Network Threats

Khaled Harras
School of Computer Science
Carnegie Mellon University

15-349 Computer and Network Security
Fall 2012

Some material borrowed from Hui Zhang and Adrian Perrig and google images
What did we talk about?
How are Networks “different”?

- **Distributed system**: Avoids single point of failure, is fault tolerant

- **Network Environment**
  - Anonymity (Who’s behind the machine?)
  - Automation (Are humans needed?)
  - Distance (So where is Google exactly?)
  - Opaqueness (Am I talking to the same entity?)
  - Routing Diversity (How many routes are there to Google?)

- **Network Topology**
  - The way in which networks are configured
  - Boundary, Ownership, Control
  - LANs, WANs, internets (not “I”nternet)
Catching-up…

- **Protocols**
  - Defining rules of communication
  - Each protocol offers an interface to its users
  - Protocols build on each other (Http->TCP->IP->Ethernet)

- **Layers**
  - Each layer relies on services from layer below and exports services to layer above
  - Interface defines interaction
  - Hides implementation - (black box)

- **Challenges**
  - Applications (Depends on what you need)
  - Transport (connection establishment, reliability, congestion control, error control, in-order delivery)
  - Network (Addressing, Routing)
  - Data-Link (Medium access control, error control,
Degradation of Internet Security

- Internet has become communication infrastructure for government, economy, society, even for safety-critical uses
- Unfortunately, trust assumptions of the early Internet do not scale to billions of users
- Indeed, hackers, criminals, terrorists, military all use the Internet for their activities
- All this, and so much more, was designed without considering security issues
- What do we do now???????????
Wear your security hats…
Today, we’re the bad guys!
Why are networks vulnerable?

- Anonymity and distance
- Many points of attack (both ways!)
- Sharing (services, files, or even medium!)
- Complexity and Heterogeneity
- Unknown paths
- Protocols were not designed with security in mind
Why attack networks?

- **Challenge & Fame**
  - Most repeat, but who will find the new exploits?

- **Money**
  - Industrial espionage (IP theft)
  - Organized Crime
    - Ex: In 06, Jeanson James infected $400,000 machines, and rented their use to others!

- **Ideology**
  - Hactivism: Disrupting operations without serious damage
  - Cyberterrorism: Politically motivated hacking to inflict damage
What do we do before entering a war?

- Reconnaissance
- Intelligence
- Interception
- Analyze info then Attack!
Reconnaissance

- Learn as much as possible about your target
- Ports are doors through which any network service communicates
- Port Scanning
  - Which ports or services are running
  - What operating system is installed
  - What applications and versions are running
- We now have an external picture, how about what’s inside?
Intelligence

- Social Engineering
  - What will you say to a yelling VP?

- Intelligence & Info gathering
  - Dumpster diving
  - Eavesdropping on employees
  - Befriending
  - Documentation!
  - Blogs, chats, bulletin boards...etc

- OS and App Fingerprints
  - Which web server, what version?
  - Protocols are standardized but implementations may slightly differ. Which protocol implementation?
Interception

- **Eavesdropping**: passively listen on a wire
- **Wiretapping**: Actively inject data into communication stream
- **How? Sniffing**: Depends on the communication medium
  - Cable: Splicing, Inductance (read emitted radiation)
  - Wireless: Share the same medium!
  - Fiber: Much harder
- **We now analyze our data, prepare our troops, then launch our attacks!**
Attacks – Authentication and Protocol Flaws

- **Authentication-based**
  - No authentication, Easy to guess passwords, Unencrypted and easy to “hear”

- **Protocol Flaws**
  - Ex: Sequence numbers in TCP
  - Implementation-related flaws (Ex: MS RPC service failure with incorrect packet format in 2003!)
  - Incomplete protocols…!
Attacks – Spoofing

- Pretending to be someone/something else
- Masquerading: One host pretends to be another (xyz.com, xyz.org)
- Phishing: Send emails that seem real, make you go to a spoofed location
- Session Hijacking: taking over an active session at some point (Ex: during checkout!)
- Man-in-the-middle: full interception and relaying of messages
Attacks – Web Vulnerabilities

- Defacement: Changing the way the site looks. Attack gains visibility
- Buffer overflows
- ../: The predecessor directory might return requested - not supposed to be seen- files
- Changing parameters in web-apps code.
- Attacks so far are related to confidentiality and integrity… How about availability?
Attacks – Denial of Service (DoS)

- Physical threats!
- Connection Flooding
  - ICMP flooding: Constant Ping requests (Ping of death)
  - Smurf: broadcasted ping, with return address of victim
  - SYN flood: Maintain connection start queues (SYN_RECV)
- Traffic redirection (from routers!)
- DNS cache poisoning
  - DoS, or advertising!
Oh my...
What do we do now?!