Network Security Practices – Attack and Defense

Vulnerabilities

How does a computer get infected with malware or being intruded?

- Executes malicious code (email attachment, download and execute trojan horses, use infected floppy/thumb drive)
- Vulnerable services that receive traffic from the network (e.g., ftpd, httpd, rpc,…)
- Vulnerable client programs (e.g., web browser, mail client) that receive input data from network
- Read malicious files with vulnerable file reader program
- Configuration errors (e.g., weak passwords, guest accounts, DEBUG options, incorrect access control settings, etc)

Defense Strategies

- Remove vulnerabilities from software
- Make vulnerabilities not exploitable
  - reactive, many mechanisms, none perfect
- Active response to malware and exploits (to vulnerable software)

Why Software Has So Many Bugs?

- Software is complicated, and created by human
- Each software is created once
- Software is exploitable in the cyber world
- Market failure for secure software
  - Market failure: a scenario in which individuals' pursuit of self-interest leads to bad results for society as a whole
  - Vendor has no incentives to produce higher quality software.
  - Users cannot just vote for security with their money.
    - lack of measurement for security

Why Vendors Lack Incentive to Produce More Secure Software

- Cash flows when product starts shipping.
- Market dominance is key to success
  - being first often means becoming de facto standard
- No liability means no need to worry about correctness and thorough testing.
- Bugs can be patched with little cost. No expensive recall.
- Thorough testing is inefficient. Let the users test it and fix only the bugs that affect users

The Perversity on Patching

- Even if thoroughly testing software were possible, venders ultimately have a perverse incentive not to make better software
- Releasing a patch costs little
- Buggy / Vulnerable software can force users to upgrade
  - Achieving market dominance means competing with previous versions
  - Stop releasing patches for old versions can force users to upgrade
- Patching provide an opportunity of offering new licensing terms