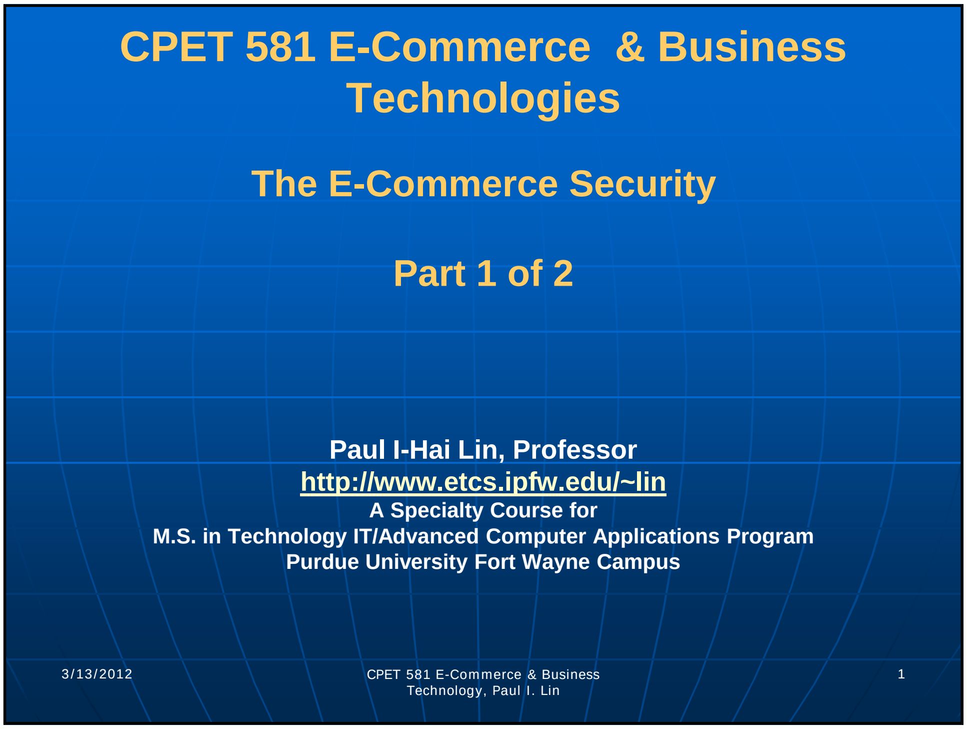
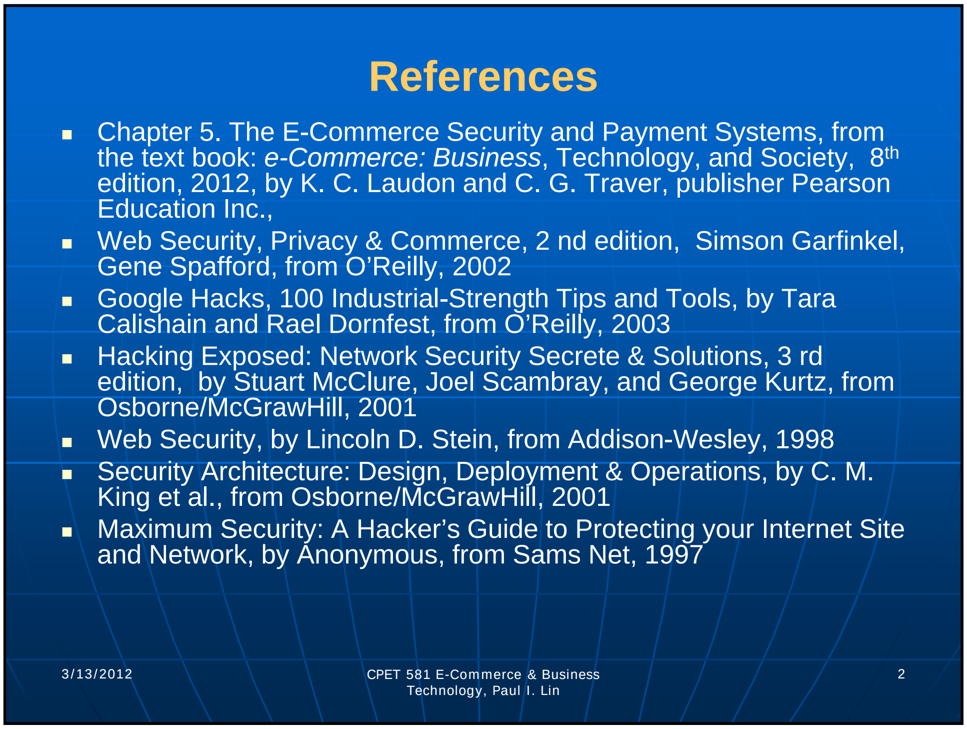


CPET 581 E-Commerce & Business Technologies

The E-Commerce Security

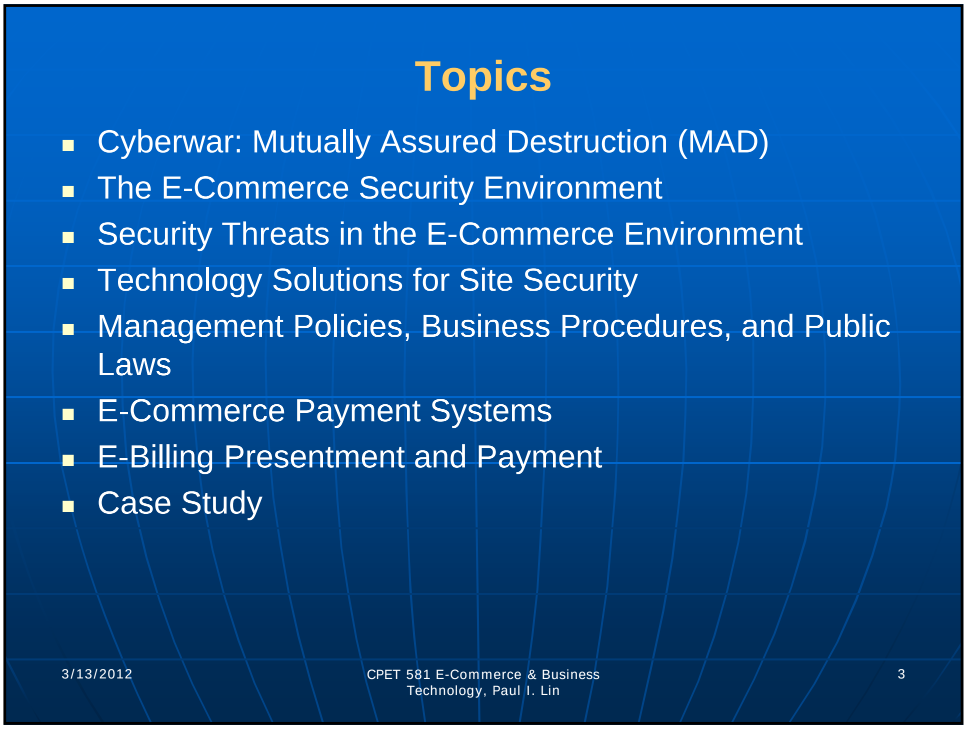
Part 1 of 2

Paul I-Hai Lin, Professor
http://www.etcs.ipfw.edu/~lin
A Specialty Course for
M.S. in Technology IT/Advanced Computer Applications Program
Purdue University Fort Wayne Campus



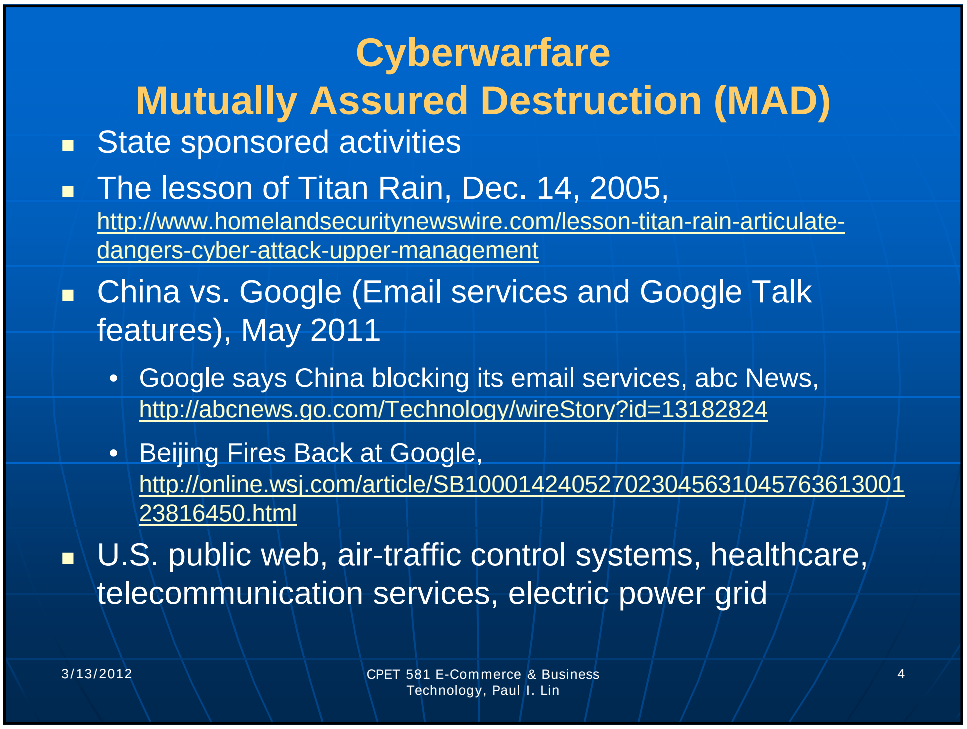
References

- Chapter 5. The E-Commerce Security and Payment Systems, from the text book: *e-Commerce: Business*, Technology, and Society, 8th edition, 2012, by K. C. Laudon and C. G. Traver, publisher Pearson Education Inc.,
- Web Security, Privacy & Commerce, 2 nd edition, Simson Garfinkel, Gene Spafford, from O’Reilly, 2002
- Google Hacks, 100 Industrial-Strength Tips and Tools, by Tara Calishain and Rael Dornfest, from O’Reilly, 2003
- Hacking Exposed: Network Security Secrete & Solutions, 3 rd edition, by Stuart McClure, Joel Scambray, and George Kurtz, from Osborne/McGrawHill, 2001
- Web Security, by Lincoln D. Stein, from Addison-Wesley, 1998
- Security Architecture: Design, Deployment & Operations, by C. M. King et al., from Osborne/McGrawHill, 2001
- Maximum Security: A Hacker’s Guide to Protecting your Internet Site and Network, by Anonymous, from Sams Net, 1997



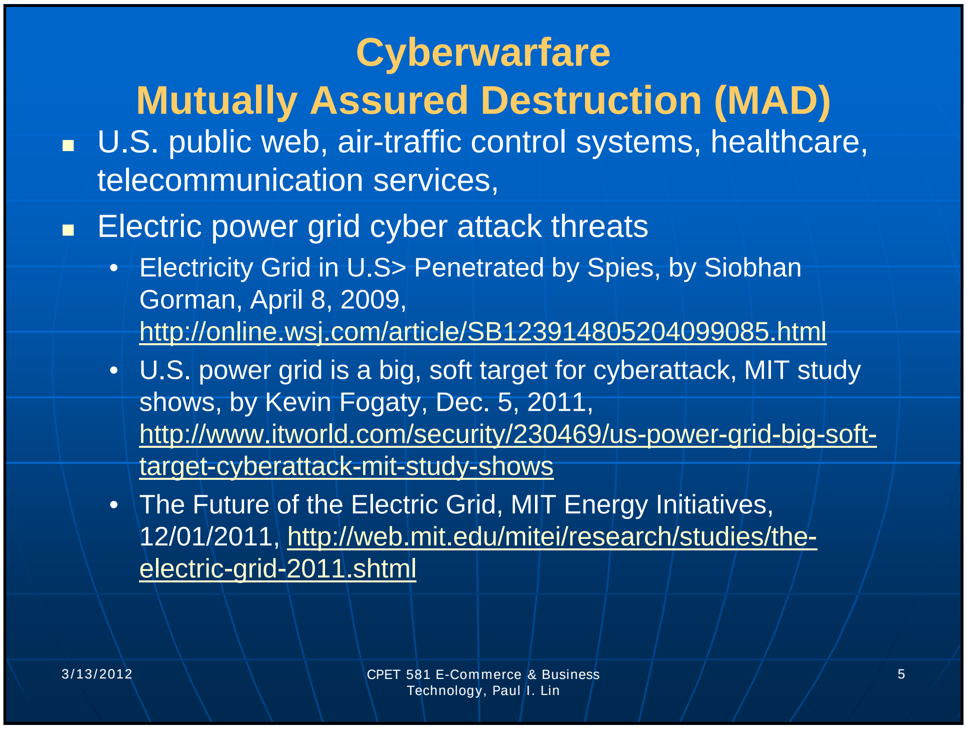
Topics

- Cyberwar: Mutually Assured Destruction (MAD)
- The E-Commerce Security Environment
- Security Threats in the E-Commerce Environment
- Technology Solutions for Site Security
- Management Policies, Business Procedures, and Public Laws
- E-Commerce Payment Systems
- E-Billing Presentment and Payment
- Case Study



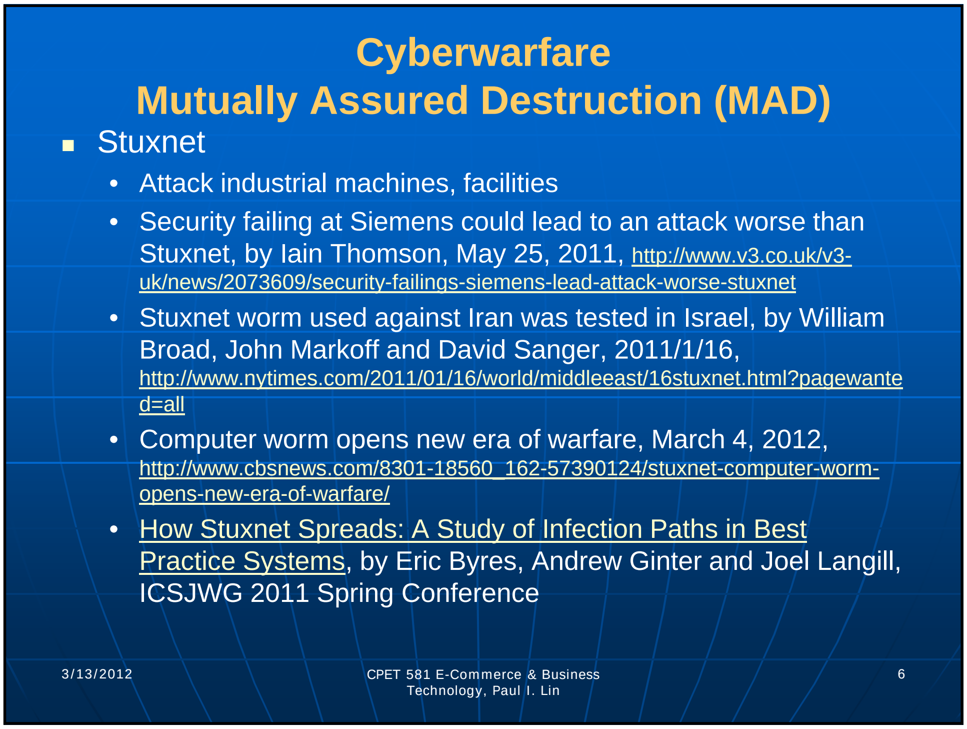
Cyberwarfare
Mutually Assured Destruction (MAD)

- State sponsored activities
- The lesson of Titan Rain, Dec. 14, 2005, http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management
- China vs. Google (Email services and Google Talk features), May 2011
    - Google says China blocking its email services, abc News, http://abcnews.go.com/Technology/wireStory?id=13182824
    - Beijing Fires Back at Google, http://online.wsj.com/article/SB10001424052702304563104576361300123816450.html
- U.S. public web, air-traffic control systems, healthcare, telecommunication services, electric power grid



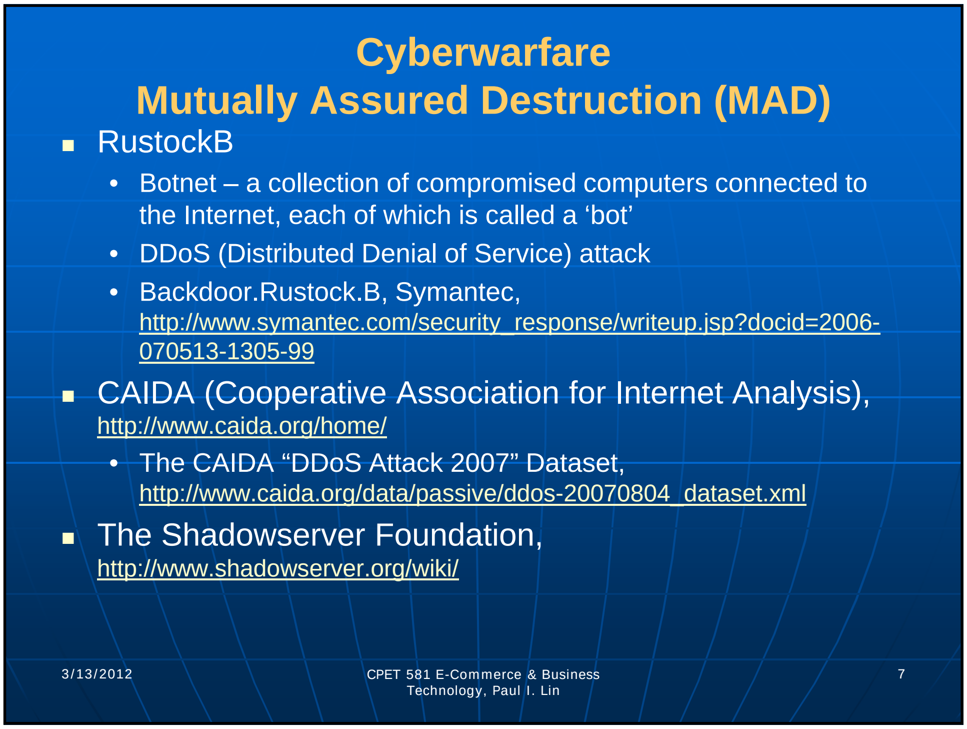
Cyberwarfare
Mutually Assured Destruction (MAD)

- U.S. public web, air-traffic control systems, healthcare, telecommunication services,
- Electric power grid cyber attack threats
  - Electricity Grid in U.S> Penetrated by Spies, by Siobhan Gorman, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html
  - U.S. power grid is a big, soft target for cyberattack, MIT study shows, by Kevin Fogaty, Dec. 5, 2011, http://www.itworld.com/security/230469/us-power-grid-big-soft-target-cyberattack-mit-study-shows
  - The Future of the Electric Grid, MIT Energy Initiatives, 12/01/2011, http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml



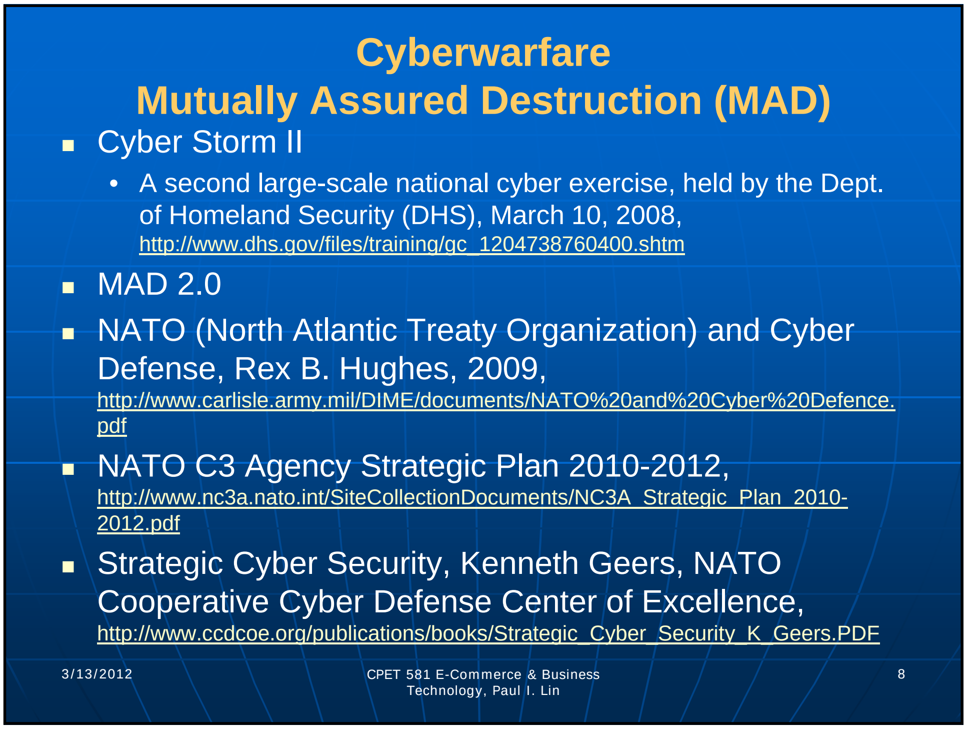
Cyberwarfare
Mutually Assured Destruction (MAD)

- Stuxnet
  - Attack industrial machines, facilities
  - Security failing at Siemens could lead to an attack worse than Stuxnet, by Iain Thomson, May 25, 2011, http://www.v3.co.uk/v3-uk/news/2073609/security-failings-siemens-lead-attack-worse-stuxnet
  - Stuxnet worm used against Iran was tested in Israel, by William Broad, John Markoff and David Sanger, 2011/1/16, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all
  - Computer worm opens new era of warfare, March 4, 2012, http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/
  - How Stuxnet Spreads: A Study of Infection Paths in Best Practice Systems, by Eric Byres, Andrew Ginter and Joel Langill, ICSJWG 2011 Spring Conference



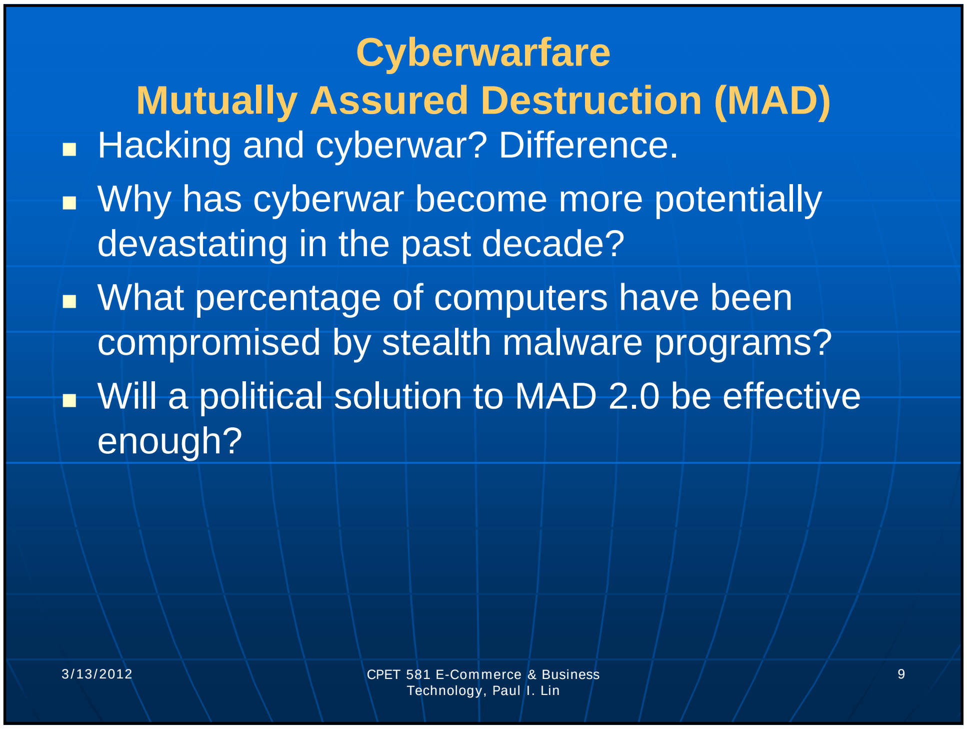
Cyberwarfare
Mutually Assured Destruction (MAD)

- RustockB
  - Botnet – a collection of compromised computers connected to the Internet, each of which is called a 'bot'
  - DDoS (Distributed Denial of Service) attack
  - Backdoor.Rustock.B, Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2006-070513-1305-99
- CAIDA (Cooperative Association for Internet Analysis), http://www.caida.org/home/
  - The CAIDA "DDoS Attack 2007" Dataset, http://www.caida.org/data/passive/ddos-20070804_dataset.xml
- The Shadowserver Foundation, http://www.shadowserver.org/wiki/



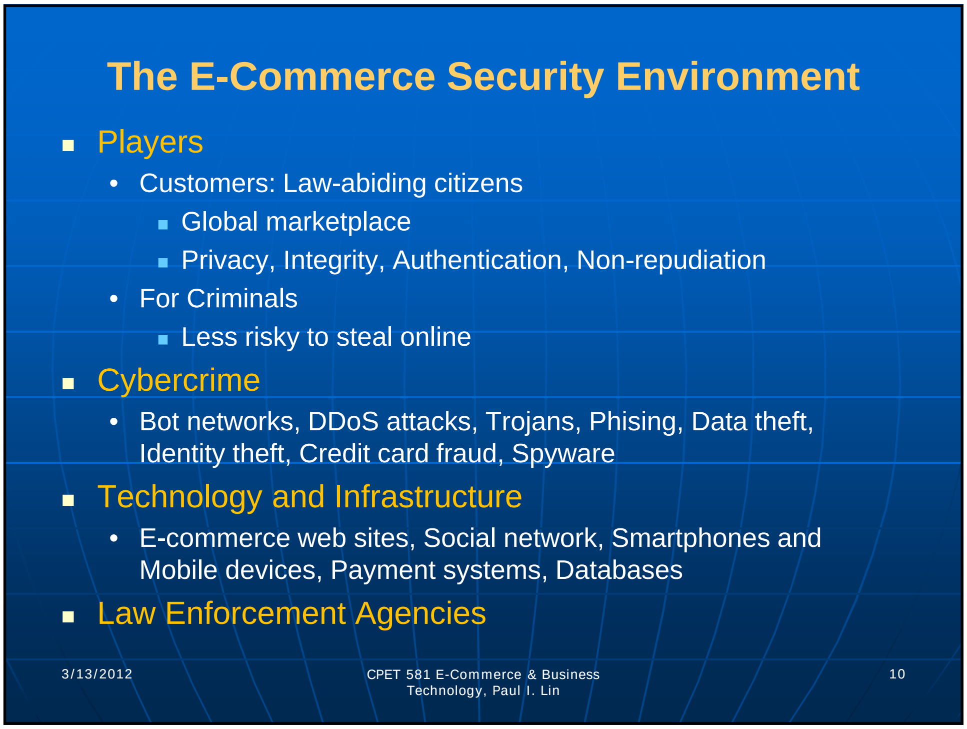
Cyberwarfare
Mutually Assured Destruction (MAD)

- Cyber Storm II
  - A second large-scale national cyber exercise, held by the Dept. of Homeland Security (DHS), March 10, 2008, http://www.dhs.gov/files/training/gc_1204738760400.shtm
- MAD 2.0
- NATO (North Atlantic Treaty Organization) and Cyber Defense, Rex B. Hughes, 2009, http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf
- NATO C3 Agency Strategic Plan 2010-2012, http://www.nc3a.nato.int/SiteCollectionDocuments/NC3A_Strategic_Plan_2010-2012.pdf
- Strategic Cyber Security, Kenneth Geers, NATO Cooperative Cyber Defense Center of Excellence, http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF



Cyberwarfare
Mutually Assured Destruction (MAD)

- Hacking and cyberwar? Difference.
- Why has cyberwar become more potentially devastating in the past decade?
- What percentage of computers have been compromised by stealth malware programs?
- Will a political solution to MAD 2.0 be effective enough?



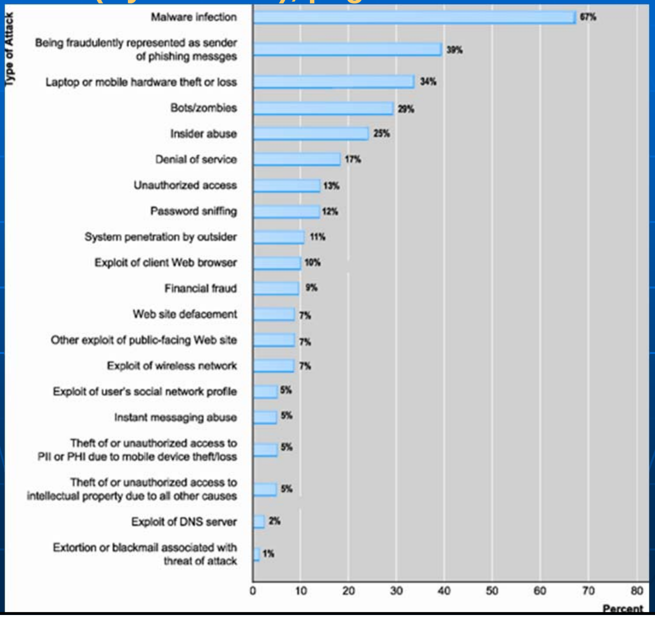
The E-Commerce Security Environment

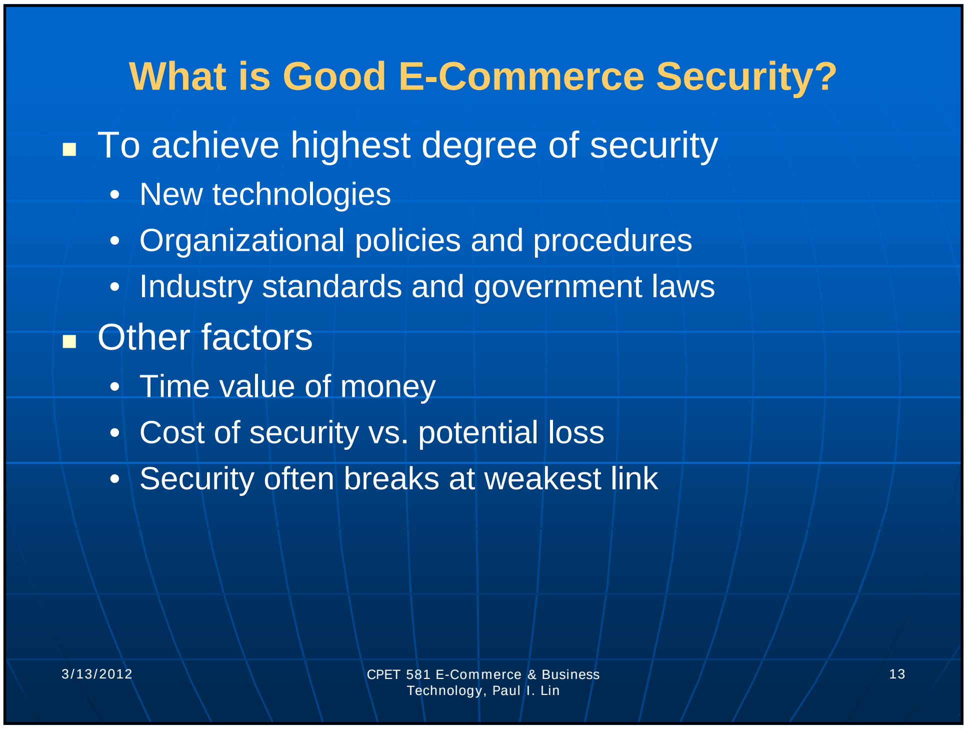
- Players
  - Customers: Law-abiding citizens
    - Global marketplace
    - Privacy, Integrity, Authentication, Non-repudiation
  - For Criminals
    - Less risky to steal online
- Cybercrime
  - Bot networks, DDoS attacks, Trojans, Phising, Data theft, Identity theft, Credit card fraud, Spyware
- Technology and Infrastructure
  - E-commerce web sites, Social network, Smartphones and Mobile devices, Payment systems, Databases
- Law Enforcement Agencies

The E-Commerce Security Environment

- Internet Information
  - Personal Identifiable Information
  - Personal Health Information
- Internet Information Security and Enforcement Agencies
  - Identity Theft Resource Center (ITRC), http://www.idtheftcenter.org/
  - Internet Crime Complaint Center (IC3), http://www.ic3.gov/default.aspx
    - Annual Reports, http://www.ic3.gov/media/annualreports.aspx
  - National White Collar Crime Center, http://www.nw3c.org/
  - Federal Bureau of Investigation, http://www.fbi.gov/
  - Computer Security Institute, http://gocsi.com/
    - CSI Reports, http://gocsi.com/members/reports

Figure 5.1 Types of Attacks Against Computer Systems (Cybercrime), page 264





What is Good E-Commerce Security?

- To achieve highest degree of security
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws
- Other factors
  - Time value of money
  - Cost of security vs. potential loss
  - Security often breaks at weakest link

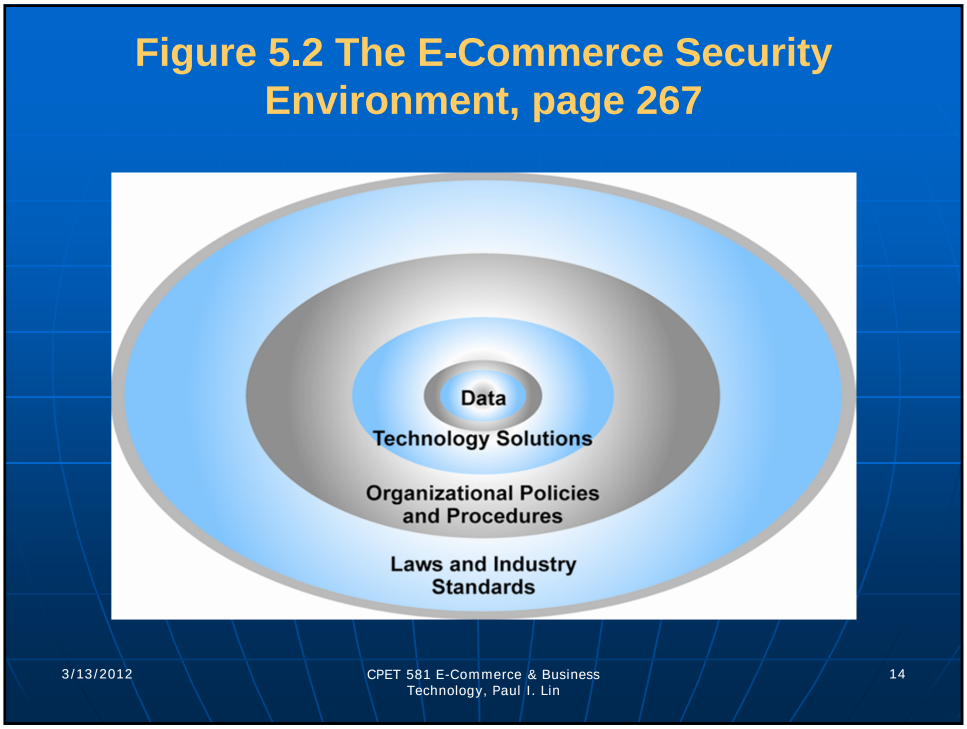


Figure 5.2 The E-Commerce Security Environment, page 267

Data
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

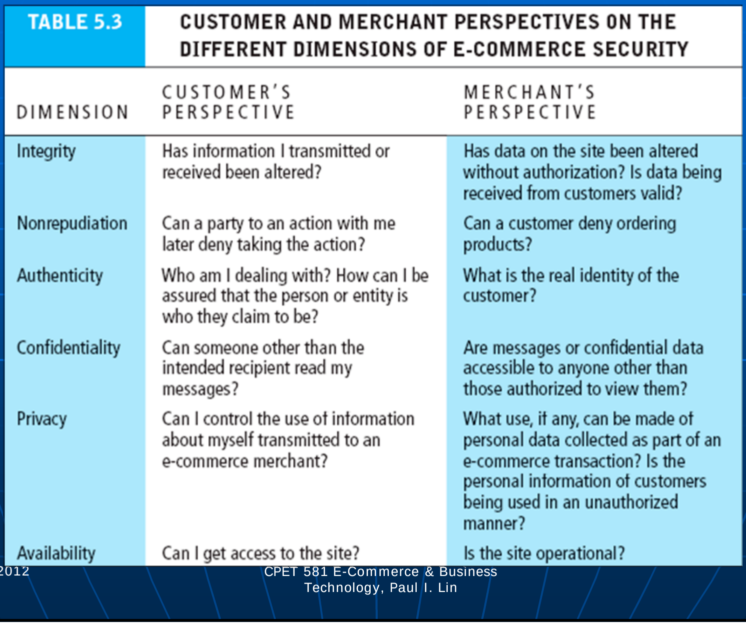


TABLE 5.3 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Security Threats in the E-Commerce Environment

- Three key points of vulnerability in E-Commerce environment
  1. Client
  2. Server
  3. Communication pipeline (Internet communications channels)

Figure 5.3 A Typical E-Commerce Transaction

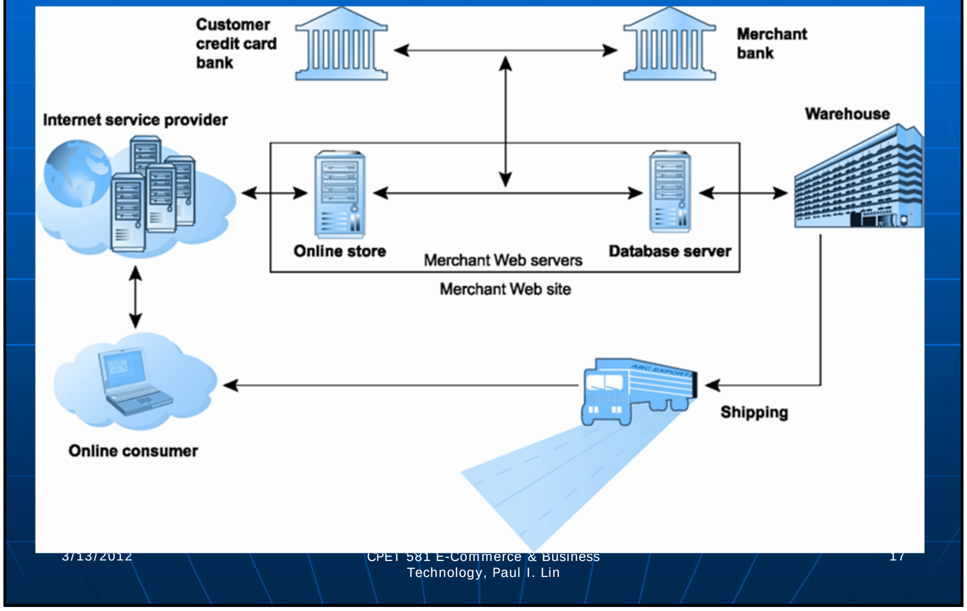
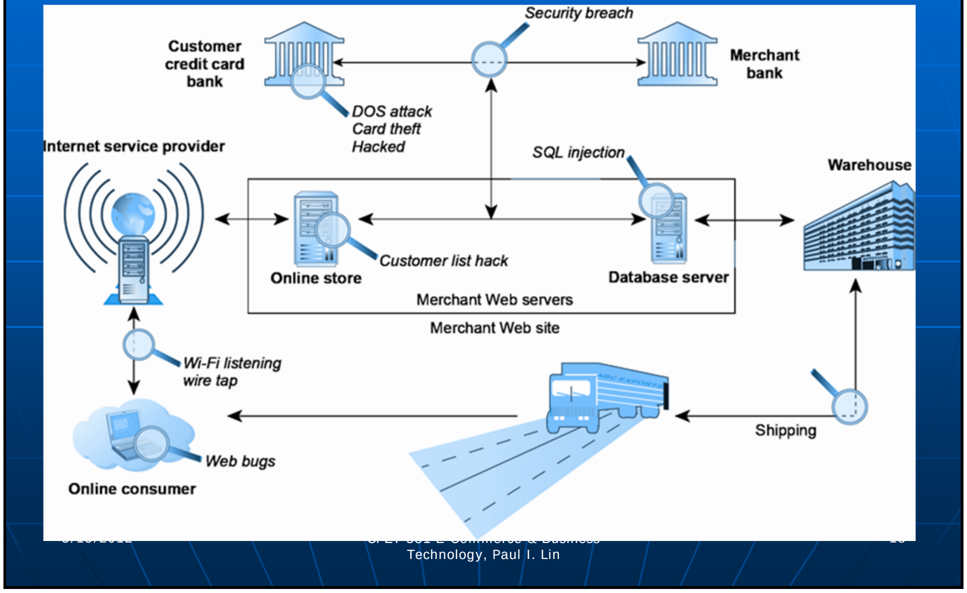
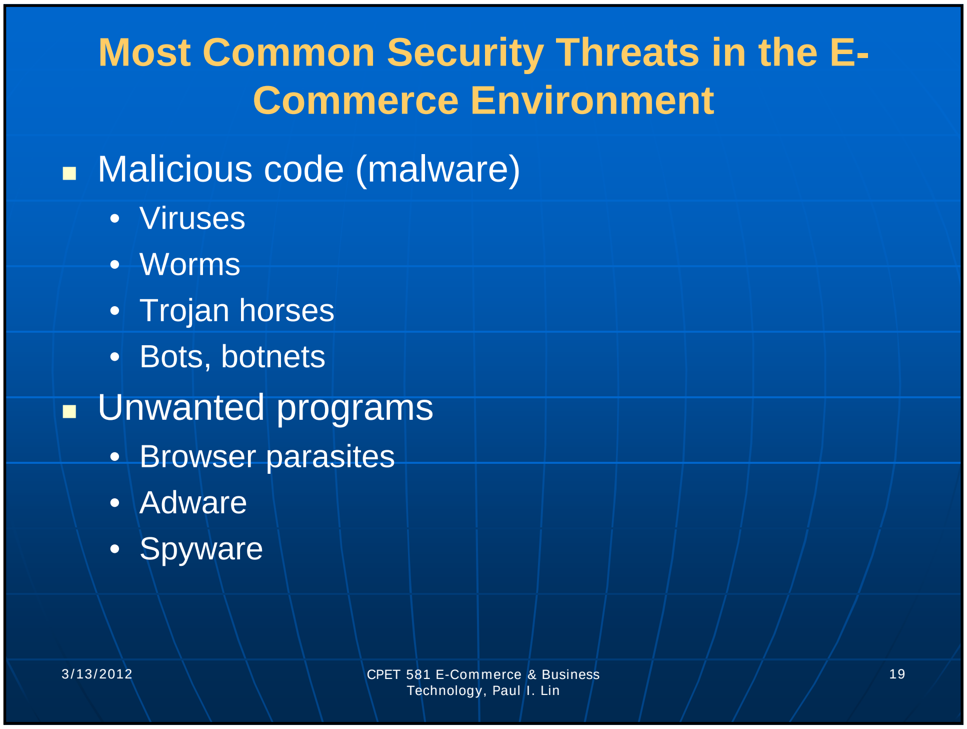


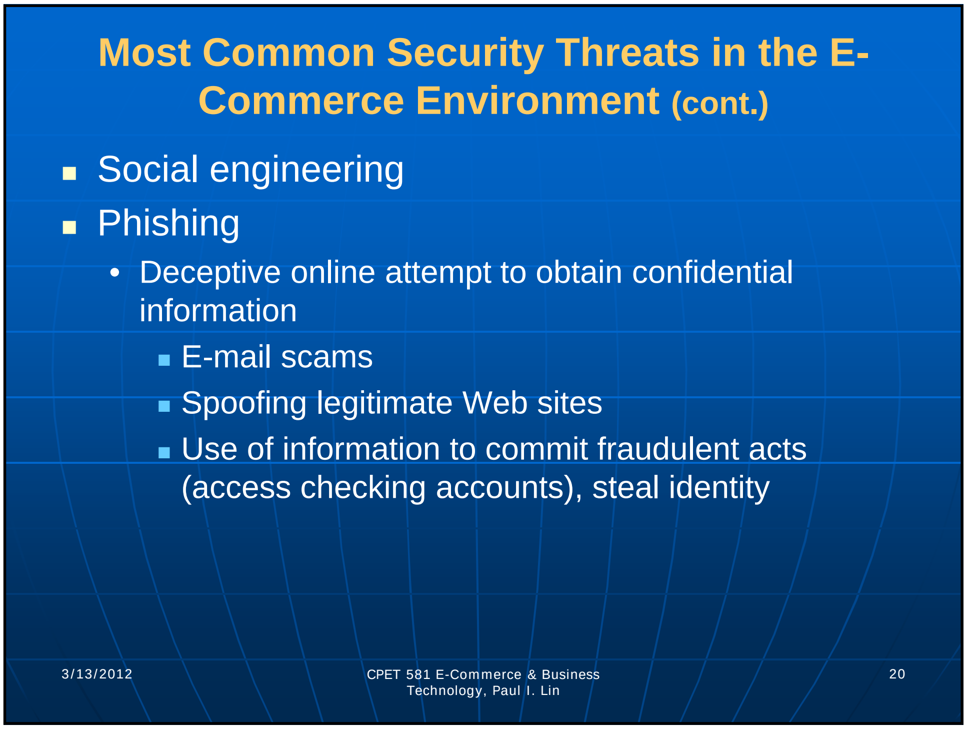
Figure 5.4 Vulnerable Points in an E-Commerce Transaction





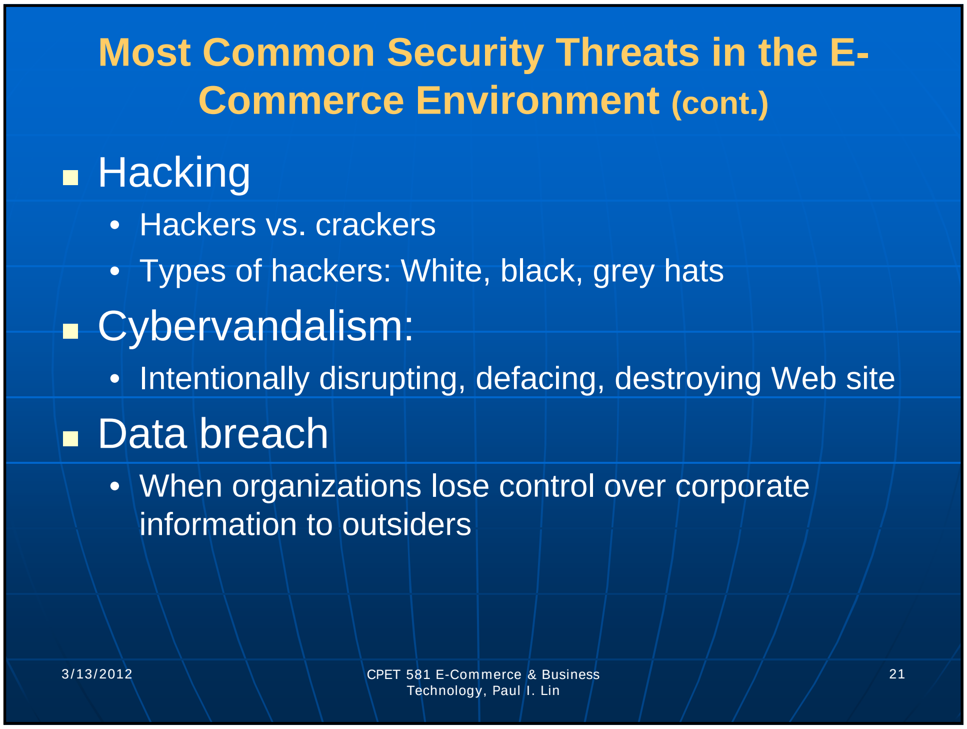
Most Common Security Threats in the E-Commerce Environment

- Malicious code (malware)
  - Viruses
  - Worms
  - Trojan horses
  - Bots, botnets
- Unwanted programs
  - Browser parasites
  - Adware
  - Spyware



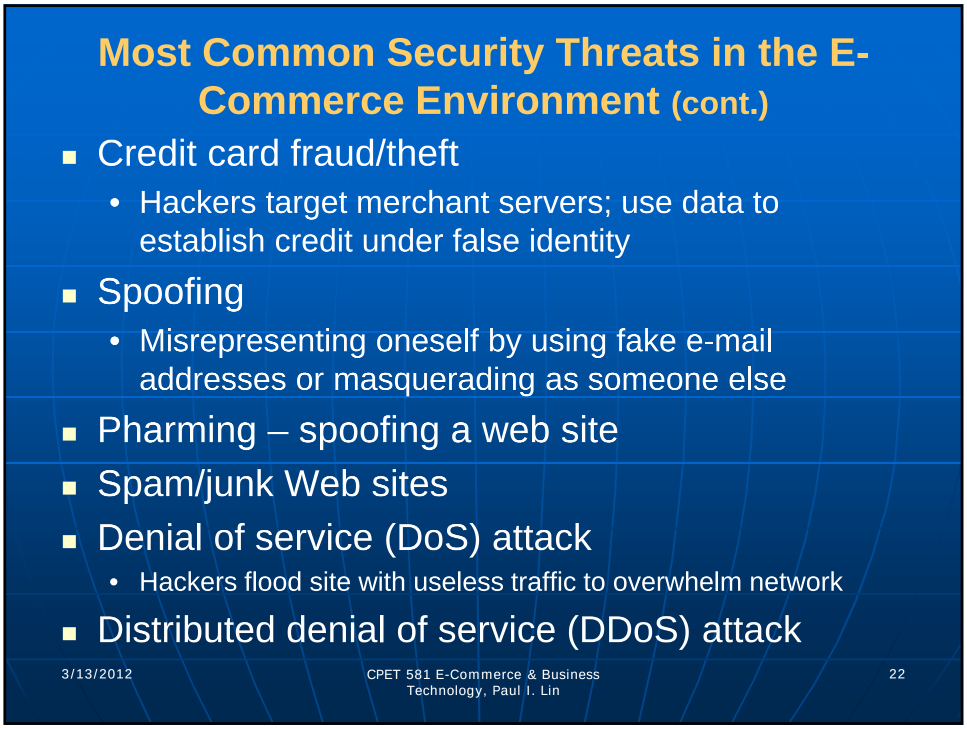
Most Common Security Threats in the E-Commerce Environment (cont.)

- Social engineering
- Phishing
  - Deceptive online attempt to obtain confidential information
    - E-mail scams
    - Spoofing legitimate Web sites
    - Use of information to commit fraudulent acts (access checking accounts), steal identity



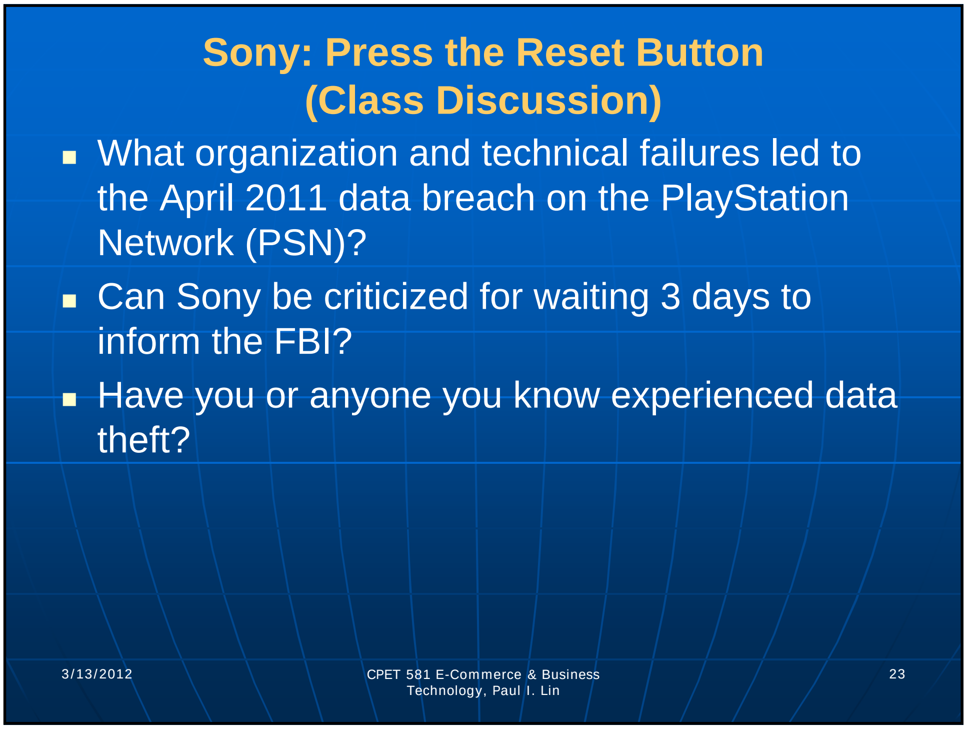
Most Common Security Threats in the E-Commerce Environment (cont.)

- Hacking
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats
- Cybervandalism:
  - Intentionally disrupting, defacing, destroying Web site
- Data breach
  - When organizations lose control over corporate information to outsiders



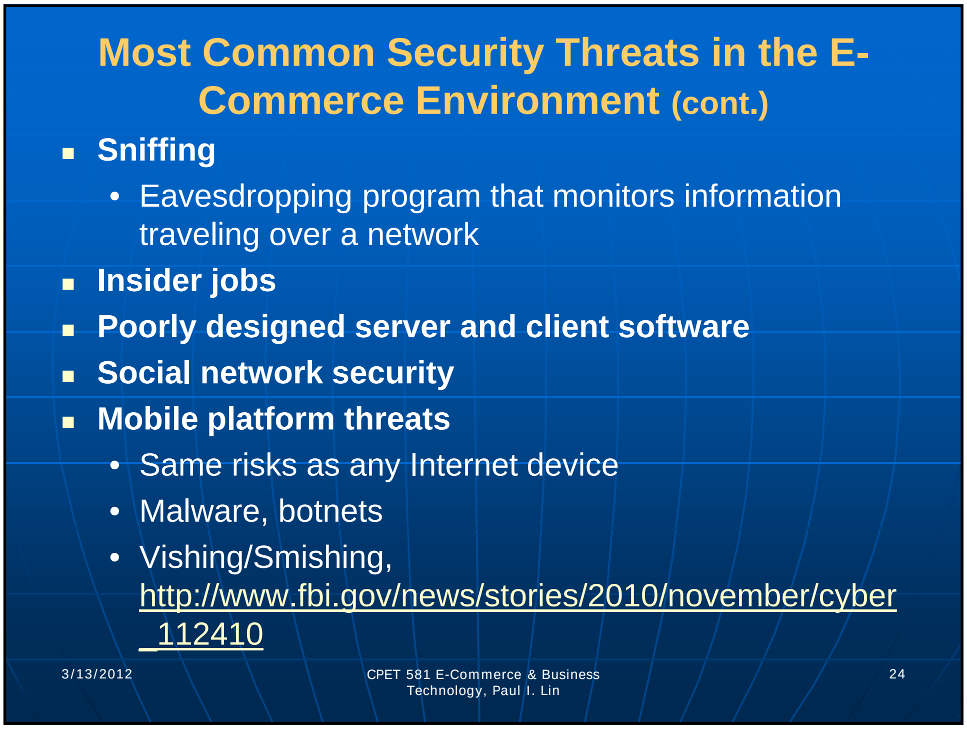
Most Common Security Threats in the E-Commerce Environment (cont.)

- Credit card fraud/theft
  - Hackers target merchant servers; use data to establish credit under false identity
- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
- Pharming – spoofing a web site
- Spam/junk Web sites
- Denial of service (DoS) attack
  - Hackers flood site with useless traffic to overwhelm network
- Distributed denial of service (DDoS) attack



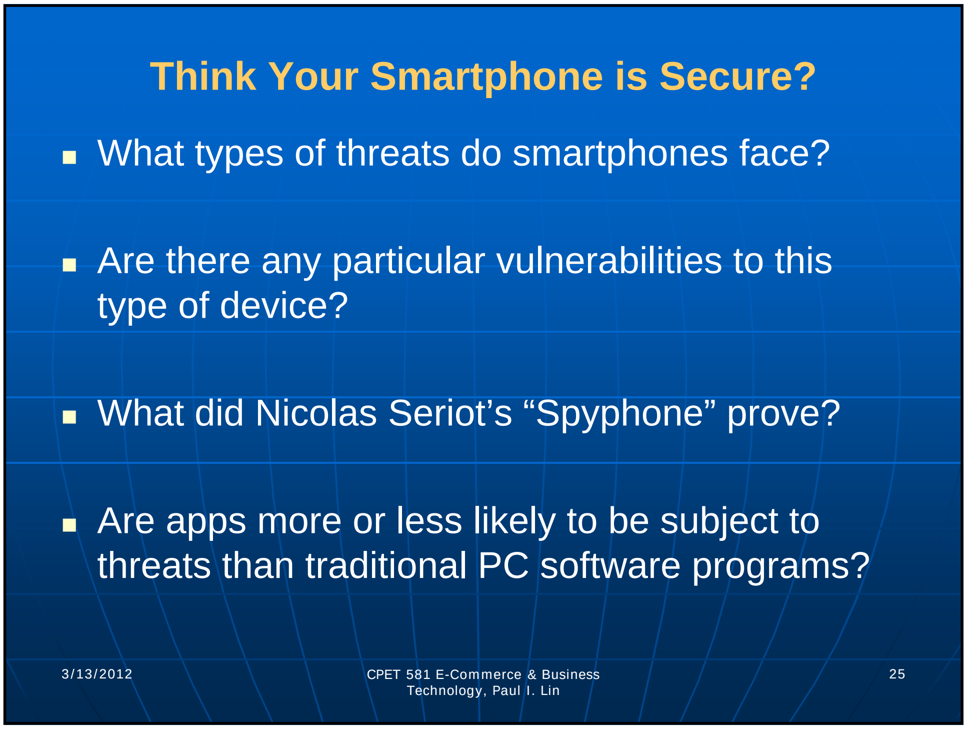
Sony: Press the Reset Button (Class Discussion)

- What organization and technical failures led to the April 2011 data breach on the PlayStation Network (PSN)?
- Can Sony be criticized for waiting 3 days to inform the FBI?
- Have you or anyone you know experienced data theft?



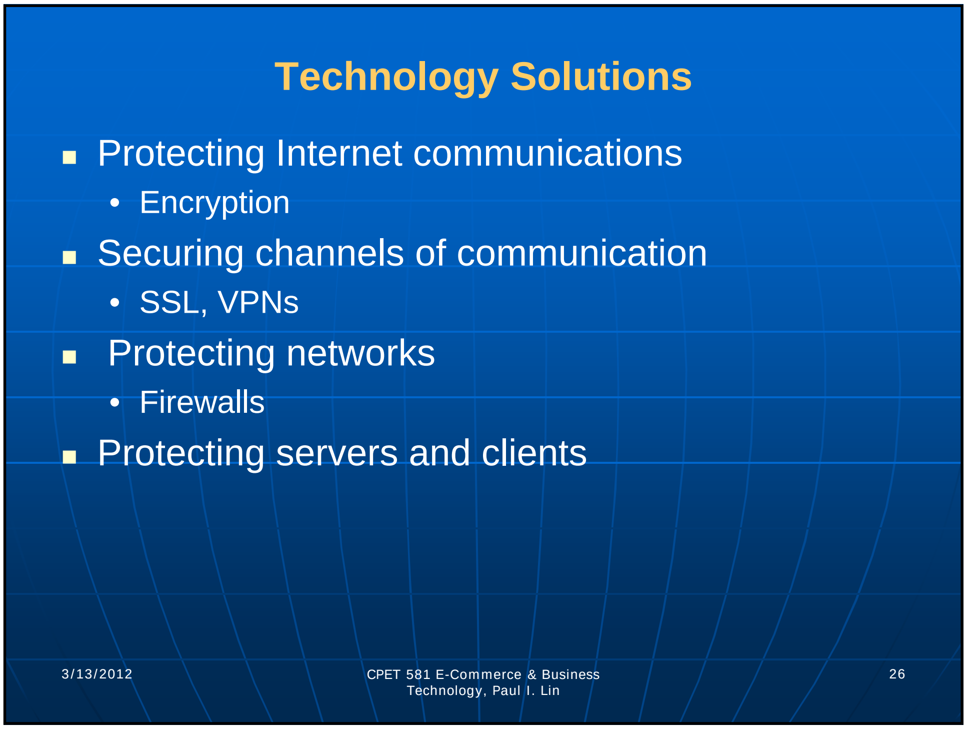
Most Common Security Threats in the E-Commerce Environment (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider jobs**
- **Poorly designed server and client software**
- **Social network security**
- **Mobile platform threats**
  - Same risks as any Internet device
  - Malware, botnets
  - Vishing/Smishing, http://www.fbi.gov/news/stories/2010/november/cyber_112410



Think Your Smartphone is Secure?

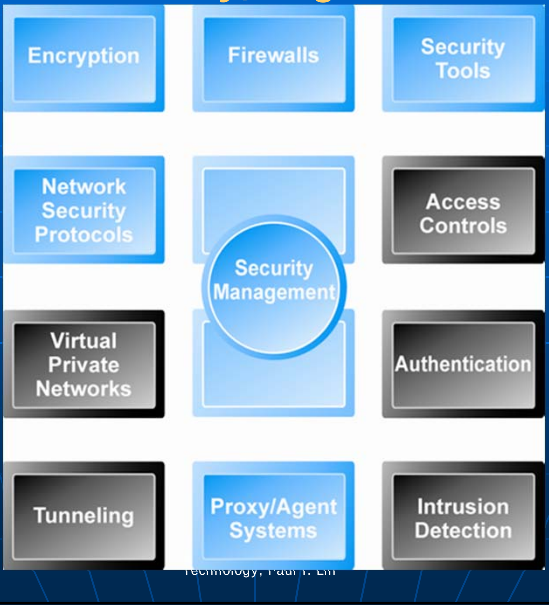
- What types of threats do smartphones face?
- Are there any particular vulnerabilities to this type of device?
- What did Nicolas Seriot’s “Spyphone” prove?
- Are apps more or less likely to be subject to threats than traditional PC software programs?



Technology Solutions

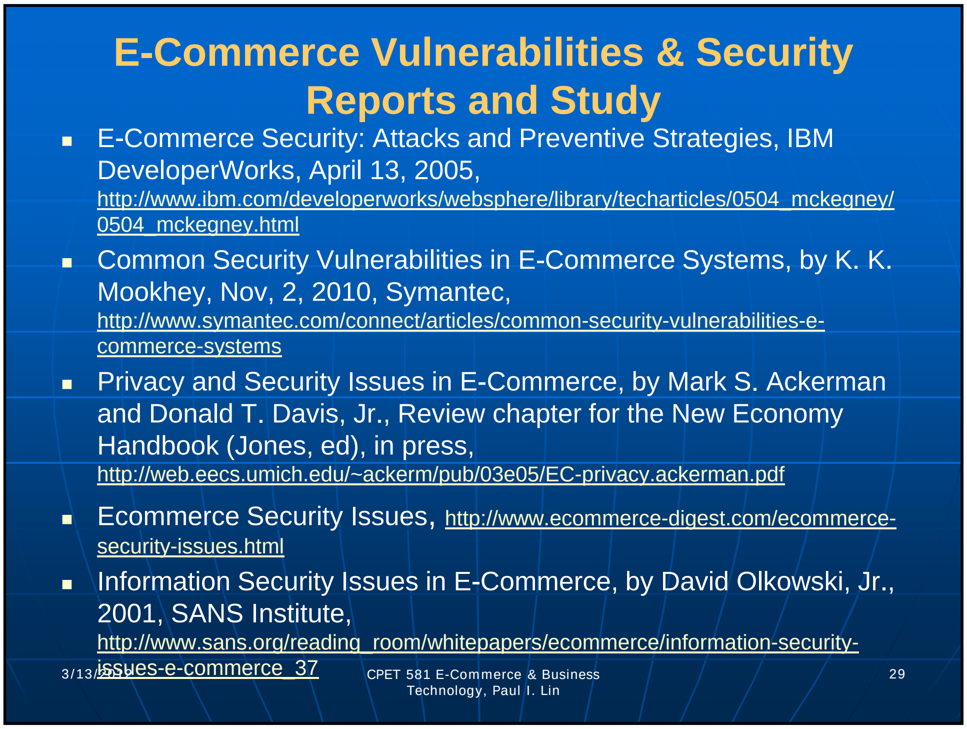
- Protecting Internet communications
  - Encryption
- Securing channels of communication
  - SSL, VPNs
- Protecting networks
  - Firewalls
- Protecting servers and clients

Figure 5.7 Tools Available to Achieve Site Security, Page 288



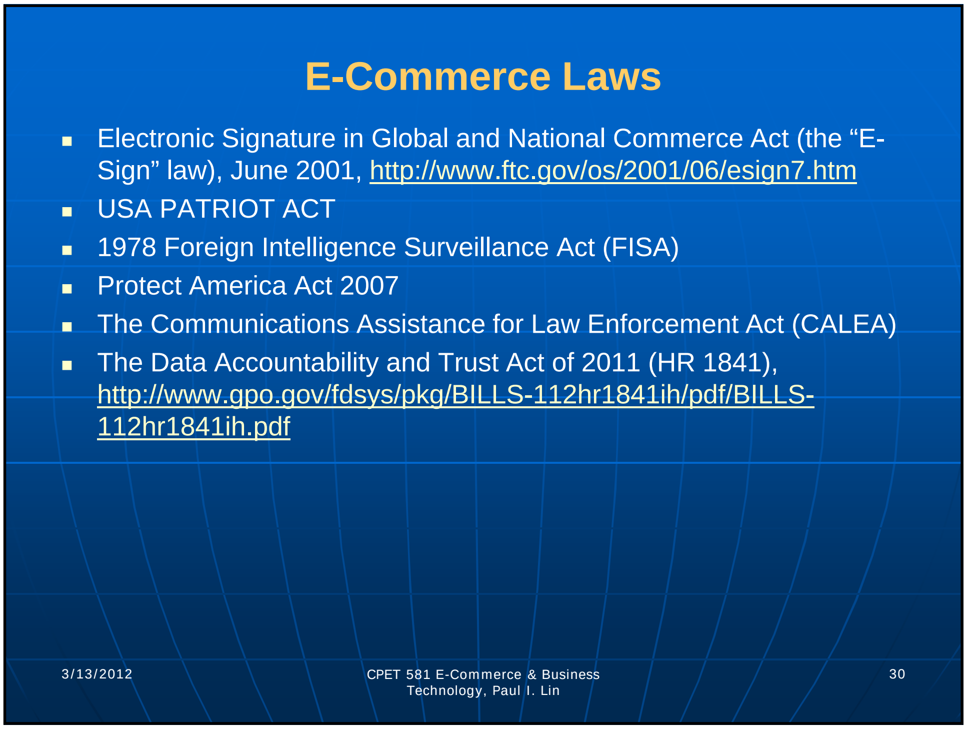
Security Software, Tools and Information

- What is Rouge Software, http://www.microsoft.com/en-us/showcase/details.aspx?uuid=bac75cc2-bb7a-4b59-ba0d-dc59ead769e3
- Rouge Security Software, Microsoft Safety & Security Center, http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx



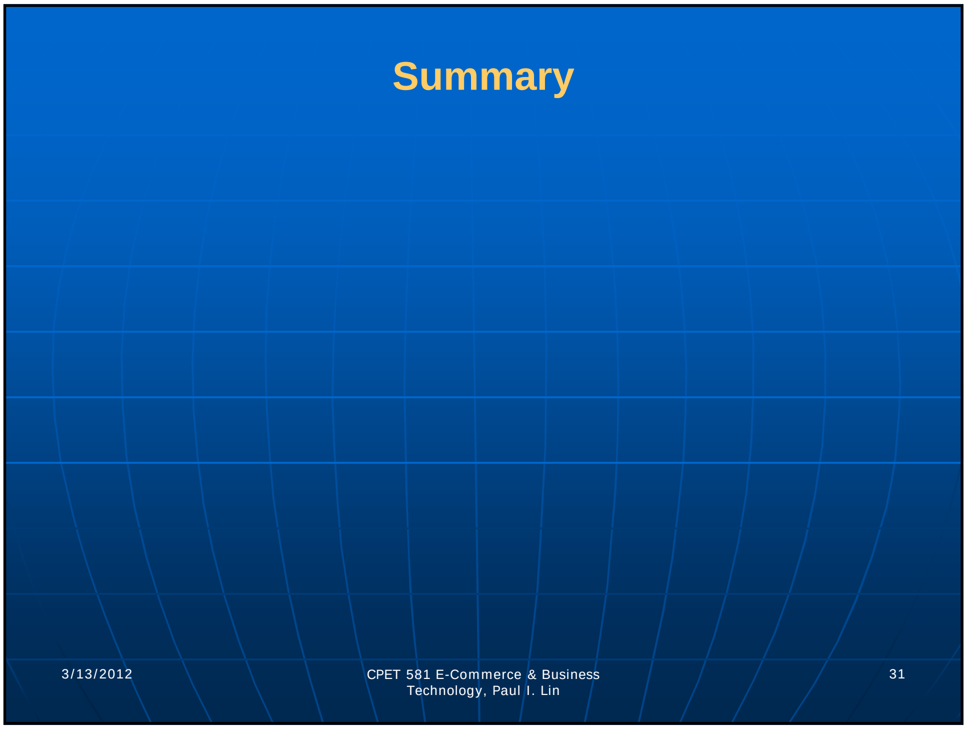
E-Commerce Vulnerabilities & Security Reports and Study

- E-Commerce Security: Attacks and Preventive Strategies, IBM DeveloperWorks, April 13, 2005, http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html
- Common Security Vulnerabilities in E-Commerce Systems, by K. K. Mookhey, Nov, 2, 2010, Symantec, http://www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems
- Privacy and Security Issues in E-Commerce, by Mark S. Ackerman and Donald T. Davis, Jr., Review chapter for the New Economy Handbook (Jones, ed), in press, http://web.eecs.umich.edu/~ackerm/pub/03e05/EC-privacy.ackerman.pdf
- Ecommerce Security Issues, http://www.ecommerce-digest.com/ecommerce-security-issues.html
- Information Security Issues in E-Commerce, by David Olkowski, Jr., 2001, SANS Institute, http://www.sans.org/reading_room/whitepapers/ecommerce/information-security-issues-e-commerce_37



E-Commerce Laws

- Electronic Signature in Global and National Commerce Act (the "E-Sign" law), June 2001, http://www.ftc.gov/os/2001/06/esign7.htm
- USA PATRIOT ACT
- 1978 Foreign Intelligence Surveillance Act (FISA)
- Protect America Act 2007
- The Communications Assistance for Law Enforcement Act (CALEA)
- The Data Accountability and Trust Act of 2011 (HR 1841), http://www.gpo.gov/fdsys/pkg/BILLS-112hr1841ih/pdf/BILLS-112hr1841ih.pdf



Summary