CS530
Authorization - Policy

Bill Cheng

http://merlot.usc.edu/cs530-s10

Authorization

- Final goal of system security
  - determine whether to allow an operation
    - authentication
    - audit - so that you can change policy to keep the bad guys out
- Depends upon
  - *policy* - rules of allowed by the system
  - possibly *authentication*
    - policy can be based on identity
  - other characteristics - e.g., time of day, network threat condition, system load

The Role of Policy in Security Architecture

Policy - defines what is allowed and how the system and security mechanisms should act
(misconfiguration - policy does not reflect intent)

Enforced By

Mechanism - provides protection
interprets/evaluates policy
(firewalls, ID, access control, confidentiality, integrity)

Implemented As

Software - which must be implemented correctly and according to sound software engineering principles

Policy: Review - The Access Matrix

- Policy represented by an Access Matrix
  - also called Access Control Matrix
  - one row per object
  - one column per subject/principle
  - tabulates permissions
  - but implemented by
    - *capability* list (like a key ring)
    - *Access Control List* (ACL)
      - recall that it's harder to determine who has access with ACL

Policy models: Bell-LaPadula

- *Discretionary* policy
  - based on Access Matrix - owner of an object can determine who has access
- *Mandatory* policy
  - owner of an object does not get to decide who has access
  - *Top Secret*, *Secret*, *Confidential*, *Unclassified*
  - ** property*: S can write O if and only if Level S ≤ Level O
    - *write UP*, *read DOWN*
      - it's possible that I can create a file that I cannot read
  - create categories so that some members in a class cannot see some documents
  - this approach tries to minimize the spread of secret leaks
- (more models in Bishop's book, e.g., integrity policy)

Role Based Access Control

- In a way, similar to groups in UNIX, but more general
  - in UNIX, an object can belong to only a single group, inconvenient to create dynamic groups
- Three phases
  - administration
  - session management
  - access checking
- Typical policies
  - object policies fairly static
  - user's roles can change
    - but no need to list all objects to which users has access
- Maps to typical organizational policies
  - can implement separation of roles

Security is More Than Mix of Point Solutions

- Today's security tools work with no coordinated policy
  - firewalls and Virtual Private Networks
  - authentication and Public Key Infrastructure
  - intrusion detection and limited response
- We need better coordination
  - intrusion response affected at firewalls, VPN's and applications
  - not just who can access what, but policy says what kind of encryption to use, when to notify ID systems
- Tools should implement coordinated policies
  - policies originate from multiple sources
  - policies should adapt to dynamic threat conditions
  - policies should adapt to dynamic policy changes triggered by activities like September 11th response

Policies Originate from Multiple Sources

- Discretionary policies associated with objects
  - read from existing applications or extended ACLs
    - e.g., one module for reading .ssh files and one module for reading .htaccess files
- Local system policies merged with object policies
  - broadening or narrowing allowed access - can ignore discretionary policy
    - e.g., deny all web accesses from certain domains
- Policies imported from policy/state issuers
  - example of policy issuers is virus checker from Network Associates or Symantec
  - example of state issuers is HIPAA - healthcare related policy for healthcare providers
  - (cont...)

Policies Originate from Multiple Sources (Cont...)

- Policies imported from policy/state issuers (cont...)
  - ID system issues state credentials
  - these credentials may embed policy as well
- Policies embedded in credentials
  - these policies attach to user/process credentials and apply to access by only specific processes
    - e.g., extra audit required from outsiders
  - this also allows chaining
- Policies evaluated remotely
  - credential issuers (e.g. authentication and authorization servers) evaluate policies to decide which credentials to issue.

Policies Origins Summary

- HIPAA, other legislation
  - e.g., access to student records
- Privacy statements
  - need to know how it is actually enforced
- Discretionary policies
- Mandatory policies (e.g. classification)
- Business policies

GAA-API: Integration through Authorization

- GAA Generic Authorization and Access-control
- Focus integration efforts on authorization and the management of policies used in the authorization decision
  - not really new - this is a reference monitor (as in TCPS-20 and MULTICS)
  - applications shouldn't care about authentication or identity
    - separate policy from mechanism
  - authorization may be easier to integrate with applications
  - hide the calls to individual security services
    - e.g., key management, authentication, encryption, audit
  - can perform adaptive audit
    - dynamic policy
    - when ID detects something, start collecting additional information or start requiring authentication even for internal users

GAA-API

- Sometimes it is not possible to plug in security at low level
  - need information at the application level
    - Ex: SSL is in the lower layer, it cannot deal with user certificates
- GAA-API: application just asks *if something is allowed*
  - return value is either yes, no, or *maybe*
    - maybe means you need additional things, e.g., network source address must come from a certain domain (this information, again, may not be available at lower layers)
- Subject/principle is represented by a Security Context (SC)
  - why not an identify?
    - because sometimes it's not necessary, e.g., to access this, pay $5 (no authentication)

GAA-API (Cont...)

- EACL (extended ACL)
  - the language used by GAA
  - extended to include information such as
    - time of day
    - network threat condition
    - system load

Authorization and Integrated Security Services