6.805/6.806/STS.085, Ethics and Law on the Electronic Frontier

Lecture 6: Technology-driven Public-Private Boundary Shifts

Lecturer: Hal Abelson

Encryption

Review of how encryption technology works. We will discuss the period of 1980 – 2001 really transformed a military, weapons technology to an everyday commonplace use. Really think about encryption as a policy stresses that are related to introduces new technology.

Pitfalls of tech and policy

-The word “privacy” has certain associations you make to it, none of them has the internet really associated with it.

- About 10 yrs. ago the word “electronic mail” had no real meaning because no one really used it.
- The image of a trusted mail carrier is not the image that we have when we speak of electronic mail and encryption

Confidentiality – you care about only the intended recipient receives the message
Authentication
Integrity – how do you know that someone didn’t intercept the message and
Non-repudiation – can’t later deny that you received the message

This is a review for those that took encryption.

These are referred to as digital signatures

1. Pre-historic cryptography (pre 1970s):
2. Public key
3. Policy of cryptography

Cryptography ca 1900 BC

This is the earliest believed formed of cryptography that people have found—heiroglyphics.

Geoffrey Chaucer was a poet and astronomer. Also wrote the first scientific manual in English *Treatise on the Astrolabe*. In part of this book, he encrypted. (class exercise)

Chaucer used a format called the substitution cipher. Simple or monoalphabetic substitution occurs when you always replace in the same way.

Julius Ceasar used substitution cipher where you shift everything by the same length to substitute.

In the 9th century, Yaqub wrote a book now know as Frequency analysis. (Graph of average frequency of letters in English.)

This is a technique since the 9th century.

A thousand years later, this form of encryption was still being used which is amazing. People still use insecure methods of encryption. If you go on the Internet (less than 5 years ago), some companies are still marketing insecure or bad encryption products.

*Vigenere Encryption

Vigenere popularized this type of encryption, but it was actually created by Alberti.

The blue letters are the key. “a” goes to “S”, b goes to “O”….and you cycle through each substitution.

This turned out to be a major breakthrough in encryption for 500 years, and was considered to be the unbreakable encryption scheme. In fact, it was broken in the middle of the 19th century.

*Breaking Vigenere
Turn this into n-different frequency distribution problems since the English language has a natural length.

The hard part is finding the length of the key.

At the end of the 1920’s, most countries had black-jammers that were math chambers to break encryption.

Friedman invented the Index of Coincidence to break the encryption. Nobody knew that Babbage had actually broken the Vigenere code until the 1920s since he didn’t announce that he broke it.

Many people that do the work actually don’t get the credit because their work ends up being classified.

Key is as long as the message – one time pad

Only proven secure encryption is the one-time pad, provided that you choose the key randomly and use it only once. But work is being done currently to find something more secure.

The Venona Project originated in 1943. Lots of examples of the one-time pad.

Claude Shannon – hero of information theory
Shannon invented the word the “bit.”

Shannon also made the first formal definition of what it means to be secure, or encryption.

Results of “Perfect Secrecy” from Shannon’s 1949 paper.

The really classified things right now are the ways and methods to generate random pads. It's actually hard to make really good one-time pads.

There's now a stream encryption that we use today that is the bit analog of Vigenere.

DES (Data Encryption Standard) is now becoming obsolete. The NSA tweaked the algorithm to make it more secure. For DES, you break the message into blocks of 64-bits and then do an S-box transformation (based on a 56-bit key) and then put it back together. This is pretty efficient since it is just scrambling and can be easily be decoded. Nicely designed so easy to undo.

Security of DES:
The only way to crack it is basically brute force. Try all the keys! In 1965, 2^56 was a pretty large number of keys. Not so much now.

The gov. was strong-arming people to discouraging using anything other than DES. NIST (National Institute of Standards and Technology).

Kerkhoffs's Principle:
Articulated by Belgium linguist that wrote a guidebook on the good properties of cryptographic systems. One of the principles is design the system so that only a tiny bit of information that needs to be secure, then this is a better design. The security should reside in the choice of key rather than in obscure design features.

Andrew "Bunnie" Huang – broke the encryption on the XBox. Digital Millenium Copyright Act prevents people from publishing or disseminating information about copyrightable material.

These early encryption principles don't work well for the internet.

Great Idea: Can create a shared key with people that have never met before or never communicated and made no prior arrangements.

Cryptosystems
Various types of attacks:
Chosen plaintext- 300 of the same character
Rubber hose – beat people with the rubber hose

None of this is adequate for Internet applications because you have to meet to exchange the key.

Diffie was an MIT undergrad and met up with Marty Hellman, who was working at Stanford. Ralph Merkle was a grad student at Berkeley. Merkle was probably the person with the idea behind public-key encryption, but Hellman and Diffie wrote the algorithm. They published the absolute break-through paper in 1976.

Only about 8 years ago, it was discovered that in 1973-74 Clifford Cocks and Malcolm Williamson were doing secret work in the British Intelligence.

Basic Idea of Diffie-Hellman-Merkle:

Idea: How can you exchange secret information even if everyone can hear what you say to one another?

Alice will compute secret information on only what she knows
Bob will compute secret information only on what he knows.
At the end, there will be a secret number that only Alice and Bob will know.

General Approach is to use a one-way function.

On one side of the coin you have a problem that you can do on any small calculator and on the other side, you have an intensively computational problem.

By the law of exponents, Bob and Alice end up computing the same number so they can use this as a shared key for encryption communication. For any eavesdroppers, this requires solving the discrete log problem (fast).

Digital Signature:
There is a thing that you can produce the signing that anyone can check but is hard to produce. Produce authentication and non-repudiation.

Certificates and Certifying Authorities
You finally get to a chain for a certification authority that is well know in order to certify authentication.

Basic Transport Layer Security Protocol (used to be known as SSL):
In this case, there is a client-side certificate that also verifies that you are who you say you are.

Diffie and Hellman didn't produce a practical method with public-key encryption. Later the RSA algorithm was produced. RSA could be used for both public-key and digital signatures. MIT and Stanford also sought patents. RSA was a good patent, but public-key was a weak patent. MIT and Stanford formed Public Key Partners and formed a cartel. They refused to license the public-key patent to others unless they also used the RSA patent. The public-key was locked up until 2001. Now there are lots of public-key encryptions floating around now.

End of 1970s and Bobby Ray, Director of NSA, became really nervous.

Encryption really was, and still is, a military weapon. The NSA began to speak up about this stuff getting out in public.

There was a meeting that ensued with MIT and NSA. MIT has been really reluctant to keep any work secret on campus. As a courtesy, they will send papers and information to NSA and other agencies along with colleagues.

Louis Freeh made this the top priority in the FBI. In 1994, encryption was an alien form of technology since it was feared to be used by criminals and terrorists.

Clipper
The public didn't want to use encrypted phones.
The clipper chip was designed by the NSA and people could do encrypted communications and it has a "built-in" back door.

So what do you think of this clipper phone? The telephone industry rejected it. A tamperproof chip would drive up costs.

The Key Escrow Wars

- consisted of complicated policy wars going back and forth
- agencies pushing to get their agendas adopted by Congress

Answer is Export Control.

If you were in the business of selling cryptographic software and products, you were registered as an arms dealer. Prior to 1995, encryption technology was classified by the State Dept. as ammunition.

CIILNKSS – Syria, Sudan, Libya countries excluded

There were rumors in 1995 that the NSA had a project that was listening in on all communications projects going on. This secret project that nobody else was speaking about was exactly what was happening.

Project Echelon listens to lots of communications around the world.

Eventually all of the talks and NIST meetings broke down. Building these systems is extremely cheap that most consumers don't realize.

May 1996

Ok, you guys can have your encryption but you have to register your key with an escrow. We're going to marry the idea of encryption and electronic commerce. The White House decided the price of certification and allowing electronic commerce was to escrow the key.

Legislation, 1997

There was a penalty for building electronics without an escrow key and a bill that forbade Congress from eliminated export of products.

In "The Risks of Key Recovery…" paper, it was decided that there would be no discussion on civil liberties. The structure of the paper is to address the risks of stopping crime and then investigate a technical analysis of their viewpoints.

Technical Observations:
Who else can get a hold of escrowed keys that government officials have quick access to.

Around 2000, the cryptography laws became liberalized. In 1994, every person or institution using the software must have a crypto license. This is a result of electronic commerce overtaking the industry.

Then came Sept. 2001…
Sen. Judd Gregg (NH) stands up in Congress and says we have to do something about encryption. It's essentially the legislation that was built into the 1997 legislation. The potential was now gone since the reality had hit. Not one other

senator agrees to co-sponsor this legislation. So by Oct, Sen. Gregg had backed off about introducing the legislation.

What has changed?

In 1995, the association with encryption and electronic mail was something different. Now encryption means protecting your credit cards, etc. Encryption has now become a consumer thing.

It's the meaning of words that has now shaped our technology and policy today. But this is probably not over yet.

Now we have to make another adjustment around the security around the phone. What kind of wiretapping authority should the gov. have? What about Internet applications like Skype? Do you have to comply with CALEA regulations?

Over the next couple of years, we will see more changes and maybe regulations about applications on the Internet.