# A Gift of Fire

Third edition

Sara Baase

## Chapter 5: Crime

Slides prepared by Cyndi Chie and
Sarah Frye

# What We Will Cover

- Hacking
- Identity Theft and Credit Card Fraud
- Scams and Forgery
- Crime Fighting Versus Privacy and Civil Liberties
- Laws That Rule the Web
- Will crime cease to exist?

# What We Will Cover 2

- Will crime cease to exist?
  - adaptive vs. maladaptive
  - job security for law enforcement
- Can crime be prevented?

- http://csc.csudh.edu/suchenek/CSC301/Censorship_and_prevention.pdf

# Hacking

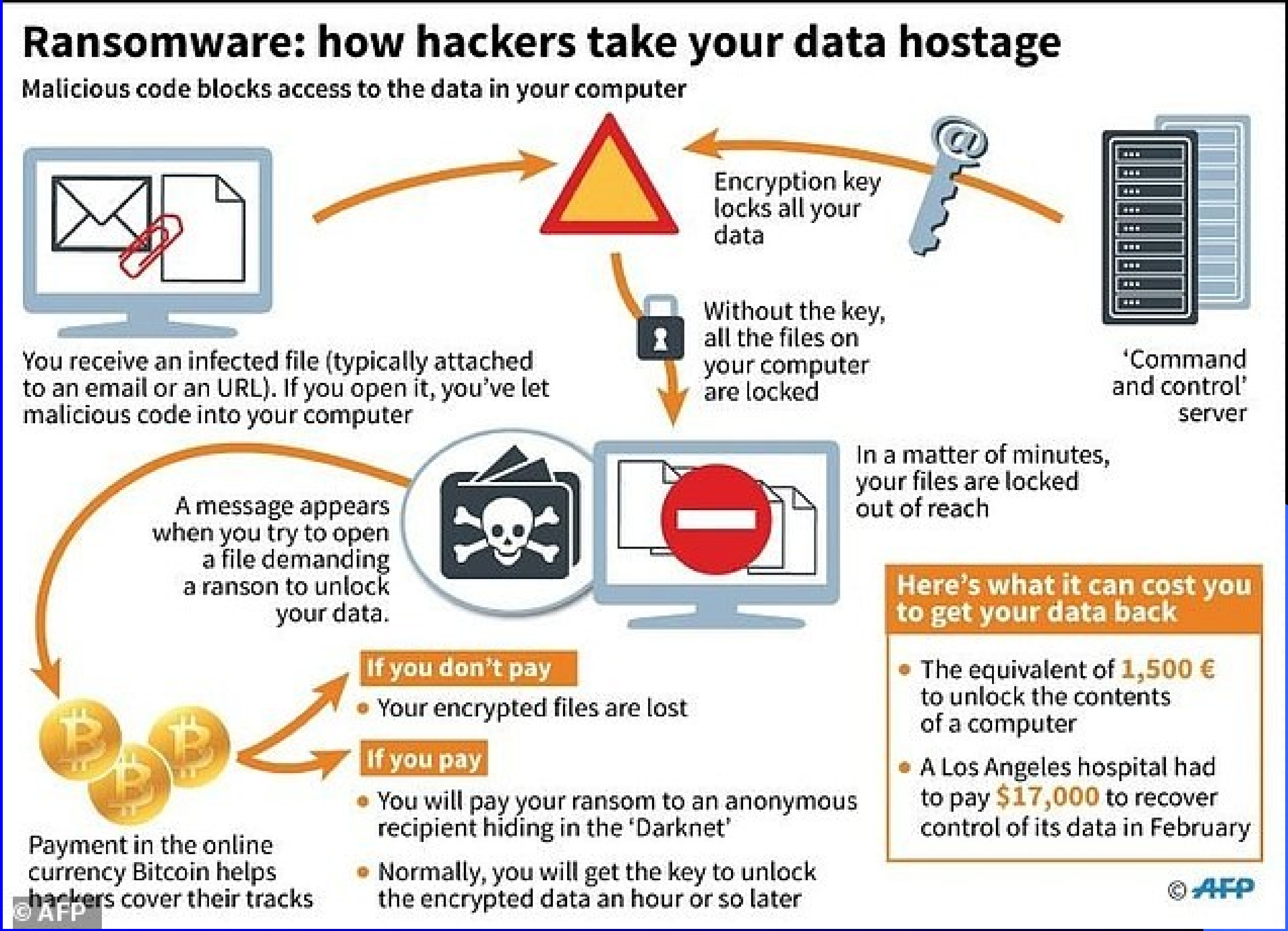
- Hacking – currently defined as to gain illegal or unauthorized access to a file, computer, or network
- The term has changed over time
- Phase 1: early 1960s to 1970s
  - It was a positive term
  - A "hacker" was a creative programmer who wrote elegant or clever code
  - A "hack" was an especially clever piece of code

# Hacking (cont.)

- Phase 2: 1970s to mid 1990s
  - Hacking took on negative connotations
  - Breaking into computers for which the hacker does not have authorized access
  - Still primarily individuals
  - Includes the spreading of computer worms and viruses and ‘phone phreaking’
  - Companies began using hackers to analyze and improve security

# Hacking (cont.)

- Phase 3: beginning with the mid 1990s
  - The growth of the Web changed hacking; viruses and worms could be spread rapidly
  - Political hacking (Hacktivism) surfaced
  - Denial-of-service (DoS) attacks used to shut down Web sites
  - Large scale theft of personal and financial information



# Ransomware: how hackers take your data hostage

Malicious code blocks access to the data in your computer

You receive an infected file (typically attached to an email or an URL). If you open it, you've let malicious code into your computer

Encryption key locks all your data

'Command and control' server

Without the key, all the files on your computer are locked

In a matter of minutes, your files are locked out of reach

A message appears when you try to open a file demanding a ranson to unlock your data.

Payment in the online currency Bitcoin helps hackers cover their tracks

**If you don't pay**

- Your encrypted files are lost

**If you pay**

- You will pay your ransom to an anonymous recipient hiding in the 'Darknet'
- Normally, you will get the key to unlock the encrypted data an hour or so later

**Here's what it can cost you to get your data back**

- The equivalent of **1,500 €** to unlock the contents of a computer
- A Los Angeles hospital had to pay **$17,000** to recover control of its data in February

# Hacking (cont.)

Hacktivism, or Political Hacking:

- Use of hacking to promote a political cause
- Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished
- Some use the appearance of hacktivism to hide other criminal activities
- How do you determine whether something is hacktivism or simple vandalism?

# Hacking (cont.)

The Law: Catching and Punishing Hackers:

- 1986 Congress passed the Computer Fraud and Abuse Act (CFAA)
  - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
  - The USA Patriot Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems

# Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- A variety of methods for catching hackers
  - Law enforcement agents read hacker newsletters and participate in chat rooms undercover
  - They can often track a handle by looking through newsgroup archives
  - Security professionals set up ‘honey pots’ which are Web sites that attract hackers, to record and study
  - Computer forensics is used to retrieve evidence from computers

# Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- Penalties for young hackers
  - Many young hackers have matured and gone on to productive and responsible careers
  - Temptation to over or under punish
  - Sentencing depends on intent and damage done
  - Most young hackers receive probation, community service, and/or fines
  - Not until 2000 did a young hacker receive time in juvenile detention

# Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- Security
  - Internet started with open access as a means of sharing information for research
  - Attitudes about security were slow to catch up with the risks
  - Firewalls are used to monitor and filter out communication from untrusted sites or that fit a profile of suspicious activity
  - Security is often playing catch-up to hackers as new vulnerabilities are discovered and exploited

# Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- Responsibility for Security
  - Developers have a responsibility to develop with security as a goal
  - Businesses have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding
  - Home users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware)

# Hacking
# Discussion Questions

- Is hacking that does no direct damage or theft a victimless crime?
- Do you think hiring former hackers to enhance security is a good idea or a bad idea?  Why?

# Identity Theft and Credit Card Fraud

Stealing Identities:

- Identity Theft –various crimes in which a criminal or large group uses the identity of an unknowing, innocent person
  - Use credit/debit card numbers, personal information, and social security numbers
  - 18-29 year-olds are the most common victims because they use the web most and are unaware of risks
  - E-commerce has made it easier to steal card numbers and use without having the physical card

# Identity Theft and Credit Card Fraud (cont.)

Stealing Identities (cont.):

- Techniques used to steal personal and financial information
  - Phishing - e-mail fishing for personal and financial information disguised as legitimate business e-mail
  - Pharming - false Web sites that fish for personal and financial information by planting false URLs in Domain Name Servers
  - Online resumes and job hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft

# Identity Theft and Credit Card Fraud (cont.)

Stealing Identities (cont.):

- Techniques used to protect personal and financial information
  - Activation for new credit cards
  - Retailers do not print the full card number and expiration date on receipts
  - Software detects unusual spending activities and will prompt retailers to ask for identifying information
  - Services, like PayPal, act as third party (escrow) allowing a customer to make a purchase without revealing their credit card information to a stranger

# Identity Theft and Credit Card Fraud (cont.)

Responses to Identity Theft:

- Authentication of e-mail and Web sites
- Use of encryption to securely store data, so it is useless if stolen
- Authenticating customers to prevent use of stolen numbers, may trade convenience for security
- In the event information is stolen, a fraud alert can flag your credit report; some businesses will cover the cost of a credit report if your information has been stolen

# Identity Theft and Credit Card Fraud (cont.)

Biometrics:

- Biological characteristics unique to an individual
- No external item (card, keys, etc.) to be stolen
- Used in areas where security needs to be high, such as identifying airport personnel
- Biometrics can be fooled, but more difficult to do so, especially as more sophisticated systems are developed

# Identity Theft and Credit Card Fraud
# Discussion Questions

- What steps can you take to protect yourself from identity theft and credit card fraud?
- How can you distinguish between an e-mail that is a phishing attempt and an e-mail from a legitimate business?

# Scams and Forgery

Auctions:

- FTC reports that online auction sites are one of the top sources of fraud complaints
  - Some sellers do not send items or send inferior products
  - Shill bidding is used to artificially raise prices
  - Sellers give themselves or friends glowing reviews to garner consumer trust
- Auction sites use various techniques to counter dishonest sellers

# Scams and Forgery (cont.)

- Click fraud - repeated clicking on an ad to either increase a site’s revenue or to use up a competitor's advertising budget
- Stock fraud - most common method is to buy a stock low, send out e-mails urging others to buy, and then sell when the price goes up, usually only for a short time
- Digital Forgery - new technologies (scanners and high quality printers) are used to create fake checks, passports, visas, birth certificates, etc., with little skill and investment

# Crime Fighting Versus Privacy and Civil Liberties

Search and Seizure of Computers:

- Requires a warrant to search and seize a computer
  - Court rulings inconclusive about whether information found on computers, but not covered by a warrant, is considered in ‘plain view’
- Automated searches
  - Can monitor constantly and less likely to miss suspicious activity
  - Can be programmed to only look for what is covered in a warrant

# Crime Fighting Versus Privacy and . . . (cont.)

The Issue of Venue:

- Charges are generally filed where the crime occurs
- Laws differ between states and countries
- Where charges are filed may have significant impact if community standards apply
- The FBI usually files in the state where the crime was discovered and the investigation began

# Crime Fighting Versus Privacy and . . . (cont.)

Cybercrime Treaty:

- International agreement to foster international cooperation among law enforcement agencies of different countries in fighting copyright violations, pornography, fraud, hacking and other online fraud
- Treaty sets common standards or ways to resolve international cases

# Whose Laws Rule the Web

When Digital Actions Cross Borders:

- Laws vary from country to country
- Corporations that do business in multiple countries must comply with the laws of all the countries involved
- Someone whose actions are legal in their own country may face prosecution in another country where their actions are illegal

# Whose Laws Rule the Web (Cont.)

Arresting Foreign Visitors:

- A Russian citizen was arrested for violating the DMCA when he visited the U.S. to present a paper at a conference; his software was not illegal in Russia
- An executive of a British online gambling site was arrested as he transferred planes in Dallas (online sports betting is not illegal in Britain)

# Whose Laws Rule the Web (Cont.)

Libel, Speech and Commercial Law:

- Even if something is illegal in both countries, the exact law and associated penalties may vary
- Where a trial is held is important not just for differences in the law, but also the costs associated with travel between the countries; cases can take some time to come to trial and may require numerous trips
- Freedom of speech suffers if businesses follow laws of the most restrictive countries

# Whose Laws Rule the Web Discussion Questions

- What suggestions do you have for resolving the issues created by differences in laws between different countries?
- What do you think would work, and what do you think would not?