Cybersecurity for Future Presidents

Lecture 3:
What public policies control surveillance and cryptography?
What is cryptography about?

Cybersecurity events from the past week (or 2) of interest to future (or current) Presidents:

- ✓ NSA Tailored Access Operations (TAO) chief gives public talk on how NSA breaks into networks (1/25/2016):
  https://www.youtube.com/watch?v=bDJb8WOJYdA
  USENIX Enigma Conference website:
  https://www.usenix.org/conference/enigma2016/conference-program
- ✓ President announces "Cybersecurity National Action Plan"
  - ✓ FY17 Budget requests $19B for cybersecurity, up 35% from FY16 ($14B)
  - ✓ Releases new National Strategy for Cybersecurity R&D
  - ✓ Establishes Chief Information Security Officer (CISO) for government
  - ✓ Establishes Commission on Enhancing National Cybersecurity (12 members)
  - ✓ Establishes National Privacy Council of privacy officials in government
- ✓ See: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
- ✓ http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003

One more item related to today's lecture

- 2/4/2016 Washington Post reports that UK and US begin negotiation on mutual respect of wiretap orders:
  - Wiretap orders on UK citizens issued by British government for British citizen's data on computers in the U.S. could be served on U.S. companies
  - Wiretap orders on U.S. citizens issued by U.S. courts for data held on UK computers could be served on UK companies
  - Negotiations expected to take several months
- Note court case in progress U.S. v. Microsoft "In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation"
  - Narcotics investigation; US wants access to emails of a certain person (nationality unspecified) held in Microsoft accounts. Has a search warrant.
  - Actual location of email servers is in Ireland
  - Microsoft is refusing to comply with search warrant, arguing US law doesn't apply in Ireland
  - US attorney agrees US law doesn't apply in Ireland but argues that they are not asking Ireland, they are asking Microsoft, a U.S. company
  - Case currently under consideration by Federal Appeals court in California

Any Questions?

My office hours:
Wed. afternoon, 12-3pm, 442 RH

- About previous lecture?
- About homework on data representation?
- About reading?

Homework for next week: Debate prep and questions for debaters; see Canvas.

There are three papers for everyone to read:

1. A report by a group of well-known technologists arguing against back doors.
2. A report from the Manhattan District Attorney's office arguing for access to stored communications
3. An article by Susan Landau that provides background on laws we will be discussing today, in the context of the Snowden disclosures.

The lecture on one slide

Public policies on wiretapping and encryption

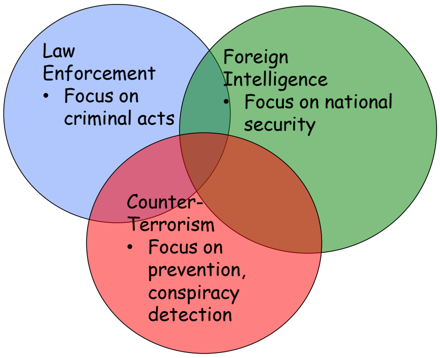
What a President needs to know about cryptography

Continuing from last week…

Surveillance for law enforcement
vs.
Surveillance for foreign intelligence
vs.
Surveillance for counter-terrorism

- What differences might there be in surveillance for these different purposes?
  - Take 3 minutes to consider: aims, scope
  - Discuss

Some Purposes for government surveillance



Law Enforcement
- Focus on criminal acts

Foreign Intelligence
- Focus on national security

Counter-Terrorism
- Focus on prevention, conspiracy detection

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act")

Added by ECPA, 1986

Why:
- Congressional investigations revealed extensive wiretapping by government agencies and private individuals without consent or legal sanction.
- Congress found that the contents of these tapped conversations and the evidence derived from them were being used by government and private parties as evidence in court and administrative proceedings.

What
- Title III provided a legal framework for wiretapping.
- Prohibits
  - Interception, use, or disclosure of wire, oral, or electronic communications UNLESS
    - A judge issues a <u>warrant</u> upon showing of <u>probable cause</u> that the intercept will reveal that the individual is committing or has committed or is about to commit a crime
  - There are also some exceptions for emergencies, system operations, comms "readily accessible to general public"and FISA (coming up)

Foreign Intelligence Surveillance Act (FISA), 1978

Why:
- Historically, President claimed authority for electronic surveillance for non-criminal, national security purposes (i.e., spying).
- FBI COINTELPRO abuses revealed in 1971 and more uncovered by Congress (Church Committee) in 1975 prompted the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978 as a means of authorizing and controlling such surveillance through warrants

What:
- FISA established that non-criminal electronic surveillances within the United States were only permissible for the purpose of collecting foreign intelligence and/or foreign counterintelligence.
- FISA set up a court (FISC) whose members were public but whose proceedings were secret to authorize (or not) such surveillances proposed by intelligence organizations
- FISA allowed warrantless wiretapping of communications outside the US and also communications terminating in the US if at least one party was outside the country (and this wasn't being used as a dodge to target a U.S. person

Electronic Communications Privacy Act, 1986

Why:
- Responding to advances in technology, including Signaling System 7 (SS7); telephone switch that made it easier to collect Call Detail Records (CDRs)

What:
- It's complicated. Distinguishes:
  - Wire communications: carrying human speech over wire, cable, or cellphone
  - Oral: by sound waves over the air
  - Electronic: any electronic communication not wire or oral (so includes email, fax (the Stored Communications Act is part of ECPA)
- Easily intercepted (e.g., unencrypted) radio communications not protected from eavesdropping
- Only a court order, not a warrant, needed for pen register. No "probable cause" demonstration required.
- Stored electronic communicatons: private interception prohibited; govt interception requires search warrant for unread mail stored for 180 days or less. Contents stored longer or stored after having been read are less protected.
- Also authorized "roving" wiretaps

Communications Assistance for Law Enforcement Act (CALEA) 1994

- Why:
  - Law enforcement not satisfied with ECPA and wanting better assistance for wiretaps
- What: CALEA required telecomm carriers to
  - design systems to quickly isolate call content, as well as origin/destination phone numbers
  - Provide this info to LE in a format and at a location of LE's choosing
- Funding provided to telecom suppliers to accomplish this
- Idea was to preserve government wiretap access in new environment, not to expand it
- FCC charged with overseeing implementation
- Controversial; took years to implement
- Extended to Internet and Voice of IP (VOIP), 2005

USA PATRIOT Act, 2001

- Why:
  - In the wake of 9/11 attacks, this act lowered the barriers between surveillance for national security / counterintelligence and law enforcement
- What:
  - Section 215 of the act enabled collection of "business records" for national intelligence purposes without a warrant.
    - This was thought to enable collection of individuals library records
    - It was used to justify NSA's massive collection of CDRs from US telephone networks.
      - Legality of this collection, when it was made public, became a significant matter of public debate and legal challenge
    - Revisions to the Act in 2015

FISA Amendments Act (FISAAA), 2008

- Why: Warrantless wiretapping program, initiated following 9/11 attacks, was revealed by New York Times in late 2005; reportedly discontinued January 2007
  - Substantial doubts raised as to whether the program was legal under existing laws
- What:
  - Added a Title VII, including Section 702
    - Authorizes Attorney General and Director of National Intelligence jointly to authorize targeting of individuals (non U.S. Persons) reasonably believed to be outside of the U.S.
    - Authorized the PRISM program of which you may have heard, and some others

USA Freedom Act, 2015

- Why:
  - June, 2013 Edward Snowden began releasing large volumes of classified data on NSA and GCHQ surveillance programs, evoking substantial public reaction, still ongoing
  - In particular, program to collect "meta-data" – CDRs of all U.S. phone calls challenged as illegal (litigation still ongoing)
- What:
  - Pres. Obama agreed to limit this program by having the telephone companies, rather than the government, hold this data, with the government allowed to query it under supervision
  - These limitations are incorporated in authorization of the program passed in the USA Freedom Act last June

Should we have export control legislation for weapons (munitions)? If so, why?

Munition:

military weapons, ammunition, equipment, and stores

<discuss>

Should cryptography be considered a munition?

<discuss>

Background of U.S. policy on cryptography

- Following World War II, Congress passed Arms Export Control Act (AECA) of 1949 to regulate munitions and the Export Administration Act (EAA) to regulate "dual-use" products (with military and civilian applications)
- ACEA is the basis of the International Traffic in Arms (ITAR) regulations, which defines a US Munitions List – items who export is controlled by Dept. of State
- EAA is the basis for Export Administration Regulations (EAR), which defines a list of "dual use" items, the Commerce Control List (CCL); EAR is administered by Dept. of Commerce
- Cryptography is classified as a munition
- Import and domestic use of cryptography has never been controlled (although it could be)
- Export of cryptography has been controlled, though the controls have been substantially relaxed since the 1980s.
- How might control of exports of cryptography affect domestic use of cryptography?
  - <discuss>

Brief History of Cryptography in the late 20th c.

- Following WWII, National Security Agency formed (1952) by President Truman, consolidating prior activities in military services
  - Its roots go back to WWI, and W.F. Friedman
- NSA aimed (and largely succeeded) in maintaining a monopoly on cryptography (both code making and code breaking) within the U.S. government for many years
- 1967: David Kahn, historian, published The Codebreakers, a massive history of cryptography and its significance, generating public interest
- 1976: Whit Diffie and Marty Hellman publish "New Directions in Cryptography", in *IEEE Trans. On Information Theory*, paving the way for public key cryptography. Ralph Merkle also a contributor
- 1978: Ron Rivest, Adi Shamir, and Len Adleman publish the RSA algorithm "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" in *Communications of the ACM*
- 1978: NBS (now NIST) release Data Encryption Standard (DES), based on algorithms developed by Horst Feistel at IBM
- Through the balance of the century, NSA generally maintains control of government cryptography while mildly discouraging outside research

Ref: Diffie and Landau: *Privacy on the Line*, MIT Press, 1998.

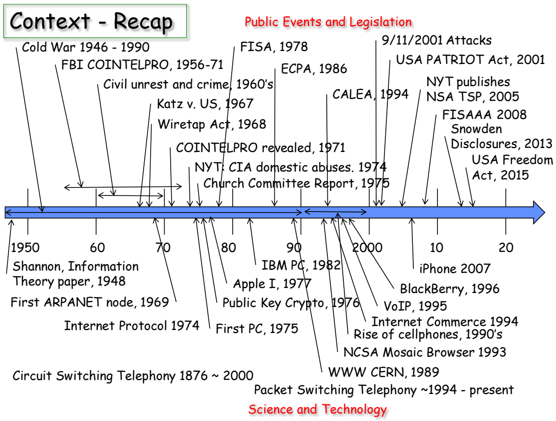
The "crypto wars" – 1990's

- 1992: AT&T's introduces a commercial phone with digital encryption, NSA is concerned about widespread commercial encryption
- 1993: Government announces "Escrowed Encryption Initiative"
  - Components "Clipper chip" using "Skipjack" encryption algorithm
    - Algorithm secret, embedded in hardware
  - Law Enforcement Access Field (LEAF) generate by chip as it encrypts message; same field needed at decryption end
  - LEAF when decrypted by a key unique to the chip will reveal the encryption key for the message
- Known as a "key escrow" scheme, because the LEAFs would be held by a third party, this proposal triggered a national debate
- Congress called for the National Research Council to study and report on the issues
- 1996: That report ultimately recommended that
  - The debate on cryptography policy could be public, not secret
  - No law should bar the manufacture, sale or use of any form of encryption within the U.S.
  - Export controls on DES products should be relaxed
- Ultimately these positions won the debate

Some Effects of U.S. Encryption Policies

- Ironically, the net result of the crypto wars was that ordinary telephone and data communications remained largely unencrypted. Commercial cryptography was not a success and the key escrow system wasn't either
- The lingering effect of earlier export controls led to weaknesses in Wired Equivalent Privacy – early encryption scheme for wireless networks based on IEEE 802.11:
    - Originally, the scheme was limited to 40-bit keys to make it exportable
    - The engineers knew that 40-bit keys would be easy to break, so they didn't worry too much about the details of the security protocols
    - When export controls were relaxed, key lengths were extended to 64 bits, much stronger, so people thought WEP would be good
    - But the unexamined protocols for keying the system proved to have serious flaws, leading to replacement by Wireless Protected Access (WPA), still in use

Context - Recap



Public Events and Legislation

Cold War 1946 - 1990

FBI COINTELPRO, 1956-71

Civil unrest and crime, 1960's

Katz v. US, 1967

Wiretap Act, 1968

COINTELPRO revealed, 1971

NYT: CIA domestic abuses. 1974

Church Committee Report, 1975

FISA, 1978

ECPA, 1986

CALEA, 1994

9/11/2001 Attacks

USA PATRIOT Act, 2001

NYT publishes NSA TSP, 2005

FISAAA 2008

Snowden Disclosures, 2013

USA Freedom Act, 2015

Shannon, Information Theory paper, 1948

First ARPANET node, 1969

Internet Protocol 1974

First PC, 1975

Public Key Crypto, 1976

Apple I, 1977

IBM PC, 1982

WWW CERN, 1989

NCSA Mosaic Browser 1993

Rise of cellphones, 1990's

Internet Commerce 1994

VoIP, 1995

BlackBerry, 1996

iPhone 2007

Circuit Switching Telephony 1876 ~ 2000

Packet Switching Telephony ~1994 - present

Science and Technology

What does a President need to know about crypto?

What cryptography can provide (not always all of these)

- Confidentiality – conceal "data in transit" or "data at rest" from eavesdroppers
- Integrity – assure that the data received hasn't been modified
- Authenticity – assure that the data came from a known sender

But:

- Although it's useful, it's also tricky to get right
    - Managing keys is particularly difficult
- It's important to understand what you are relying on
- It has been classed as a munition (and therefore subjected to export controls) because it can blow up in your face:
    - if you lose the key
    - if you depend on it, and it's broken

Terminology

- **Cryptography** – science of secret writing
    - **Cipher** (or **cryptoalgorithm**): secret method of writing that transforms **Plaintext** (= unencrypted) into **Ciphertext** (= encrypted) under control of a **Key**
- **Cryptanalysis** – science and study of breaking ciphers – trying to retrieve the plaintext from the ciphertext without knowing the key
- **Cryptographic protocol**: method for exchanging keys and data using cryptographic algorithms to achieve some desired end

Boolean Arithmetic

AND (written as ∧ or sometimes & or •):

$0 \wedge 0 \rightarrow 0$

$0 \wedge 1 \rightarrow 0$

$1 \wedge 0 \rightarrow 0$

$1 \wedge 1 \rightarrow 1$

OR (written as ∨ or sometimes ‖ or +):

$0 \vee 0 \rightarrow 0$

$0 \vee 1 \rightarrow 1$

$1 \vee 0 \rightarrow 1$

$1 \vee 1 \rightarrow 1$

Exclusive OR (XOR) : (A or B but not both)

$0 \oplus 0 \rightarrow 0$

$0 \oplus 1 \rightarrow 1$

$1 \oplus 0 \rightarrow 1$

$1 \oplus 1 \rightarrow 0$

Plaintext

Key

Ciphertext

Note: if you XOR twice with the same bit, you get back the original bit:

$0 \oplus 0 \rightarrow 0 \quad 0 \oplus 0 \rightarrow 0$

$0 \oplus 1 \rightarrow 1 \quad 1 \oplus 1 \rightarrow 0$

$1 \oplus 0 \rightarrow 1 \quad 1 \oplus 0 \rightarrow 1$

$1 \oplus 1 \rightarrow 0 \quad 0 \oplus 1 \rightarrow 1$