Revising Previous Material

Sankardas Roy
Department of Computing and Information Sciences
Kansas State University
What We Learned Thus Far

- Computer / software vulnerability is very common

- How an adversary exploits a vulnerability to launch an attack
  - As an example, the attacker can get an “admin shell” to a remote victim computer when a user opens a malicious web page

- The common countermeasures are firewall, software updates, anti-malware, etc.

- For web browsing, we should use HTTPS protocol
  - It ensures confidentiality and authentication while HTTP does NOT

- Do not add exceptions when we get certificate error
  - We should not proceed to visit the particular web site unless we are very sure
Questions

- In the “malicious web page” demo, the attacker gets a “remote shell” to the victim’s machine
  - How to prevent/detect this attack?
  - Can firewall (on victim’s machine) help prevent this attack?

- In typical HTTPS sessions, the web server first authenticates to the browser by presenting a certificate.
  - Why? Why cannot the browser authenticates itself first?

- In the MITM demo with the proxy server
  - Why does the Firefox browser forward the traffic to the proxy server?
  - How can you detect this forwarding in the Firefox setting?
  - What certificate does the browser receive? From whom?
Reminders

- Please answer/work on each part of the homework problem
  - Otherwise, you will not get full points

- Please carefully observe your homework grade
  - KSOL can show some “zeros” by default

- You can always email me (sroy@ksu.edu) if any confusion
  - We can meet off the class

- Please attend each class
  - 30% of the grade comes from the class participation
  - Ask questions; raise relevant issues in class or via emails