Introduction to Security

October 7, 2014

Course Information

Lecture Structure

No.	Lecture Title	Date
1	**Introduction to Security**	2014-10-07
2	Security Threats	2014-10-14
3	Securing Network Devices	2014-10-21
4	ACLs & AAA	2014-10-28
5	Firewalls	2014-11-04
6	IDS & IPS	2014-11-11
	Midterm Assessment	2014-11-18
7	Endpoint Security	2014-11-25
8	Cryptography	2014-12-02
9	VPNs	2014-12-09
10	MPLS	2014-12-16
11	MPLS VPN	2015-01-09

Schedule

	All Tuesdays
16-18	ED 011
18-20	This room
20-22	ED 011

- Lecture:
  - Laura Gheorghe (laura.gheorghe@cs.pub.ro)
  - Sergiu Costea (sergiu.costea@cs.pub.ro)
  - Invited speaker: Bogdan Sass
- Laboratory:
  - Răzvan Prejbeanu (prejbeanu.razvan@gmail.com)

Grading

- The course grade is made up of:
  - Midterm assessment – single choice, multiple answer, from the first 6 lectures: 2.5 points
  - Final assessment – the final 6 lectures: 2.5 points
- The lab grade is made up of:
  - Lab activity: 2.5 points
  - Hands-on exam: 2.5 points
- There is a bonus of 1 point for course involvement
- The PASSING grade is 5.00

Intro to Network Security

Code Red Worm

- July 2001
- More than 350,000 infected web servers
- Affected local networks => DoS to millions of users

- Proper security policy and security patches applied
  - Smaller impact of Code Red Worm

Network Breaches

- Security Breaches may:
  - Disrupt e-commerce
  - Cause loss of business data
  - Affect people's privacy
  - Compromise data integrity

- Result in:
  - Financial loss for corporations
  - Theft of intellectual property
  - Lawsuits
  - Threat to public safety

Network Security

- Awareness of:
  - New threats
  - Attacks
  - Vulnerabilities of devices and applications
- Develop mitigation techniques
- Users receive security awareness training

Some History

First Virus

- Email virus named Melissa
- March 1999, David Smith
- Memory overflows in mail servers
- David sentenced to 20 months in federal prison and $5,000 fine

First Worm

- November 1988, Robert Morris
- 10% of the Internet users were infected
- Increased CPU load, many worm processes
- Robert sentenced to 3 years probation, 400 hours of community service, and $10,000 fine

First Spam

- May 1978
- Distributed on the Advanced Research Projects Agency Network (ARPAnet)
- Regarding a product presentation

First DoS attack

- Called Mafiaboy DoS attack
- February 2000, “mafiaboy”, 17 years
- Paralyzed many important websites for one week (Yahoo, eBay, Amazon)
- Sentenced to 8 months in a youth detention center, one year of probation, donate $250 to charity

Evolution

Evolution of Security Threats

- In the early days of the Internet
  - Use for research and development
  - Not for commercial purposes
  - No security measures
- After first malware and attacks
  - Network security professionals
  - Secure existing networks
- Over the years, the sophistication of the attacker tools grows and the technical knowledge is less required

Evolution of Network Security Tools

- One of the first security tools
  - Intrusion Detection System (IDS)
  - Developed by SRI International, 1984
  - Real-time detection of attacks
  - In 1990, Intrusion Prevention System (IPS) -> block attacks

- First Network Firewall
  - Digital Equipment Corporation (DEC), 1988
  - Packet filter
  - Predefined rules
  - Inspect each packet separately
  - Stateless firewall

Evolution of Network Security Tools (2)

- First Stateful Firewall
  - AT&T Bell Laboratories, 1989
  - Keep track of established connections
  - Packet is part of an existing flow
- Routers with integrated firewall
  - Cisco Integrated Services Router (ISR)
- Dedicated firewall equipments
  - Cisco's Adaptive Security Appliance (ASA)
  - Context-aware firewall

Evolution of Network Security Tools (3)

- Threats become more sophisticated
  - Network filters look into the network and application layer
  - Dynamic updates
  - Quick response times
- Cisco Security Intelligence Operations (SIO)
  - Cloud-based service
  - Global threat information, reputation-based services, complex analysis on network devices
  - Stronger protection and fast response times

What to secure?

What is there to secure?

- Stored data
  - Business data must not be leaked to competitors
  - Personal information
  - Copyrighted software
  - Securing data must also ensure persistence
    - Data must not be lost due to attacks or lack of skill
- Transactions
  - Protect information from being tampered with
  - Make sure that the sender is who he/she claims to be
  - Make sure the receiver is the one intended
  - Data is often sent across public (insecure) networks – it can easily be intercepted

Security Policy

- Complex document
- Secure network design and deployment
- Rules for:
  - Data access
  - Web browsing
  - Password usage
  - Encryption
  - Email attachments
- Specify the hierarchy of access permissions
  - Minimal access
- Protected assets, security devices, mitigation techniques

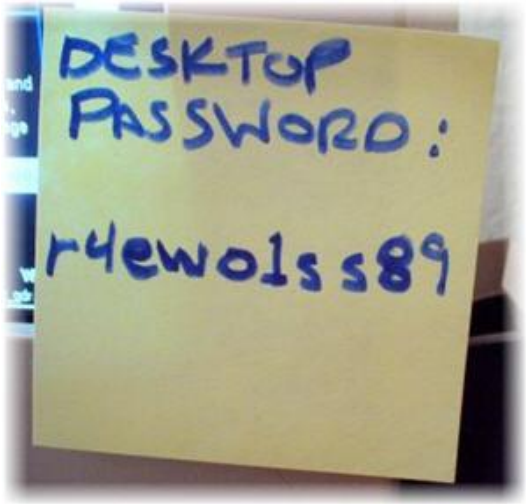
Social Engineering

Security and humans

- Security policies must be in place

  …and must be followed

- Regardless of how strong (and expensive) your secure deployment is:
  - Humans can still write their passwords on post-it notes
  - Humans can still give their passwords to anyone they trust
  - Humans can still open tempting attachments…



Social engineering

- Non-technical intrusion
- Involves tricking people to break security policies
  - Manipulation
- Relies on false confidence
  - Everyone trusts someone
  - Authority is usually trusted by default
  - Non-technical people don’t want to admit their lack of expertise
    - They ask fewer questions
  - Most people are eager to help
    - When the attacker poses as a fellow employee in need

Social engineering

- People are not aware of the value of the information they possess
- Trust, vanity, eavesdropping, etc.
- Obtain passwords, confidential data/documents, physical access to devices, etc.
- When successful, social engineering bypasses ANY kind of security

Least Privilege Principle

Security and Complexity

- Downside: Complexity brings vulnerability
  - How secure is a 1000-computer network with >1000 users and 200 different applications?
  - How secure is a simple button?
- Still, we DO need complexity to accomplish our tasks
  - … so security becomes a continuous process

…and a tedious one!

Least Privilege

- Complex systems are more difficult to secure
- The more application deployed, the more possible vulnerabilities

- Users and applications must receive the **least** amount of privileges as possible
- “The things you have access to are the things you can break”

The Final Truth

"There is no security on this Earth.
There is only opportunity."

Douglas MacArthur

US WWII general & war hero