CS475: Lecture 1
Computer and Network Security

High Level Information

- Instructor: Prof. Gaurav Naik
  - Office: 3401 Market, Ste 300 (CCI) Room 319
  - Office Hours: Wednesday 2:30-3:30 pm
  - E-mail: gn @ drexel.edu (Put CS475 in Subject)
- Course Website: Drexel Learn
- Syllabus: on Drexel Learn

TA

- Alex Duff - amd435@drexel.edu

Introductions

- Your name
- Year at Drexel
- Why interested in Computer Security and CS 475?

Overview

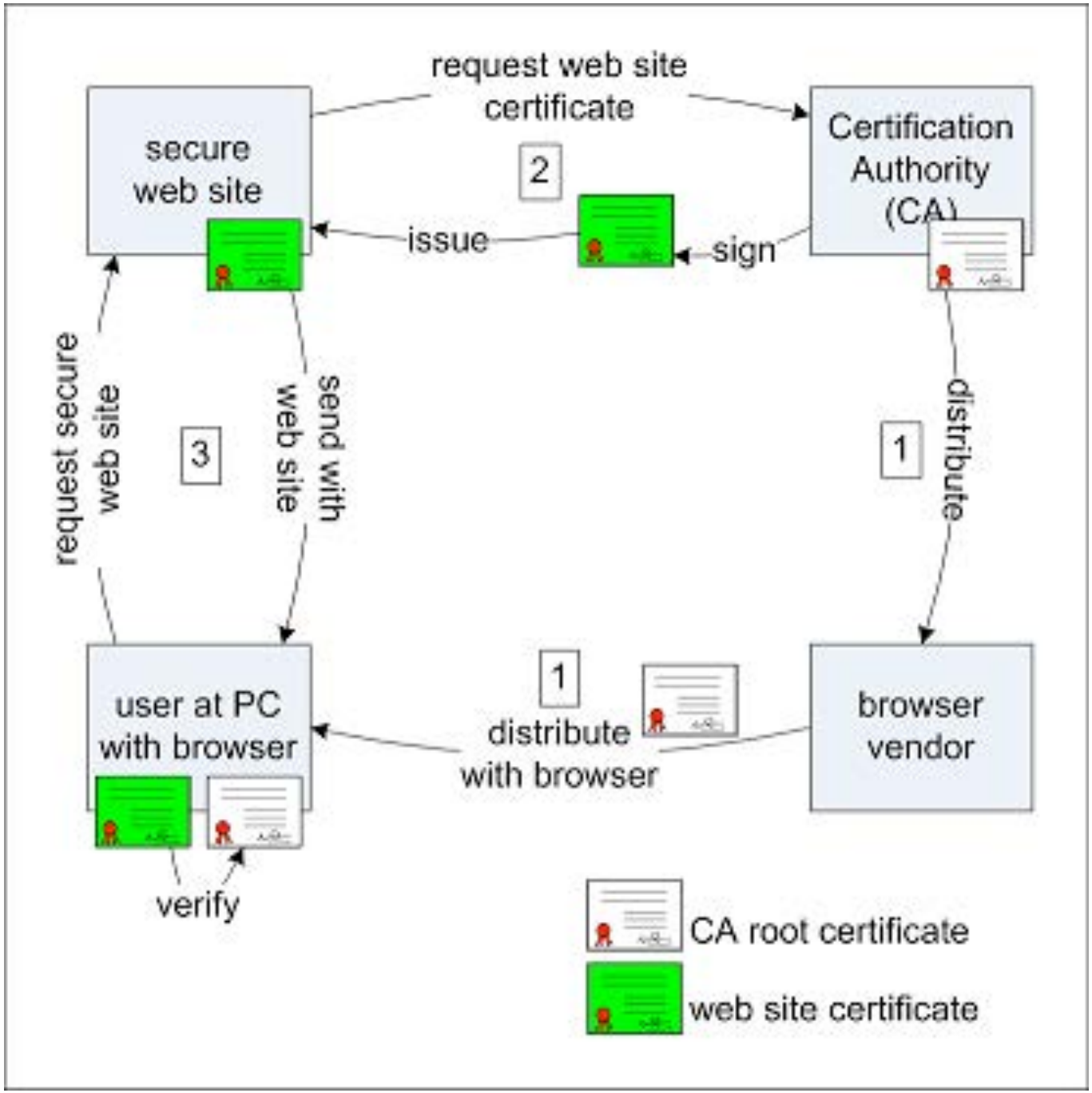
- Current Events in "Computer and Network Security" (far from complete)
- About CS 475
- Security Reviews

Computer security is an oxymoron

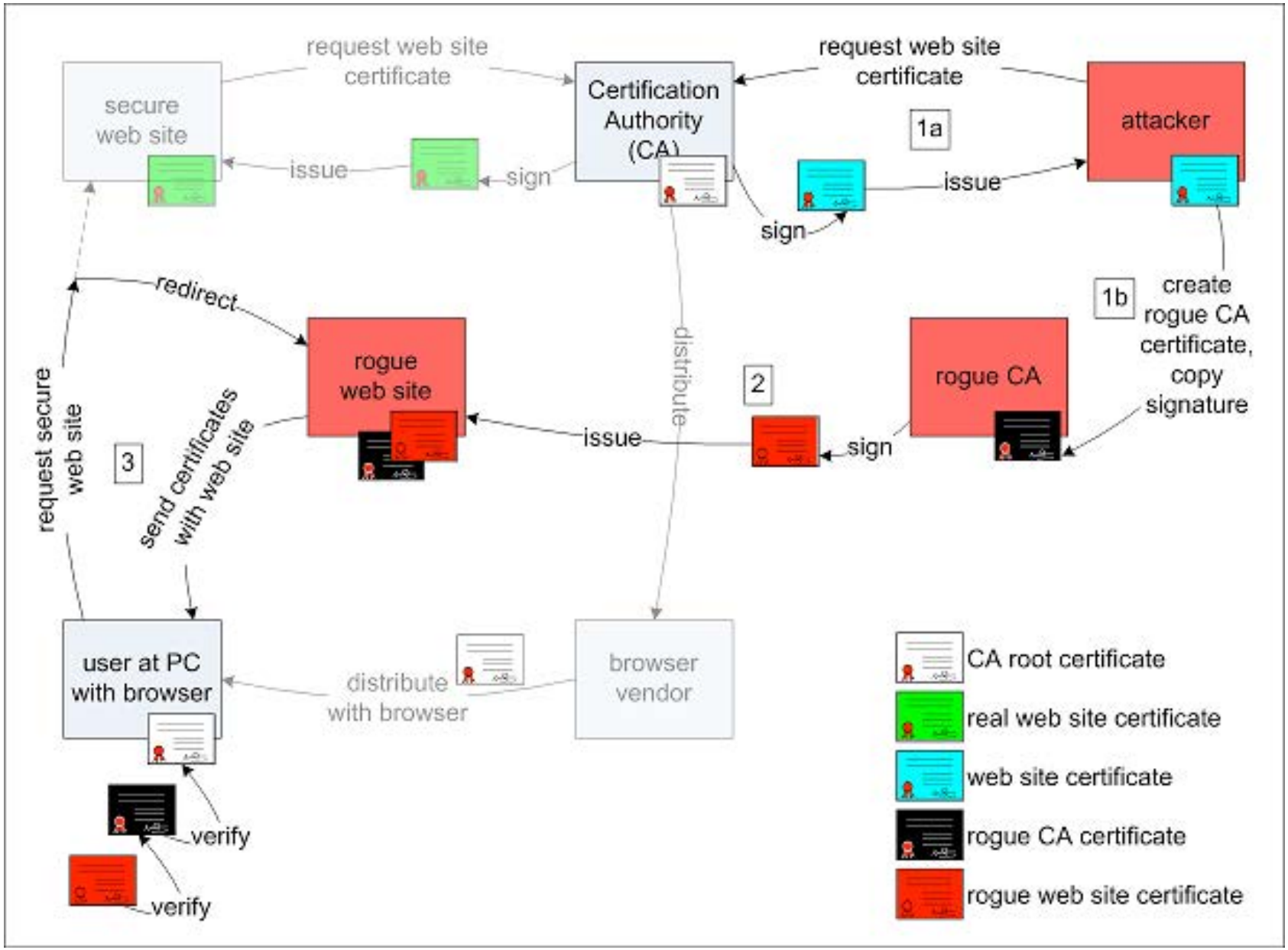
- Software is not secure
- Networks are not secure
- Trust infrastructures are not secure
- And users...well....I think I might have a bank in Nigeria to sell to you
- We like to talk about crypto --- it's the only thing we've got that really works

The Internets are Broken: SSL

How ssl web security is supposed to work



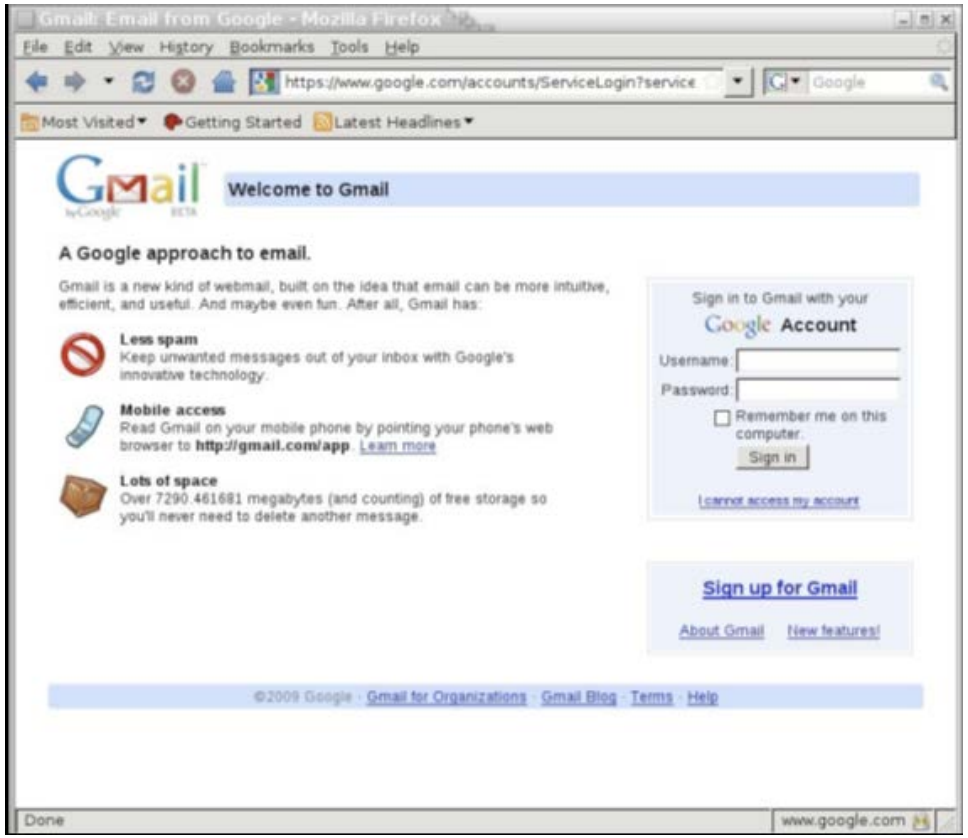
Creating a Rogue CA

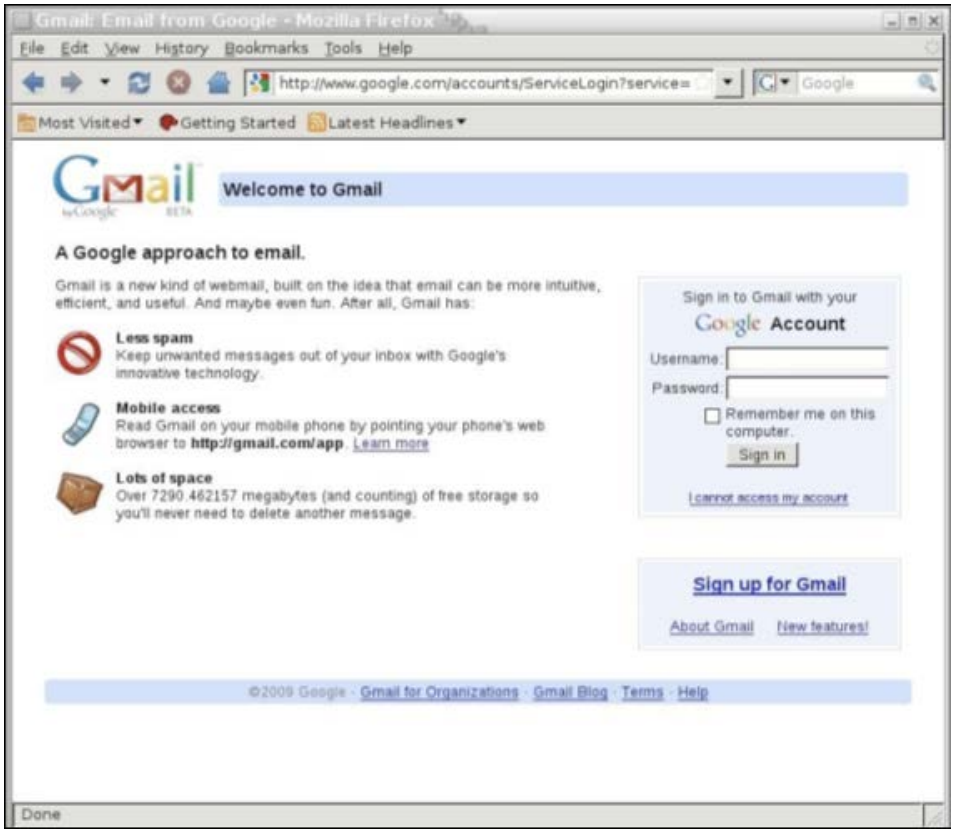


How to Create a Rogue CA

- 2009 : Buy cert for “paypal.com\0.mydomain.com” results in cert for due parsing error
- 2011 : Break into a CA or someone who has signing capacity (DigiNotar/Comodo)
- 2014: Heartbleed - buffer overrun in openssl
- 2015: google.com “mistake” ssl certificate

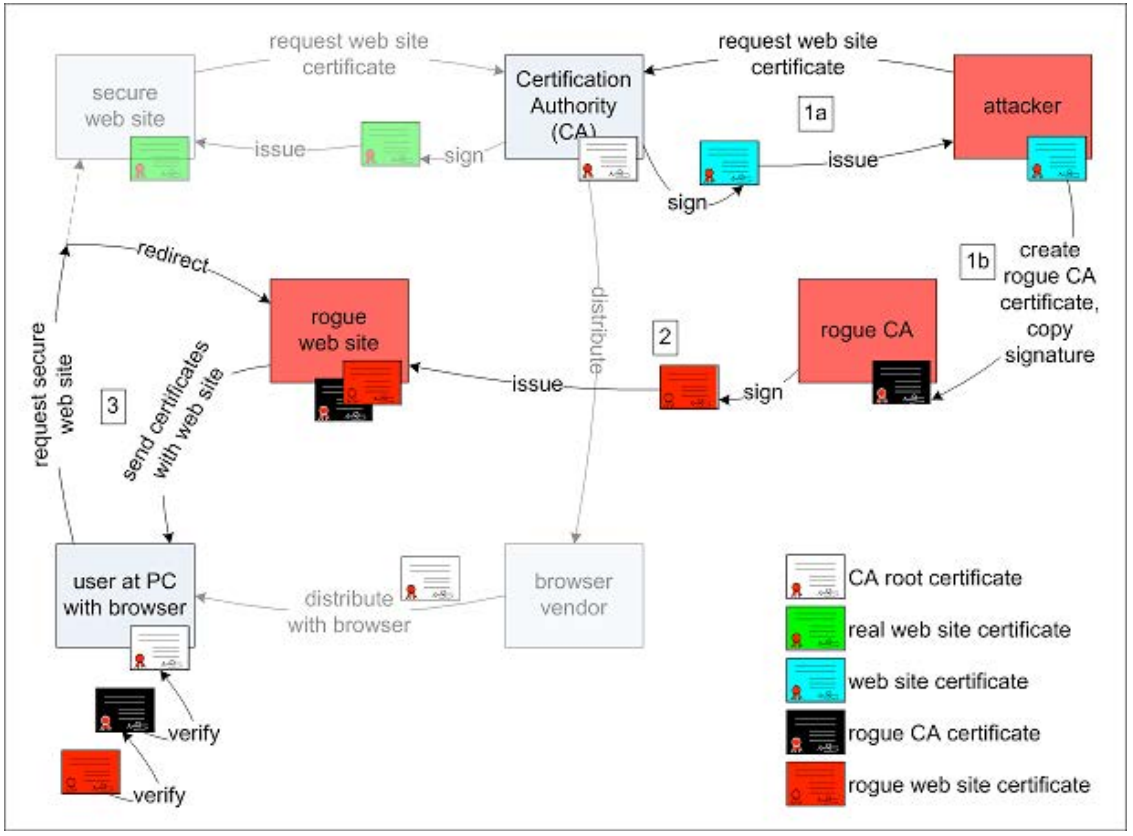
But then again, why bother?





Superfish (2015)

- Lenovo and Dell busted for installing a custom man in the middle root cert



Crypto is hard: Debian

- The following lines were removed from *md_rand.c*

```
MD_Update(&m,buf,j);
[ .. ]
MD_Update(&m,buf,j); /* purify complains */
```

- valgrind and purify (useful debugging tools) complained about uninitialized memory
- As a result, randomness in debian generated keys (SSL and SSH) was reduced to 15 bits (32,768 unique keys) and cryptographic ops were suspect

More Recently: RSA

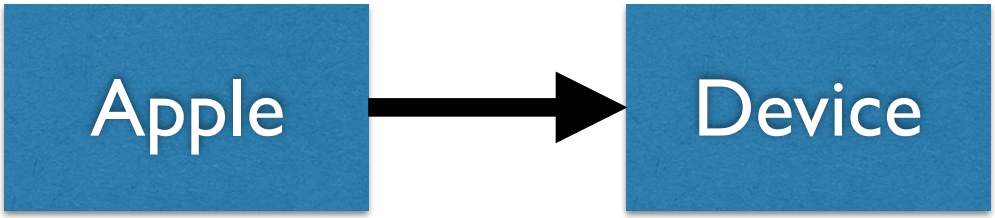
- Lenstra et al
  - Of 6.6 million distinct X.509 certificates and PGP keys (cf. [1]) containing RSA moduli, 0.27 million (4%) share their RSA modulus, often involving unrelated parties. Of 6.4 million distinct RSA moduli, 71052 (1.1%) occur more than once, some of them thousands of times.
- Heninger et al
  - Remote compromise of 0.4% of keys. Due to poor random number generation. Affects various kinds of embedded devices such as routers and VPN devices, not full-blown web servers

Release Engineering is Hard: Windows

- Flame broke into computers, spied on audio, keystrokes, etc.
- 2012.06.03 Microsoft "We recently became aware of a complex piece of targeted malware known as `Flame' and immediately began examining the issue...We have discovered through our analysis that some components of the malware have been signed by certificates that allow software to appear as if it was produced by Microsoft."

Release Engineering: Complicated

- Apple iOS



- Google Android

iOS 10.3 (and 10.3.1)

https://support.apple.com/en-us/HT207617

- CVE-2016-1734
- CVE-2016-1740
- CVE-2015-8659
- CVE-2016-1748
- CVE-2016-1752
- CVE-2016-1750
- CVE-2016-1753
- CVE-2016-1751
- CVE-2016-1757
- CVE-2016-1756
- CVE-2016-1754
- CVE-2016-1755
- CVE-2016-1758
- CVE-2016-1760
- CVE-2015-1819
- CVE-2016-1763
- CVE-2016-1788
- CVE-2016-1766
- CVE-2016-1950
- CVE-2016-1775
- CVE-2016-1778
- …

CVE vulnerabilities

- ~5,000 per year since 2005
  - https://cve.mitre.org/
  - National Vulnerability Database: https://nvd.nist.gov/
- 1700-3000 high severity (remote system compromise without user action)
- Not to mention governments hoarding

The web is a sewer…

Internet users can be infected simply by *viewing* a compromised website.


```
<body leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
<script language='JavaScript' type='text/javascript' src='fsvfk.js'></script>
<table width="99" border="1" align="center" cellpadding="0" cellspacing="0" bordercolor="#001D3C">
```

https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop.html

Data Protection doesn't exist

- Data aggregators compile in-depth dossiers on everyone
  - Choicepoint sold 163,000 record to identity thieves in 2005
- Often this data is lost, stolen, or misused
  - See Petraeus, David
- Privacy Rights Clearinghouse documents the loss of 246,134,559 sensitive records since 2005

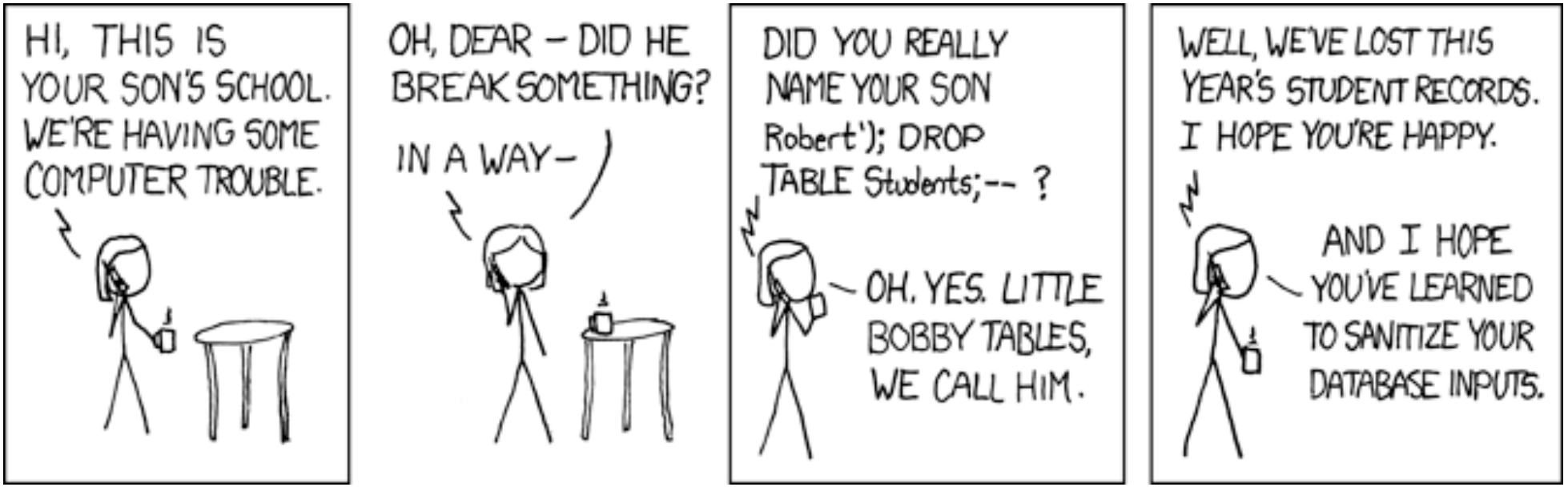
Not to mention the other dossiers...

- Microsoft. Yahoo. Google. Facebook. YouTube. Advertising => NSA
- Also, Verizon, AT&T, other telcos…
- Broadband Privacy Protections (2017)

Privacy in Apps?

- iOS plaintext file keeping track of fine-grained location info
- Malicious apps accessing address books, making premium phone calls, sending text messages to pay services
  - How many of you pay attention to permissions on apps you download?

SQL Injection



Govt Oppression 2.0

- Countrywide censorship via deep packet inspection, MiTM - Iran, China, Burma, etc
  - But also US, Germany, Aus, UK, etc
  - US companies leading the way
- Info warfare - Russia/Estonia 2007
- Hack of the DNC (2016) and US Elections

Apple vs FBI (2016)

- Can the courts compel companies to assist in breaking cryptography they have implemented?
- iOS will delete contents after 10 attempts
- Apple can make a custom iOS that disables that feature.

Why are things so bad?

- "Ship it today, get it right by version 3"
  - Features too far ahead of security
- Failure of software engineering field to be competent
- Lack of security metrics

Or maybe it's just the Internet [Lampson]

- Attack from anywhere
- Sharing with anyone
- Automated infection
- Hostile code
- Hostile physical environment
- Hostile hosts

The Malware Economy

- Revenue sources: SPAM, phishing, stolen data (credentials, game items)
- Revenue conversion: money mules
- Enabled by: Botnets of infected machines
- Enabled by: Infection vectors: Drive-by-downloads, email attachments, removable media
- Enabled by: Automated exploit packs (mpack, etc)
- Enabled by: Malware writers
- Enabled by: Exploit writers
- Enabled by: Software vulnerabilities/bad release engineering

Inspirations and Acknowledgements

- This class is based in part on
  - Rachel Greenstadt's CS475
  - Jeremy Johnson's CS 475
  - Dan Boneh's CS 155
  - Yoshi Kohno's CSE 484
  - Ron Rivest's 6.857
  - Radia Perlman's CS 243

What will we cover?

- Applied security topics, network and software attacks/defenses
- The “security mindset”
- Applied cryptography
- Economics/usability/privacy/AI

Prerequisites

- C, x86 and stack basics, network socket programming, operating system principles and machine organization, Unix related software engineering tools, Math (algorithms, probability, exponentiation/modular arithmetic, proofs), critical and devious thinking skills

Grading

- Exams: Midterm (15%), Final (15%)
- Projects 1,2, and 3: 3 x 20%
- Homework and participation 10%

Late Submission Policy

- You have two late days to use on your Projects 1 and 2
  - **Any other Late assignments will be dropped 20% per day.**
- No make up exams.

Cheating Policy

- department-wide cheating policy
  - See Syllabus
- When in doubt, err on the side of transparency
  - list collaborators and sources
  - if you wonder if it's ok, ask

Projects
Done in Groups of 2-3

- Project 1 : Software/Application Security
- Project 2 : Cryptography
- Project 3 : Security Review

Security: Whole System is Relevant

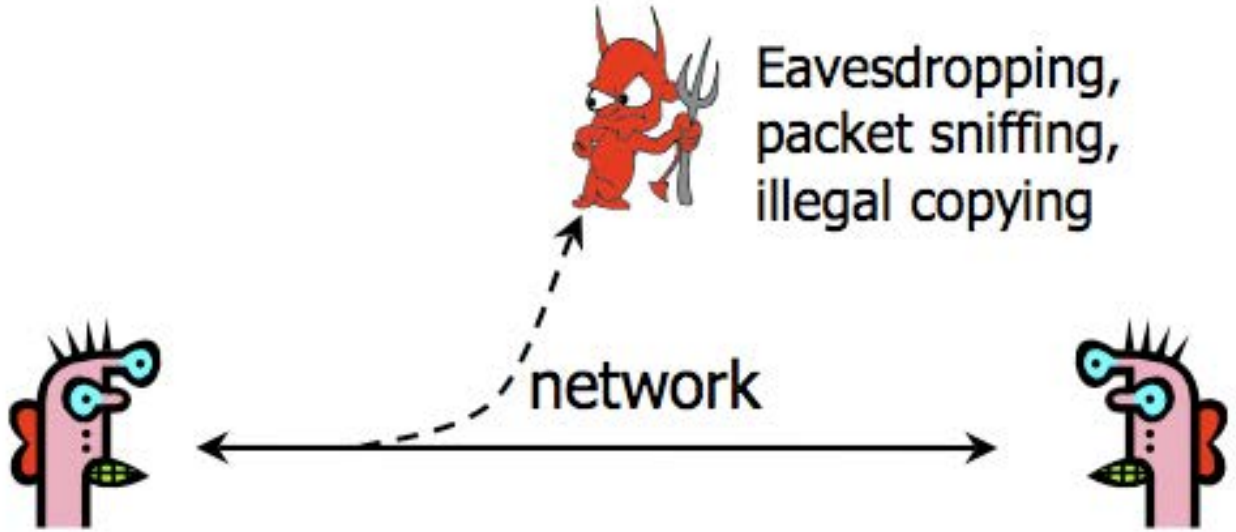
- Security requires a whole-system view
  - Cryptography
  - Implementation
  - People
  - Physical Security
  - Everything in between
- "Security is only as strong as the weakest link"
  - Many places to fail

Security Properties

- Confidentiality
- Integrity
- Authenticity
- Availability

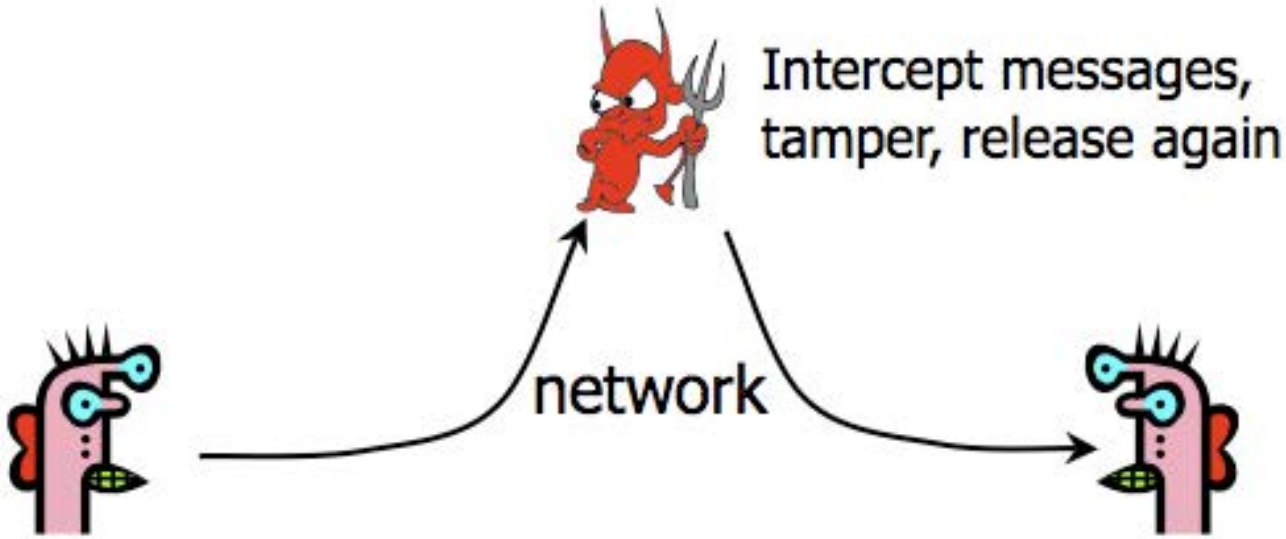
Confidentiality (Privacy)

- Confidentiality is concealment of information



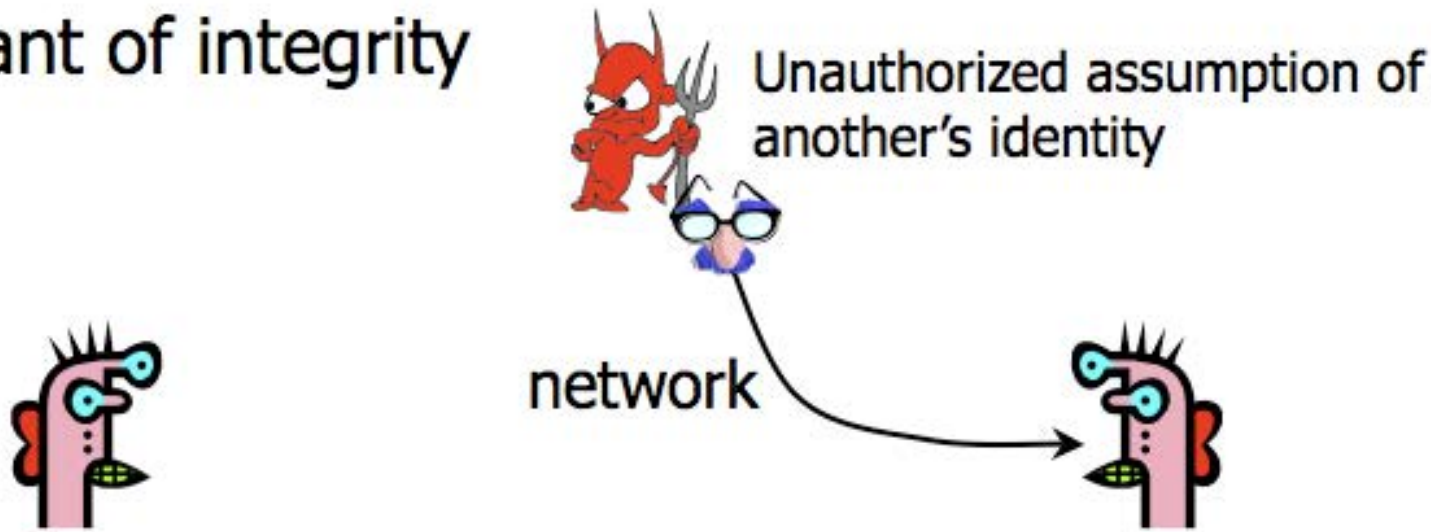
Integrity

- Integrity is prevention of unauthorized changes



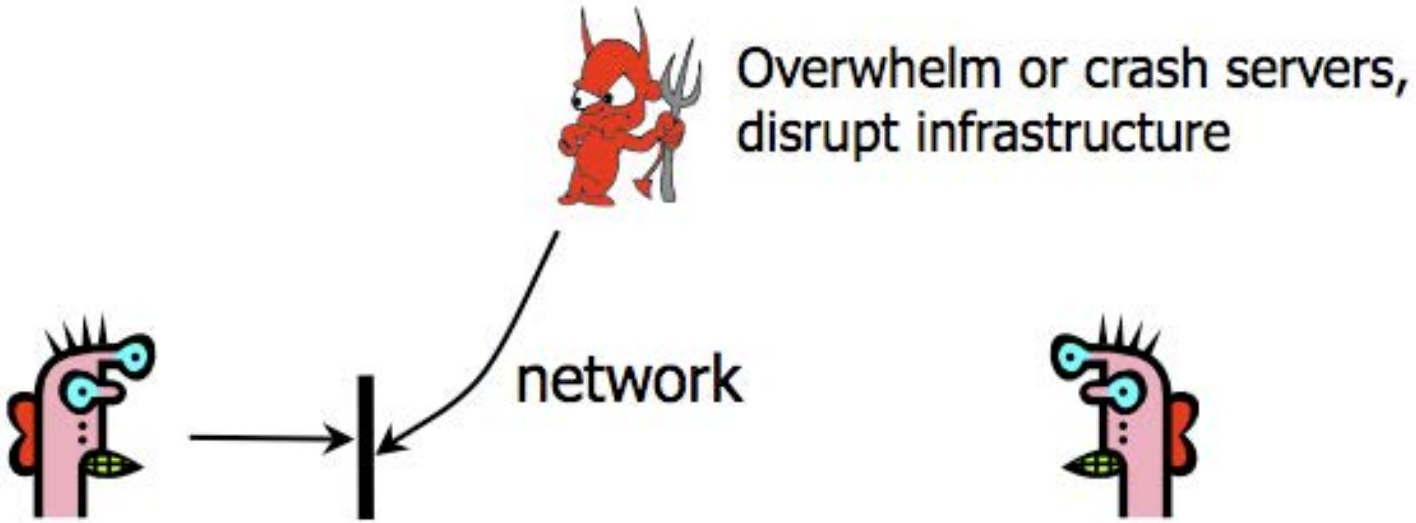
Authenticity

- Authenticity is identification and assurance of origin of information
- Variant of integrity



Availability

- Availability is ability to use information or resources desired



Analyzing the Security of a System: Part 1

- **First thing** : Summarize the system clearly and concisely
  - Absolutely critical
  - Can't summarize, how can you analyze? Ask:
    - What are the systems' goals?
      - How does the system achieve them?
    - Who are the players/stakeholders?
      - What are their incentives?

Analyzing the Security of a System: Part 2

- Subsequent steps
  - Identify assets: What do you wish to protect
  - Identify adversaries and threats
  - Identify vulnerabilities
  - Calculate the risks
  - Evaluate controls/mitigation strategies
  - Iterate

Assets

- Need to know what you are protecting!
  - Hardware: Laptops, servers, routers, PDAs, phones, ...
  - Software: Applications, operating systems, database systems, source code, object code, ...
  - Data and information: Data for running and planning your business, design documents, data about your customers, Reputation, brand name
- Assets should have an associated value (e.g., cost to replace hardware, cost to reputation, how important to business operation)

Adversaries

- National governments
- Terrorists
- Thieves
- Business competitors
- Your supplier
- Your customers
- Your enemies

- ...

Threats
Voting Machine Example

- Threats are actions by adversaries who try to exploit vulnerabilities to damage assets
  - Spoofing identities: Attacker pretends to be someone else
  - Tampering with data: Change outcome of election
  - Denial of service: Attacker makes voting machines unavailable on election day
  - Elevation of privilege: Regular voter becomes admin
- Specific threats depend on environmental conditions, enforcement mechanisms, etc
  - You must have a clear understanding of how the system works

Classifying Threats

- By damage done to the assets
  - Confidentiality, Integrity, Availability
- By source of attacks
  - (Type of) insider
  - (Type of) outsider
  - Local attacker
  - Remote attacker
  - Attacker resources
- By the actions
  - Interception
  - Interruption
  - Modification
  - Fabrication

Identify Vulnerabilities or Weaknesses

- How things can go wrong, not what
- Weaknesses of a system that can be exploited to cause damage
  - Accounts with system privileges where the default password has not been changed (Diebold: 1111)
  - Programs with unnecessary privileges
  - Programs with known flaws
  - Known problems with cryptography
  - Weak firewall configurations that allow access to vulnerable services
  - ...

Helpful Tables

Asset	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
...			

Homework 1

- Due April 13, 2:00PM
- Security review of Snapchat
- Bring a copy to class on the 13th

- READINGS:
  - Chapter 1 of Textbook
  - Towards Community Standards…

- Your goal with a security review is to evaluate the potential security and privacy issues with new technologies, evaluate the severity of those issues, and discuss how those technologies might address those security and privacy issues. The technology that you will be reviewing for this assignment is Snapchat. This review should reflect deeply on the technology that you're discussing, and should therefore be around two pages in length.
- Summary of the technology that you're evaluating. This summary should be at a high level, around one or two paragraphs in length. State the aspects of the technology that are relevant to your observations below. If you need to make assumptions about a product, then it is extremely important that you state what those assumptions are. To elaborate on the latter, if you end up making assumptions about a product like the Miracle Foo, then you are not studying the Miracle Foo but "something like the Miracle Foo" and you need to make that extremely clear in your review. It is important that you also state what the goals of the product are (not just the security goals) as this will inform your analysis.
- State at least two assets and security goals. Please explain why the security goal is important. This should be around one or two sentences per asset/goal.
- State at least two potential adversaries and threats. You should have around one or two sentences per adversary/threat.
- State at least two potential weaknesses. Again, justify your answer using one or two sentences per weakness.
- State potential defenses. Describe potential defenses that the system could use or might already be using to address your potential weaknesses above.
- Evaluate the risks associated with the assets, threats, and potential weaknesses that you describe. Also discuss relevant bigger picture issues (ethics, likelihood that the technology will evolve, and so on). (Being qualitative is fine; you don't need to be formal in you risk analysis.)
- Conclusions. Give some conclusions based on your discussions above. In your conclusions you should reflect thoughtfully on your results above.