What is the Internet?

Session 6: Internet Security

Elena Silenok @silenok
Charlie Robbins @nodejitsu

Questions? Just Raise Your Hand

Topics

- Ports / Protocols / OS / Packets
- Types of Threats
  - Worms, viruses
  - Social engineering, phishing
  - Facebook / data sharing
  - Mobile
- Ways to mitigate the vulnerabilities

Ports

- Communications endpoint
- Used by TCP/IP, UDP
- Identified by IP address, port number, protocol
- Numbered 0 to 65535
- HTTP 80, HTTPS 443, SMTP 25, DNS 25, FTP 21
- Make computer communication easier

Port Scanning

- Attack that that sends a request to a port on a host in an attempt to find a vulnerability
- Background and targeted
- Script kiddies & more serious attackers
- Illegal in most countries without legitimate motive
- ISP/Firewall protection and blocking

Worms/Viruses/Trojans

- Creeper (1971), Elk Cloner (1981)
- Morris worm (Robert Morris, MIT CSAIL), 1988
- Virus needs a host file, worm doesn't
- Worms normally don't need user action
- Trojans seem useful but are malicious, can install backdoors (granting unauthorized access)

Social Engineering/ Phishing

- Phishing - masquerading as trustworthy
- “Verify your account”, “Confirm billing info”
- Over 70% success on social networks
- Spear phishing, whaling
- Link manipulation/website forgery

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Browser Security

- Phishing
- Malware, identity theft, fraud, espionage
- 1 in 10 pages may contain malicious code
- SQL injection
- Cross-site scripting (XSS), 70% vulnerable

SQL Injection

- Exploits database layer of an application
- Incorrectly filtered escape characters
- Incorrect type handling
- Blind SQL injection
- 2009 - US Justice Dept charged Albert Gonzalez and two unnamed Russians with the theft of 130 million cc numbers

Cross-Site Scripting (XSS)

- 80% of all vulnerabilities in 2007
- Twitter, MySpace, Facebook affected
- Persistent and non-persistent (reflected)
- Traditional and DOm-based

Non-persistent XSS scenario

1. Alice goes to Bob's website, logs in, and stores her billing info.
2. Mallory observes that Bob's website contains a reflected XSS vulnerability.
3. Mallory sends Alice an email with the URL that points to Bob's website but contains Mallory's malicious code
4. Alice clicks on this URL and visits the URL provided by Mallory while logged into Bob's website.
5. The malicious script embedded in the URL executes in Alice's browser, as if it came directly from Bob's server (this is the actual XSS vulnerability). Script sends session cookie to Mallory. Mallory steals Alice's info (authentication credentials, billing info, etc.) without Alice's knowledge.

Persistent attack

Mallory posts a message with malicious payload to a social network.

1. When Bob reads the message, Mallory's XSS steals Bob's cookie.
2. Mallory can now hijack Bob's session and impersonate Bob.

Cross-site request forgery (CSRF/XSRF)

1. Mallory posts a message with malicious code pointing to Bob's bank's website

```
<img src="http://bank.example.com/withdraw?account=bob&amount=1000000&for=mallory">
```

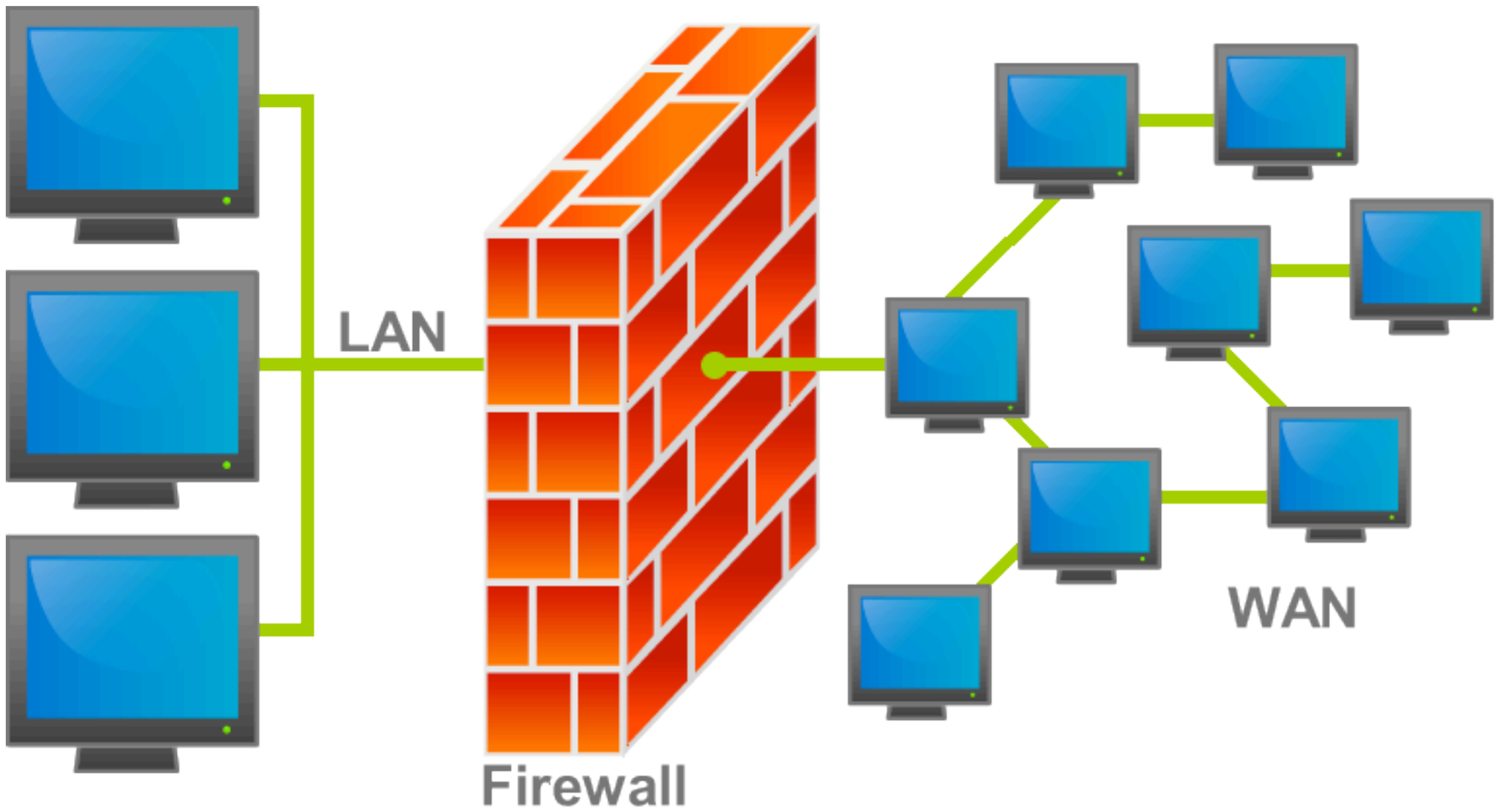
2. If Bob's bank keeps authentication info in a cookie, and cookie hasn't expired, BAD NEWS!

3. Bob's browser tried to load an image, instead executes a withdrawal request without Bob's approval

Wireless security

- Data sent unencrypted unless using HTTPS
- Accidental association
- Ad-hoc network (Microsoft "on" by default)
- Bluetooth - not secure
- MAC spoofing
- Man-in-the-middle
- Denial-of-Service attack

Firewall



Firewall (cont.)

- Device or software that permits/denies network transmissions based upon a set of rules
  - 1st gen: Packet filters (source/destination, type)
    - 1988, DEC, later AT&T Labs
  - 2nd gen: Application layer (content, use)
    - "Next gen" - most modern firewalls
  - 3rd gen: "Stateful" filters (connection-based)

User-side protection

- Do not open attachments that look suspicious
- Type in the website URL manually
- Only run software/visit websites you trust
- Update your software/OS/antivirus regularly
- Use a firewall (especially on a PC)
- Firewall / Antivirus / Adware removal

Laws

- Most of these activities are obviously illegal
- Port scans made illegal in the last 10 years unless used for legal purposes
- Botnets - international operations
- “Kill switch bill”

Questions/Suggestions?

- Elena Silenok
  - silenok@gmail.com, twitter: @silenok
- Charlie Robbins
  - charlie@generalassemb.ly, twitter: @nodejitsu