Computer and Network Security

Lecture 8

Protocols

Outline

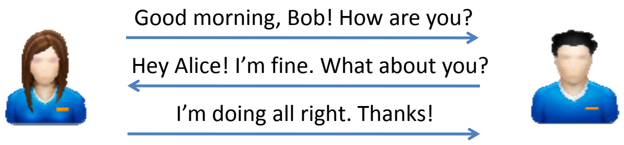
- Protocols
- Authentication
  - Standard techniques
  - Biometrics

Where are we now?

- So far…
  - Conventional cryptography
  - Hash functions and MACs
  - Public key cryptography
    - Encryption
    - Signatures
    - Identification (Fiat-Shamir), Zero Knowledge
- And now what?
  - Protocols
    - Authentication/Identification
    - Key distribution

Secure protocol

- A **protocol** is a set of rules for exchanging messages between ≥ 2 parties
  - Number of rounds (≥1)
  - Number of messages (≥1)


Good morning, Bob! How are you?
Hey Alice! I'm fine. What about you?
I'm doing all right. Thanks!

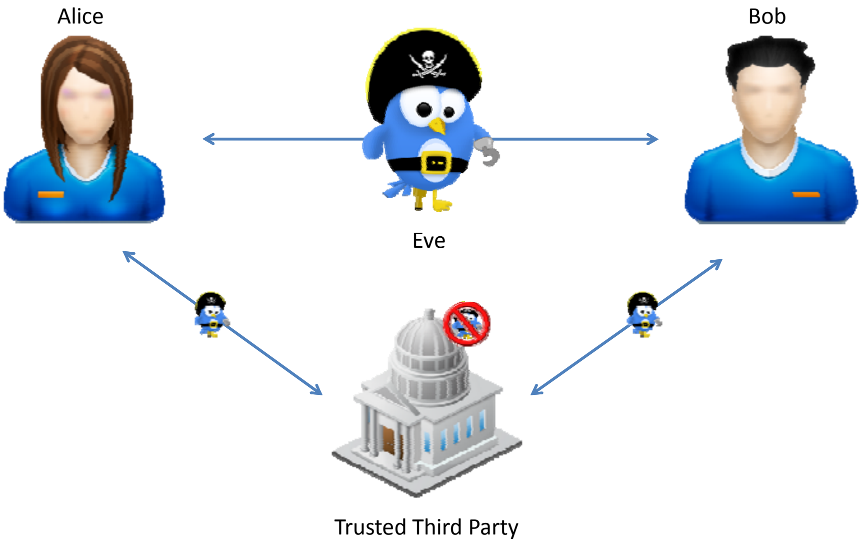
Secure protocol

- Message
  - unit of information send from one entity to another during a protocol run
- Round
  - Basic unit of time in a protocol

Secure protocol

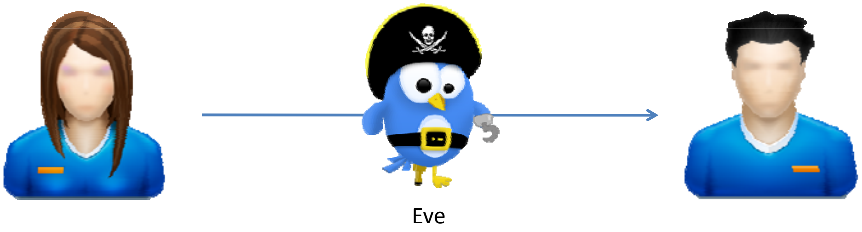
- When acting honestly, entities (participants) achieve the stated goal of the protocol
  - E.g, Alice successfully authenticates to Bob, or
  - Alice and Bob exchange a fresh session key
- Neither passive nor active adversary can defeat this objective
  - E.g., by successfully impersonating Alice in an authentication protocol with Bob

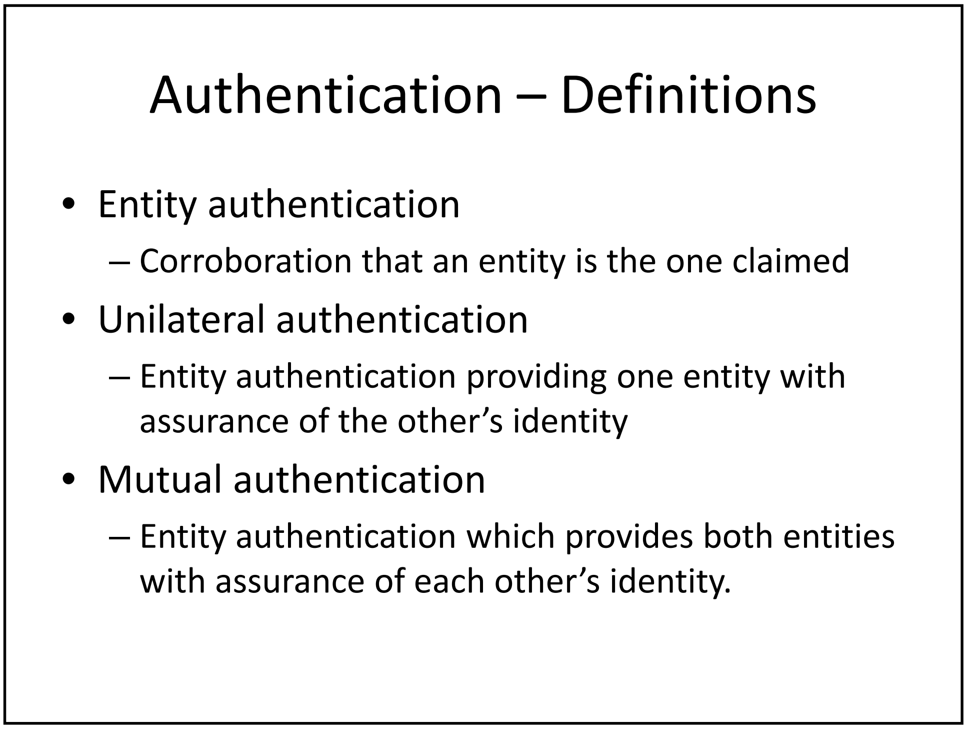
The entities



Authentication

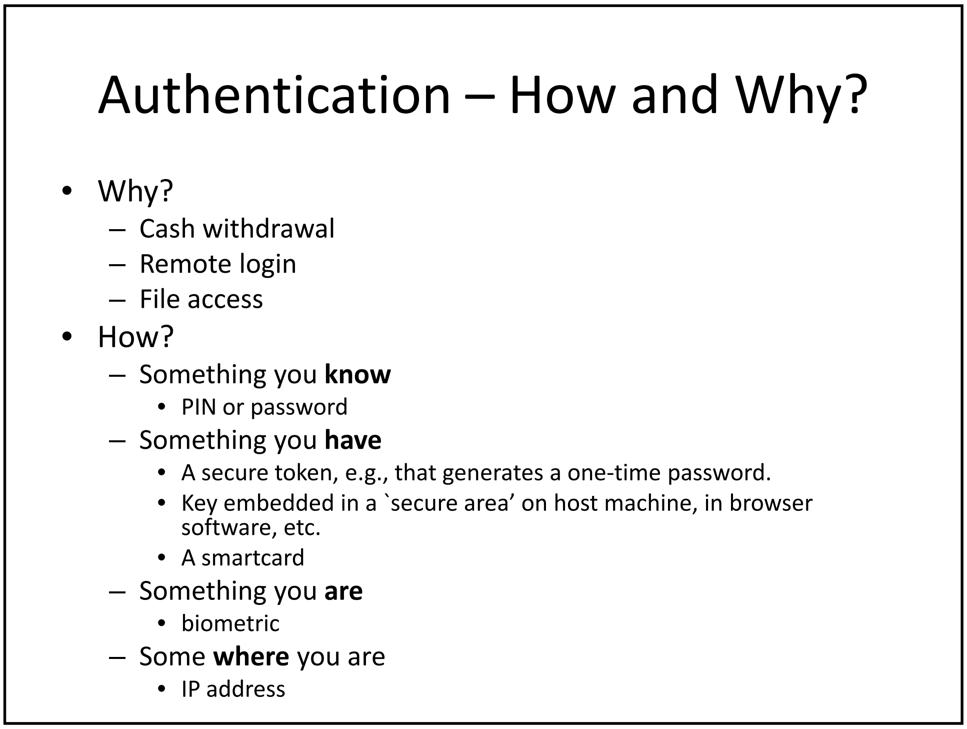
- How does Alice prove to Bob that she is indeed Alice?
  - Remind Eve is around…





Authentication – Definitions

- Entity authentication
  - Corroboration that an entity is the one claimed
- Unilateral authentication
  - Entity authentication providing one entity with assurance of the other's identity
- Mutual authentication
  - Entity authentication which provides both entities with assurance of each other's identity.

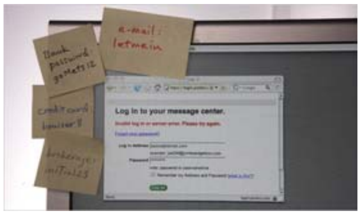


Authentication – How and Why?

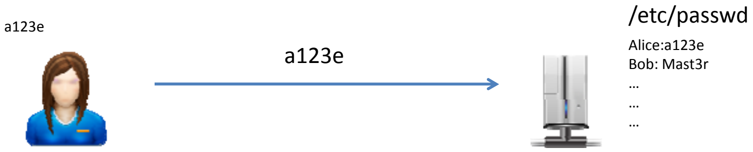
- Why?
  - Cash withdrawal
  - Remote login
  - File access
- How?
  - Something you **know**
    - PIN or password
  - Something you **have**
    - A secure token, e.g., that generates a one-time password.
    - Key embedded in a `secure area' on host machine, in browser software, etc.
    - A smartcard
  - Something you **are**
    - biometric
  - Some **where** you are
    - IP address

Password based authentication

- User has a secret password
  - System checks it to authenticate the user
- How is the password communicated?
  - Eavesdropping risk
- How is the password stored?
  - Clear
  - Encrypted
  - Hashed
- How does the system check the password?
- How easy is it to guess the password?
  - Easy-to-remember passwords tend to be easy to guess
- Password file is difficult to keep secret



Unix Passwords



a123e

a123e

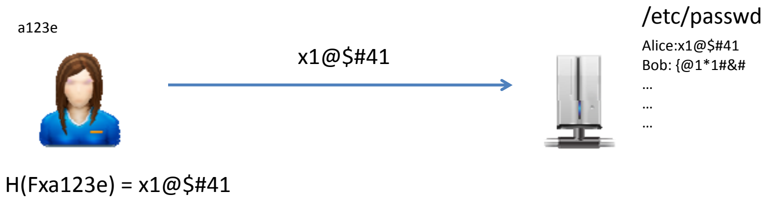
/etc/passwd

Alice:a123e
Bob: Mast3r
…
…
…

- Eavesdropper
- Intruder

- Brute force attack
- Dictionary attack

Unix Passwords



a123e

x1@$#41

/etc/passwd

Alice:x1@$#41
Bob: {@1*1#&#
…
…
…

H(Fxa123e) = x1@$#41

- One way?
- Collision resistance?

- Password reply?
- Brute force attack
- Dictionary attack (offline!)

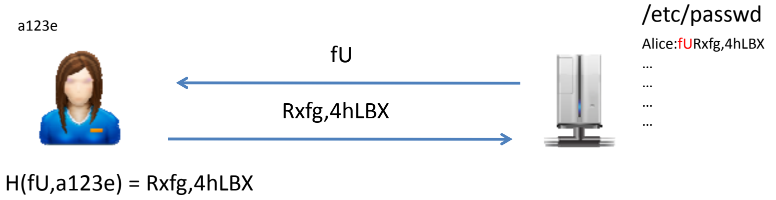
Unix Passwords

- char *crypt(const char *key, const char *salt);
- DES_k(m)
  - k = password
  - m= 000000
  - Truncates passwords to 8 characters!
  - Iterate 25 times
    - Discourage brute-force

- Relies on the randomness of the key
  - A, .., Z, a, .., z, 0, .. 9, +, -, … 94^8 possible password
  - Humans like to use dictionary words
    - Around one million passwords
      - Easy dictionary attack

Add a little Salt

- Alice:fURxfg,4hLBX:14510:30:Alice:/users/alice:/bin/csh
- Salt picked at password-creation time
  - 4096bits
  - Harder offline dictionary attack
    - 1M password now hash to 4096M strings



Weakest link

- No matter how secure the system is
  - The human factor is the problem!

- Write it down
- Use a single password at multiple sites
  - Do you use the same password for Amazon and your bank account?
- Make passwords easy to remember
  - “password”, “Kevin123”, “popcorn”
- Some services use “secret questions” to reset passwords
  - “What is your favorite pet’s name?”

Password Survey

- Klein (1990) and Spafford (1992)
  - 2.7% guessed in 15 minutes
  - 21% in a week
  - Sounds Ok?
    - Not if passwords last 30 days or more!
  - Much more computing power is available now!
- U. of Michigan: 5% of passwords were “goblue”
  - How many passwords on this campus involve “madrid”, “ronaldo”, etc.?

Biometrics

- Why?
  - Something you know might be
    - stolen
    - guessed
  - Nothing to remember
  - Passive (no typing, no choosing, …)
  - No sharing
- Two categories
  - Behavioral
    - Speech, keystroke timing
  - Psychological
    - Iris, Fingerprint, Face recognition

Authentication process

- Registration
  - Acquisition
  - Creation of Master characteristics
  - Storage of Master characteristics
- Authentication
  - Acquisition
  - Comparison
  - Decision

Biometric recognition errors

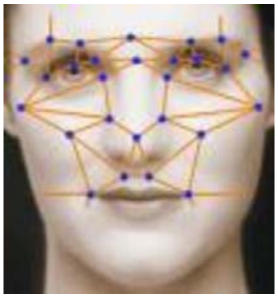
- Security is overestimated
  - Based on weak assumptions
- Error rates
  - Fraud = system accepts a forgery
  - Insult = system rejects valid user
  - Higher acceptance threshold
    - Higher fraud rate
    - Lower insult rate
- U.K. banks set target fraud rate of 1%, insult rate of 0.01% [Ross Anderson]

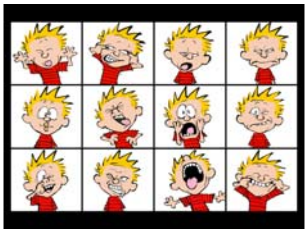
Finger Recognition

- Contact
- Dirt , grime and wounds
- Placement of finger
- Can be cloned… or cut!
  - – Play-Doh fingers fool 90% of fingerprint scanners
    - Clarkson University study

Face Recognition

- Contactless
- Light
- Expression





Voice Recognition

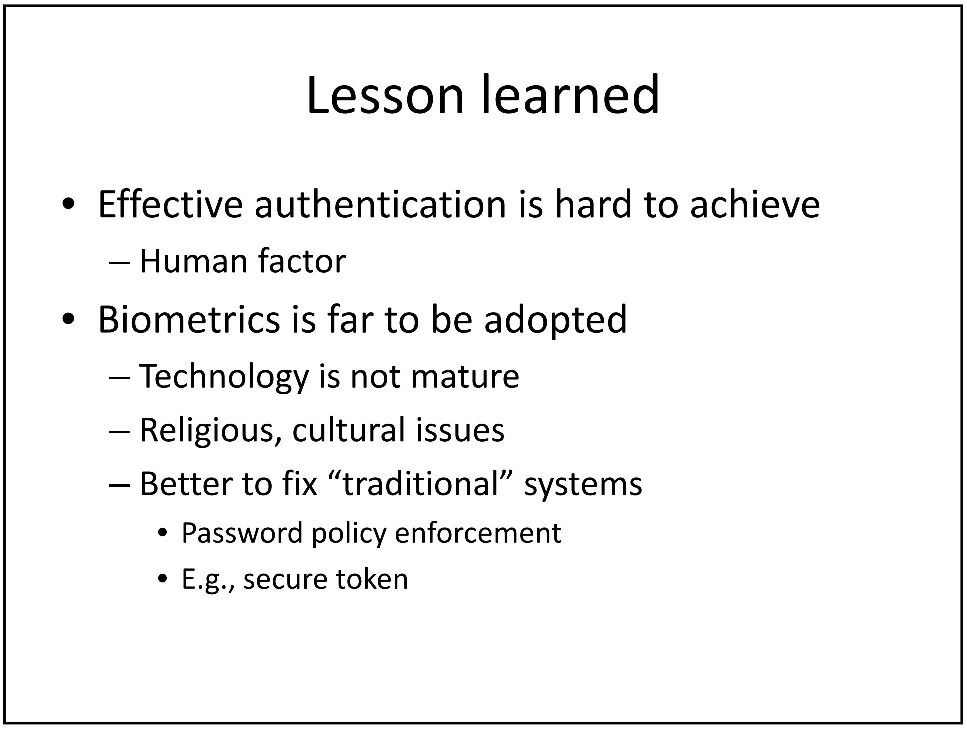
- Speech input
  - Frequency
  - Duration
  - Cadence

- Liveness
- Background noise
- Cold?

Signature recognition

- Speed
- Velocity
- Pressure

- Signature changes with
  - Age
  - Mood
  - Illness



Lesson learned

- Effective authentication is hard to achieve
  - Human factor
- Biometrics is far to be adopted
  - Technology is not mature
  - Religious, cultural issues
  - Better to fix “traditional” systems
    - Password policy enforcement
    - E.g., secure token