Lecture 11

Representing Identity

Wholeness Statement

In computer systems, an identity is the basis for assignment of privileges and exists in a protection domain (e.g. cs.mum.edu). In SCI, higher states of consciousness identify the knower with the field of pure consciousness.

Reading

- You just have to skim Chap 13.
- A lot of the material requires knowledge of Unix, networks, and distributed computing which we can't assume that people have.
- The things we want you to know are given in the lecture notes below (and on the web page)

Overview

1. Terms related to Identity
   Principal: a unique entity
   Identity: specifies a principal (like a primary key in relational databases)
   Authentication: binding of a principal to a representation of identity internal to the system. All access and resource allocation decisions assume this binding is correct.
2. Certificate is issued to a principal; the distinguished name in the certificate is the identifier of the principal
3. Login dialogs don't directly use a certificate to authenticate
4. Explore what it takes to be anonymous on the web using a sample web site
5. Look at the sin of "magic" URLs and hidden form fields (in today's lab).
   Example: http://gwigle.varten.net/

Identity

- Identity is simply a computer's representation of an entity

Definition 13-1. A *principal* is a unique entity. An *identity* specifies a principal.

- Authentication binds a principal to a representation of an identity internal to the computer.
- Each system has its own way of expressing this representation
- All decisions of access and resource allocation **assume** that the binding is correct

Purpose of Identity

- Accountability and access control
  - *Accountability* requires an identity that tracks principals across actions and changes
  - *Access control* requires an identity for determining whether access is allowed

Accountability

- Tied to logging and auditing
- Requires an unambiguous identification of the principal
  - Not always possible
  - Logged identity is mapped to a user account, group, or role

Access Control

- Processes are run on behalf of a principal
- The identity of the principal associated with an executing process determines its access rights
  - Some processes do not have all the rights of the principal associated with it
  - e.g., a process assigned a different role (with fewer rights) than the principal

Files and Objects

- Also have identity
- Depends on the system
- On local systems, objects (such as files)
  - are identified by name or path (by humans)
  - are identified by a file descriptor or handle (by a process or program)
  - are identified by a FAT entry or inode in the OS kernel
- Objects on a network have a name that encodes their location
  - URL (uniform resource locator) identifies an object by location and the protocol needed to access it
    - protocol://host/object
    - http://location
      - Hypertext transfer protocol (http)

Users

- A user is an identity tied to a single entity
- Represented in different ways
  - May be different depending on the context
    - E.g., login name is used when logging in
    - After that the OS may use a unique integer (UID in Unix) to represent the user (more efficient and easier to work with than a string)

Example: Course Web Site

- When you use the course web site you are the principal.
- You are authenticated using your login name and password.
- Once authenticated, your Student ID (SID) is used as a representation of your identity.
- Your SID can be stored in a computer memory, but you cannot.
- Your identity determines what labs and exams you can see and modify (rights).
- Authentication essentially associates something that cannot be stored in computer memory with something that can be.
- After authentication, the computer uses the identifier in its memory to determine the rights of the principal.

Groups and Roles

- Example of an identity that represents a set of entities
  - Each member has a separate identity
- Used to assign rights to a set of principals

Naming and Certificates

- Certificates are issued to a principal
  - *Issuance policy* specifies to which principals the CA will issue certificates
- Distinguished name in a certificate is the identifier of the principal.
  - It must uniquely identify the principle.
  - For example, "Ralph Bunker" is not enough
    - Likely more than one person with that name
  - Ralph Bunker, Asst. Prof Computer Science, M.U.M. Fairfield, IA is better
    - Should be enough to identify the principal uniquely
  - All of the identifying information is included in the distinguished name
- A certificate binds an external entity (principal) to a public key and a distinguished name

Main Point

1. Certificates are a way of associating an identity with a public key and distinguished name. The regular practice of TM over time associates individual identity with the key to all life, pure consciousness.

Meaning of the Identity

- The authentication policy defines the way principals prove their identities
- Each CA has its own requirements
  - Constrained by contractual requirements such as with PCAs
    - PCAs issue certificates to CAs
    - CAs issue certificates to individuals and organizations
  - All rely on non-electronic proofs of identity such as biometrics (fingerprints), documents (drivers license or passport), or personal knowledge
- The specific authentication policy can be determined by checking the policy of the CA that signed the certificate

Example CA authentication policy

- There are different classes of certificates.
- The more money you pay, the more time and effort the CA spends verifying that the principal is who he says he is.
- For the www.mumde.net site certificate, all the CA wanted was Ralph's voice print and presumably they verified that the company hosting his software was registered somewhere.
- If he would have paid more money, they would investigate further
- Extended Validation (EV) certificate is a certificate that will cause the location bar of IE to turn green, indicating that the web site is highly trusted.
- See GeoTrusts requirements at http://www.geotrust.com/ev/ev_authentication_requirements.asp

Kinds of Certificates

There are at least four kinds

1. **site certificates** (e.g, www.mumde.net)
2. **personal certificates** (e.g. used if the server wants to authenticate the client. You can install a personal certificate in your browser.)
3. **software vendor certificates** (e.g. used when software is installed. Often when you run a program, a dialog box appears warning that "The publisher could not be verified. Are you sure you want to run this software". This is caused either because the software does not have a software vendor certificate or because you do not trust the CA who signed the software vendor certificate).
4. **anonymous certificates**, e.g., used by a whistle blower to indicate that the same person sent a sequence of messages. But don't know who that person is.

Other Types of Certificates

- Certificates can also be based on a principal's association with an organization (such as MUM), where the principal lives, or the role played in an organization (such as the comptroller)

Trust

- Goal of certificate: bind correct identity to a Distinguished Name (DN)
- Question: what is the degree of assurance?
  - X.509v3, certificate hierarchy
    - Depends on policy of CA issuing certificate
    - Depends on how well CA follows that policy
    - Depends on how easy the required authentication can be spoofed
  - Trust is an estimate based on the above factors

PGP

- Four levels of trust of the signature field
  - Generic (no trust assertions)
  - Persona (no verification)
  - Casual (some verification)
  - Positive (substantial verification)
- Meaning
  - Not given by OpenPGP standard
  - Signer determines what level to use
  - Casual to one signer may be positive to another

CA Authentication

Suppose a Passport is Required

DN has name from passport, number and issuer of passport (country)

What are points of trust?

- Passport is not forged and name on it unaltered
- Passport issued to person named in passport
- Person presenting passport is person to whom it was issued
- CA has checked passport and individual using passport

Identity on the Web

- Internet requires every host to have an address
  - Without cryptography, the binding is weak
- Host identity
  - Bound to networking
  - If not connected to any network, then can have any name since the name is only used locally
  - If connected to a network, then can have many names or one name (depending on network and context of use)

Login dialog

Does not use certificates directly but probably uses SSL which uses a certificate

Static and Dynamic Identifiers

- Static identifiers do not change over time
- Dynamic identifiers change either as a result of an event (connection to a network) or change over time

Domain Name Server Security

- DNS maps host names to IP addresses and IP addresses back to host names
  - Without cryptographic authentication of hosts, provides weak authentication
  - Trust relies on the integrity of the DNS database and cache
- Threats
  - Data base corruption (malicious or accidental)
  - Unauthorized updates
  - IP address spoofing (impersonating an update source)
  - Subverted DNS host
  - Denial of service (vulnerable if single point of failure)
  - Information leakage that gives information about an internal network

Gateways

- Gateways can translate between a local address and a global address
- MUM has two gateways
  - all outgoing traffic must go through one of them (translates the IP address to a gateway address)

State and Cookies

State and Cookies

Definition 13-4. A *cookie* is a token that contains information about the state of a transaction on a network.

- The term is most widely used in reference to interactions between Web browsers and clients
- Used to minimize the storage requirements of servers
  - Puts the burden of maintaining required information on the client

Cookie Structure

- Consists of several values
  - *Name* with an associated *value*; both are encoded into the cookie and represent the state
  - *Expires* field indicates when the cookie is valid
    - Expired cookies are discarded
    - If field is not present, then deleted at end of session
  - *Domain* states the domain for which the cookie is intended
    - Consists of the last n fields of the domain name of a server (must have at least one dot)
    - Sent to servers in the specified domain
  - *Path* further restricts dissemination of the cookie
    - If server specifies a path, it must be the leading substring of the path in the cookie
  - *Secure* field indicates that the cookie is only sent over a secure connection ("https" which uses SSL)

Who can send or receive a cookie?

- The Web server sends cookies to the client (browser) initially
- A Web browser sends these cookies back to the Web server
  - whenever the cookie's domain matches that of the web server
    - and the cookie's path (if included in the cookie) also matches

Main Point

2. Cookies are a way of saving state, including identity, on the browser. It is a purely cause and effect phenomenon. Any cookie sent by server to the browser will be sent back to the server whenever a request is made to the server. Nature is orderly. A bunyan seed produces a bunyan tree.

Anonymity on the Web

- Recipients can determine origin of incoming packet
  - Sometimes not desirable
- Anonymizer: a site that hides origins of connections
  - Usually a proxy server
    - User connects to anonymizer, tells it the destination
    - Anonymizer makes connection, sends traffic in both directions
  - Destination host sees only the anonymizer
- Can be attacked by monitoring traffic in and out of the anonymizer site

Anonymity

- Provides a shield to protect people from having to associate their identity with some data
- Is this desirable?
  - Allows statements without fear of retaliation
  - With appropriate choice of pseudonym, can shape course of debate by implication
  - Protects whistleblowers

Anonymity

- Also hinders monitoring to deter or prevent crime
- Conclusion: anonymity can be used for good or ill
  - Right to remain anonymous entails responsibility to use that right wisely

Summary

- Identity specifies a principal (unique entity)
  - Same principal may have many different identities
    - Function (role)
    - Associated principals (group)
    - Individual (user/host)
  - These may vary with view of principal
    - Different names at each network layer, for example
- Trust cannot be measured in absolute terms other that complete trust or no trust
  - How the identity is bound to a principal provides insight into the trustworthiness of that identity
- Anonymity is possible; may or may not be desirable
  - Power to remain anonymous includes responsibility to use that power wisely

Main Point

3. Anonymity is good and bad. It respects privacy but may bring about mediocrity. Scientific research on the TM technique has shown that excellence grows with the continued practice of the technique.

CONNECTING THE PARTS OF KNOWLEDGE WITH THE WHOLENESS OF KNOWLEDGE

1. You enter a user name when you log onto Windows XP.
2. The user name is mapped to an internal identity that is used to determine privileges.

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.