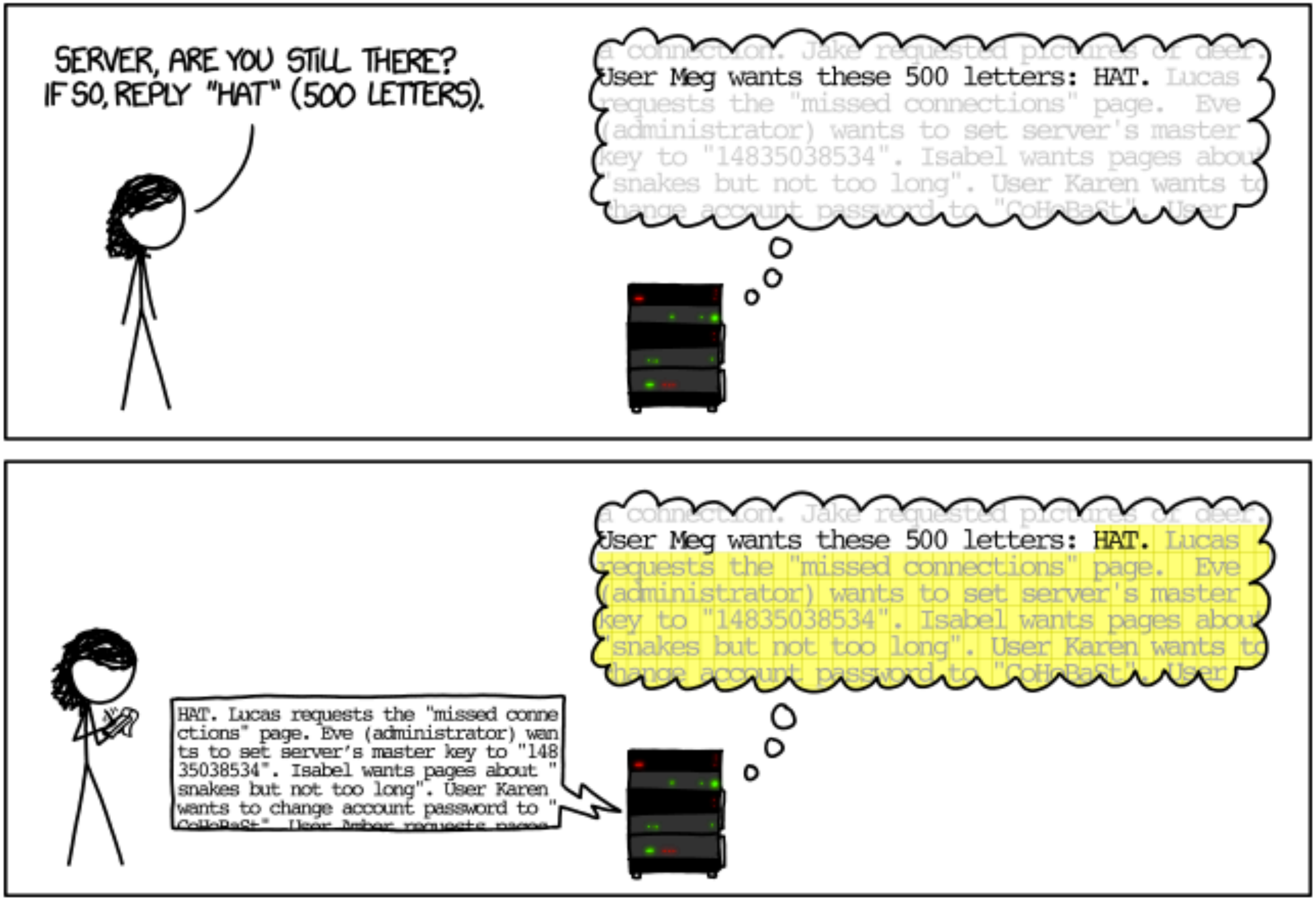
From XKCD cartoons: http://www.xkcd.com/1354/

Panopticon – Stateville penitentiary, Illinois




SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 348 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
HMM...
User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 348 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD

From XKCD cartoons: http://www.xkcd.com/1354/


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages

From XKCD cartoons: http://www.xkcd.com/1354/

<Back>

From Symantec's report on Stuxnet: *global infection rates*

We have observed over 40,000 unique external IP addresses, from over 155 countries. Looking at the percentage of infected hosts by country, shows that approximately 60% of infected hosts are in Iran:

<back>

Some Current U.S. Federal Laws and Regulations relating to Cybersecurity, including Privacy

- Wiretapping / surveillance:
  - Domestic telephone calls: In general, federal wiretaps are permitted only if a warrant has been issued (this requires a judge to approve a detailed request) [ref: episodes of "The Wire"]
  - Domestic e-mail: Stored Communications Act (SCA)
  - Foreign / national security surveillance: Foreign Intelligence Surveillance (FISA) act, PATRIOT Act
- Healthcare information: HIPAA (Health Insurance Portability and Accountability Act) 1996
- Financial records and information:
  - GLB: Graham-Leach-Bliley 1999 – requires written security plan to protect client nonpublic data
  - SOX: Sarbanes-Oxley Act 2002 – accountability for internal controls on financial reporting, fraud prevention/detection

Security Breach notification laws in the U.S.

- California passed a laws requiring notification of breaches of unencrypted personal data in 2002
- As of 2014, 47 states in the U.S. have passed laws requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information ("PII")
- Verizon now publishes and annual "Data Breach Report" summarizing results of the past year
- U.S. Congress has had several bills introduced to establish a national standard for breach notification, but none have passed

Additional Breach Examples

Retail: Home Depot breach

- POS malware installed mainly on self-checkout lanes in 1,700+ stores; 56,000,000 credit cards collected over period 4/14 – 9'14
- How: "BlackPOS" malware variant, according to KrebsOnSecurity
- Reported 9/2/14++

Estonia (2007): large scale denial of service attacks cripple national economy for several days following removal of Soviet era statue from prominent public location. Russian government/"citizen hackers" strongly suspected, not proven

"Aurora" attacks on Google and 20 other companies (2009-2010): "zero-day" vulnerabilities in Internet Explorer and other means used to compromise systems; backdoors installed to communicate with remote servers and exfiltrate intellectual property (e.g. programs). Chinese involvement strongly argued.

Saudi-Aramco cyber attack (Aug. 2012): "Shamoon" virus damages thousands of computers at government oil company; large scale hardware replacements required. Hacker group claims credit; Iranian participation strongly suspected.

Additional security infrastructure breach examples

- Shellshock (2014): widely used open source software turned out to have an exploitable flaw; servers might execute bogus privileged commands. Had been in place for many years. Highlights latent vulnerabilities in open source software.
- RSA breach (2011): attack on major supplier of certificates and tokens compromised security infrastructure. Highlights effectiveness of "spear-phishing" in conjunction with latent vulnerabilities in software, even in sophisticated security firms.
- Diginotar: Dutch certificate issuing company suffers security breach and is discovered to have issued fraudulent certificates facilitating man-in-the-middle attacks. Highlights vulnerabilities of certificate-issuing infrastructure

Some Current U.S. Federal Laws and Regulations relating to Cybersecurity, including Privacy (1 of 3)

- Wiretapping / surveillance / law enforcement:
  - Title III of Ominibus Crime Control and Safe Streets Act of 1968. Federal wiretap law specifies basis for legal wiretaps.
  - Electronic Communications Privacy Act (ECPA) of 1986; intended to control wiretaps but now somewhat outdated
    - Incorporates/updates "Title III" of Ominibus Crime Control and Safe Streets Act of 1968.
    - Federal wiretap law specifies basis for legal wiretaps.
  - PATRIOT Act
  - FISA / FISA Amendments Act
  - Stored Communications Act
  - CALEA

Some Current U.S. Federal Laws and Regulations relating to Cybersecurity, including Privacy (2 of 3)

- Healthcare information:
  - HIPAA (Health Insurance Portability and Accountability Act) 1996
- Financial records and information:
  - GLB: Graham-Leach-Bliley 1999 – requires written security plan to protect client nonpublic data
  - SOX: Sarbanes-Oxley Act 2002 – accountability for internal controls on financial reporting, fraud prevention/ detection

Some Current U.S. Federal Laws and Regulations relating to Cybersecurity, including Privacy (3 of 3)

- Government systems
  - Privacy Act of 1974: focus on government databases, 6 “Code of Fair Information Practices” established; amended 1988.
  - FISMA: Homeland Security Act (includes Federal Information Security Management Act
- Children:
  - COPPA: Child’s Online Privacy Protection Act 1998
  - Controls online collection of information from children < 13 years. Not really cybersecurity per se

Some recent happenings – II: Security Infrastructure

Heartbleed (2014):

- widely used open source software for SSL
- Had an exploitable flaw;
  - buffer overflow problem could allow sensitive data to be scavenged.
- Had been in place for years.
- Highlights latent vulnerabilities in open source software.
- XKCD Heartbleed Explanation:
  - http://www.xkcd.com/1354/
  - Or see callouts

2015

Some recent happenings – III: Govt. / Military

Stuxnet (2010): "SCADA" system attack.

Targeted malware exploits several "zero-day" vulnerabilities

Causes physical damage to Iranian centrifuges on "air-gapped" network;

Widely seen as nation-state attack and attributed to US/Israel.

<geographic infection rates and photo>

2015

Other recent happenings

- Sony breach
- Snowden disclosures: discuss
- Activities of “Anonymous” hackers
- Ferment in Intellectual Property business models

2015

	Lecture		Lab	HW
1 – Jan 27		Intro / Where are we today?	Set up debate teams	Wat deba
2 – Feb 3		Data representation, analog and digital		
3 – Feb 10		Cryptography technology and policy		
4 – Feb 17	Debate 1	The U.S. government should mandate that communications and storage technology incorporate mechanisms to ensure law enforcement access to information under lawful court order.		
5 – Feb 24		What is cybersecurity about? What is privacy about?		
6 – Mar 2		How do cyberattacks work?		
Mar 9		<no class>	Spring	Bre
7 – Mar 16	Debate 2	Congress should adopt the EU's "Right to be forgotten" online	MIDTERM	
8 – Mar 23		Cybersecurity aspects of elections		Eas
9 – Mar 30	Debate 3	U.S. Election Assistance Commission should promote Internet elections along Estonian model		
10 – Apr 6		How is accountability provided within a computer? + genomic data policy background		
11 – Apr 13	Debate 4	Commercially stored genomic data needs no		