Regulation, Cryptography, and Internet Security

Steven M. Bellovin

smb@research.att.com

http://www.research.att.com/˜smb

+1 973-360-8656

AT&T Labs — Research

Florham Park, NJ 07932, USA

Why Encrypt?

- General Internet security: many security holes caused by lack of encryption.
- Guard against targeted spying.
- Guard against widespread “harvesting” of traffic.

Protecting Passwords

- Ordinary passwords are a very bad form of authentication, for many reasons.
- Password eavesdropping programs (commonly known as “sniffers”) are quite common.
- Encryption protects passwords from this threat (though there are still other problems with using passwords).

Cryptographic Authentication

- In some cases, we can use cryptographic techniques for authentication, instead of passwords.
- This use of cryptography does not require secrecy, so it is much less controversial.

But. . . Many applications don't support this. It isn't always easy to retrotfit. And some such techniques have bad side-effects.

Stimulating Commerce

- Consumers are afraid of Internet hackers.
- Encryption makes people *feel* more secure.
- Of course, some of this faith is misplaced, but encryption is important for electronic commerce.

One Site's Assurances

"Our secure server software (SSL) is the industry standard and among the best software available today for secure commerce transactions. It encrypts all of your personal information, including credit card number, name, and address, so that it cannot be read as the information travels over the Internet."

Preventing Crime

- Computer hacking is a crime
- Encryption, by blocking hacking attempts, can reduce crime.
- Other crimes can be prevented as well: credit card theft, spying, etc.

Hong Kong

From www.newsbytes.com:

> . . . Along with stronger fines, the Police are hoping for stronger encryption and the use of key recovery systems in the fight against hacking. Chan said the use of key escrow systems would enable companies to access their employee's e-mails and the police to access suspects' files. Meanwhile, stronger levels of encryption would make hacking more difficult and enhance public confidence in the network. "We definitely support strong encryption for e-commerce," he said. "The stronger the better; the greater the public confidence. We also support the individual's right to encrypt their data."

(I'll discuss key escrow later.)

Preventing Economic Espionage

- Intelligence agencies are known to spy on other countries' businesses.
- Some companies do the same thing.
- Widespread use of encryption can protect valuable information.

Cryptography in France

“The Government allowed itself time to reflect. After consulting those involved, experts and international partners, it became convinced that the dispositions which result from the law of 1996 are no longer appropriate. They strictly restrain the use of encryption in France, without allowing the authorities to efficiently combat criminal acts where encoding could facilitate dissimulation. They also make apparent a risk of isolation for France with regard to her main partners.

“The Government has therefore decided to opt for a fundamental change of direction, which aims to make the use of encryption totally permitted in France, while adapting the means at the disposal of the authorities to guarantee public liberty in this new environment and to combat the use of encoding methods for illicit ends.”

Economic Impact

- Developing cryptographic products is good for business.
- One study showed that export controls could cost the U.S. economy \$96,000,000,000 over five years.
- Restricting export or use of cryptography can hurt a country's economy!

Cryptography and National Security

- Yes, terrorists, drug dealers, and spies will use cryptography.
- They're also unlikely to abide by laws against it.
- Government purchases of "ordinary" encryption products, to protect its own, non-classified computers, is easier (and cheaper) if cryptography is widely available.
- Furthermore, a country's security also depends on its companies being protected — see above.

Restricting Cryptography

- Knowledge of cryptography is widespread.
- Anyone can get it or implement it.
- Easy-to-use cryptography isn't widespread — but the real enemies are motivated to use inconvenient schemes.
- In other words, restricting cryptography hurts only the legitimate users.

Key Escrow

- Some governments have proposed “key escrow” mechanisms. They won’t work.
- Key escrow requires a a very complex, highly secure infrastructure. Those are *very* hard to build.
- The escrow centers are a prime target for hacking by spies, drug dealers, terrorists, etc.

Conclusions

- Cryptography is necessary (though not sufficient) to secure the Internet.
- Government restrictions on cryptography hurt computer security, and often hurt national security as well.
- Key escrow mechanisms won't work.