

Lecture 10: Identity Management

Date: October 18, 2013

Homework Due: Oct. 18 at 5:00pm

1. Challenge-response
 - a. Computer issues challenge, user presents response to verify secret information known or item possessed
 - b. Example operations: $f(x) = x + 1$, x random; string (for users without computers); something based on time of day; computer sends $E(x)$, you answer $E(D(E(x)) + 1)$
 - c. Note: password never sent on wire or network
2. Biometrics
 - a. Depend on physical characteristics
 - b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
3. Location
 - a. Bind user to some location detection device (human, GPS)
 - b. Authenticate by location of the device
4. Multi-factor authentication
5. Identity on the computer
 - a. Real identity
 - b. Effective identity
 - c. Audit identity
6. Host identity
 - a. MAC address
 - b. IP address (static, dynamic)
 - c. Binding MAC address to IP address
 - d. Host name
 - e. Domain name service
7. Web identity
 - a. Cryptographic Key Infrastructure
 - b. Certificates (X.509, PGP)
 - c. State and cookies
8. Anonymity