Revising Previous Material

Sankardas Roy
Department of Computing and Information Sciences
Kansas State University
What We Learned in the Last Class

- Open public WiFi hotspots pose many threats
  - Eavesdropping
  - Web session hijacking
  - Existence of a fake AP

- We discussed two standard solutions
  - Access only secure websites (HTTPS)
  - Use a VPN connection (e.g. run the KSU VPN client in full mode)
Questions

- How far does HTTPS / VPN connection prevent us from the “fake AP / evil twin” attack?

  - Is MITM still there? Does our data still flow through the fake AP?
  - Can the attacker get confidential information?
Reminders

- The next class (smart phone security) will be in Room 128
  - Get credentials to use computers in Room 128

- 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