Information Protection in Computer Systems

Paper focus:

Protecting information from unauthorized use or modification.

Main mechanisms: Hardware and software for information protection.

Basic Principles of Information Protection

Importance of protecting information in computer systems. Examples of scenarios with different user access levels.

Definitions: privacy, security, and protection in computer systems.

Design Principles

Eight Design Principles:

1. **Economy of Mechanism**: Keep the design simple and small to facilitate error detection.
2. **Fail-Safe Defaults**: Base access decisions on permission rather than exclusion, with the default being lack of access.
3. **Complete Mediation**: Every access to every object must be checked for authority.
4. **Open Design**: The design should not be secret, relying on specific keys or passwords rather than secrecy.
5. **Separation of Privilege**: Systems should require two keys for access, providing more robust security.
6. **Least Privilege**: Programs and users should operate with the minimum set of privileges necessary.
7. **Least Common Mechanism**: Minimize shared mechanisms to reduce potential security compromises.
8. **Psychological Acceptability**: Design the human interface for ease of use to ensure correct application of protection mechanisms.

Protection Mechanisms

Implementation Challenges:

Acknowledgment of imperfect systems. Relying on design principles for mitigation.

Technical Underpinnings

Multiuser System Model:

- Descriptor register for memory access control.
- Privileged state bit managed by supervisor program.
- Protection mechanisms safeguard users and system implementation.

Virtual Processor Implementation

Protection Mechanisms Associated with Abstractions:

I. Memory Access Protection
II. Descriptor Register Protection
III. Privileged State Bit Protection
IV. Virtual Machine Concept:
V. Combining virtual processor, memory area, data streams, and isolated long-term storage.

Authentication Mechanisms

I. Time-sharing Systems:
II. User identity verification via passwords.
III. Weaknesses of password-based systems.

Sharing Information Among Users

- Implementations for Protection Mechanisms:
- List-oriented and Ticket-oriented approaches.
- Introduction of principals for virtual processor activities.

Implications of Sharing

Sharing a Procedure Among Multiple Virtual Processors:

I. Temporary Result Storage
II. Expansion and Generalization
III. Capability Systems vs. Access Control List Systems
IV. Slide 10: Capability System

Separation of Addressing and Protection:

- Descriptors for protection and addressing.
- Unique identifiers and segments.

Capability System Overview:

Capabilities as key concepts.

Dynamic Authorization and Authentication

Capability System's Dynamic Authorization:

- Protocol for secure principal identifier exchange.
- Revocation and Control of Propagation.

Constraints on Capabilities:

- Copy bit, depth counters, and potential issues.

Redell's Proposal

- Extension of Capability Mechanism:
- Indirect objects for systematic revocation.
- Comparison with ACL system.

Access Control List (ACL) System

i. Reversibility of Bindings:

- Inserting authorization check at the latest possible point.
- Introduction of access controllers and protection groups.
- Slide 14: Discretionary and Nondiscretionary Controls

ii. Implementation Challenges:

- Coexistence of controls.
- Compartmentalization and label-based access.

Challenges in Achieving Complete Confinement

I. Security Concerns:

- High water mark, Bell and LaPadula's strategy.
- Human judgment in declassification.

Protection of Objects and Protected Subsystems

Type in the Protection System:

- Different operations based on object types.
- Introduction of protected subsystems.

Challenges in Implementing Domain Switching

- Coordination of Protection Domains:
- Dynamic activation records, variable storage.
- Controlled passing of arguments between domains.

Conclusion

- Summary of protection mechanisms.
- Importance of coordination and careful implementation.