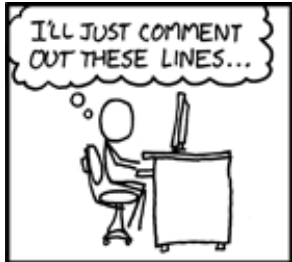


THE ETHICS OF ENCRYPTION

Abhi Devireddy

What's with the systems?

Everything's insecure



IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:



AFFECTED SYSTEM SECURITY PROBLEM

FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES



Steps to complete computer safety:

1. Unplug your computer
2. Move it to the basement
3. Add physical security

-Abhi Devireddy

Outline

- Introduction
- History of Encryption
 - Origin and Need
 - Early Ciphers
 - Modern Ciphers
 - Uses and Misuses
- Legal Aspects
- Controversies with Encryption
- Ethical Analysis of Encryption
 - Personal Issues
 - Professional Issues
 - Ethical Issues
 - Legal Issues
 - Kantian Evaluation
 - Utilitarian Evaluation

Introduction

- Encryption: Converting Plaintext to Ciphertext using an Algorithm (Cipher)
- Sender uses a secret in the cipher so that it is hard to get plaintext without the secret
- Receiver has prior knowledge of the secret so they can easily get to the plaintext
- Easy in one direction but hard in the other without the right knowledge
- Integrity of the message is based on the key and the cipher

Encryption algorithms (ciphers)

- What makes a good cipher?
 - ▣ Easy and fast encryption: O of the algorithm
 - ▣ Fast decryption with secret
 - ▣ Impossible to decrypt without secret
 - ▣ Language analysis is difficult
 - ▣ Higher Entropy: Hard to guess what the plaintext is
 - ▣ Ciphertext shouldn't be much larger than Plaintext
 - ▣ Diffusion: small change in plaintext \rightarrow large change in ciphertext

History of Encryption

- Closely correlated with how civilizations have developed
- Addresses our innate need for privacy
- Started with kings who wanted to send messages to generals who were at war
- Issues with trust in the message delivery mechanism
- Issues with validating integrity and authenticity of message

Need for Privacy

- We need privacy so that we may experience intimacy
- People have the right to, and should be given the freedom to share information with people of our choice
- This ability to choose who we share information with is vital in our society
- Encryption enables us to exercise this ability

Early Ciphers

- Caesar Cipher: Simple substitution cipher
 - Simple to crack
 - Low entropy: 1-1 substitution
 - Transposition is easy to perform
- Enigma Machine, WW II machines
 - First origins of modern ciphers
 - Higher entropy
 - Polyalphabetic Cipher
 - Took lots of research and manpower to crack

Modern Ciphers

- Consists of complex algorithms and computations performed by computers and microcontrollers
- Examples of modern ciphers in everyday life:
 - ▣ Transmitting Credit Card information on the internet
 - ▣ Logging in to Facebook or other online service
 - ▣ Sure of an emails origin and authenticity
- Very needed component of the internet
- Multiple ciphers in use on the internet, with varying keylengths
 - ▣ Rivest, Shamir and Adleman(RSA)
 - ▣ Advanced Encryption Standard(AES)
 - ▣ Data Encryption Standard(DES)
 - ▣ Triple Data Encryption Standard(3DES)
- Could be considered a hashing function (one way) without secret

Legal aspects of encryption

- As of 25th June 2010, restrictions were removed on software and encryption algorithms that made it possible to export these out of the country
- They were initially under controlled substances as they were classified as weapons, based on how they could aid criminals
- Dept. of commerce requires all companies selling encryption software to register with them
- Started with relaxation of some regulations in 1999 and took 11 years for the regulations to be removed
- Sanctions used to run as high as \$1,000,000 for exporting the software

Privacy for the common man

- PGP, Pretty Good Privacy was an encryption program aimed at the general public and was written by Phil Zimmerman
- Great example of how people can be given the power to choose
- Became very famous and useful in a short period of time
- Lots of emails and communications were being encrypted
- PGP became the defacto standard in sending and receiving encrypted emails and messages
- Gave people confidence to share confidential information over an insecure medium
- Enabled people to send and receive controversial emails
- Possible to verify who sent the message using a web of trust method
- Solved problems of Authentication and Integrity

How random is our random number generator

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
             // guaranteed to be random.  
}
```

RFC 1149.5 specifies 4 as the standard IEEE-vetted random number.

Encryption Controversies

- Given enough time and resources (computing power), all these encryption ciphers are breakable
- Modern ciphers take too long to be brute forced
- Rumors about the NSA and the FBI building in secret backdoors into AES
 - ▣ Designed to help with investigations and gathering evidence
- DRM is a form of encryption. Content is scrambled
 - ▣ CSS: Encrypts the media so its not readable without key
 - ▣ AACs: Encrypts all the info other than the metadata
- Bugs in programs that implement these algorithms
 - ▣ Debian Random Number Generator Bug
 - ▣ Reduced sample space of seed value to about 32,000 keys

Ethical Considerations and Evaluations

- Cryptography by itself is amoral
- Application of cryptography to processes gives us a framework and a structure to study it in
- Concerns with encryption
 - ▣ Criminals using it to hide illegal information
 - ▣ Law enforcement gaining access to passwords and other sensitive information
 - ▣ Users control over his personal information that is encrypted
 - ▣ Ethicality of having backdoors for legitimate purposes

Personal and Professional Issues

- Users have right to share information how and with who they want to
- Information in the private domain is off limits and out of bounds unless warranted by the law
- Companies have to deal with sensitive information and they need to encrypt this data
- Companies that store sensitive information have a lot of responsibility to make sure that this data is kept secure
- Depends on the company or the individual to guard the integrity and the security of the key and the cipher where applicable

Ethical Issues

- Is it right to coerce a criminal to reveal their private key passphrase if it would lead to further breakthroughs
- Is it right to limit access to a technology to a certain group of people based on their location
- What about people who want to just keep their information safe from prying eyes
- What about companies who have the best interests of their employees at heart
- Is there a fundamental need for encryption in the world

Legal Issues

- Freedom of speech
 - Article 19, Universal Declaration of Human Rights
- Right to privacy
 - Broadly defined as the right to be left alone
 - 1st amendment – Freedom to assemble
 - 4th amendment – Search and Seizure
 - 14th amendment – Due process right
- Right to withhold information?

Kantian Evaluation

- A person is coerced into revealing their password
 - ▣ Universal Rule: Everyone could be forced to reveal their passphrase to their private keys
 - ▣ Result of the universal rule: People have access to others messages, thus negating the need for encryption in the first place as everything is common knowledge now.
 - ▣ Thus this is a contradiction unto itself
 - ▣ We can conclude that coercion to reveal passwords is **UNETHICAL**

Utilitarian Evaluation

- Action: Employee of a company is forced to reveal a cipher and the associated keys
 - ▣ Good: Law enforcement saves a lot of time and money in getting to the root of the issue and finishes their investigation
 - ▣ Bad: According to best practices, the company needs to change all their keys and alert their users.
 - ▣ Here the bad affects more people and outweighs the good
 - ▣ Act Utilitarian evaluation shows this is **UNETHICAL**

Social Contract theory

- Contract Statement: Every one will reveal their passphrase when asked to do so
 - ▣ Result: Everyone has access to everyone else's keys and private messages, thus once again negating the need for encryption
 - ▣ Thus, according to Social Contract theory, coercion to reveal passwords is **UNETHICAL**

Ethical evaluation of the need for Ciphers

- People need to be able to transit information in private with another person. This provides for intimacy over an un-trusted medium.
- By a Kantian Evaluation, we can say this is a universal principle and is **Ethical**
- Using a Utilitarian evaluation, we can say that there is a lot of good coming from this, although it can be used for illegal purposes; thus this would be **Ethical** as well

Real World Issues

- The most important achievement of the operation wasn't killing Osama, It was the US Navy SEALs' booty: dozens of computers, memory sticks and disks loaded with information that might just crush all of al Qaeda's network.
- After shouting "Geronimo!" to their commander over radio—the signal that indicated the death of bin Laden from a shot above his eye—the SEALs grabbed all the electronic material they could find in the compound and ran with it and Osama's body to their custom MH-60 Black Hawk helicopters. With their weapons still hot, the commando handed the electronic material to a special team of CIA and military intelligence operatives. According to a US official, hundreds are going through the data in a secret location in Afghanistan. They cleaned it out.
- **Decrypting "the mother lode of intelligence"**
- We don't know if "the mother lode of intelligence"—as that official called it—in the hard drives and memory sticks is encrypted or not. But even if the data is encrypted, **the US intelligence agencies have the necessary computing power and the expertise to crack the information open, even if the terrorists are using the AES-256 standard. You can be sure that, if there are any encrypted files, they are now being processed by supercomputers at CIA's headquarters. The only question is how fast they can access the information.** That's the critical part: the fastest they get it, the more actionable that information would be, leading to the fast capture or killing of other leaders and operatives in the al Qaeda network.

Sources

- Aljifri, H., & Navarro, D. S. (2003). International Legal aspects of cryptography: Understanding cryptography. *Computers and Security* , 22 (3), 196-203.
- *Cryptography*. (n.d.). Retrieved April 23, 2011, from Wikipedia: <http://en.wikipedia.org/wiki/Cryptography>
- Daview, D. (1983). Applying the RSA Digital Signature to Electronic Mail. *Computer* , 16 (2), 55-62.
- *Encryption*. (n.d.). Retrieved April 14, 2001, from Wikipedia: <http://en.wikipedia.org/wiki/Encryption>
- Eskicioglu, A., & Litwin, L. (2001). Cryptography. *Potentials, IEEE* , 20 (1), 36-38.
- How Stuff Works. (n.d.). *How Encryption Works*. Retrieved April 20, 2011, from How Stuff Works: <http://computer.howstuffworks.com/encryption.htm>
- Konheim, A. G. (1981). *Cryptography, A Primer*. New York: Wiley.
- Mel, H. X., Baker, D., & Kinyon, J. (2001). *Cryptography decrypted*. Addison Wesley.
- Miller, M. S. (2000). *The Encryption Export Policy Controversy: Searching for Balance in the Information Age*. National War College, Washington DC.

Sources (contd.)

- Needham, R., & Schroeder, M. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM* , 21 (12).
- Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics and Behavior* , 207-219.
- Rivest, R. (1998). The case against regulating encryption technology. *Scientific American* .
- Schneier, B., & Sutherland, P. (1995). *Applied Cryptography: Protocols, Algorithms and Source Code in C*. New York: John Wiley & Sons.
- South Asian Network Operators Group. (2003, January 23-28). www.sanog.org. Retrieved April 17, 2011, from SANOG I: www.sanog.org/sanog1/networksecurity1.ppt
- US Department of Commerce. (2010, June 25). *Bureau of Industry and Security*. Retrieved March 15, 2011, from <http://www.bis.doc.gov/encryption/default.htm>
- Wayne Madsen, D. L. (1998, Spring). Cryptography and Liberty: An International Survey of Encryption Policy. *The John Marshall Journal of Computer and Information Law* .
- Zimmermann, P. (1995). *The Official PGP User's Guide*. MIT Press.