Encryption and electronic evidence-gathering

Enigma Machine

Encryption

- Plaintext
- Cipher (Algorithm) + Key
- Ciphertext

Simple Encryption

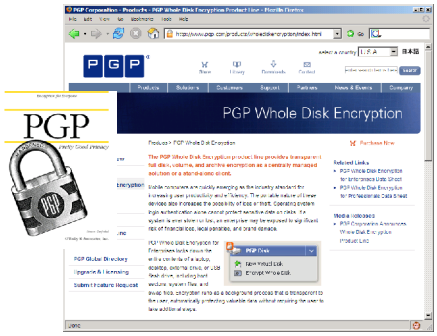
- Plaintext: “HELLO WORLD”
- Cipher, Key: shift forward, 3 letters
- Ciphertext: “KHOOR ZRUOG”

Decryption of Simple Cipher

- Ciphertext: “KHOOR ZRUOG”
- Cipher, Key: shift **backwards**, 3 letters
- Plaintext: “HELLO WORLD”
- Decryption reverses the process, using the same or a related algorithm.

Public-key encryption

- Each participant to the communication generates a pair of mathematically related keys, one public and one private.
  - One-way functions make this keypair computationally easy to create, but very difficult to reverse.
  - Messages encrypted with the public key can be decoded with the private key, and vice versa.
  - The basis of PGP and digital signatures.

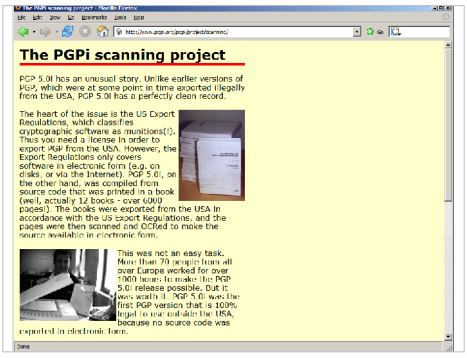


Regulating encryption

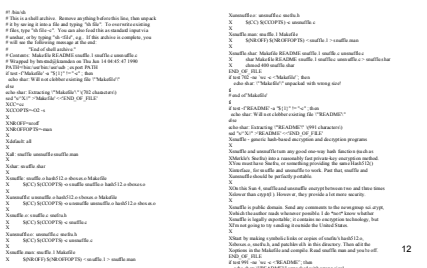
- Law
  - International Traffic in Arms Regulations (ITAR) / Bureau of Export Adminstration (BXA) Export Administration Regulations (EAR)
  - Clipper
- Market
  - Government market pressure
- Technology
  - Greater processing power makes it easier to use strong encryption, easier to crack weak encryption
- Norms
  - How many people use encryption?

How does encryption fit the law?

- First Amendment?
- Fourth Amendment?
- Fifth Amendment?

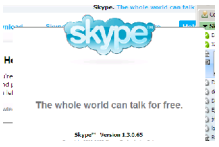


Snuffle



Everyday uses of encryption

- Securing communications
- Securing commerce
- Digital signatures



Encryption's uses

The same mathematics can be used to provide

- Privacy/Secrecy
- Authentication
- Verification of data integrity
- Non-repudiation

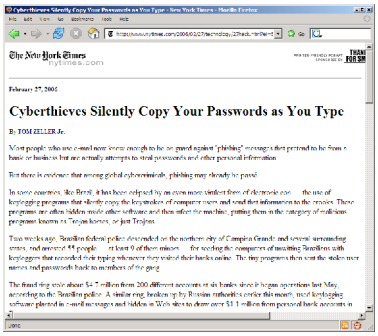
How can you gain access to an encrypted communication?

United States v. Scarfo

- Recognizing that Scarfo's computer had a modem and thus was capable of transmitting ***electronic communications*** via the modem, the F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports… To do this, the F.B.I. designed the component "so that each keystroke was evaluated individually." As Mr. Murch explained: The default status of the keystroke component was set so that, on entry, a keystroke was normally not recorded. Upon entry or selection of a keyboard key by a user, the KLS checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity, meaning that the modem was not using any port at that time, then the keystroke in question would be recorded.

Why does everything turn into a wiretap question?

- Were the FBI's precautions necessary?
- Should the FBI have taken more/different precautions against capturing non-key data?
- Is a message being prepared for communication subject to interception or search?



The New York Times
nytimes.com

February 27, 2005

Cyberthieves Silently Copy Your Passwords as You Type

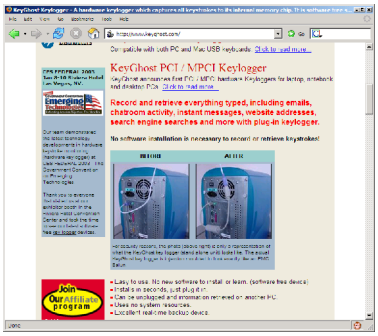
By TOM ZELLER Jr.

19

Keylogging Kriminals?

- Jane suspects that her husband John is concealing something from her, since he spends lots of time on the computer with his office door closed. Searching the web for surveillance tools leads her to "KeyGhost," a piece of hardware that connects to the computer and logs keystrokes.

20



KeyGhost PCI / MPCI Keylogger

Record and retrieve everything typed, including emails, chatroom activity, instant messages, website addresses, search engine searches and more with plug-in keylogger.

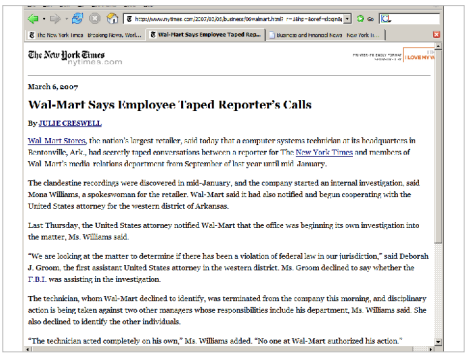
No software installation is necessary to record or retrieve keystrokes!

21

Keylogging Kriminals?

- If Jane installs KeyGhost on the family computer, has she committed a crime?
- While Jane is entering the office to install KeyGhost, she spots checks for large sums of money – which she knows haven't gone into the family account. She calls the DA's office to ask for advice. You pick up the phone. What advice would you give?

22



The New York Times
nytimes.com

March 6, 2007

Wal-Mart Says Employee Taped Reporter's Calls

By JULIE CRESWELL

Wal-Mart Stores, the nation's largest retailer, said today that a computer systems technician at its headquarters in Bentonville, Ark., had secretly taped conversations between a reporter for The New York Times and members of Wal-Mart's media relations department from September of last year until mid-January.

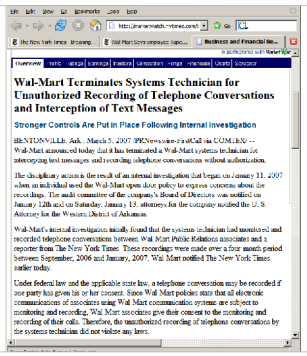
The clandestine recordings were discovered in mid-January, and the company started an internal investigation, said Mona Williams, a spokeswoman for the retailer. Wal-Mart said it had also notified and begun cooperating with the United States attorney for the western district of Arkansas.

Last Thursday, the United States attorney notified Wal-Mart that the office was beginning its own investigation into the matter, Ms. Williams said.

"We are looking at the matter to determine if there has been a violation of federal law in our jurisdiction," said Deborah J. Groom, the first assistant United States attorney in the western district. Ms. Groom declined to say whether the F.B.I. was assisting in the investigation.

The technician, whom Wal-Mart declined to identify, was terminated from the company this morning, and disciplinary action is being taken against two other managers whose responsibilities include his department, Ms. Williams said. She also declined to identify the other individuals.

"The technician acted completely on his own," Ms. Williams added. "No one at Wal-Mart authorized his action."



Wal-Mart Terminates Systems Technician for Unauthorized Recording of Telephone Conversations and Interception of Text Messages

Stronger Controls Are Put in Place Following Internal Investigation

24