CS 3IS3 Fall 2007

04 Authentication

William M. Farmer

Department of Computing and Software
McMaster University

23 October 2007

Authentication Basics

- Authentication is the binding of an identity to a subject (Bishop).
- The following kinds of information can be used to confirm the identity of an entity:
  - Secret information that the entity knows (such as a password).
  - Certification that the entity has (such as a badge, card, or passport).
  - Physical characteristics of the entity (such as fingerprints or eye characteristics).
  - Location of the entity (such as at a particular terminal).
- The authentication process compares information from an entity with stored data about the entity.

Authentication System

- An authentication system is a tuple (A, C, F, L, S) where:
  - A is a set of authentication information with which entities prove their identities.
  - C is a set of complementary information that the system stores and uses to validate authentication information.
  - F is a set of complementation functions $f : A \rightarrow C$ that generate complementary information from authentication information.
  - L is a set of authentication functions $l : A \times C \rightarrow \{\text{true}, \text{false}\}$ that verify identity.
  - S is a set of selection functions that enable an entity to create or modify the authentication and complementary information.
- Example: Unix password system.

Passwords

- A password is information associated with an entity that confirms the entity's identity (Bishop).
- In an authentication system based on passwords, it is crucial that the passwords are protected.
- Two approaches to protecting passwords:
  1. Hide the information needed to verify a password. (In Unix, this is the passwords, the encrypted passwords, and the one-way function that is used to encrypt passwords.)
  2. Prevent access to the authentication functions. (In Unix, these are the login function, `su`, `sudo`, etc.)

Dictionary Attacks

- A dictionary attack is the guessing of passwords guided by a list of words called a dictionary.
- A dictionary attack type 1 compares the complimentary information produced for a list of guesses with the stored complimentary information.
  - Requires access to the complementation function and the stored complimentary information.
- A dictionary attack type 2 submits a list of guesses to an authentication function.
  - Requires access to the authentication function.
- Both types of attack can be automated.

Countermeasures for Type 1 Dictionary Attacks

- Random selection of passwords.
  - A brute force attack may work if the period of the password generator is too small.
  - The passwords are more likely to be written down.
- Pronounceable passwords.
  - The passwords are easy to remember.
  - A brute force attack may work if the total number of pronounceable passwords is too small.
- Proactive password selection.
  - Users may propose passwords but those that possess certain "easy to guess" characteristics are rejected.
- Salting.
  - The complementation function includes as input randomly selected data that is different for each user.
- Password aging.
  - A password must be changed periodically.
  - Makes it harder to remember passwords.

Countermeasures for Type 2 Dictionary Attacks

- Type 2 attacks cannot be prevented since legitimate users need to be authenticated.
- Countermeasures:
  - Exponential backoff for retries.
  - Disconnection.
  - Account disabling.
  - Controlled access (jailing, honeypots).

Challenge-Response Systems

- How a challenge-response authentication system works:
  1. The user and verifier agree on a secret function f.
  2. The verifier sends a random message m (the challenge) to the user and the user replies with a transformation m' of the message (the response).
  3. The verifier checks that $m' = f(m)$.
- A one-time password is a password that is invalidated immediately after it is used.
- How a time-synchronized one-time password system works:
  1. The verifier sends the user a value m.
  2. The user inputs m into a smart card.
  3. The smart card computes an output m' at time t using a time-dependent algorithm f.
  4. The user sends m' to the verifier.
  5. The verifier checks that $m' = f(m, t)$.

Biometrics

- Biometrics is the automatic measurement of biological or behavioral features that identity a person.
- Examples of biometrical features;
  1. Fingerprints: A graph is generated from an optically scanned fingerprint that is compared with a stored graph.
  2. Voice: Verbal answers to questions are recorded and then compared to stored recordings.
  3. Eyes: The iris or retina is scanned and then the resulting image is compared with a stored image.
  4. Faces: The face is scanned and then the resulting image is compared with a stored image.
  5. Keystrokes: An annotated keystroke sequence is recorded and then compared with a stored keystroke sequence.
  6. Combinations: Using more than one biometrical feature at a time greatly improves accuracy.
- Replay attacks are a danger with authentication based on biometrical features.

Location

- Since a person can only be at one place at a time, location can be used as a basis for authentication.
- The Global Positioning System (GPS) can be used to create a location signature.
  - The location signature is unique within a few meters and a few milliseconds.
  - The user and verifier create and compare location signatures.