Cybersecurity for Future Presidents 2016

Lecture 5:
Cybersecurity Foundations & Privacy Policy Background

Office Hours:
442 RH Wednesdays, noon-3pm

Cybersecurity events from the past week of interest to future (or current) Presidents:

- ✓ Apple – FBI face-off:
  - A moment on the technical details
  - Read more on Apple's security technology:
    - https://www.apple.com/business/docs/iOS_Security_Guide.pdf
    - Some parallel information for Androidhttps://source.android.com/security/
- ✓ Hospital pays ransom of 40 BTC = $17,000
- ✓ Are regular (e.g. GSM) cellphone calls encrypted?
  - Yes, over the air, but not after they get into the wired network
  - And the over-the-airencryption is generally not too strong
- ✓ What about Skype calls?
- ✓ WH appoints chair, vice-chair of Commission on Enhancing National Cybersecurity

Readings and Exercises

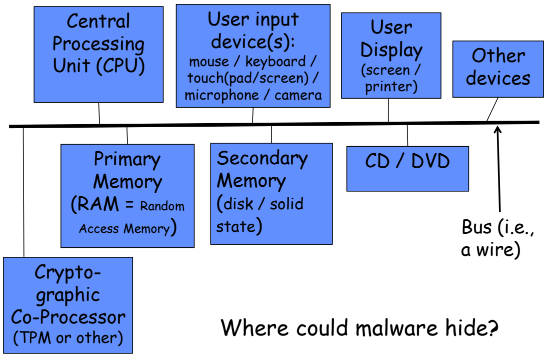
- For this week, you read:
  - How the web works (D is for Digital Chapter 10) and some attacks
  - Exercises to show something about how cryptography is used in the WWW
- Any Questions?
- For next week:
  - Reading about
    - What's inside a computer (D is for Digital, Chap 1)
    - Security engineering overview (Anderson Chapter 1)
- Today:
  - Quick review
  - Cybersecurity basics
  - Privacy policy basics

Quick review

Technology
- Digital vs analog, and why digital?
- Digital Data representation
- Telephony: Circuit switching to Packet Switching
- Cryptography fundamentals and application:
  - True Random vs pseudorandom numbers
  - Symmetric vs Asymmetric crypto
  - Cryptography in the World Wide Web

Policy
- Legal background on search and seizure
  - Writs of Assistance, Fourth amendment
- Wiretapping decisions and legislation
  - Katz v. U.S., Smith v. Maryland
  - ECPA, CALEA
- Foreign intelligence legislation
  - FISA, PATRIOT Act, FISAAA, USA FREEDOM Act

What Does a Computer Look Like (simplified)?


Central Processing Unit (CPU)
User input device(s): mouse / keyboard / touch(pad/screen) / microphone / camera
User Display (screen / printer)
Other devices
Primary Memory (RAM = Random Access Memory)
Secondary Memory (disk / solid state)
CD / DVD
Bus (i.e., a wire)
Crypto-graphic Co-Processor (TPM or other)

Where could malware hide?

What is cybersecurity about?

It's about assuring computer-based systems will behave reasonably even in the face of malicious attacks
- What are we trying to protect?
  - Data: bits at rest or in transit
  - System control
- What properties do we want to assure?
  - Security is a system property
  - CIA = Confidentiality, Integrity, Availability
- What kinds of threats should be considered?
- Systems view of security
  - Security Policies,
  - Security Mechanisms
  - Security Assurance
  - Incentives

Cybersecurity, Secrecy, Confidentiality, and Privacy

What properties do we want to assure?

- Security as a system property
- The importance of having a security policy:
  - "Without a security policy, there can be no security violations, only surprises"
- Policy needs to specify what's allowed and what isn't
  - This can get complex!
- Consider the complexity of the four environments Ross Anderson outlines:
  - Bank
  - Military base
  - Hospital
  - Home
- In each environment there are different kinds of things to be protected and different policies are needed
- But there are some commonalities in the the terms and content of such policies as well
- Key issues: Defining the scope of the system (see Anderson's discussion) to which a policy is to be applied

What properties do we want to assure?

General Security Properties of interest

"C,I,A":

- Confidentiality: no unauthorized viewing of information
- Integrity: no unauthorized modification of information
- Availability: no unauthorized denial of service

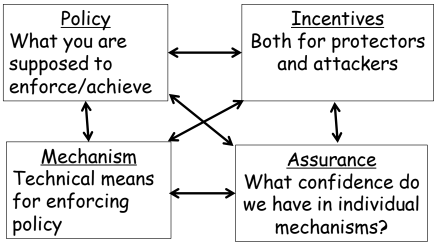
These three are primary. Others sometimes mentioned include non-repudiation, authentication

Anderson's discussion of the meanings of secrecy, confidentiality, privacy worth considering (p.13)

What threats are of concern?

- Mistakes and accidents
  - These are significant; some argue dominant
- Malicious actors
  - Insiders: people with authorized access to a system
  - Outsiders: people external to the system (could be users, e.g. of set-top boxes, ATMs, etc.)
  - Rank by
    - Technical expertise (unsophisticated → expert)
    - Resources available (individual -> criminal group -> nation-state)
    - Motive: financial gain, political objective, espionage, terrorism, war

Systems from a Security Engineering View



Policy
What you are supposed to enforce/achieve

Incentives
Both for protectors and attackers

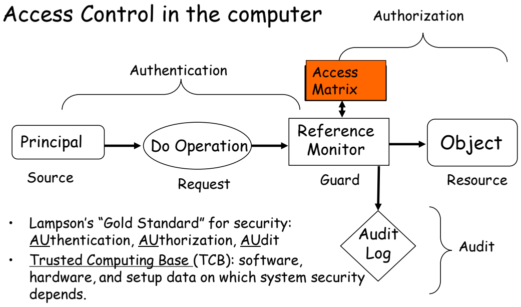
Mechanism
Technical means for enforcing policy

Assurance
What confidence do we have in individual mechanisms?

- Anderson Fig. 1.1, p. 5
- Note that "incentives" is meant to cover both the incentives of those protecting the system and those who might attack it – the threat

Mechanisms

Access Control in the computer



- Lampson's "Gold Standard" for security: AUthentication, AUthorization, AUdit
- Trusted Computing Base (TCB): software, hardware, and setup data on which system security depends.
- In general, try to minimize TCB size and make it as simple as possible
- Note "trusted" vs. "trustworthy"!

Mechanisms

Access Control Matrix

Objects (files/ devices)

Subjects		MS-Word	Photo lib	Camera	etc/passwd	Alicefile	Evefile
Alice:	P1	RX	RW		R	RW *	
Bob:	P2	RX		RW*	R		
Eve:	P3	RX	RW		R	R	RW *
SU:	P4	RWX	RWX	RWX	RWX	RWX	RWX

Operations
R = Read
W= Write
X= eXecute
* = owner

Subjects, Objects, access modes

Access Control List: associate permissions with objects (columns in above fig.)

Set of rules controls changes to this matrix:

create a file: add a column with creator having ownership, full access delete a file: remove column for that file

grant permission: owner can grant permission it holds to another subject

Unix / Linux / MacOS simplify this so that permissions are specified only for "owner, group, everyone else" on each file (rather than by individual subject)

Privacy

- What is it?
  - Sklansky: Privacy as refuge – a place to which one can retreat*
    - "privacy should be understood as respect for a sphere of individual sovereignty partially shielded from public scrutiny and regulation"
    - Protection from invasive searches
    - Basis for informational privacy
  - Here we address primarily informational privacy:
    - Ability to understand and to a degree control the flow of personal information
- General attitude in U.S.: control govt. records systems, not private
- General attitude in E.U.: control private record systems, not govt.

* David Alan Sklansky, Too Much Information: How Not to Think About Privacy and The Fourth Amendment, 102 Cal. L. Rev. 1069 (2014). Available at: http://scholarship.law.berkeley.edu/californialawreview/vol102/iss5/7

Brief history of government and privacy of computer-based records

Concern with creation of government databases and potential linkage of records across agencies – early 1970s

1973: Fair Information Practices (FIPs) code formulated by Dept. of HEW (forerunner to HHS/HUD) advisory committee:

1. No personal-data record-keeping systems whose existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about himself.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Led to passage of Privacy Act of 1974, which applied these principles to U.S. Federal agencies – governs all Federal "systems of records"

Augmented by Computer Matching & Privacy Protection Act of 1988

U.S. Federal Privacy legislation: "Sectoral"

- Business generally: Federal Trade Commission Act
  - FTC has authority to regulate privacy practices under the umbrella of controlling "unfair business practices"
  - FTC can issue "best practice" and other guidance; can sue
- Healthcare: Health Insurance Portability and Accountability Act (HIPAA)
  - Defines
- Financial: Fair Credit Reporting Act, 1970
  - Provides consumers access to their records held by Credit Reporting Agencies (e.g., Experian, Equifax, TransUnion) and some rights to contest/emend/remove information in the record
- Education / Children
  - Family Educational Rights and Privacy Act (FERPA) 1974
    - Restricts access to educational records
  - Children's Online Privacy Protection Act of 1998 (COPPA)
    - Limits collection of data online from children younger than 13
- Video Privacy Protection Act (1988) – restricts release of video rental records; prompted by release of Supreme Court nominee's records.

States have privacy laws (e.g., breach notification) as well

EU Privacy Regulation: General

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 "Data Protection Directive":

- Aim was to provide a common framework for regulating protection of personal data to allow free flow of data across borders within EU
- Personal data = "information that relates to an identified or identifiable natural person"
  - The person is the "data subject"
- Data controller: entity that has custody of the data
- Person suffering damage from unlawful processing is entitled to receive damages from the data controller
- Export of data outside EU permitted under condition that the receiving country can provide similar level of protection
  - This led to the ~2000 "safe harbour" agreement with the U.S.; US companies would "self certify" that they provided "adequate" protections

- See: http://ec.europa.eu/justice/data-protection/index_en.htm

7 Safe Harbour Principles ~2000

1. Notice - Individuals must be informed that their data is being collected and about how it will be used.They must provide information about how individuals can contact the organization with any inquiries or complaints.
2. Choice - Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.
3. Onward Transfer - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
4. Security - Reasonable efforts must be made to prevent loss of collected information.
5. Data Integrity - Data must be relevant and reliable for the purpose it was collected for.
6. Access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
7. Enforcement - There must be effective means of enforcing these rules.

Recent EU/US history

- Austrian privacy activist Max Schrems created a group called "Europe v Facebook" and files complaint with Irish Data Protection Commissioner against Facebook
- June 2014: Irish DPC rejects complaint, but Irish High Court granst review, but then refers to Court of Justice of the EU, saying Safe Harbour pre-empts Irish review.
- Oct 2015: CJEU rules that
  - (1) Ireland still could review EU-US data transfers in spite of Safe harbor and
  - (2) Safe Harbour framwork is invalid. Commercial agreements between US and EU (contracts) still possible however
- 2 Feb 2016: US/EU announce tentative "Privacy Shield" agreement
  - Details not yet known

EU & "Right to be forgotten"

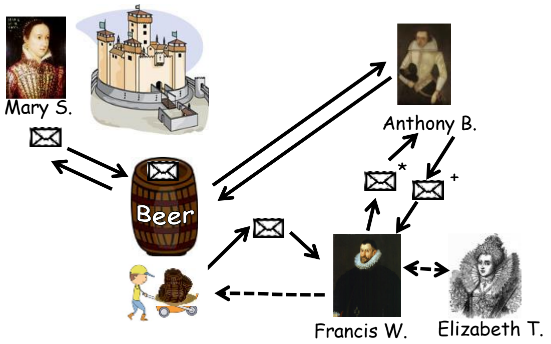
- Concept discussed in Europe for some years
  - "Reflects the claim of an individual to have certain data deleted to that third persons can no longer trace them"
  - "The right to silence on past events in life that are no longer occurring."
- Example: long ago criminal conviction might be expunged
- Distinct from right to privacy, which covers information not publicly known; RTBF covers public information to be (perhaps) erased
- May 2014: Google v Mario Costeja Gonzalez: requesting removal of a link to a Spansih newspaper article about auction of his foreclosed home for a debt that he had subsequently paid.
  - Couldn't get news article removed because it was lawful and accurate
  - But as a search engine and not a media outlet, CJEU ruled Google must comply and remove article from its search results
  - Google has implemented means for doing this, and has now responded to thousands of additional requests
- In the U.S., this right appears to conflict with first amendment (freedom of speech) and the notion of transparency

The Frosting

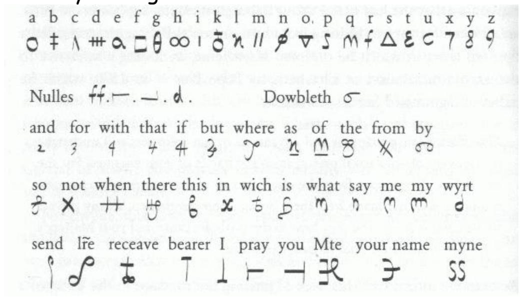
The frosting:

- How Mary Queen of Scots lost her head because of bad crypto and a Man in the Middle Attack

What's a "Man in the Middle" attack, or How Mary Queen of Scots lost her head in 1587



Cipher used by Mary Queen of Scots and Anthony Babington


a b c d e f g h i k l m n o p q r s t u x y z
Nulles
Dowbleth
and for with that if but where as of the from by
so not when there this in wich is what say me my wyrt
send lre receave bearer I pray you Mte your name myne