CSE 509: Lecture notes for 2/8/07 (Topics : Implementing Capabilities, Authentication)

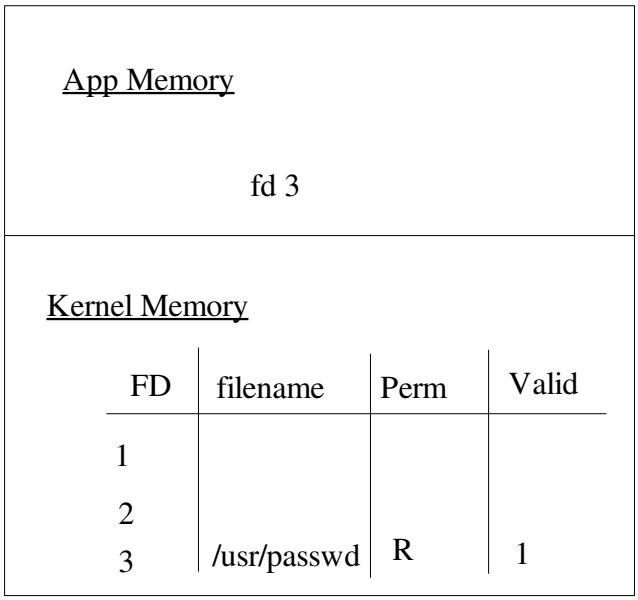
Implementing Capabilities

Capabilities are implemented using:

1. Cryptography
2. Unforgeable pointers/handles (UNIX file descriptors)

Unforgeable Handles

- capabilities are non-transferable (*per process* tables)
- revocation --> easy (by simply flipping valid bit)



Application Source

```
read(fdid,...);
```

- statement identifies objects
- represents application's right to return on that object
- can only create entry in table via syscall that does some permission check.

Cryptography

Message Authentication Code --> MAC

- similar to Error Correcting Code

- but you need to know the secret (key) to compute MAC

Message (M)	ECC(M)

ECC(M) --> Checksum

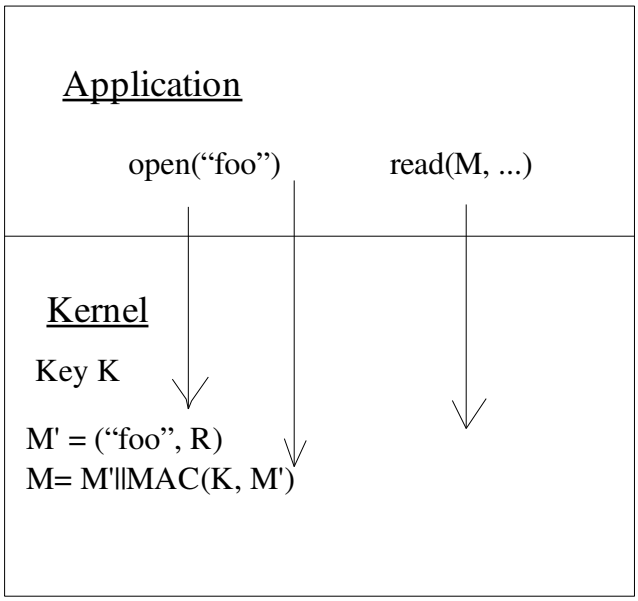
What if ECC is computed on M along with a secret ? --> ECC(M,K) --> MAC !

Alice Bob

1) MAC(K,M)

2) verifies that MAC(K,M) is still correct

Examples for MAC: HMAC, SHA256 (usually some timestamps and counters are used to avoid replays)



Capability Transfer

- capability can be copied without OS interaction
- capability is forever => Revocation is impossible
- can be transferred even over network

Alternate Scheme (Revocation and Non-Transferable)

- Capabilities can expire
  - applications must renew capabilities (M' = (foo, R, Exp))
- Blacklist capabilities --> maintain a list of revoked capabilities

  - whoops : state
- Add Process ID to capability (M' = (foo, R, Exp, PID))
- e.g. Kerberos

Authentication

How does a computer know 'who you are', given 'who you say you are' ?

- password } something that you know
- biometrics } something you are
- secure token } something you have

Biometrics are a very simple password scheme.

- Each reading differs slightly so we can only do appropriate match.

    => cannot use fingerprints as keys

Iris Scan

- Iris scan converted to 2048 bit string
- Two scans of same iris agree on >= 1600 bits
- Two scans of different iris agree on < 1200 bits

Biometric Attacks

- Iris photograph
  - Solution -> liveness detector
- Thumb prints – gummy-bears
  - Solution -> liveness detector

Iris Scan Implementation

There is an ECC that can correct 400 bit errors in a 2048 bit message and no more.

I --> [ECC] --> (I CRC_I)

--> | SCANNER | --> I' -->

OS	
Rob	CRC_I

I, if I' is valid } <-- [ECC^{-1}]

Fail, otherwise

Note: In out threat model CRC_I is assumed public.