Mar 9, 2005 -- Lecture? 21

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Review

What have we covered?

Definitions

Attacker, vulnerability, defense ...

Cryptography

Plaintext, cyphertext, encrypt, decrypt
Symmetric-key cyphers
Stream cyphers, random numbers
Block cyphers, DES, AES
Trapdoor functions, public-key cyphers
RSA, authentication, signature
PK to encrypt symmetric session key

What have we covered II

Program security

- *Errors, faults, failures*
- *Security error by design or specification*
- *Unsafe tools, implementation errors,*
- *User errors, impact of the marketplace,*
- *Viruses, antivirus measures, worms*

Security models

- *Domains, overt and covert channels*
- *Parameter validity, gate crossing,*
- *Access control models and mechanisms*
- *Memory and file protection mechanisms*
- *Access Control lists, Capability lists*
- *Hierarchic models*

What we have covered III

Kernel examples

- *Multics, Cap, Mach*

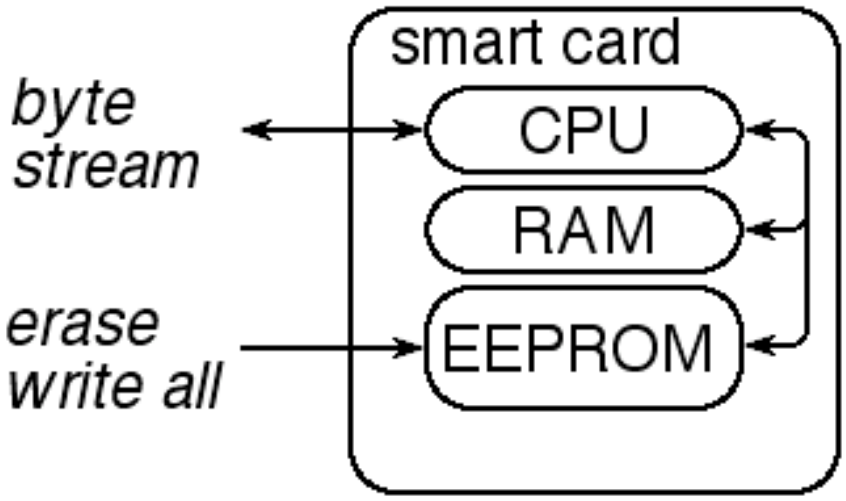
Capability based addressing

- *MMU as C-list, Directory as C-list*
- *Capabilities for objects*
- *Capabilities for servers*

Trusted servers

Idea for an exam question

Consider smart cards:



Suggested questions

What attacks are possible
(consider ATM example)

How can card authenticate self
so it is resistant to all attacks?

What is role of:
random number generators?
trapdoor functions? cryptography?
passwords? pass functions?

Warning

Do not focus too much on smartcards

Questions derived from this will be selected on the basis of coverage

For the sake of coverage

Expect questions from all areas