

University of Rochester  
CSC290B  
Introduction to Computer Security

---

Authentication & Identity,  
continued

January 29, 2009

# Previously, on CSC290B: Authentication

- Identity, stated
- Credentials, presented
  - E.g. passwords
  - Other factors
- Complementary information, checked
  - E.g. cleartext, or hashes
- Dictionary attacks
- Counter-measures
  - E.g. salted hashes

# Biometrics

- Automated measurement of biological, behavioral features that identify a person
  - Fingerprints: optical or electrical techniques
    - Maps fingerprint into a graph, then compares with database
    - Measurements imprecise, so approximate matching algorithms used
  - Voices: speaker verification or recognition
    - Verification: uses statistical techniques to test hypothesis that speaker is who is claimed (speaker dependent)
    - Recognition: checks content of answers (speaker independent)

# Other Characteristics

- Can use several other characteristics
  - Eyes: patterns in irises unique
    - Measure patterns, determine if differences are random; or correlate images using statistical tests
  - Faces: image, or specific characteristics like distance from nose to chin
    - Lighting, view of face, other noise can hinder this
  - Keystroke dynamics: believed to be unique
    - Keystroke intervals, pressure, duration of stroke, where key is struck
    - Statistical tests used

# Attacks on Biometrics

- Impossible to change
  - Therefore more like an identifier than an authenticator (see Riley reading)
- Fake biometrics
  - fingerprint “mask”
  - copy keystroke pattern
- Fake the interaction between device and system
  - Replay attack
    - *Authenticate the authentication device!*

# Authentication Systems: Location

- Based on knowing physical location of subject
- Example: Secured area
  - Assumes separate authentication for subject to enter area
  - In practice: early implementation of challenge/response and biometrics
- What about generalizing this?
  - Assume subject allowed access from limited geographic area
    - I can work from (near) home
  - Issue GPS Smart-Card
  - Authentication tests if smart-card generated signature within spatio/temporal constraints
  - Key: authorized locations known/approved in advance
    - *E.g.: If I know I'll be traveling, login from my office disabled!*

# Multiple Methods

- Example: “where you are” also requires entity to have LSS and GPS, so also “what you have”
- Can assign different methods to different tasks
  - As users perform more and more sensitive tasks, must authenticate in more and more ways (presumably, more stringently) File describes authentication required
    - Also includes controls on access (time of day, *etc.*), resources, and requests to change passwords
  - Pluggable Authentication Modules

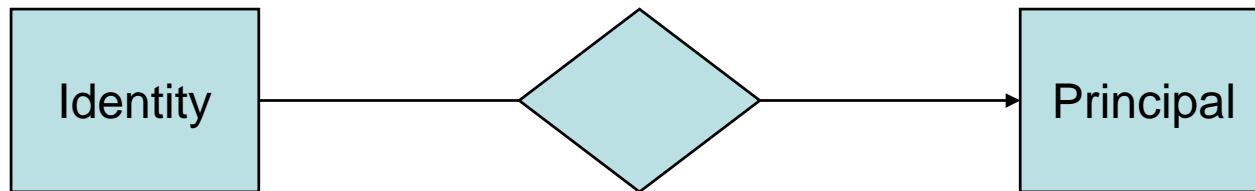
# Two significant authentication systems

- Kerberos: Trusted Key Distribution Center (KDC) authenticates a user, and issues encrypted tickets that applications use for further authentication. Users and applications use shared secret keys and symmetric encryption
- Public-key infrastructure (PKI) uses private keys for authentication, public keys for verification, and certificates for key management.
- We will discuss both, in detail, later!

# Authentication vs. Identity

- Authentication: Binding of identity to subject
  - We know how
  - We've discussed subjects
  - *But what precisely is identity?*
- **Principal**: Unique Entity
  - Subject
  - Object
- **Identity**: Specifies a principal

# Identity = Principal?



- Identity to Principal may be many-to-one
  - Given identity, know principal
  - Other direction unimportant?
- Examples: Unix
  - User identity
  - File identity

# What is a Principal?

- Entity
  - Subject
  - Object
- Also a set of entities
  - Think of subject as “power user”, not individual
- Examples:
  - Groups: defined collection of users with common privileges
  - Roles: membership tied to function

# Representing Identity

- Randomly chosen: not useful to humans
- User-chosen: probably not unique
  - At least globally
- Hierarchical: Disambiguate based on levels
  - File systems
  - X.500: Distinguished Names
    - /O=University of Rochester/OU=Computer Science/CN=bukys

# Internet Identity

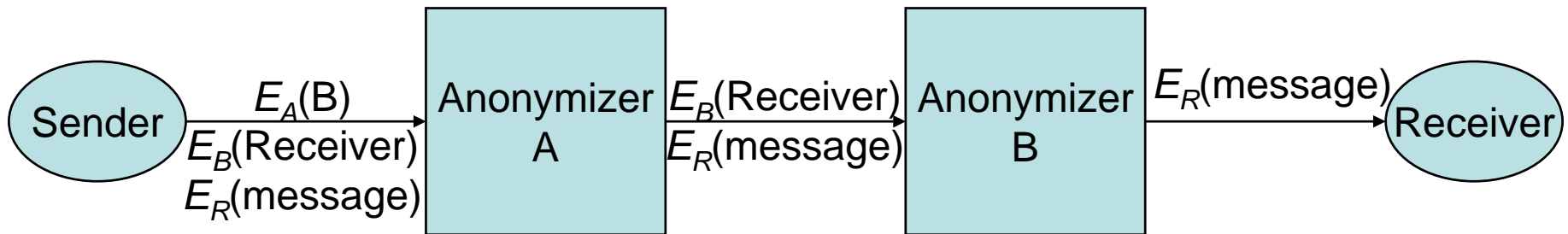
- Host Identity: Who is this on the network?
- Ethernet: MAC address
  - Guarantees uniqueness
- IP address: aaa.bbb.ccc.ddd
  - Provides hierarchy to ease location
- Domain Name Service
  - Human-recognizable name to IP
  - aliasing
- Issues: Spoofing
  - At any level, change mapping of identity to principal

# Anonymity

- What if identity not needed?
  - Web browsing
  - Complaints about assignments
- Removing identity not as easy as it sounds
  - I can send email without my userid
  - But it still traces back to my machine
- Solution: anonymizer
  - Strips identity from message
  - Replaces with (generated) id
  - Send to original destination
  - Response: map generated id back to original identity

# Anonymity

- Problem: Anonymizer knows identity
  - Can it be trusted?
  - *Courts say no!*
- Solution: multiple anonymizers
  - Onion Routing
  - Crowds



# Acknowledgements

- Substantial portions of these slides are courtesy of Matt Bishop and Chris Clifton and used with permission