Module 22: Multi-core Computing Security
Lecture 43: Multiprocessor Techniques

The Lecture Contains:

Previous Next

Producer and Consumer Code

```
BUF_Data consume(void) {
while (buffer.outptr == buffer.inptr) ;
buffer.items[buffer.outptr];
buffer.outptr = (buffer.outptr +1)%BUF_SZ;
return (buffer.items[buffer.outptr-1]%BUF_SZ;);
}
```

- What is wrong with this code?

Message Passing

- Communication channel
  - How to name the channel between two processes?
- Direct Communication
  - The sender process (P) must know the receiver process (Q) and vice versa
    P: send(Q, msg) ♦ Q: receive(P, msg);
  - Some versions may have receive(ANY, msg);
- Indirect Communication
  - Mailboxes must be named rather than the processes.
  - Sender: Create_mailbox(Name, Properties);
  - Sender: Send(Name, msg);
  - Sender: Distroy_mailbox(Name);
  - Receiver: Open_mailbox(Name);
  - Receiver: Receive(mailbox, msg);

Previous Next

Synchronization With Messages

- Send:
  - Blocking send
    - Sender process is blocked till receiver process receives the message
  - Non-blocking send
    - Sender process resumes after send.
- Receive
  - Blocking receive
    - Receiver process waits until a message is received
  - Non-blocking receive
    - Receiver process does not wait if the message is not ready.
      Return status indicates if message is ready or not.

Buffering Model

- Buffer capacity:
  - Zero capacity.
    - Link can not have any waiting message.
    - Sender must block till receiver is ready to receive
  - Bounded capacity.
    - Finite storage of waiting messages.
    - Sender blocks when link is full.
  - Unbounded capacity.
    - Sender never blocks.

Previous Next

Multiprocessor Techniques

- Depends upon the hardware services.
  - Shared memory machines usually provide shared memory IPC.
  - Distributed memory machines usually provide message passing.
- On networked machines: Message passing.
- On multi-core machines: Shared memory and threading.

Multi-core Computing Security

First Job

- A quote from Network Security book by Charlie Kaufman, Radia Perlman, Mike Speciner.

Si spy net work, big fedjaw iog link kyxogy

Please decipher it for me.

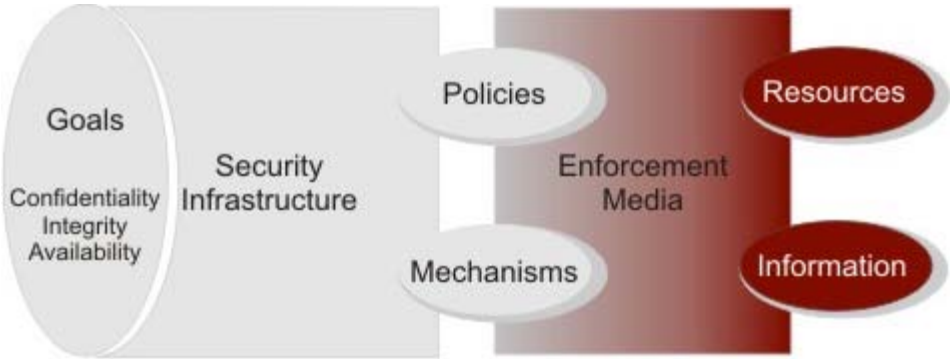
Hint: Dedication.

Previous Next

Decipher

Si spy net work, big fedjaw iog link kyxogy
Replace S by T → Ti tpy net work, big fedjaw iog link kyxogy
Replace i by o → To tpy net work,bog fedjaw oog lonk kyxogy
Replace p by h → To thy net work,bog fedjaw oog lonk kyxogy
Replace y by e → To the net work,bog fedjaw oog lonk kyxoge
Replace n by b → To the bet work, bog fedjaw oog lobk kyxoge
Replace e by a → To the bat work,bog fadjaw oog lobk kyxoge
Replace t by d → To the bad work,bog fadjaw oog lobk kyxoge
Replace k by s → To the bad wors, bog fadjaw oog lobs syxoge
Replace w by g → To the bad gors, bog fadjag oog lobs syxoge
Replace o by u → To the bad gurs, bog fadjag oug lobs syxuge
Replace g by r → To the bad gurs, bor fadjag our lobs syxure
r byy,bbyf, ... → To the bad guys, for making our jobs secure

Security Infrastructure



Previous Next

Goals: Confidentiality

- Access to information or resources only to authorized users/entities/persons.
- Mechanism:
  - Access Control List (ACL) or Access control specifications
  - Data encryption
- Must have a mechanism to authenticate
  - Password, Cryptographic techniques
- Some time necessary to even conceal the fact that the information exist.
  - Access control on directories, Steganography

Goals: Integrity

- “Can I trust the information?”
- Data integrity to ensure that the data is genuine and is not modified
- Some time need to ensure that data originated from the right place
  - Origin integrity
- Mechanism
  - Cryptographic techniques
  - Hashing techniques
  - Checksums and use of alternate channels to send them.

Previous Next

Goals: Availability

- A most common attack is “denial of service” attack.
- Attacker does not get the access but can prevent other authorized users getting access as well.

Policies

- “What is permitted”
  - For example “only course students can have read access to the these lecture notes”
- Policies are usually defined by the administrator or owner of the resource.

Mechanisms

- Mechanisms are techniques/methods to enforce a policy
- For example a “attributes” associated with a file can be changed by the owners
- Mechanism need not even be technical
  - A lost ID card application must be approved by the Dean’s office before a new one is issued.
- In computer related security, typically procedural mechanisms are used.

Previous Next

Enforcement Media

- The channel through which the information or a resource access is granted.
  - OS for example.
- Sometimes the media may not be trustworthy (for example the network)
  - In the security policies and mechanism this aspect has to be taken care of.

Threat and Attack

- Threat is a potential violation of security
- Attack is actual violation.
- Leakage of information
- Modification of message while in transit
- Loss of information
- Proxy
- Active and passive attacks

Previous Next

Module 22: Multi-core Computing Security

Lecture 43: Multiprocessor Techniques

Information Security

- Mechanism to ensure that none of the threats, applicable to a scenario, apply.
- Techniques
  - Authorization
    - “Should you be doing that?”
  - Authentication
    - “Who are you?”
  - Cryptography

Threat Perception and Cost of Security

- Securing a system has three components
  - Prevention, intrusion detection and recovery
- Each system has its own cost.
- Security techniques may not be easy to use
- Cost of securing a system must match the threat perception and value of information.

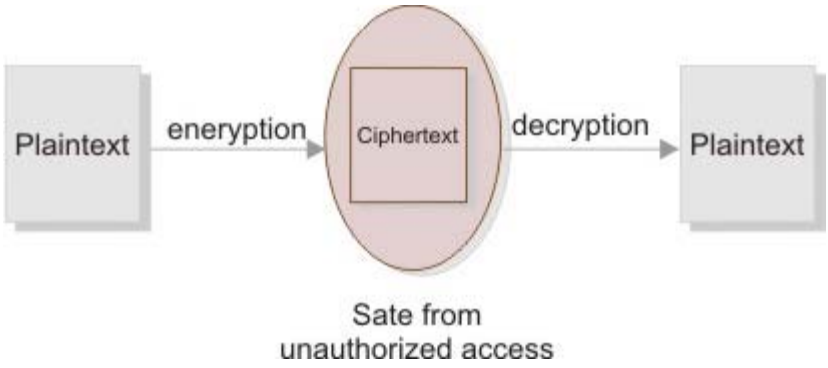
Previous Next

Cryptography: κρυπτο γραφη

(hidden writing)

- Mangling of information in a way that unauthorized parties not able to de-mangle.
- Applications include integrity checking and authentication.
  Plaintext or cleartext: The message in its original form.
  Ciphertext: The mangled information.

Cryptography



Previous Next