Politics and Cryptography in the United States

Syval Lee
April 11, 2006

Outline
- Bill of Rights
- Security versus Freedom
- Current Trends in Computer Security
- Export Control on Cryptography
- Pretty Good Privacy (PGP)
- Results of Cryptography Control
- Current Status of Control
- Clipper Escrow
- VoIP Encryption
- Future Trends
- Conclusion

What are Your Rights?

Bill of Rights guarantees:
- Freedom of speech, association and assembly
- Freedom of the press, and religion
- Privacy (Amendment IV):
  - “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
- Freedom from unwarranted government intrusion into personal and private affairs
Security versus Freedom
- Balance between national security & law enforcement, and personal freedom
  - Law enforcement agencies would like to keep control of civilian encryption technologies
  - Rights advocates fight to expand their ability to distribute and use cryptographic products
  - Necessary to protect personal information to prevent identity theft or blackmail by criminals

Current Trends in Encryption Technology
- Increased use of Internet, e-commerce, electronic communications (e.g., Electronic Funds Transfers), wireless communication, e-government, leads to:
  - Increasing miniaturization of hardware-based encryption products
  - Increasing use of private and public key cryptography
  - Continued development of increasingly secure algorithms

Export Control on Cryptography
- In the past, U.S. Export Control Policy categorized many encryption items as “munitions-related”, and subject to applicable export laws
- Companies wanting to export strong encryption products was therefore required, under the Arms Export Control Act
  - Obtain individual licenses from the Office of Defense Trade Controls at the State Department, which includes a review by the National Security Agency
- Led to prohibition on the export of encryption products using DES algorithm (or stronger) for file and data encryption, except to financial institutions
Export Control on Cryptography

- Government believed that restricting access to DES prevented terrorists, criminals, hostile foreign powers from acquiring advanced encryption technology
- However, DES algorithm and DES-based encryption software was available on Internet
- Exported encryption products could only contain 40 bits (DES is 56 bits)
- In 1998, a $250,000 special-purpose machine cracked a DES-encrypted message in 56 hours
  - U.S. export controls were then relaxed to allow DES in exported products, further relaxed in 2000

Pretty Good Privacy (PGP)

- First developed by Phil Zimmermann in 1991
- Provides cryptographic privacy and authentication with keys always over 128 bits
- PGP violated the munitions export ban
  - Justice Department launched a 3-year criminal investigation of Zimmermann from 1993-96
- Since 2000, compliance with export regulations is much easier, and PGP no longer meets the definition of a non-exportable weapon

Results of Cryptography Control

- Difficult to control use of cryptography inside the U.S., so governments chose to control the access to American developments by others
- Some U.S. officials believe that availability of strong cryptographic algorithms has hampered the ability of NSA to interpret potentially hostile communications, and could have been prevented by not relaxing cryptography control
- Others feel that the controls discouraged incorporation of cryptographic tools into commercial products (e.g. Operating Systems), and significantly reduced trade
Current Status of Control

- Cryptography exports from the U.S. are now under the control of Commerce’s Bureau of Industry and Security
- Still some restrictions, even on mass market products, particularly in regard to rogue states or terrorist organizations
- Many cryptographic products, even consulting services, still require an export license

Clipper Escrow

- Law enforcement officials can obtain (with court order) both parts of a special key that allow them to decrypt transmissions encrypted with a particular hardware chip
- Developed by U.S. government, but the algorithm it used was classified as secret, so not subject to peer review and testing
- Public worried that it was insecure and allowed possible illegal government surveillance
- In 1998, encryption algorithms were declassified, one was Skipjack which was broken in a few days

VoIP Encryption

- VoIP utilizes an internet connection to place a phone call instead of traditional phone lines
- In Aug. 2005, Federal Communications Commission announced that the Communications Assistance for Law Enforcement Act (CALEA) applied to VoIP
  – Meant that all VoIP implementations sold in the U.S. had to be wire-tapped enabled
VoIP Encryption

- Currently, most VoIP is unencrypted, vulnerable to eavesdropping anywhere along the transmission path by hackers, criminals, government
- However, enabling wiretapping to VoIP would involve introducing surveillance capabilities into the network protocol stack
  - Internet Engineering Task Force (IETF) said that this could not be done securely, weaken Internet security

- However, even without CALEA applied to VoIP, it is still possible to wiretap at the application layer (by the VoIP Provider) or the link layer (monitoring the target’s network connection)
- If CALEA was extended to VoIP to help ease law enforcement use of wiretapping, it would be at the sacrifice of Internet security

Future Trends

- USA PATRIOT Act allows judges to grant government investigators to examine personal records on the basis of relevance to ongoing terrorist investigations instead of probable cause as outlined in 4th Amendment
  - Theoretically, this would eliminate the need of key escrow to examine the key request for ‘legitimacy’
- Numerous polls indicate that Americans are concerned that their civil liberties are being reduced in response to the government’s fight against terrorism
Future Trends

- U.S. Government appears to be leaning towards a more tolerant stance for cryptographic products in today’s increasingly networked society.
- New cryptography algorithms will continue to be developed and tested by the public, as it is the only way to ensure that it is reliable.
- New technologies will continually push for redefinition of current laws regarding their use in public and criminal investigations.

Conclusion

- Cryptography can be used with malicious intent, when it actually designed to protect people’s privacy.
- Necessary to find a balance between the need of the public for privacy and the need of the law enforcement agencies for surveillance.
- Zimmermann believes that “the world was better off with cryptography in the hands of the masses rather than just in the hands of government.”

References