Capabilities

COS 316: Principles of Computer System Design

Amit Levy & Wyatt Lloyd
Last Time - The Guard Model

Subject

Request

Guard

Object

Object

Object

Object

Is subject allowed to access resources?
Last Time - Access Control Lists

Associate a list of (user, permissions) with each resource

Repositories

cos316/assignment4-alevy.git

[(alevy, [PUSH,PULL]), (wlloyd, [PUSH,PULL]), (will, [PULL])]
select count(*) > 0
    from repositories, acls where
    repositories.name = 'cos316/assignment4-aalevy'
    and acls.repo_id = repositories.id
    and acls.user = 'alevy'
    and acls.permission = 'push';
Advantages

- Simple to implement
- Simple to administer
- Easy to revoke access

Drawbacks

- Tradeoff granularity for simplicity
  - More granular permissions require more complex rules in the guard
- Doesn’t scale well
  - E.g. need up to Users X Repos X Access Right entries in ACL table
- Centralized access control
  - Needs server’s cooperation to delegate access
An Alternative - Capabilities

“[A] token, ticket, or key that gives the possessor permission to access an entity or object in a computer system.” - *Capability-Based Computer Systems*

- **Self-describing**
  - Contains both object name and permitted operations
- **Globally meaningful**
  - Object and operation names are not subject-specific
- **Transferrable**
  - A subject can pass a capability to another (e.g. a sub-process, via IPC, a third-party app, etc)
  - Ideally can delegate subset of capabilities
- **Unforgeable**
  - Subjects cannot create capabilities with arbitrary permissions
FileDescriptors as Proto-Capabilities

- **Unforgeable ✓**
  - Process-level fd is just an index in a kernel structure

- **Self-describing ✓**
  - Kernel fd contains reference to inode + permissions

- **Globally meaningful ✗**
  - Fds are process-specific

- **Transferrable ✓/ ✗**
  - Via IPC sendmsg/recvmsg
Consider a GitHub-like Ecosystem

- Continuous Integration
- Git pages
- PR bot
- Autograder
- Central code DB
- Apps access DB resources to provide extra services
- Application access must be restricted:
  - E.g. don’t make private repos public
User Permissions using Capabilities

Hand out communicable, unforgeable tokens encoding:

- Object
- Access right

Users store capabilities, not the database

E.g.

“push(cos316/assignment4-aalevy)”

“pull(cos316/assignment4-aalevy)”
Implementing Capabilities with HMAC

HMAC - a keyed-hash function: \( \text{hmac(secret\_key,\ data)} \) hash of data

```rust
def gen_capability(op, repo)
    hmac(db_secret, fmt.Sprintf("%s(%s)\", op, repo))

def verify_capability(cap, op, repo)
    cap == hmac(db_secret, fmt.Sprintf("%s(%s)\", op, repo))
```
Capabilities in Action

Push(cos316/assignment4-aalevy, Cap)

Guard

Doesn't matter who

verify_capability(Cap, “push”, “cos316/assignment4-aalevy”)

Error!

False?
Extending Capabilities to Applications

- Users can simply give applications a subset of their capabilities

Push to cos316/assignment4-.
Extending Capabilities to Applications

verify_capability(Cap, "push", "cos316/assignment4-aalevy")

Push(cos316/assignment4-aalevy, Cap)

Guard

cos316/assignment4-aalevy

False?

Error!
Capabilities

Advantages

- Decentralized access control
  - Anyone can “pass” anyone a capability
- Scales well
- Granular permissions are simple to check

Drawbacks

- How do you revoke a capability?
- Moves complexity to users/clients
  - Users have to manage their capabilities now
Capabilities In The Wild

- Operating Systems
  - History of industry and research operating systems
    - FreeBSD’s Capsicum
    - Fuschia OS
- Web
  - S3 Signed URLs
    - URL to private resources, contain signature, expiration, permitted HTTP methods, etc
  - CDN-hosted images/videos (FB, Instagram, YouTube)
    - Browsing via Web page/app is protected by login+cookie, but media typically fetched unauthenticated
Next time...

We still have a problem!

The autograder is allowed to:

- read all cos316/ repositories
- comment on all cos316/ repositories

Can code from a private repository end up in a comment on a public repository?