02- Introduction to Security / Usable Encryption

Lorrie Cranor, Blase Ur, and Rich Shay

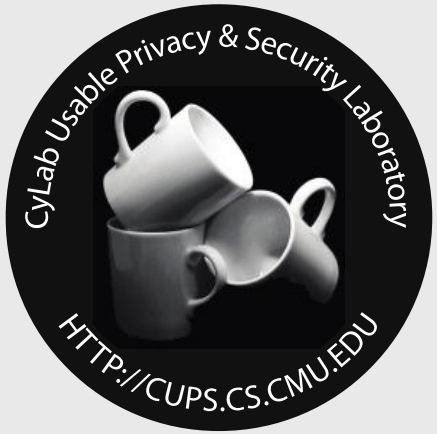
January 15, 2015

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy



Today's class

- Quick intro to security
- Quick intro to encryption
- Discussion of Johnny
- Why Glenn, like Johnny, couldn't encrypt
- The usability of Truecrypt

Intro to security

Computer security

- Key properties include:
  - Confidentiality (information isn't disclosed)
  - Integrity (information isn't changed)
  - Availability (information can be accessed)
- Other properties might be desirable:
  - Access control, Anonymity, Auditability, Authenticity, Privacy, Secrecy,…

What could go wrong?

- Attackers exploit bugs
  - Software/hardware bugs
  - Humans (social engineering)
  - Unintended characteristics (e.g., side channels, poor sources of randomness)

The Morris Worm

- Released in 1988, its stated purpose was to measure the size of the Internet
- Exploited three bugs:
  - An issue with debug in sendmail
  - Buffer overrun in fingerd
  - Remote logins using .rhost files
- Author was the first indicted under the Computer Fraud and Abuse Act of 1986
  - Where is he now?

Modeling the system

- What are our assets, and what is their cost?
  - What is the cost of an outage?
- What is the overall architecture?
- How does the system communicate?
- What humans are involved?
- How valuable is this system to attackers?
  - How valuable is it to us?
- What are we worried about?

Modeling the attacker

- What type of action will they take?
  - Passive (look, but don’t touch)
  - Active (look and inject messages)
- How sophisticated are they?
- How much do they care?
  - How much time will they spend?
- How much do they already know?
  - External / internal attacker?

Group exercise in attacker modeling

- Think about the security of a home
- Come up with at least two attacker models that lead to totally different ways of architecting security for the home
  - Be able to explain your attacker model
  - What is the threat you're worried about?
  - What is your defense?

Defending against attackers

- Legal or policy threats, but no “security”
- Strong “walls”
  - Cryptography, firewalls, etc.
- Redundancy
  - Multiple backup systems
- Detection
  - Intrusion detection systems
- Offense / counterattack

Allocating your resources

- It is impossible to stop everything
  - Time
  - Cost
  - People
  - You probably have better things to do
- What are the most likely threats?
- What are the possible consequences?
- What are relatively simple defenses?

Intro to encryption

Encryption

- Putting a message in code so that other people can’t read it
- Two main approaches:
  - Symmetric encryption (same key used for encryption and decryption)
  - Asymmetric encryption (keypair: public key and private key)

Encryption

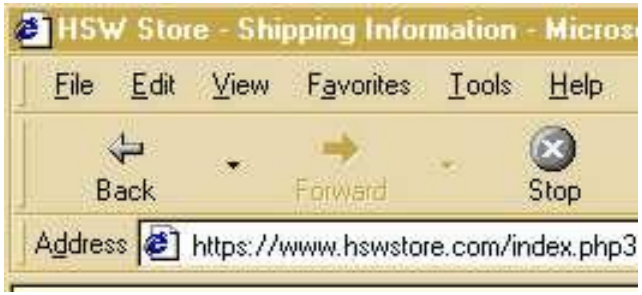
- What might you want to encrypt?
  - Hard drive (or some part of it)
  - Emails you send
  - Messages you send (off-the-record messaging)
  - “Everything” you’re sending when you’re browsing the web
  - (Many others)

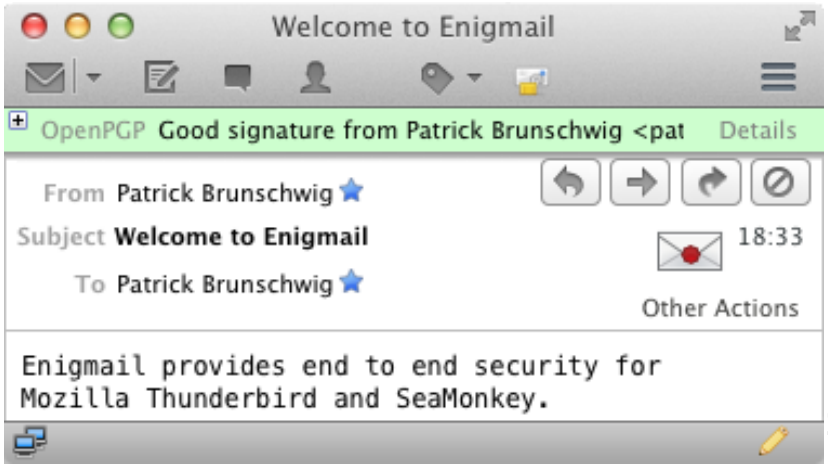
Properties of encryption

- Secrecy
  - Is Blase the only person who can decrypt my message?
- Authenticity
  - Did this message really come from Blase?
- Integrity
  - Has someone tampered with Blase's message?

Encrypting data in transit

- SSL/TLS
- VPN
- WPA/WPA2
- Email encryption
  - Client add-ons
    - Thunderbird/Enigmail/OpenPGP
    - Galaxkey
  - Web-based solutions
    - SendInc, JumbleMe
- Text messaging
  - CyanogenMod





Encrypting data at rest

- TrueCrypt
- File Vault (OSX)
- BitLocker (Windows)
  - Requires TPM (Trusted Platform Model) chip

Usability problems

- Encryption is rarely configured by default
- You need a good password
  - …and you can't lose it or forget it
- Public/private key encryption
  - How to get someone's public key?
  - How do I make it work on my phone?
- "Only paranoid people use encryption"

Lavabit

Ladar Levison, Lavabit CEO

Lavabit

My Fellow Users,

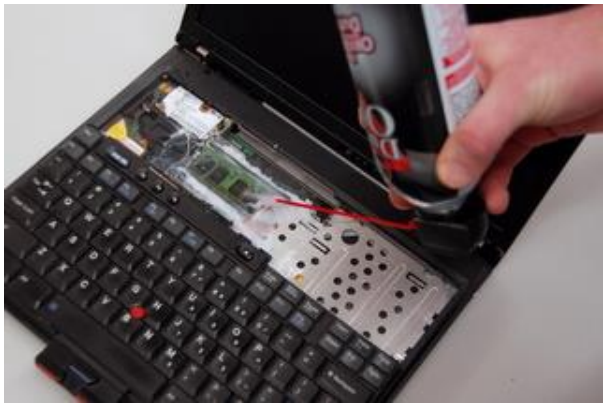
I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on--the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.

What's going to happen now? We've already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.

Sincerely,
Ladar Levison
Owner and Operator, Lavabit LLC

Cold booting



- DRAM does not lose its data instantly
  - Loses it on the order of seconds at room temperature
    - Hours if cooled
- If you store your keys and/or passwords in memory (like normal people), you are at risk!
  - How to prevent a cold boot attack?
- Halderman et. al describe cold booting in detail

Why Johnny Can’t Encrypt

Why was it so hard?

- “In order to complete this task, a participant had to generate a key pair, get the team members’ public keys, make their own public key available to the team members, type the (short) secret message into an email, sign the email using their private key, encrypt the email using the five team members’ public keys, and send the result.”

What makes usable security special?

- 1) “Unmotivated user” (secondary task)
- 2) Abstraction
- 3) The lack of feedback property
- 4) The barn door property
- 5) The weakest link property

Study principles

- Security tasks should come up organically
- Study participants should protect something of value
- Recruit participants who are likely users (did they do this?)

Design principles

- Make consequences clear (e.g., publishing or revoking a key)
- Hide advanced operations
  - “Users who are sophisticated enough to make intelligent use of that information are certainly sophisticated enough to go looking for it.”
- Have an initial wizard to explain ecosystem
- Defaults make sense (e.g., key backup)

Design principles

- Steps should make sense (revoking a key should lead you to publish revocation)
- Is tool use mandatory or voluntary?
- Avoid dangerous errors
- Encourage the user to keep using it
- Keep mental model in mind (e.g., keypairs)

Why Glenn Couldn’t Encrypt

The motivation

- Imagine that Ed wants to send a message to Glenn and worries that others might want to intercept his messages

What happened

- Snowden asked Greenwald for his PGP key
- “And yet, Greenwald still didn't bother learning security protocols. ‘The more he sent me, the more difficult it seemed,’ he says. ‘I mean, now I had to watch a f***ing video . . . ?’”
- http://vimeo.com/56881481

http://www.rollingstone.com/politics/news/snowden-and-greenwald-the-men-who-leaked-the-secrets-20131204

What happened

- Snowden ended up reaching out to Laura Poitras instead
- …you've probably heard the rest of the story

http://www.dailydot.com/politics/edward-snowden-gpg-for-journalists-video-nsa-glenn-greenwald/

Can you do better?

- In teams of 3-4, spend 5 minutes trying to develop a succinct introduction to email encryption (similar to what you just saw) for someone who knows nothing, but fears an attacker. This should be the first thing that is explained when they open an email encryption program the first time.

The usability of TrueCrypt

What is (was) TrueCrypt

- Disk encryption program
- Windows and Linux
- Anonymous developers
- Since discontinued under debated circumstances

Let’s check out the usability

- ☹