CS530 Authentication

Bill Cheng

http://merlot.usc.edu/cs530-s10

Identification vs. Authentication

- Identification
  - associating an identity (or a claimed identity) with an individual, process, or request
- Authentication
  - verifying a claimed identity
- Ex: user ID is identification, password is authentication

Basis for Authentication

- Ideally
  - who you are
- Practically
  - something you know
    - e.g., password
  - something you have
    - e.g., smartcard, magnetic stripe card, passport, driver's license
  - something about you
    - e.g., face, hand, voice, fingerprint (i.e., biometrics)
    - sometimes mistakenly called things you are
- Note: policy determines how and what to do

Something You Know

- Password
- Algorithm
  - e.g., encryption key derived from password
- Issues
  - someone else may learn it
    - find it, sniff it, trick you into providing it
      Ex: e-mail from eBay or Paypal asking you to validate your password
  - other party must know how to check
    - keep in table
      once this table is obtained, the attacker may use it to login to other systems
  - you must remember it (tend to use same password)
  - how stored and checked by verifier

Examples of Password Systems

- Verifier knows password
  - can one crack password one letter at a time (as often seen in movies)?
    - timing attacks (look at power consumptions, time between successive guesses)
- Encrypted Password
  - one way encryption
  - Ex: UNIX
    - login name, UID, GID, encrypted password all stores in /etc/passwd
    - old systems make /etc/passwd globally readable
    - new systems move encrypted passwords to /etc/shadow
    - salt the password (~ 24-bit salt) to protect against pre-computed dictionary attack

Examples of Password Systems (Cont...)

- Third Party Validation
  - Ex: Liberty Alliance
    Microsoft Passport
    Kerberos
    Public key systems with Directory Services

Attacks on Password

- Brute force
- Dictionary
- Pre-computed Dictionary
- Guessing
  - what's your pet's name? (favorite city, birth place, ..)
- Finding elsewhere
  - sitting in Windows' Registry
  - sitting on USB harddrive

Something You Have

- Cards
  - mag stripe (= password?)
  - smart card, USB key
    - something your device knows
    - verifier knows that the device is present
  - time varying password
    - secure ID card
    - challenge/response card
    - smartcard requires special reader, this does not
      the user is the device
      limited data length to reduce human mistakes
- Issues
  - how to validate
  - how to mail (i.e. infrastructure)

Something About You

- Biometrics
  - measures some physical attribute
    - iris scan (can't really scan the retina)
    - fingerprint
    - picture
    - hand scan (geometry of hand)
    - voice
    - keystroke patterns?
- Issues
  - how to prevent spoofing
    - solved when biometric device is trusted/secure, not solved otherwise
  - fingerprint reading device at home, is that a good idea?
    - must be connected to a tamper-proof device

Other Forms of Authentication

- IP address, MAC address
  - e.g., NFS, DHCP
- Caller ID (or call back)
  - also works with e-mail
- Past transaction information
  - e.g., what's the amount of your last bill?

"Enrollment" (for Something You Know)

- How to initially exchange the secret
  - in-person enrollment
  - information known in advance
    - e.g., what's the amount of your last bill?
  - third party verification
    - e.g., a notary public
  - mail or email verification
    - e.g., activation code in e-mail, click here to activate

Multi-factor Authentication

- Require at least two of the three *classes* above
  - e.g. Smart card plus PIN
  - e.g. credit card plus zip code or billing address
  - e.g. biometric and password
- Issues
  - better than one factor
  - be careful about how the second factor is validated
    E.g., on card, or on remote system
    - PIN goes to remote system (or goes through smartcard and then remote system)

General Problems with Password

- Space from which passwords are chosen
- Too many passwords
  - and what it leads to
  - solution is "single sign on"?

Single Sign On

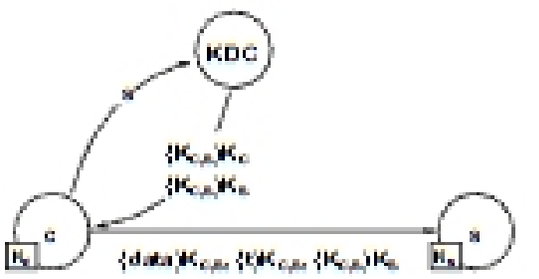
- "Users should log in once and have access to everything"
- Many systems store password lists
  - which are easily stolen
- Better is encryption based credentials
  - usable with multiple verifiers
  - interoperability is complicating factor
- Liberty Alliance
  - communicating information about authentication using a markup language (Security Association Markup Language)
- Microsoft Passport
  - original version based on cookies and hotmail passwords
  - next version based on Kerberos (cross realm authentication)

Encryption Based Authentication

- Proving knowledge of encryption key
  - nonce = non repeating value

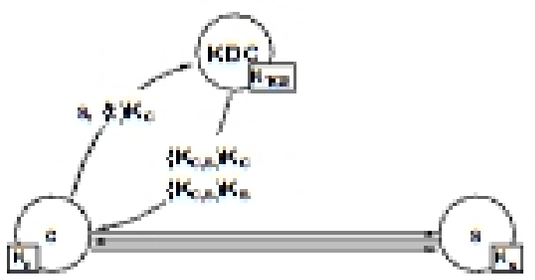
Authentication with Conventional Cryptography

- Kerberos



Authentication with Conventional Cryptography

- Kerberos or *Needham-Schroeder*
  - includes challenge/response
  - optional pre-authenticator in original message



Kerberos

- Third-party authentication service
  - distributes session keys for authentication, confidentiality, and integrity
    - KDC & TGS is usually combined
    - KDC can generate cross realm TGT (pre-arranged)