CSE508: (Intro to) Systems Security

Fall 2012

Radu Sion

Recap

Final Recap

- Cryptography
  - Encryption
  - Cryptohashes
  - Signatures
  - Ciphers
  - Semantic Security
  - anything else
- Analytical Thinking
  - Protocol attacks/vulnerabilities
- Assigned Reading
  - “aha” factor mainly !
- Systems
  - Access Control
  - Authentication
  - Security policies
  - SELinux concepts
  - HiStar concepts
  - SSL/IPSec
  - Malware
  - Trusted Hardware
  - Cloud Cartography
  - Covert channels
  - Trust Management
  - Malware
  - Encryption FS concepts

Diffie-Hellman

- Discrete logarithm problem hardness:
  - Given integers n and g and prime number p, compute k such that $n = g^k \bmod p$
  - Solutions known for small p
  - Solutions computationally infeasible as p grows large

Algorithm

- Constants: prime p, integer $g \neq 0, 1, p-1$
  - Known to all participants
- Alice chooses private key k_{Alice}, computes public key $K_{Alice} = g^{k_{Alice}} \bmod p$
- To communicate with Bob, Alice computes

  $K_{shared} = K_{Bob}^{k_{Alice}} \bmod p$
- To communicate with Alice, Bob computes

  $K_{shared} = K_{Alice}^{k_{Bob}} \bmod p$
  - It can be shown these keys are equal

RSA: Rivest,Shamir,Adleman

- Exponentiation cipher
- Relies on the difficulty of determining the number of numbers relatively prime to a large integer *n*
- Or equivalently, on the difficulty of factoring of large numbers into prime factors

RSA Algorithm (animated version)

Alice

message $m<n$

RSA Encryption

1 $n=pq$

2 $e=17$

3 Extended Euclidean

$d = e^{-1} \bmod (p-1)(q-1)$

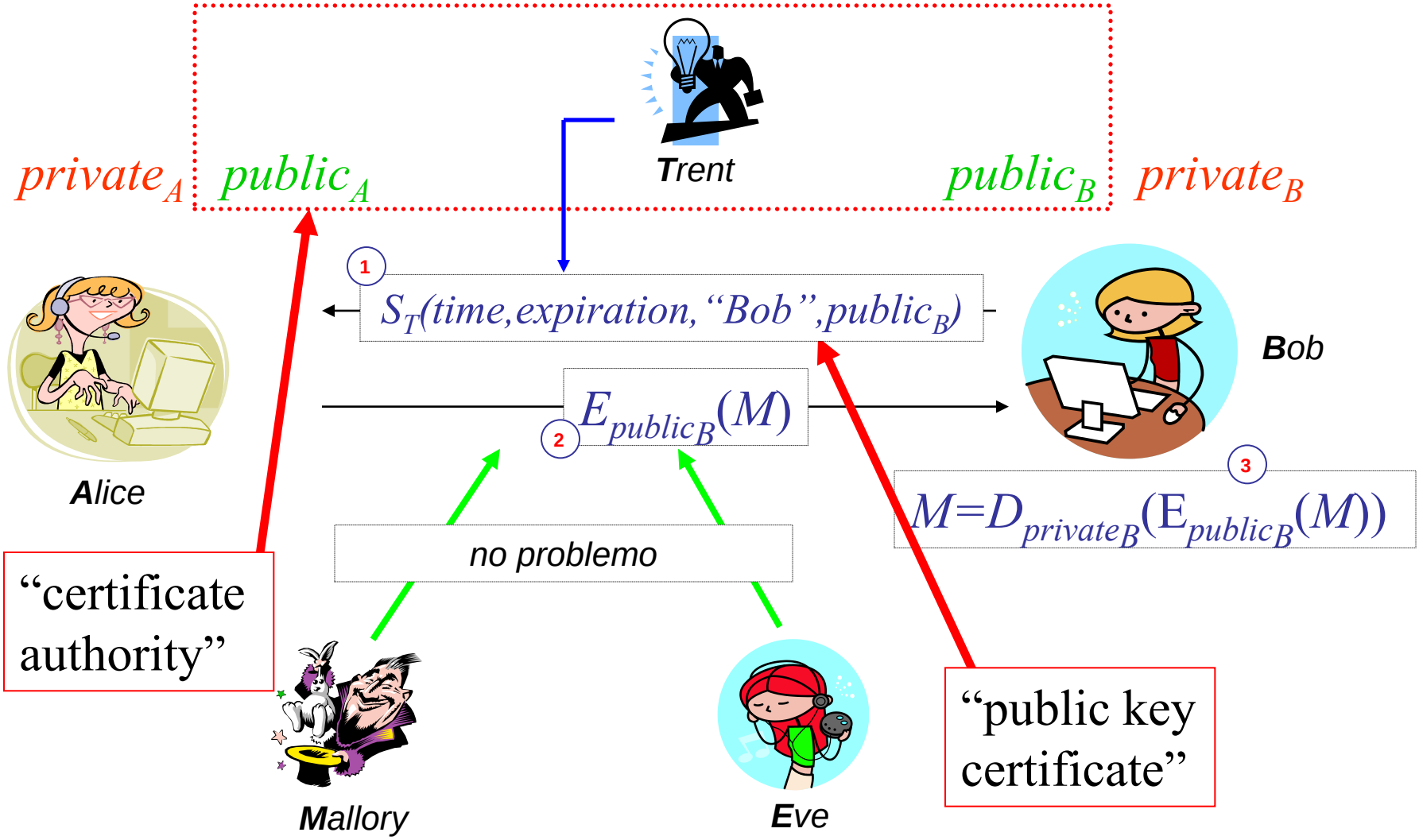
4 $c=m^e \bmod n$

RSA Decryption

5 $m=c^d \bmod n$

Bob

Certificate Authorities



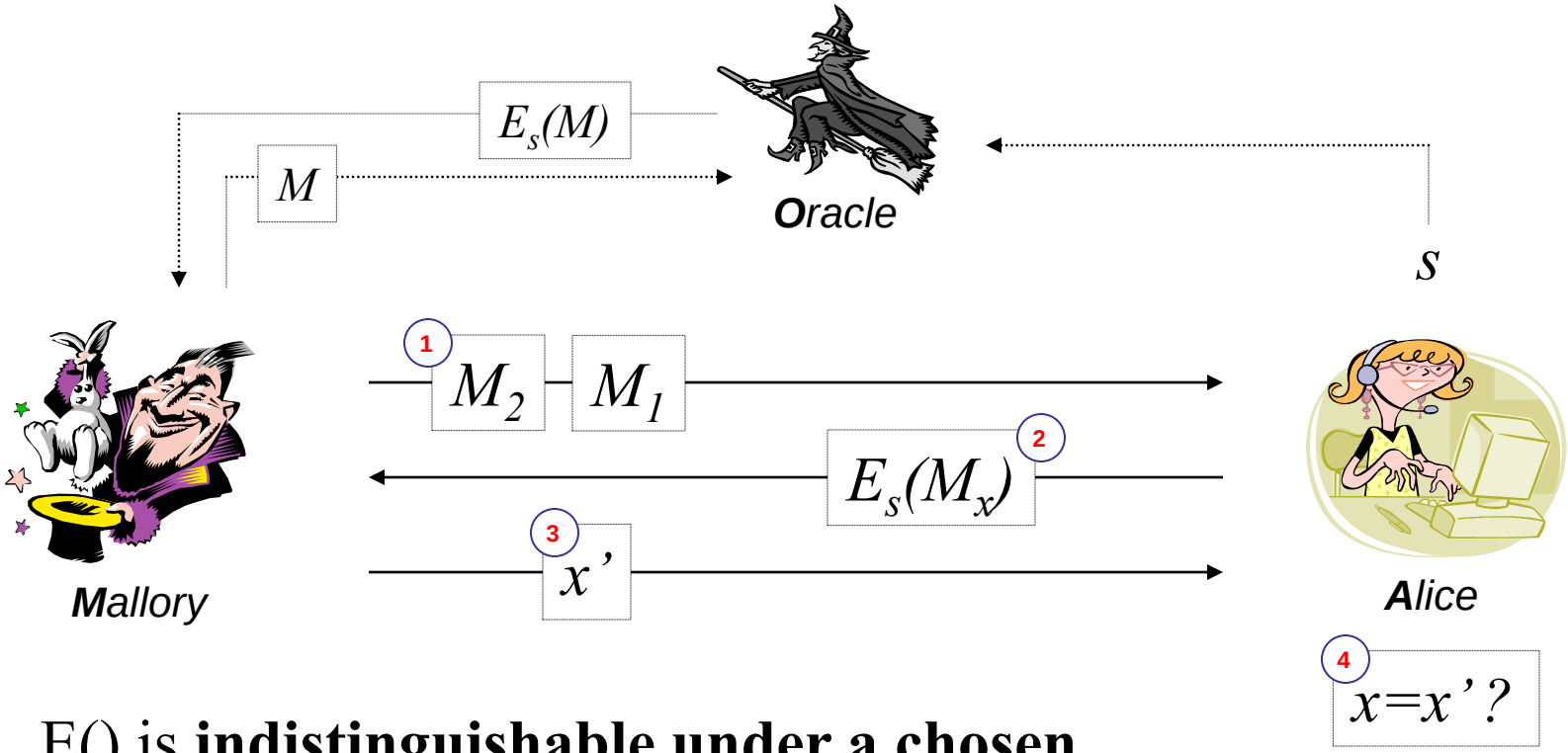
Ciphers: CTR

- *Counter mode (CTR)*:
  - Key constructed by encrypting block counter
    - $k_i = E_k(unique\_nonce||i)$
    - $c_i = m_i \oplus k_i$

  e.g. unique_nonce=(message number)

  - Question: why do we need the *nonce* ?
  - Careful: never use same (*k,nonce*) pair !!!

Semantic Security (IND-CPA)



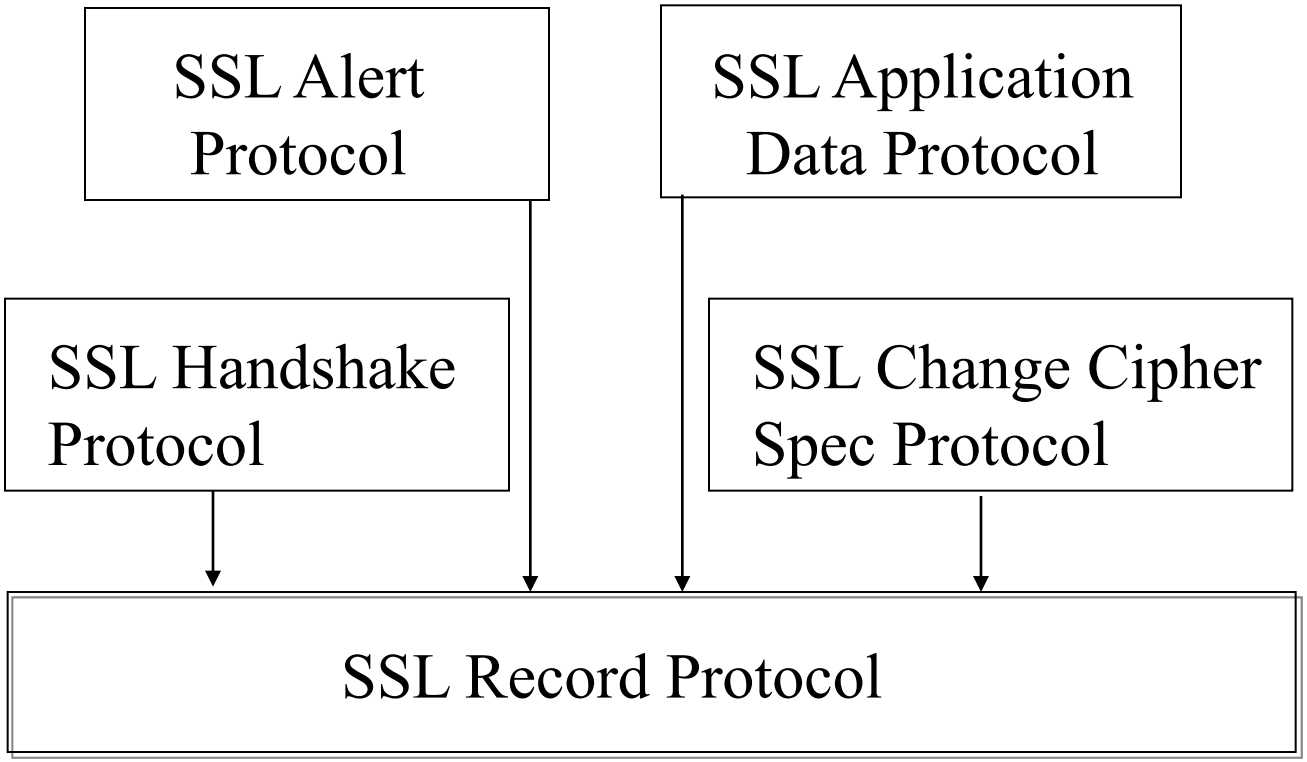
E() is **indistinguishable under a chosen plaintext attack** ("semantically secure") if no probabilistic polynomial time-bounded Mallory can succeed significantly better than guessing.

Semantic Security: why do we care ?!

Deterministic, stateless schemes are insecure !

Semantic security implies bit security !

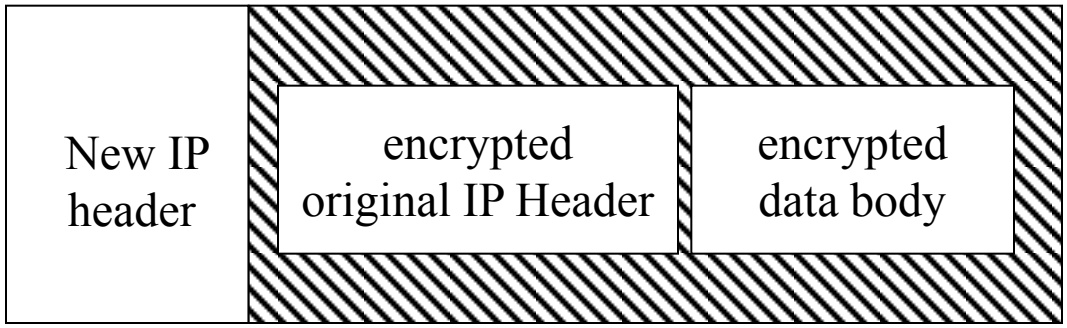
Structure of SSL



SSL Handshake: Overview of Rounds

1. Create SSL client-server connection
2. Server authenticates itself
3. Client validates server, begins key exchange
4. Acknowledgments all around

IPsec Tunnel Mode

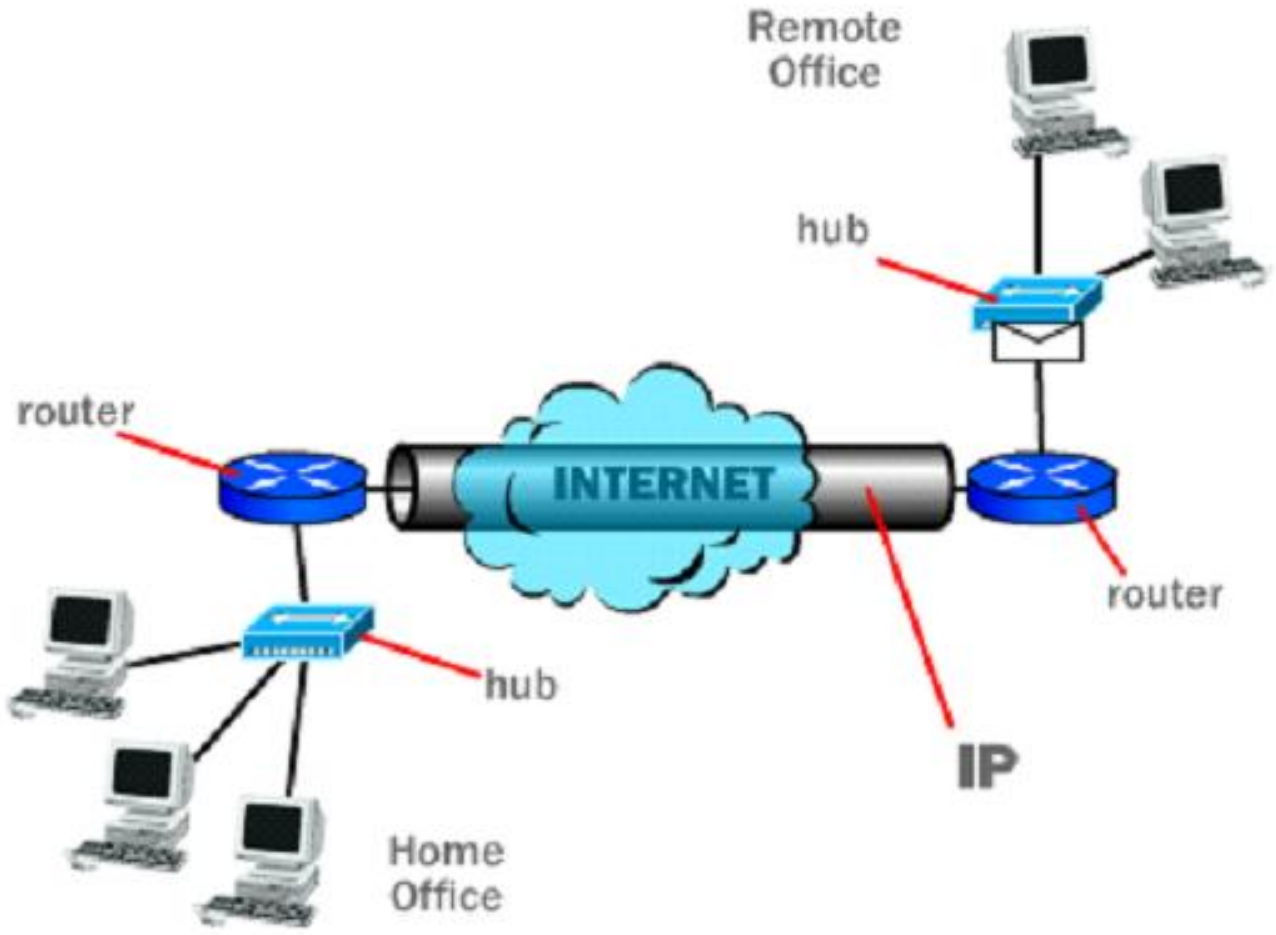


- Encapsulate IP packet (IP header *and* IP data)
- Use IP to send IPsec-wrapped packet
- Note: IP header protected
- Used: When only two intermediate hosts support IPSec

IPsec Sub-Protocols

- Authentication Header (AH) Protocol
  - Adds authentication to an IP datagram: crypto-hash (e.g. SHA) of all unchangeable or predictable fields
  - Message integrity
  - Origin authentication
  - Anti-replay (!) – sequence numbers, 32 slot packet window at receiver
- Encapsulating Security Payload (ESP)
  - Confidentiality – encrypts IP payload
  - Supports: tunnel/transport modes
- IPComp
  - Compress BEFORE encryption (otherwise harder !!!)
- IKE
  - Internet Key Exchange

Site to Site VPN



Protocol types

- **Passenger -** original data being carried (IPX, NetBeui, IP)

- **Encapsulator -** "wrapper" for original data (GRE-Cisco, IPSec, L2F, PPTP, L2TP)

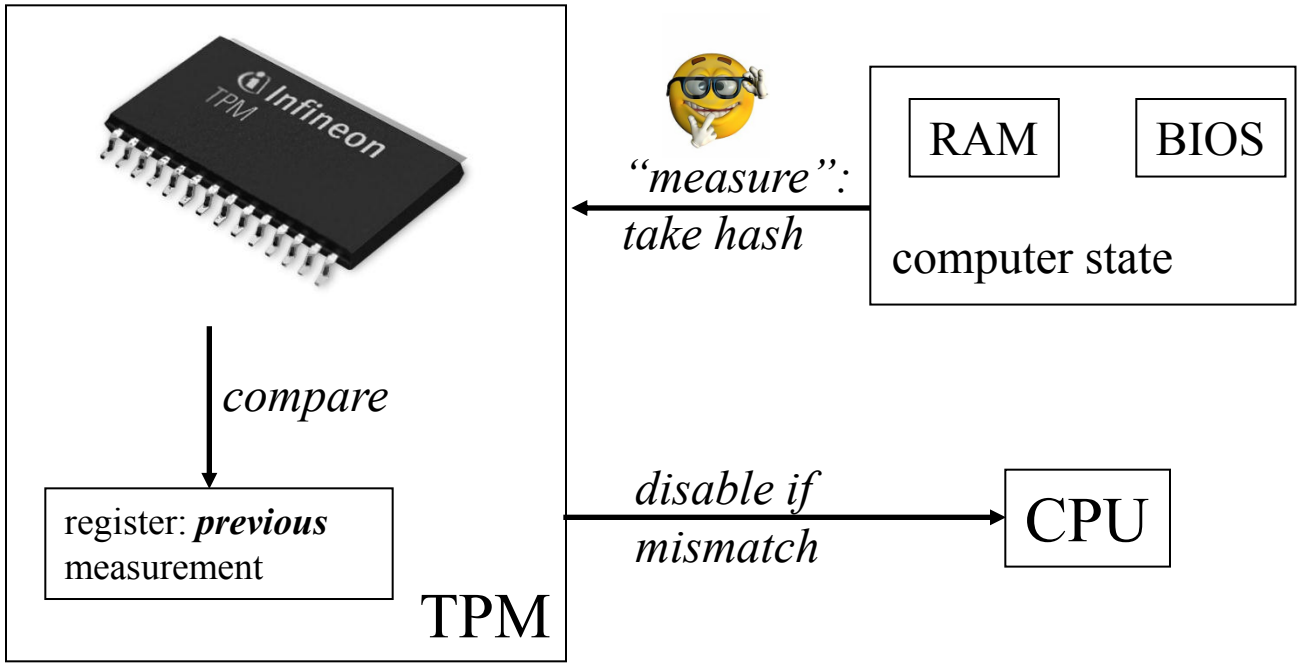
- **Carrier -** the network that the information is traveling through (IP)

Secure Hardware

- FIPS Certification
- RSA SecurID
- TPMs
- Smart cards
- SCPUs: IBM 4764
- Others

Secure Hardware

Idea: measure and verify next link in chain before passing control.
e.g., BIOS to OS, VMM to VM to Guest OS



SCPU: IBM 4764

IBM 4764-001: 266MHz PowerPC. 64KB battery-backed SRAM storage. Crypto hardware engines: AES256, DES, TDES, DSS, SHA-1, MD5, RSA. FIPS 140-2 Level 4 certified.

SCPUs: Important limiting factor

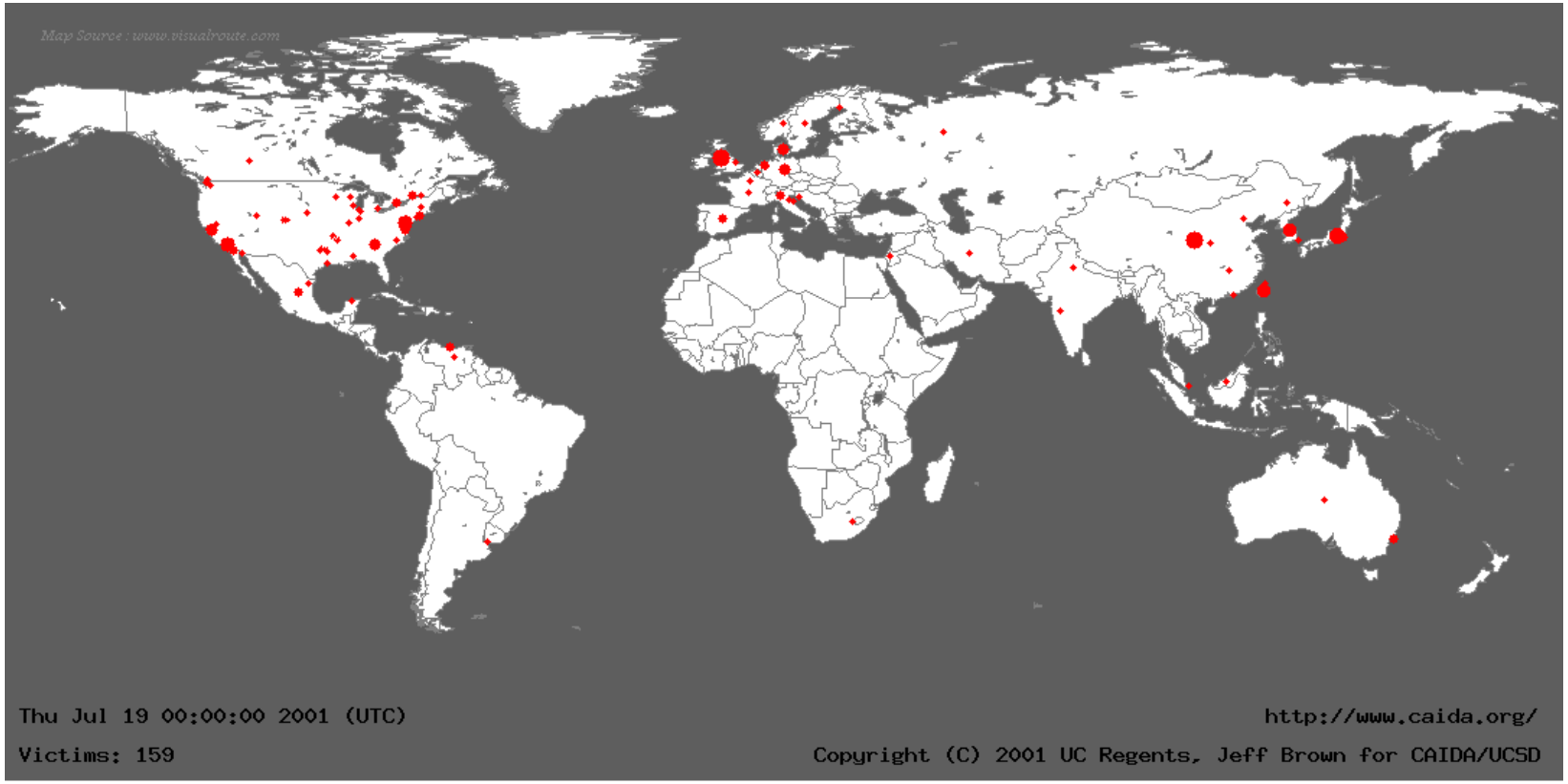
Dissipating heat while being tamper-proof

Q: what is the difference/relationship between "tamper-evident", "tamper-resistant", "tamper-proof" ☺

Types of Malware

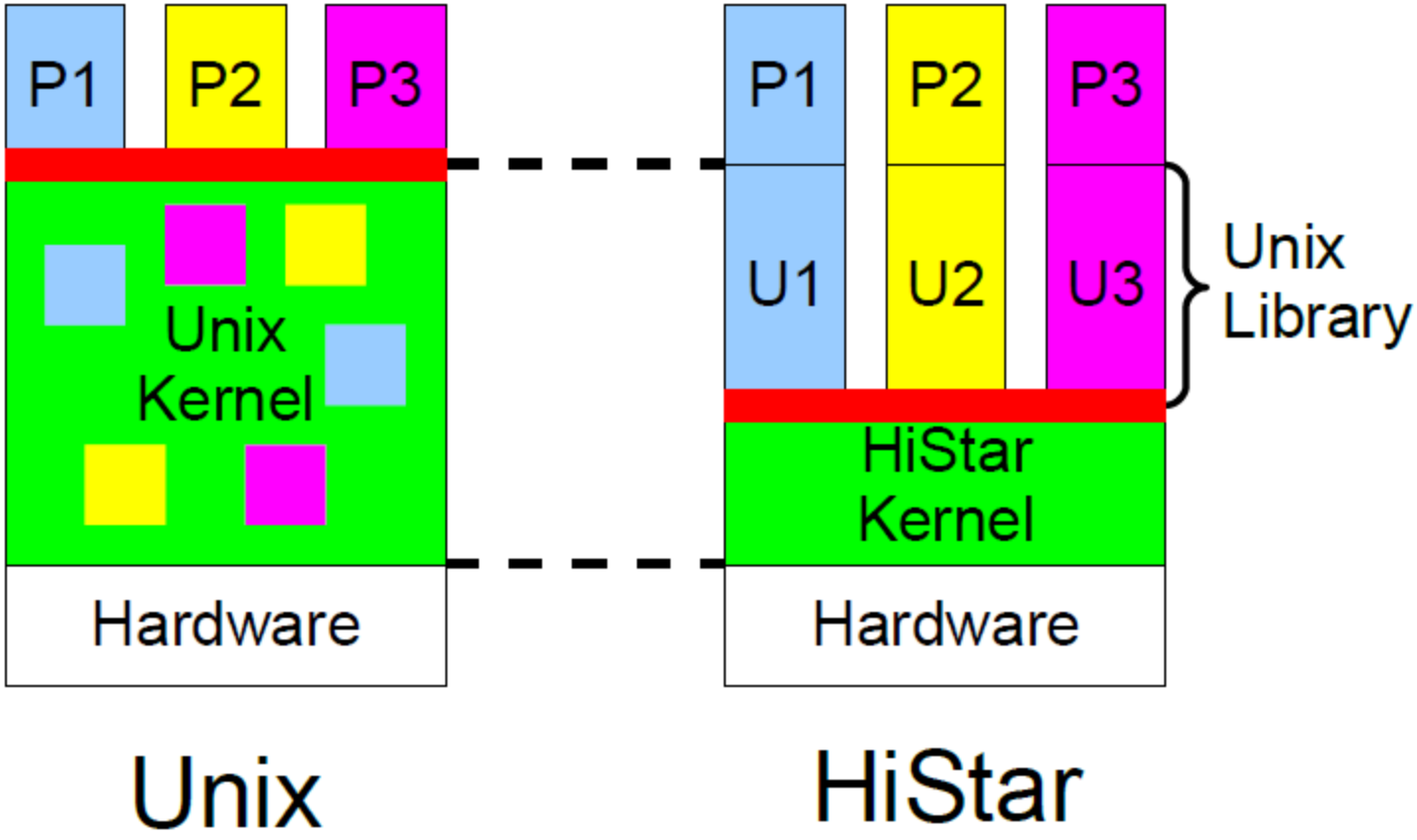
- Boot sector infectors
- Executable infectors
- Multipartite viruses
- TSR viruses
- Stealth viruses
- Encrypted viruses
- Polymorphic viruses
- Macro viruses
- Worms vs. Viruses

Worms: main lessons ?

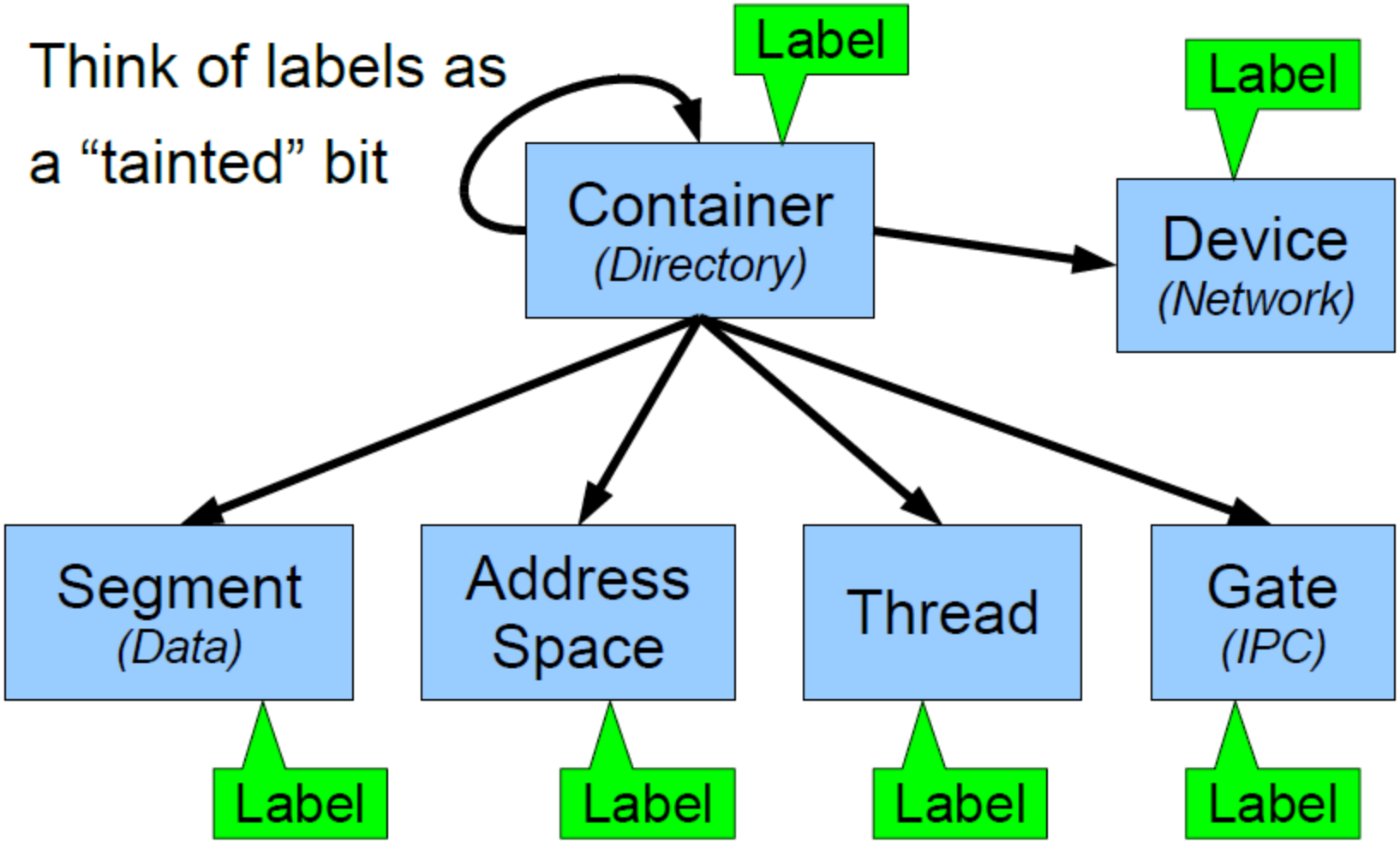


HiStar Idea

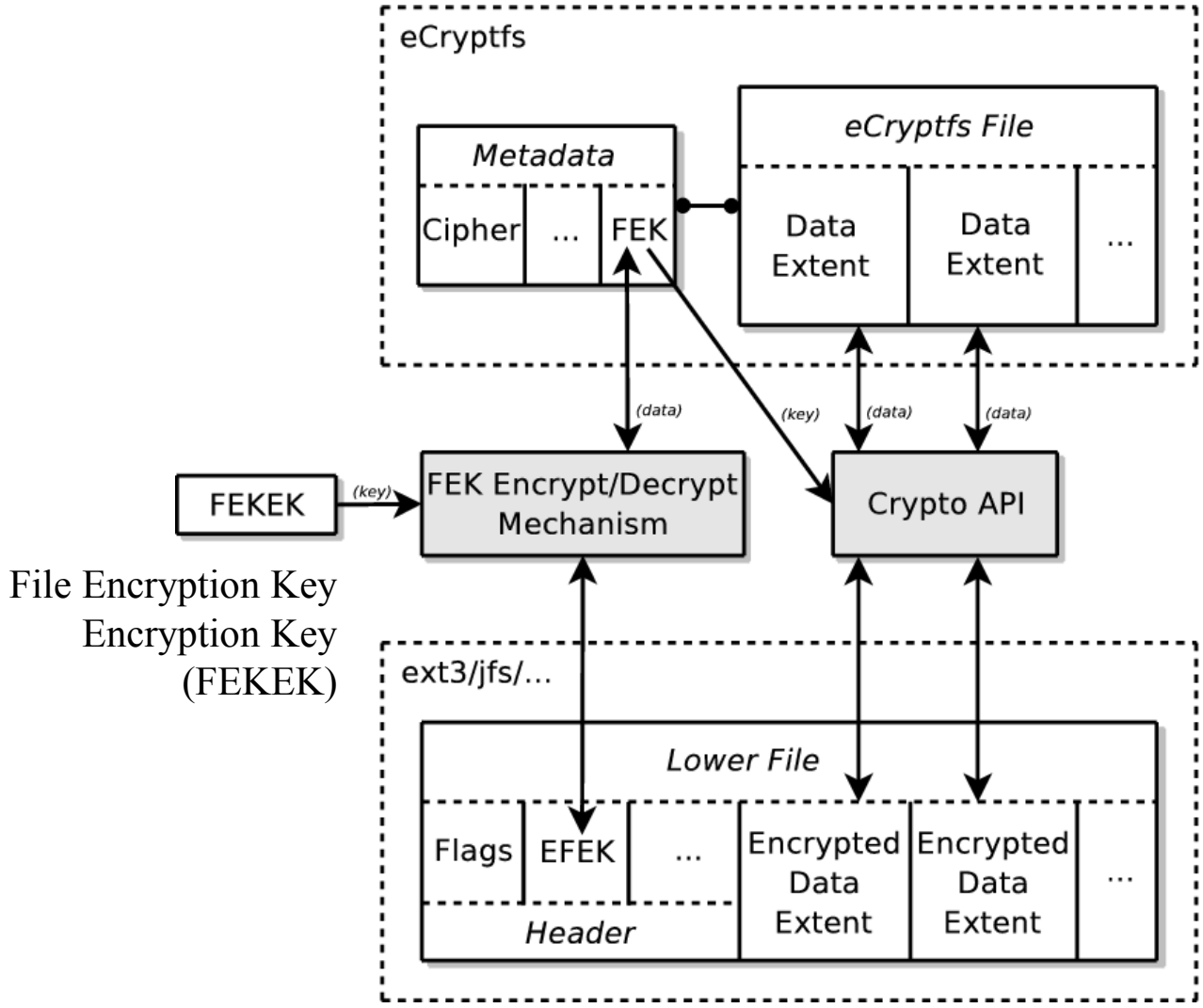
- Make all state explicit, track all communication



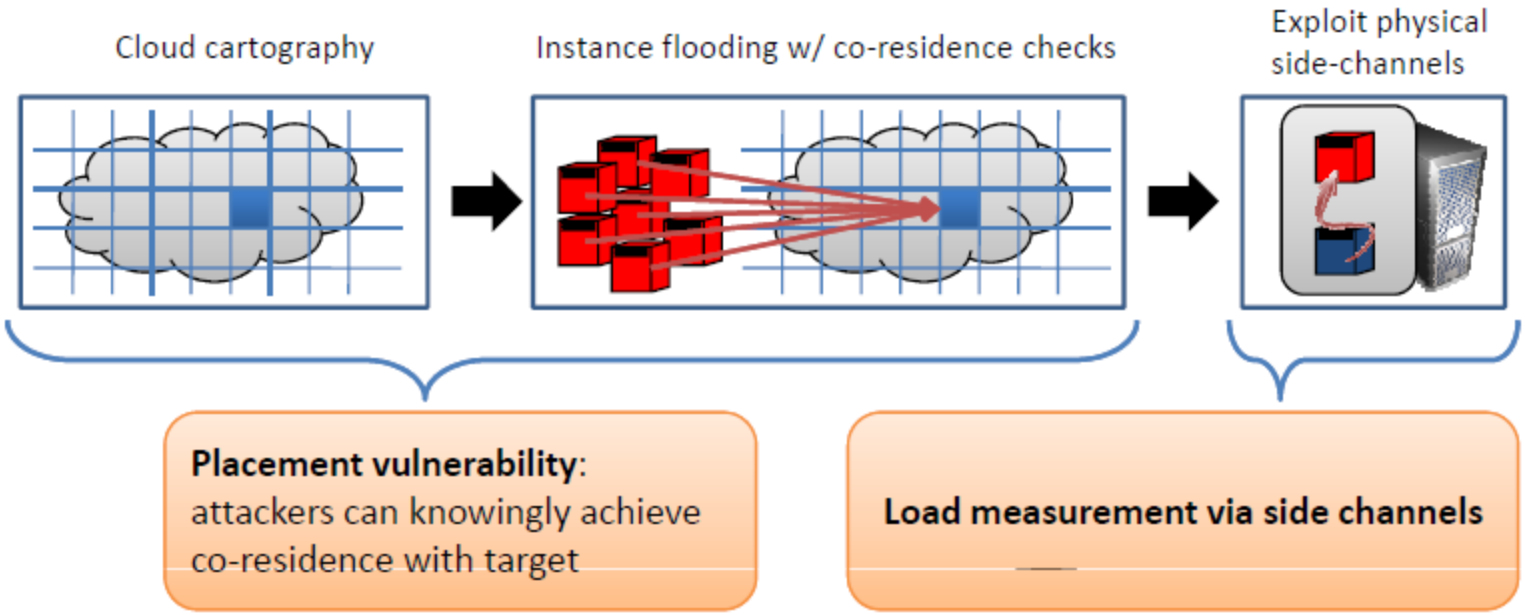
HiStar Kernel Objects



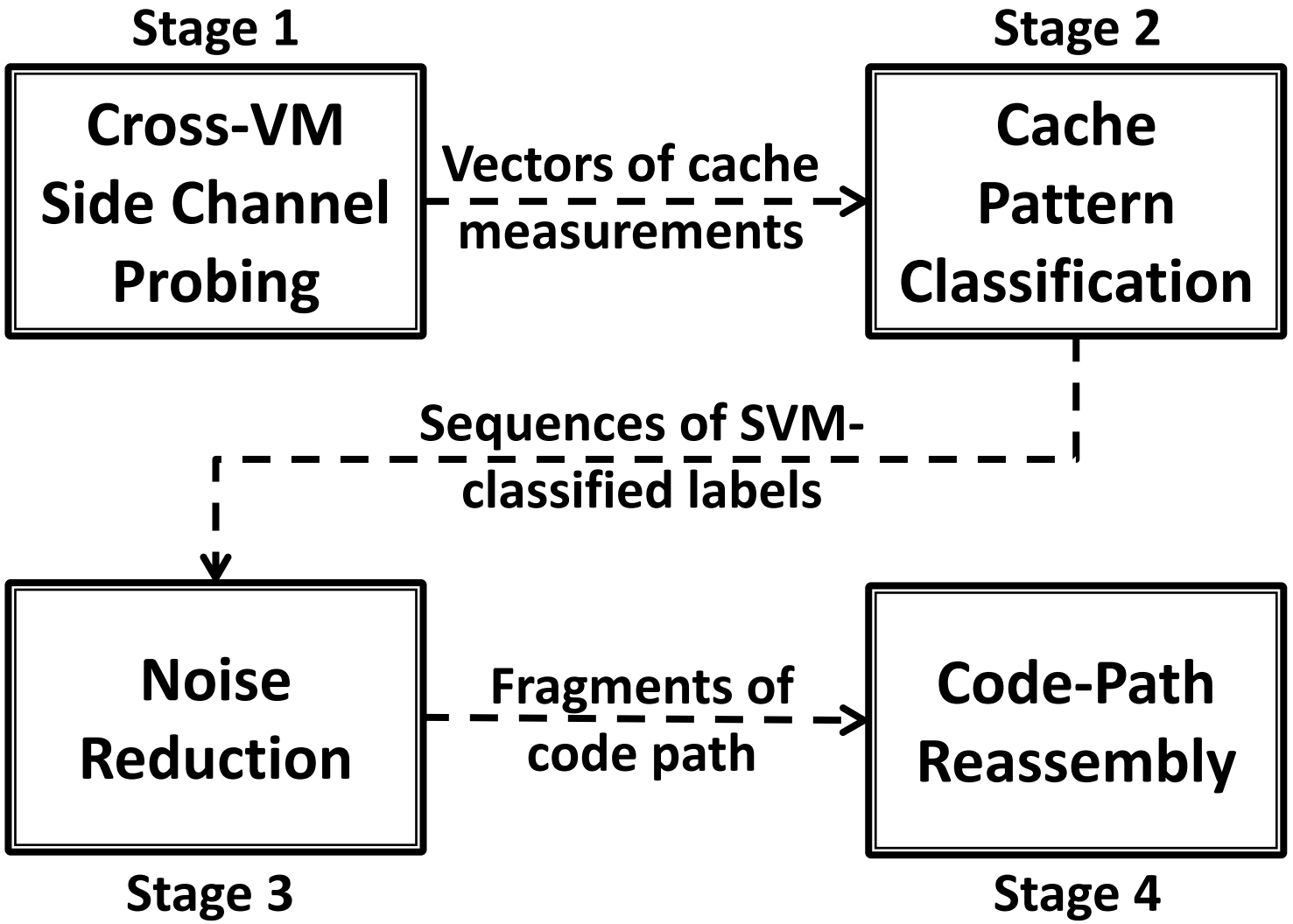
eCryptfs (IBM)



Cloud Cartography paper



Cross-VM Side Channel paper



Final

- 30-50 questions (~1 min. each)
- Everything is included
  - but ~ 40/60% before midterm/new split
- Closed-book
- Bring ID (!)