Lecture 13: Network Security

Date: October 25, 2013 ***Homework Due***: Nov. 1 at 5:00pm

Puzzle. Sarah Palin's email account was compromised because the attacker could ask that the password be reset and then answer the three security questions based on public information from Sarah Palin's Wikipedia page. Suppose she asked you how she could prevent this from happening again. What would you suggest?

1. Personal firewalls
2. Computer science view of networks
   a. Layers
   b. Networks and subnets
   c. IP addresses and port numbers
   d. Connection vs. connectionless communication
3. Protecting network traffic with encryption
   a. Link encryption
   b. End-to-end encryption
   c. Virtual private networks (VPNs)
4. Basic network protocols
   a. icmp: Internet control management protocol
   b. tcp: transport control protocol; three-way handshake to open connection
   c. dns: domain name system; and dnssec (dns secure)
5. About the cloud
   a. Origins: VPNs; large-scale distributed computing (SETI@home)
   b. Why create and use a cloud?
   c. Idea: share large-scale resources among many clients; called a "Service-Oriented Architecture" (SOA)
   d. Types of services: software (middleware or in support of other services), applications, business processes, etc.
   e. Examples: salesforce.com, Amazon Web Services Elastic Compute Cloud (E2C), Web 2.0
6. Security in the cloud
   a. Encryption of data – who does this, user or cloud provider?
      i. User: cloud can store encrypted data, but operating on it is hard ("homomorphic encryption")
      ii. Cloud: user must trust cloud to protect the data
   b. Preventing unauthorized access or changes to data
      i. Physical security: how does the provider protect access?
   c. Keeping data available at all times
   d. Legal considerations
      i. Differences in laws; whose apply to data?
      ii. Differences in policies among cloud providers
      iii. Public clouds vs. private clouds