Lecture 10

Authentication:
I am That, Thou are That,
All this is That

Wholeness Statement

Authentication is the process of reliably verifying the identity of someone (or something). In cosmic consciousness one's identity is associated with the Self, the field of pure consciousness. I am That.

Overview

1. Authentication uses one or more of the following:
   a. Something you know (password)
   b. Something you have (badge)
   c. Something you are (fingerprint)
   d. Where you are (in a locked, guarded room)
2. Passwords:
   a. Storing
   b. Selection
   c. Cracking
   d. Managing
   e. Protecting

Authentication

- Authentication is the process of reliably verifying the identity of someone (or something)
- Example of "something"
  - Directory service replicas might coordinate updates amongst themselves and need to prove their identity to one another.

Authentication

- Subjects inside a system act on behalf of some other, external entity such as Alice or Bob
- The identity of that external entity controls the allowed actions of its associated subjects
- Thus subjects must bind to the identity of the external entity

Definition 11-1. *Authentication* is the binding of an identity to a subject.

A subject is a computer entity such as a process

Establishing Identity

- External entities must provide something to confirm their identity
- That can be
  - Something they know (password)
  - Something they have (badge)
  - Something they are (fingerprint)
  - Where they are (in a locked, guarded room with a computer terminal)

Main Point

1. What you know authenticates who you are. In SCI, what you know depends on your state of consciousness.

80% of Problems

- The Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie-Mellon University (CMU) estimates that 80% or more of the problems they see have to do with poorly chosen passwords.

Passwords

- Sequence of characters
  - Generated by user, by computer from user input, or randomly
- Algorithms
  - Challenge-response, one-time passwords

Problems with passwords

1. Shoulder surfing
   It is good manners to look away if you are next to someone typing in their password.
2. Eavesdropping
   The password is sent in plaintext and somebody is using a packet sniffer
3. Server's password database can be compromised
   If attacker breaks into server database and passwords are stored in plaintext, then he has all the passwords. Course website stores the hash of your password in the database. (It is generally believed that far more passwords are stolen by breaking into databases than by eavesdropping with a packet sniffer).

Problems with passwords

4. People pick easy to guess passwords
   System can help make passwords harder to guess by rejecting easy to guess ones.
5. Crackable using a dictionary attack
   Attacker can write a program to try all the words in a dictionary.
6. Too complex a password will cause users to write it down (or having too many to remember)
7. Users can be tricked into giving out their password over the telephone.
   If you remember one thing from this lecture, let it be this:
   Never tell anybody your password!!.
   If somebody asks for your password, they are almost certainly up to no good.
   Of course, you should never ask anybody for their password.

Rules of Good Password Management

Password rules

1. Should be hard to guess
2. Should not be written down
3. Should be different on different systems
4. Should be changed regularly

- Very few people do all of the above.

Techniques to make on-line password guessing difficult

- Lock account after a consecutive number of wrong guesses.
  - If attacker attempts this with administrator account, or with a friend's account, this would be a form of denial of service
- Process passwords slowly or slow down as number of incorrect guesses accumulate
- Eliminate accounts not in regular use
- Make passwords complex enough to thwart a dictionary attack. (users hate this)
- Pronounceable passwords. Based on the unit of sound called a *phoneme*. The advantage is passwords can be longer since only have to memorize chunks of characters. Not enough of them.
- Force users to make a good choice when they select or change their password.
- Use pass phrase acronym, e.g. phrase "**I** **a**te **t**en **a**pples **o**n **m**y **f**ifth **b**irthday" would yield the password Iataomfb

Techniques to make Off-line password guessing difficult

- Here we assume that the attacker has a list of hashed passwords.
  - If this is possible then passwords have to be stronger!!
- Encrypt the password file
  - (the course website uses a hash of passwords instead)
- Beware of backups of password files if stored as plaintext
- Salt the passwords
  - When the user chooses a password, the system chooses a random number (the salt).
  - It then stores both the salt and a hash of the combination of the salt and the password.
  - Using a salt slows down dictionary attacks since the attacker must try all salts with each candidate password.
  - The course website is not doing this.

- Store hash of passwords.
  - An early version of the course web site stored passwords in plaintext in the database. This made it very easy to email students their password if they forgot it.
  - However, it was likely that some students were using the same passwords they were using for other accounts so the website needs to protect those passwords (even though they were advised to use different passwords for different accounts).
  - The current version of the program stores the hash of the password in the database. Now if someone breaks into the course website's database, they will have to do a dictionary attack to discover what the passwords are.
  - When the login page receives the password from the browser, it hashes it and compares the hash with the one stored in the database. If they are the same, it lets the user in.

How Big Should a Password Be?

- The secret needs about 64 bits of randomness (need to search 2^64 possibilities, or password is a 20 digit number)
- 11 character alphameric password has 66 bits of randomness
- 16 character pronounceable password has 64 bits of randomness
- 32 character user chosen password has 64 bits of randomness
- SANS Password Policy
  - (Recommends 15 character passwords!)

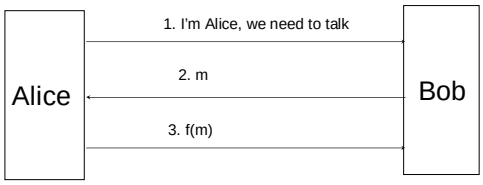
Eavesdropping

- Shoulder surfing
  - Don't stand too close to the person at the ATM machine
  - Don't display password on screen
- Key logger
  - Can be installed on public terminal in an Internet café;
  - Records all keystrokes including those of the password.
  - See How to log in from an Internet Cafe.

Challenge-Response

Definition 11-7. Let user U desire to authenticate himself to system S. Let U and S have an agreed-on secret function f. A *challenge-response authentication* system is one in which S sends a random message m (the challenge) to U, and U replies with the transformation r = f(m) (the response). S validates r by computing it separately.

Authentication through Challenge-Response



2. Is the challenge and 3. is the response
The function that changes the message
is secret (only Alice and Bob know about f)

One-Time Passwords

Definition 11-9. A *one-time password* is a password that is invalidated as soon as it is used.

- Impervious to eavesdropping
- Are a challenge-response mechanism
  - The number of the authentication attempt is the challenge
  - The password is the response
- User has a numbered list of passwords and the system asks for a number at login
- Problems: synchronization and password distribution

Other advice

Don't use browser feature to save passwords.
http://www.cnn.com/video/#/video/tech/2008/09/06/dcl.data.doctor.passwords.cnn

Don't use unencrypted password files

- Using a Password in Multiple Places
- Cascaded breakin (breaking into a system that contains no "important information" may lead to breakins of important systems, e.g., email address and password is stored in the clear)

Require frequent password changes

- In general it is impossible to make a system secure without the cooperation of the legitimate users.

Beware of something that looks like a log in screen but isn't.

- In a Windows machine, always do Ctrl-Alt-Del to make the login screen appear. Don't type your password into a login screen that is already visible on the screen. It may be a trojan horse that will send your password to the attacker.

Initial Password Distribution

- Acquiring a password in person
  - If you can impersonate the user (i.e., identity theft) to the system administrator, you can get the password by whatever mechanism the user could.
  - After showing credentials in person, then may be allowed to type in the new password on a sysadmin terminal.
  - This is a little scary since if the administrator is polite he will look away leaving the user unsupervised on a terminal that has superuser privileges.
- Pre-expired strong passwords.
  - User has to change password on first login.
- Avoid default passwords, especially if they are not pre-expired
  - Attacker could log in before user and plant Trojan horses

Authentication Tokens (something you have)

- An *authentication token* is a physical device that a person carries around and uses in authenticating.
  Examples:
  Regular household key
  Credit card with picture
- Some tokens require special hardware
- Most tokens offer little or no protection against eavesdropping. (You can look at someone's badge)
- Tokens can be lost
  - This is why they are generally coupled to either passwords or biometrics to be completely secure.
- "I forgot my token" should be as inconvenient as "I forgot my password"

.

Main Point

2. What you have authenticates who you are. In SCI, what you have is a function of your past actions. As you sow so shall you reap.

Biometric devices (something you are)

- "Biometric devices sell best in places where users aren't afraid of technology or don't have a choice".
- Examples:
- Retinal scanner
  - ("psychologically threatening" user interface)
- Fingerprint readers
- Face recognition
  - (don't show up to work with a black eye or a swollen jaw)
- Iris scanner
  - (don't need laser, can be done with camera, maybe even covertly, and hence is less threatening).

Biometric devices (something you are)

- More examples:
  - Handprint readers
    - (measure hand dimensions, some false positives)
  - Voiceprints.
    - Can be defeated with a tape recording
    - May be a problem if person has a cold.
  - Keystroke timing,
    - Intervals, pressure, duration, where on the key, etc.
    - Injury distorts it as does network latency.
  - Signatures
    - (pressure, etc)

Main Point

3. What you are authenticates who you are. In SCI what you are is ultimately pure consciousness. In unity consciousness, you experience that all of creation is an expression of your own Self.

Location (where you are)

- If a computer is in a locked guarded room, then the mere fact that you are using the computer will let you into the system.
- For example, ATMs and teller terminals connect to the same computer, but support different transaction types.
  - The system knows the address of ATM machines and doesn't let them do teller transactions.
  - Furthermore, the central computer assumes that the teller machines are not accessible to the general public

Advantages of Passwords

A professor asked his class the following question:

Q. Are there any advantages of passwords over biometric devices?

Careless Users

A student answered

A. When you want to let someone use your account it is easy to give them your password, but with biometric you have to go with them to log in.

- This indicates that many people regard security as a nuisance

CONNECTING THE PARTS OF KNOWLEDGE WITH THE WHOLENESS OF KNOWLEDGE

1. A password is required if you buy something from amazon.com.
2. A password should have about 64 bits of randomness.

3. Transcendental Consciousness is our true identity; I am That.
4. Wholeness moving within itself: in Unity Consciousness, one realizes the unity of life; I am That, thou art That, all this is That.