Usable Encryption

Usable Security and Privacy
2/27/14

Sean Segreti

Lecture Outline

- Kinds of encryption
- Usability problems
- Readings discussion
- Real-world example
- Exercise

Why encrypt things?

What things need encryption?

Why encrypt things?

- Personal privacy
- Business confidentiality
- Financial security
- “One more layer”

What things need encryption?

- Communications
  - Email
  - Online banking
  - Private correspondence
- Storage
  - Intellectual property
  - Personal details
  - Medical records
  - Things that could be plagiarized

Something to Keep in Mind...

- Grandma needs to digitally store her baby pictures of you. These pictures are in physical (paper) form, so she is scanning them into her computer. She may find another picture she wants to scan at any time.

- You will need to design a system that allows Grandma to easily encrypt and back up the pictures. Because these pictures are important, make sure there is no possible way the encryption keys or images could be lost or stolen.

Kinds of Encryption

- Symmetric
  - Requires all parties to agree on shared secret key
  - Order N2 keys
- Public/private key
  - Requires knowledge of recipient's public key to encrypt messages for them
  - Order N keys
  - Scalable public key infrastructure needed
    - pgp.mit.edu

Properties of Encryption

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

Encryption Software: Communications

Encryption Software: Communications

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

Encryption for communications is still inconvenient (mostly)

Encryption Software: Storage

Encryption Software: Storage

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

Usability Problems

- Encryption is rarely configured by default
  - Most users don’t know how or don’t want to go through the effort to do this.
- Symmetric key encryption
  - Password must be strong and not forgotten/lost.
- Public/private key encryption
  - How to get someone’s public key?
  - How to make it work on my phone?
  - Wait, I can’t read my email unless I have my keys?

Secrecy, Flagging, and Paranoia Takeaways

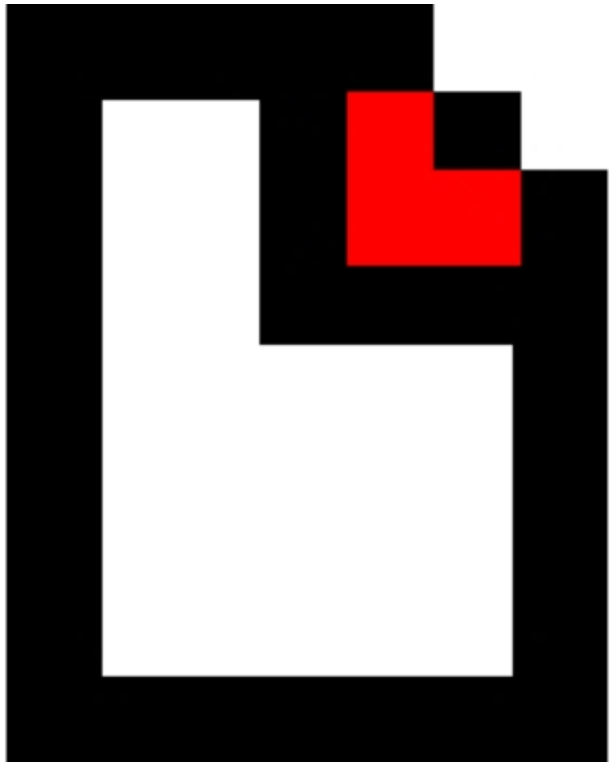
Gaw et. al

Secrecy, Flagging, and Paranoia Takeaways

Gaw et. al

- Where is the line between cautious and paranoid?
- Once a (secrecy) flag is set, people tend to maintain the flag.
- “Key management is without a doubt the most difficult issue in cryptographic systems.”
  - Encrypting is “really simple if everything is set up for you”

Lavabit



Ladar Levison, Lavabit CEO

Lavabit

My Fellow Users,

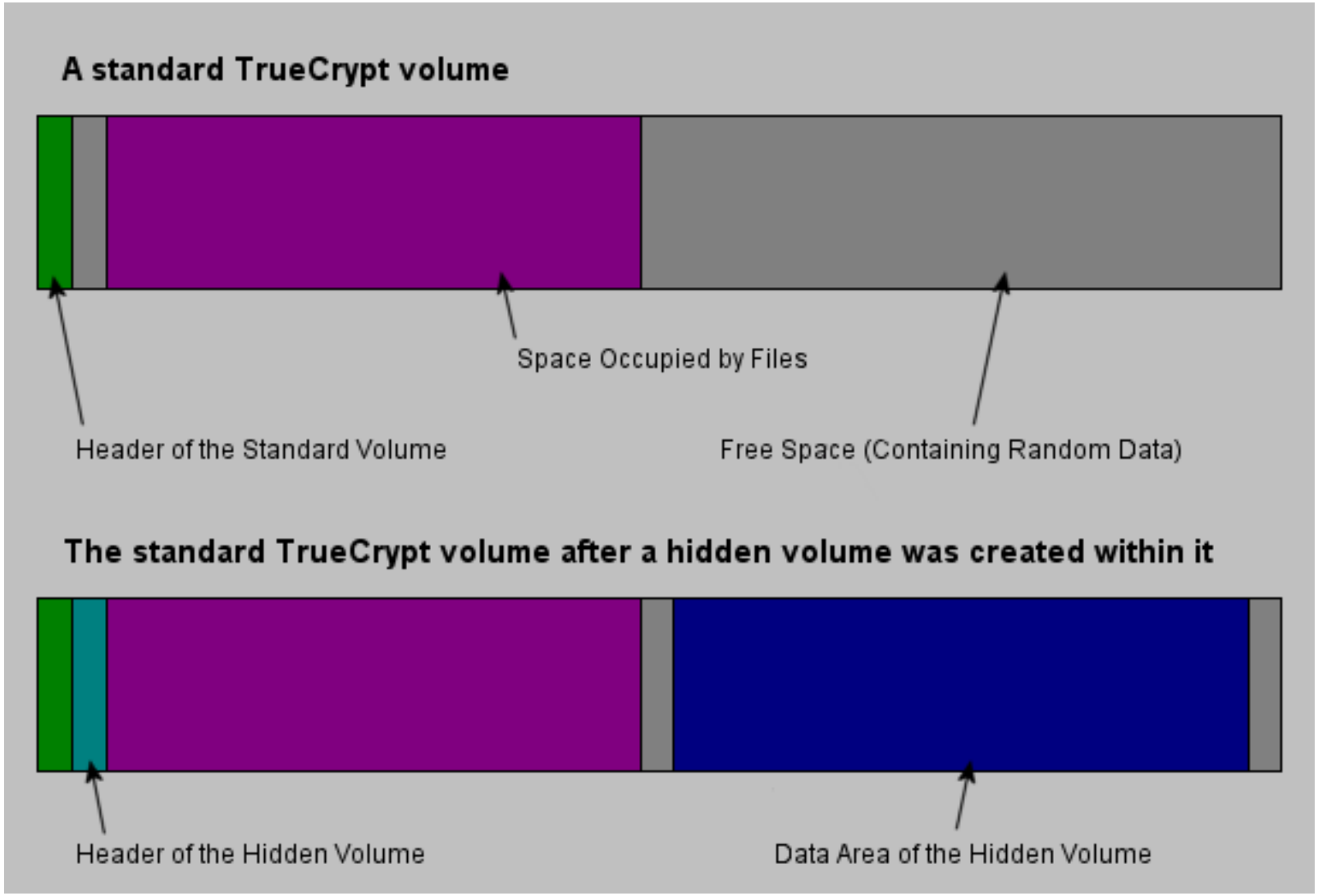
I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit. After significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events 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

If my keys can forcibly taken, what should I do?




BUT WAIT
SANDSTRÖM
ONTV COMPANY
THERE'S MORE
quickmeme.com

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 in the readings describes cold booting in detail

Design Exercise

- Groups of 4-5, 5 minute design time
- Grandma needs to digitally store her baby pictures of you. These pictures are in physical (paper) form, so she is scanning them into her computer. She may find another picture she wants to scan at any time.
- Design a system that allows Grandma to easily encrypt and back up the pictures. These pictures are your childhood, make sure there is no possible way the encryption keys or images could be lost or stolen.
- Groups will present their designs, and other groups will attempt to find flaws in the designs.