CE 817 - Advanced Network Security

Lecture 1

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

How to think about insecurity

- The bad guys don’t follow the rules
- To understand how to secure a system, you have to understand what sort of attacks are possible
- NOTE: That is not the same as launching them

Data Breach

- Major retailer, TJX
  - Disclosed massive data breach of its network in 2007 (1386)
  - Estimated 94 million accounts compromised
    - Customer records
    - Credit card accounts

- Other data breaches
  - LinkedIn
    - 2012, 6.5 million user passwords stolen
  - Dropbox
    - 2012, user passwords stolen
  - .....

Code Red

- Worm released July 13, 2001 (1380)
- Exploited buffer overflow on unpatched Microsoft Servers
- 395,000 computers infected in one day alone
- It defaces Web sites and launches Trojan code in a denial-of-service attack against fixed IP addresses,
  - including the White House and Microsoft.
- The event prompts the director of the FBI's National Infrastructure Protection Center to hold a press conference.

Botnets

- The Department of Defense discovers computer systems compromised and turned into a botnet to send spam, launch DoS attacks and commit other crimes in 2004 (1383)
  - Ancheta, 20 years old, admits to generating more than $107,000 in payment for sending spam or launching DoS attacks through 400,000 infected computers.
- Amazon, eBay, Yahoo, Dell, E-trade and CNN are all struck down by a massive distributed denial-of-service attack in February 2007 (1386)
- Storm Botnet
  - Discovered in early 2007 (1386)
  - Compromised machines used for spam and phishing attacks
  - Compromised machines estimated from a few million to 50 million [Messmer 08]

Phishing

You have 1 New Alert Message
This is to inform you that Mohammad Fazli has
transferred **100,000,000 Rial(s)** to your Mellat account via Ebank mellat.
Please check your account balance.

To Login, please click ebanking.bankmellat.ir/ ebanking

Bank Mellat Ebanking
This is a system generated email. Please do not reply to it.
Copyright 2009 Bank Mellat Iran.

Cyber War

- Estonia, a country of about 3 million people bordering Russia, has a well-developed network infrastructure
- After a dispute with Russia, it came under a crushing cyberattack in 2007
- most important government, banking and media Web sites unavailable
- Security experts analyzing the cyberattack believe it was triggered by the "Russian blogosphere," which triggered a second phase that included specially designed bots, dropped onto home computers

It happens Quickly

- A student in our lab installed an unpatched Linux distribution
- Left it connected to internet overnight
- Next day the university admin was notified by the university service provider that a compromised machined in the university was causing trouble
- There was allot of yelling directed at the student!

Details on the Course

Administrivia

- Website:
  - sharif.edu/~kharrazi/courses/40817-931/
  - You are expected to check the website regularly
- Mailing List
  - Register for it
  - Registration link will on the website

Administrivia

- Prerequisites
  - Computer networks
  - Data and network security
- Grading (tentatively)
  - 50% Homework
  - 50% Final

References

- Lot’s of research papers

Policies

- Late Homework
  - One day late will cost you 25%, two days 50%, and three days 75%.
  - No homework will be accepted after the third day.
- Cellphones
  - Please turn them off before entering class.
- Cheating and Copying
  - First time you are caught you will get a zero for the task at hand.
  - Second time you are caught you will fail the course.
  - Providing your assignment to someone else is considered cheating on your behalf.

Ethics of security

- Taking a network security class is not an excuse for hacking
- “Hacking” is any form of unauthorized access, including exceeding authorized permissions
- The fact that a file or computer is not properly protected is no excuse for unauthorized access
- Absolutely no Trojan horses, back doors, or other malicious code in homework assignments

Network Security

Goals

- Usual security trinity: confidentiality, integrity, availability
- Must insure these in two domains:
  - Over-the-wire
  - On the host (for network connected applications)
- Strategies are very different

Host

- The host is (or can be) well-controlled
- There are well-developed authentication and authorization models
- There is a strong notion of privileged state, as well as what program can use it
- Non of that is true for networks

Networks

- Any one can (and does) connect to the network
- Connectivity can only be controlled in very small, well-regulated environments, and maybe not even then
- Different operating systems have different notions of userIDs and privilages

Benign Failures

- On top of that, most network failures are benign
- You have to program for such failures:
  - data corruption, timeouts, dead hosts, routing problems, etc.
- Anything that can happen by accident, can happen by malice. ONLY MORE SO.

Trust Nothing

A host can trust nothing that comes over the wire

Unproductive Attitudes

- “Why would anyone ever do that?”
- “That attack is too complicated”
- “No one knows how this system works, so they can’t attack it”

Better Attitudes

- Assume that serial number 1 of any device is delivered to the enemy
- You hand your packets to the enemy to deliver; you receive all incoming packets from the enemy

Familiar?

- SYN flooding
- Trojans
- Bloom filters
- Onion routing
- Snort
- tcpdump
- Traffic analysis
- TCP 3-way handshake
- Code Red
- Buffer Overflow
- IP Fragmentation
- man-in-the-middle attack

Familiar?

- IDS
- Wireshark
- IP Spoofing
- ICMP Redirect
- OS Fingerprinting
- DNS Cache Poisoning
- DDoS
- Botnets
- Phishing
- BGP
- Morris worm

Course Outline

- Threats and Attacks
- Firewalls
- IDS/NIDS
- DoS/DDoS
- Worms/Malware
- Botnets
- Honeypots
- Spyware
- Phishing

Course Outline

- Privacy/Traffic Analysis
- Anonymity
- Routing Security
- Network Forensics
- Wireless Security
- VoIP Security

Homework 0

- Watch the video by Dr. Kiarash Bazargan on scientific ethics (will post the link on the web):

http://profs-against-plagiarism.blogspot.com/2008/09/blog-post_14.html

Acknowledgments/References

- [Bellovin 06] COMS W4180 — Network Security Class Columbia University.
- [Messmer 08] 10 of the Worst Moments in Network Security History, Events that shock sensibilities and shaped the future, By Ellen Messmer, Network World, 03/11/08