SECURITY AWARENESS

Module 5

COURSE OBJECTIVES

Upon completion of this course, you will be able to:

- List latest skills and techniques to provide protection.
- Describe the fundamentals of an effective computer security system.
- Identify and recognize the different security solutions.
- Formulate a security plan utilizing the latest security technologies.
- Explain the techniques of computer security.

COURSE PRINCIPLES

This module provides the latest security tips and techniques on Internet and computer security best practices.

Topics include: important privacy legislation, selection of IT security products, firewall benefits and limitations, intruder detection, correct ways to configure your computer, browser settings, virus settings, operating system vulnerabilities, strong password techniques, parasite detection, and encryption techniques.

- Computer Systems
  - Can be represented by:
    - **Subjects**
      - Active entities that access objects
    - **Objects**
      - Passive entities that must be protected
      - Examples: data, hardware, software and communication links
  - **Access Control Policy**
    - Describes how objects are accessed by subjects
  - **Flow Control Policy**
    - Regulates the information flow between objects and subjects

IT SECURITY TOOLS

- **Finding a way into the network**
  - Firewalls
- **Exploiting software bugs, buffer overflows**
  - Intrusion Detection Systems
- **Denial of Service**
  - Ingress filtering, IDS
- **TCP hijacking**
  - IPSec
- **Packet sniffing**
  - Encryption (SSH, SSL, HTTPS)
- **Social problems**
  - Education

Three common types of firewalls

- Packet-filtering-router
- Application-level-Gateways
- Circuit-level-Gateways
- (Bastion Host)

Firewall benefits and limitations

- Advantages
  - One screening router can protect entire network
  - Can be efficient if filtering rules are kept simple
  - Widely available. Almost any router, even Linux boxes
- Disadvantages
  - Can possibly be penetrated
  - Cannot enforce some policies. For example, permit certain users
  - Rules can get complicated and difficult to test

INTRUSION DETECTION SYSTEMS

- **Full-time monitoring tools placed at the most vulnerable points of corporate networks to detect and deter intruders**
- IDSs serve three essential security functions; *monitor*, *detect* and *respond* to unauthorized activity

Benefits of IDS

- Monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms
- Allows administrator to tune, organize and comprehend often incomprehensible operating system audit trails and other logs
- Make the security management of systems by non-expert staff possible by providing nice user friendly interface
- Extensive attack signature database against which information from the customers system can be matched
- Recognize and report alterations to data files

ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE

- Public key encryption: Uses two different keys, one private and one public. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key
- Digital signature: A digital code attached to an electronically transmitted message that is used to verify the origin and contents of a message

IPSEC INTERNET PROTOCOL SECURITY

- IPsec is a set of security protocols and algorithms used
  to secure IP data at the network layer.
- IPsec provides data confidentiality (encryption), integrity (hash), and authentication (signatures and certificates) of IP packets while maintaining the ability to route them through existing IP networks.

REFERENCES

Inoculating The Network"

By Mathias Thurman

EBSCO HOST Research Databases

National Strategy To Secure Cyberspace

Draft September 2002

http://www.dhs.gov/national-strategy-secure-cyberspace

An Introduction to Intrusion Detection / Assessment

By Rebecca Bace

http://www.icsalabs.com

White paper on "The Science Of Intrusion Detection System

– Attack Identification"

http://www.cisco.com

REFERENCES

Harkins, D. *ISAKMP/Oakley Protocol Feature Software Unit Functional Specification.* ENG-0000 Rev A. Cisco Systems.

Madson, C. *IPSec Software Unit Functional Specification ENG-17610 Rev F.* Cisco Systems.

Kaufman, C. Perlman R. and Spencer, M. *Network Security: Private Communication in a Public World.* Prentice Hall, 1995.

Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Second Ed. John Wiley & Sons, Inc.

CYBER CRIME

HAVE YOU EVER BEEN UNDER A CYBER SECURITY ATTACK?

- Received an Email with URL from unknown person
- Been asked to provide personal information

High-Tech Heist 2,100 ATMs Worldwide Hit at Once

- Three 20-something Eastern Europeans and an unnamed person called simply “Hacker 3.” Working together, the four hackers cooked up “perhaps the most sophisticated and organized computer fraud attack ever conducted,” according to Acting U.S. Attorney Sally Quillian Yates of the Northern District of Georgia.
- Network of thieves around the world—called “cashers”—who used a total of 44 counterfeit cards to withdrawal the $9 million

Operation Phish Phry Major Cyber Fraud Takedown

Operation Phish Phry targeted U.S. banks and victimized hundreds and possibly thousands of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled.

More than 50 individuals in California, Nevada, and North Carolina, and nearly 50 Egyptian citizens have been charged with crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identify theft.

CYBER CRIME TIP

- Don't Become a Phishing Victim
- Most banks or other companies will not request your personal information via e-mail. If you get an e-mail asking for such information, call the bank—but don’t use the phone number contained in the e-mail. - Use a phishing filter on your computer. Many current web browsers have them built in or offer them as plug-ins. - Never follow a link to a secure site from an e-mail—always enter the URL manually. - Don't be fooled by the latest scams

WHY ARE CYBER CRIMINALS ATTACKING?

- Hackers **attack small businesses looking for customer data** (such as credit card numbers), intellectual property and small-business bank account information.
- Attacks often seek information small businesses have obtained from their customers through online transactions.
  - **Another example: hackers could plant malware software on a small business website. A customer or client visiting a compromised site then unknowingly shares their information with the hackers.**
- When targeting companies to attack or steal data from, hackers do not just target upper management. Attacks are frequently launched against every level of an organization. **Knowledge workers**, i.e., employees in roles such as **research and development**, as well as **sales employees** are the most targeted.

Ultimately criminals are seeking information or activity that they can make money from.

COMUPTER SECURITY

TOOLS AND TECHNIQUES

ONLINE SHOPPING AND BANKING

Online Banking service incorporates industry-leading safety features that give you greater security and peace of mind as you manage your money. Taking some common-sense steps to protect yourself adds an extra layer of protection to your online experience.

Secure your computer

- Make sure your computer is equipped with comprehensive spyware and virus-protection software
- Make sure your computer is equipped with a firewall, which prevents unauthorized users from gaining access to your computer or monitoring transfers of information to and from the computer

Stay informed

- Follow internet security issues in the news and discuss them with friends, family and colleagues. Explore online resources like the National Cyber Security Alliance and Microsoft® Security At Home websites that provide comprehensive information about topics such as securing your computer and safe online behavior.

Check Filters and Forwarding Addresses

- In the event of a hack and after reclaiming the account, go through the existing filters to check if there are some sneaky filters set up that forward all your credit card, login info, bank account and other sensitive correspondence to an email address that is not yours. Go to the forwarding page and see that all your incoming mails are not forwarded to the hacker either. This helps you avoid getting hacked in the future too.

Avoid Public Wi-Fi

- Happy to have discovered an unsecured Wi-Fi hotspot? Or mooching your neighbor's spilt Wi-Fi? Enjoying the free Wi-Fi of the coffee shop round the corner? Good for you and so is for the hacker sitting nearby to sniff the packets right out of thin air. Avoid using public Wi-Fi for accessing email or transacting online with a credit card. Casual browsing and YouTube watching (without logging in) are Ok. Accessing emails is a big no, no.

Do not share your login information

- Another obvious fact. But at times, it’s necessary for small businesses and online entrepreneurs to share login information with colleagues. For example, accessing Google AdSense, Analytics or Microsoft Live services etc. The ideal solution is to create a dedicated account for accessing these services instead of linking everything to your personal email id and sharing it.

Login regularly

- Even if a hacker gets hold of the answer to your security question, they cannot use it immediately to reset the password and break into your Gmail account. Password reset with security question is possible only after 24 hours of your account being inactive after receiving the password reset instructions. So for once, checking your mail regularly is a good thing. Also, it will help reset the Hotmail account’s expiry date. Unfortunately Hotmail and Yahoo do not have this useful restriction in place.

Special Features

Gmail

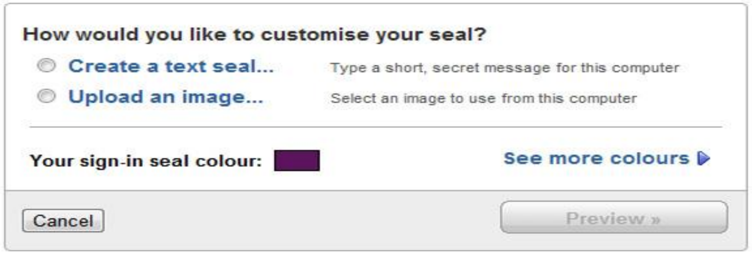
- Enable HTTPS by default from your account settings. This helps from the password getting sniffed when transmitted over public Wi-Fi hot spots. If you are a Google Apps user, enable pre release features to avail the upcoming two factor authentication system before it launches.

Hotmail

- Use the Windows Live Essentials package and verify the computer you are using as reliable. “Trusted PC” is a unique new proof that lets you link your Hotmail account with one or more of your personal computers. Then, if you ever need to regain control of your account by resetting your password, you simply have to use the trusted computer and Hotmail will know you are the legitimate owner. It’s a great feature for those who are really paranoid about email security.

Yahoo

YAHOO! Mail



How would you like to customise your seal?

○ Create a text seal... Type a short, secret message for this computer

○ Upload an image... Select an image to use from this computer

Your sign-in seal colour: ■ See more colours ▶

Sign In Seal

- Make use of the sign in seal option to verify the computer. Sign in seal is basically an image or color that Yahoo displays for each of your computers adding another layer of security to the login process

BACKING UP DATA

Have a backup ready. You never know when things may go away of your hands and you lose all the data that holds key to success to your business. Throughout the year, you need to upgrade the systems and take occasional backup of data in a safe and secured place. This will make sure that even if the cyber attack takes place, your have your critical data save in a secured place. Keep the backup away from Office.

- Choosing good passwords

Make Passwords Long, Strong and Unique. Combine capital and lowercase letters with numbers and symbols to create a more secure password. Have a different password for each account.

Cookies and other privacy threats

Mmmm… cookies - chocolate chip and oatmeal with raisins! Cookies are one of the most popular snacks that exist today.

Did you know you can get “browser” cookies almost every time you go on the Internet?

These cookies help with Internet commerce, allow quicker access to web sites, or can personalize your browsing experience. However, there are some privacy and security issues to be aware of, so it is important to understand the purpose of a “browser” cookie and manage their use on your computer appropriately.

BACKING UP DATA

Recommendation

- Set your cookie preferences using your browser privacy settings.
- Periodically delete cookies from your computer.
- Session cookies should be automatically deleted when you have completed a financial transaction online. By clearing your cookies from your browser periodically you can decrease the risk of the misuse of information accidentally or intentionally stored in cookies.
- Do not allow cookies to store login information.
- Keep your system and browser up-to-date on patches, update your anti-spyware software, and only visit trusted web sites.
- If you do not want to share your online behavior data with third-parties, set your privacy settings to not allow third-party cookies. Note, this may impact your browsing experience.
- Be cautious when sharing your computer. If you stored credential information using a browser cookie (user names and password), the individual using your computer will have access to your account and will be able to process transactions in your name.

CURING VIRUSES AND TROJANS

- **Keep Your Firewall Turned On:** A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.
- **Install or Update Your Antivirus Software:** Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.
- **Install or Update Your Antispyware Technology:** Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store.
  - Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust.

KEY POINTS

- Identify vulnerabilities
- Human error is biggest threat
- Fix vulnerabilities (patches, etc.)
- Have policies and procedures
- Computer maintenance program
- Educate staff
- Stay informed of latest and greatest

REFERENCES

Randy Chow, Theodore Johnson. Distributed Operating Systems and Algorithms, Addison-Wesley 1997

Agent Approach for Providing Security in Distributed Systems; TCSET'2006, February 28-March 4, 2006, Lviv-Slavsko, Ukraine

GHIDS:Defending Computational Grids Against Misusing of Shared Resources", Feng et all, IEEE 2006

www.cse.sc.edu/~farkas/csce522-2003/lectures/csce522-lect22.ppt (2003)

REFERENCES

Inoculating The Network"
By Mathias Thurman
EBSCO HOST Research Databases

National Strategy To Secure Cyberspace
Draft September 2002
http://www.dhs.gov/national-strategy-secure-cyberspace

An Introduction to Intrusion Detection / Assessment
By Rebecca Bace
http://www.icsalabs.com

White paper on "The Science Of Intrusion Detection System – Attack Identification"
http://www.cisco.com

REFERENCES

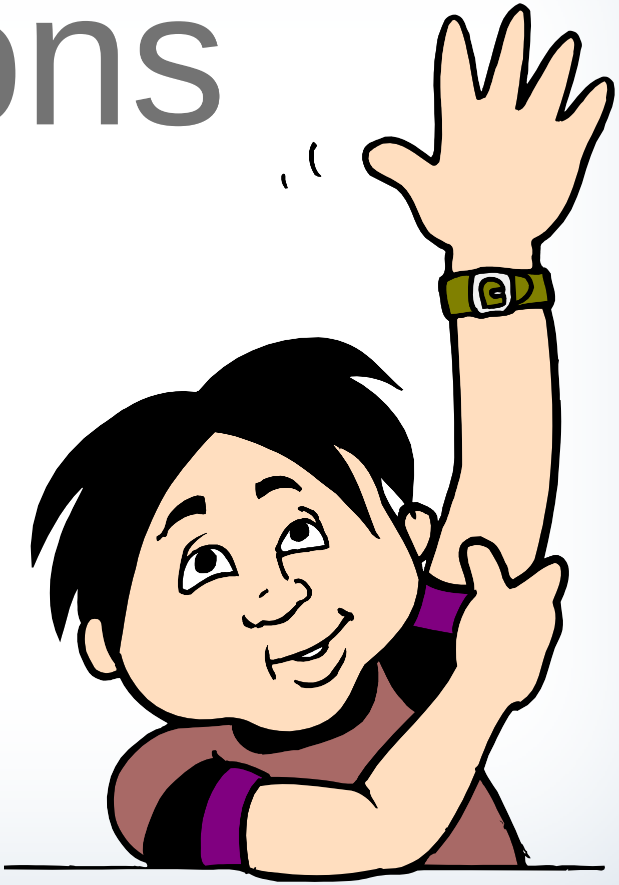
Harkins, D. *ISAKMP/Oakley Protocol Feature Software Unit Functional Specification.* ENG-0000 Rev A. Cisco Systems.

Madson, C. *IPSec Software Unit Functional Specification ENG-17610 Rev F.* Cisco Systems.

Kaufman, C. Perlman R. and Spencer, M. *Network Security: Private Communication in a Public World.* Prentice Hall, 1995.

Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Second Ed. John Wiley & Sons, Inc.

Questions



THANK YOU