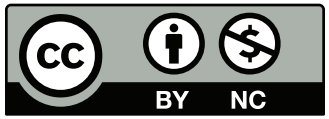
Wiretapping and Surveillance II



Snowden and the NSA

- Edward Snowden took a lot of documents from the NSA
- He gave them—many of them? most of them? all of them?—to a few reporters whom he trusted. (See Poitras' new documentary *Citizenfour*.)
- These documents have painted a broad, but not complete, portrait of the activities of the NSA and related organizations—and they lack context
- Some of these activities are customary for an intelligence agency; others are rather more surprising

How Did Snowden Get the Documents?

- Snowden was an employee of an NSA contractor
- He was the system adminstrator of some computers and networks in Hawaii
- He used the privileges of a sysadmin to override normal security controls
- It is unknown, apparently even internally, what he took or even how much

What is the NSA?

- Intercept other nation's communications
- ☞ Done by the Signals Intelligence Directorate (SID)
- Protect US communications
- ☞ Done by the Information Assurance Directorate (IAD)
- Also (of course) does cryptology, both creating and breaking mechanisms

Definitions

Cryptanalysis breaking codes and ciphers; ability to read traffic without knowing the key

Cryptography "secret writing"; creating codes and ciphers, and using them

Codes operate on semantic concepts; they're seldom used today.

Ciphers operate syntactically, i.e., on letters or bits, without regard to meaning.

Cryptology The academic field, including cryptography and cryptanalysis

SIGINT Signals Intelligence. Includes all forms of information, and includes (among other things) **COMINT** (communications intelligence) and **ELINT** (electronic intelligence)

HUMINT Human intelligence, i.e., spies

60-Second Cryptology Tutorial

- A cipher is a pair of mathematical functions:

$$\begin{aligned} C &\leftarrow F(K, P) \\ P &\leftarrow F'(K, C) \end{aligned}$$

  that use a *key* to map *plaintext* to *ciphertext* and ciphertext to plaintext
- A key is a large, random number
- If you know the key, you can convert ciphertext to plaintext
- If you don't, it should be impossible to invert the function
- It's always conceptually possible to try every possible key, so your design should have far more keys than can be tried
- Always assume that your enemy knows F and G

Public Key Cryptography

- Decryption may use a different key K' not derivable from K; this is called public key cryptography, because encryption key K can be public
- But K is derived from K'
- Public key crypto is at the heart of all Internet encryption
- Invented by Cocks and Ellis at GCHQ in 1970; they called it *non-secret encryption*
- Reinvented publicly by Diffie and Hellman in 1975; Ralph Merkle had some of the concepts, too

IAD

- Works with outside agencies and organizations to promulgate security technology
- Helps create encryption technology
- Develops computer security standards

The Groups Cooperate

- IAD learns from SID about vulnerabilities that should be fixed
- SID tries out their techniques against SID-protected systems
- There's an obvious tension here. . .

SIGINT is Traditional

- Clear, sophisticated descriptions of cryptanalysis in a 14th century Arabic book, implying a long history of practicing it.
- During the Renaissance, major European governments had "Black Chambers"—organizations that would intercept diplomats' mail, cryptanalyze them, and reseal the messages with forged seals
- (This implies that countries also had people devising codes)
- King Philip of Spain complained that King Henry of France must be using black magic to read his codes, since there was no other way they could be broken

☞ The pope did nothing, since his own Black Chamber had also broken the Spanish codes, without resorting to the supernatural. . .

SIGINT Continued in Importance

- Britain was the hub of the 19th century international telegraph network
- They used this to intercept other countries' messages
- Their own messages went via the "all red route": telegraph lines that only came ashore somewhere in the British Empire

The American Black Chamber

- The US did little of this, but learned rapidly during World War I
- Herbert Yardley, with money from the State Department and the War Department, created the post-war *American Black Chamber*; among other things, it spied on delegates' traffic during the 1921 Naval Disarmament Conference, with particular focus on Japan
- In 1929, new Secretary of State Henry Stimson declared "Gentlemen do not read each other's mail" and shut down the operation
- (Other countries didn't have the same attitude. . .)
- The military continued its SIGINT activities, including (during the 1930s) Japanese diplomatic traffic

Post-War SIGINT

- After World War II, there was the Cold War
- The US (mostly) abandoned its traditional isolationist policies, and did not disband its intelligence agencies
- In 1952, all SIGINT and cryptologic activity was moved to a new (and then-classified) organization: the NSA

Enter the Computer

- The NSA has *always* used computers for SIGINT
- The Army and Navy used standard and customized punch card equipment for cryptanalysis, starting around 1930
- During the 1950s and 1960s, the NSA was a major force behind the development of high-end computer technology
- Probably by 1965, they started using using computers to do cryptography (my opinion)
- Started developing bit-oriented ciphers no later than that (ditto)
- The NSA evaluated—and may have helped with and/or tampered with—the development of the Data Encryption Standard in 1976
- In the late 1970s, they started developing computer security standards

The Reality of Espionage

- Nations spy. They always have, and always will. Espionage will end some time well after a sustained outbreak of world peace.
- (Stimson's attitude was highly anomalous, and his attitude was only possible in a large, geographically isolated country with no nearby strong enemies)
- So why were Snowden's revelations so surprising?
- ☞ **Scale, targets, and techniques**

Scale

- The NSA is spying on far more targets than had been realized
- They're spying in far more ways than had been realized
- There were no major technical surprises—everything they've been revealed as doing had been seen as plausible—but their scale of operations was a surprise.

Targets

- Allies (e.g., German Chancellor Angela Merkle)
- Most Americans (or at least their metadata)
- Private companies (or their users' traffic), including American companies
- Diplomats at the London G20 summit (shades of Yardley!)

Techniques

- Hacking computers
- Sabotaging cryptologic standards
- Physically tampering with equipment shipments to selected targets
- Bribing companies to install “back doors”

Scale According to Rumor

- They're tapping large numbers of cables—apparently, even undersea fibers (US attack submarines, notably the *USS Jimmy Carter*, have long been believed to have that ability)
- Rumor has it that they listen to every phone call and every Internet connection, world-wide
- They have databases with all metadata information on all US phone calls. (Is that even legal?)
- They have partnerships with intelligence agencies in many other countries, notably the "Five Eyes" countries (US, UK, Canada, Australia, New Zealand), Israel, and many NATO countries

Scale: Reality Check

- Even the NSA can't listen to everything
- There's a *lot* of undersea fiber:
  `http://www.submarinecablemap.com`
- Processing voice takes too much CPU power—how do you plant that many computers (and their power lines!) under the sea?
- If they want to relay it all back to Fort Meade, they need a tremendous amount of fiber of their own
- The same is true for Internet traffic—and much, like Netflix and much of YouTube, just isn't interesting to them
- One of their hardest problems is figuring out what's interesting
- That said, they seem to pick up an awful lot

How Much Do They Intercept?

- According to outside estimates (guesses), they pick up less than $\frac{1}{1000}$ of traffic
- They then select less than $\frac{1}{1000}$ of that
- They probably use metadata to decide what content to grab
- (Most of us just aren't that interesting. . .)
- Very little of what is collected is actually useful

Is This Legal?

- Spying is not against international law
- Generally speaking, the NSA is not allowed to operate within the US
- But what about the metadata database (about 37% of Americans' calls)?

FISA: The Foreign Intelligence Surveillance Act

- For purely criminal cases, a warrant or other court order is necessary for wiretapping, getting metadata, etc.
- For foreign intelligence operations, it's considered a military function, under direction of the Commander-in-Chief; no warrants are needed
- But what about a foreign intelligence operation *within the US*? In particular, what about NSA collecting information about a "US person"?
- That is governed by FISA. A special (and secret) court can issue FISA warrants permitting such activities

Section 215

- Section 215 of the PATRIOT Act authorized access to "business records" for terrorism investigations
- The FISA court issued a (secret) order permitting bulk collection: metadata for all calls, from all carriers
- Note well: this did not include content. Also remember that under the law, metadata is only very lightly protected
- Members of the House and Senate Intelligence Committees knew that §215 was being used that way, but that was classified; most people did not know. Some Senators did warn that controversial things were happening.
- Conclusion: the NSA (mostly) acted within the scope of proper legal authorization, but the legality of those court orders has been challenged.

Section 702

- Section 702 of the FISA Amendments Act permitted "targeting" warrants
- ☞ Pick up traffic *about* a subject, if one end of the communication is abroad
- (The NSA appears to go to considerable effort to ensure that that requirement is met)

Targets

- That the NSA spies on, e.g., China or Iran isn't odd
- That it spies on NATO allies is rather more surprising
- They apparently gave GCHQ (the British equivalent of NSA) data on Britons; GCHQ couldn't legally monitor them itself
- They apparently listened in on the internal backbone nets of Google, Yahoo, etc. (Claims that this was done with the cooperation of those companies appear to be incorrect.)
- There has apparently been some economic espionage, but allegedly only to detect misbehavior (e.g., bribery or spying) by the target companies
- There seems to be a lot of "preparing the battlefield"—planting back doors in routers, computers, etc., against future need

Techniques

- Large-scale monitoring of major Internet links (but that's more or less their main job anyway)
- Cryptanalysis—but how much they can actually do is still unclear. Bruce Schneir has said "the math is still secure", but they can and do exploit implementation flaws
- Even for stuff they can break, the attack isn't free
- Hacking—they're *very* good at it

☞ New information suggests that they're worried that Iran has learned attack techniques from Stuxnet

- Sabotaging standards
- Bribing companies

Random Number Generator Standards

- Recall that cryptographic keys are supposed to be random numbers
- For complicated reasons, random numbers are used in other ways in cryptography; some of these values are transmitted unencrypted
- Computers are bad at randomness, so they use *pseudo-random generators* with a true-random *seed*:

static S
$S \leftarrow F(S)$
return $G(S)$

- G should not be invertible; an attacker who sees the output of the function should not be able to recover S

DUAL_EC_DBRG

- When NIST was standardizing some pseudo-random number generators, the NSA said “use this one”

☞ The scheme came from IAD!

- NIST was puzzled; it seemed very slow
- The NSA said “trust us; it’s necessary for national security”—but didn’t say why. . .
- NIST figured it was harmless to include: it was so slow that no one would use it
- Allegedly, though, the NSA paid RSA to make it the default in their popular BSAFE package
- BSAFE is heavily used for cryptography in embedded systems, including on-board encryptors for network cards

A Clever Design

- An invertible PRNG would be too dangerous; anyone else could read traffic
- DUAL_EC_DBRG is more clever than that: it's effectively a public key encryption system, and only the NSA knows the decryption key K'
- Result: the NSA can invert G; no one else can
- The possibilty was detected by outsiders, but it didn't draw much attention until the Snowden revelations confirmed it

The Results

- There have been many calls for reform of the NSA, and at least three different official investigations
- The NSA has changed some of its procedures, but no bills have made it through Congress yet
- It was the 1971 discovery of illegal FBI spying on the anti-Vietnam War movement that led to the passage of FISA—and that discovery was the result of illegal activity, too. . . (For details, read Medsger's *The Burglary* and watch the new documentary *1971*.)

International Reprecussions

- Some US allies are very, very annoyed
- Some countries are moving their data out of the US—but ironically, this may make them more vulnerable to the NSA, since the data is now abroad: no FISA warrant needed
- It has cost the US the moral high ground when it complains about China spying on US companies.

Computers Are Heavily Involved

- The scale would not be possible without computers
- Most of the exploits involve computers
- (The entire leadership of the NSA has a cyber background—that's where their energy is)
- But Snowden couldn't have taken as much if the records were all on paper (though 45 years ago, Daniel Ellsberg took a lot of paper documents)

What Do We Do?

- There are deep philosophical tradeoffs here: personal privacy versus national security; treatment of US persons versus everyone else; how to provide oversight of and accountability for a secret agency, how to treat (and how much to trust) allies, and more
- In intelligence, most *sources and methods* are very fragile; an enemy can move away from compromised schemes much more easily than the NSA can break new ones
- It's a hard area for Congress to control, partly because of secrecy but also because it's a very technical field
- Unless you reject the very concept of SIGINT, it's a very hard question