• Authentication
  1. Multifactor Authentication
     a. Something an individual “knows”
        i. Password
        ii. Challenge questions
     b. Using something you “possess”
        i. Types of cards/tokens used
           1. Embossed – raised characters on a card
           2. Magnetic stripes – ie Bank Cards
              a. Added pin number on back of card to increase security.
           3. Memory – Electronic Memory inside
              a. Does not process data
              b. Vulnerable to theft/loss
           4. Smartcards / Smart Tokens –
              a. Takes different forms
              b. Typically has a microprocessor on it.
              c. Likely time sync’d to address replay attacks.
              d. Vulnerable to being stolen
              e. Expensive
        ii. All require a registration system.
     c. Something the individual “is”
        i. Biometric – Creates a digital template
           1. Examples
              a. Fingerprint
              b. Retina / Iris
              c. Facial Recognition
              d. Voice
              e. Handwriting
              f. Hand Geometry
              g. Signature
           2. Has to deal with some uncertainty.
              a. False matches and False non-matches
                 i. Typically done by plotting them on a bell curve and taking the highest point.
                 ii. Want to enforce false matches kept to a minimum
                 iii. At times we may want minimize false non-matches
                    1. “More Suspects the better”
                    2. Can always discount later.
                    3. Limit User frustration
        3. Accuracy vs Cost
           a. Iris – Very Accurate but Costly
b. Various Charts in notes showing accuracy of each method

4. Enrollment
5. Attacks on Data itself become an issue.

d. Something the user “does”

2. Remote Authentication vs Direct Authentication
   a. Remote
      i. Some random number is generated and sent to the host along with the password or whatever is used
      ii. Host then uses both to Authenticate.
      iii. Generally relies on some form of challenge/response
      iv. Types of attack to protect against
         1. Replay Attacks
         2. Eavesdropping
         3. Table 3.4 – Potential Attacks and Defenses

3. Authentication Security Issues
   a. Denial of Service
   b. Trojan Horse
   c. Client Attacks
   d. Replay
   e. Host Attacks
   f. Eavesdropping