Computer Security in 3D

Christian Damsgaard Jensen,

Department of Applied Mathematics and Computer Science
Technical University of Denmark

Christian.Jensen@imm.dtu.dk

Traditional Security – Perimeter Defense
Traditional Computer Security in Practise

- Distinguish between logical and physical security
  - Logical Security is enforced by the computer system
    - Login performs authentication
    - Access control enforced when resources are accessed
  - Physical Security is enforced by external “agents”
    - Locked server rooms (keys/access card/biometrics to enter)
    - Guards and alarms

- Logical security requires physical security
  - Servers are locked in secure server rooms
  - Assumes that the person who logged in is now sitting at the terminal
  - Object can only be accessed by subject who requested the operation
    - Printing exam scripts on shared departmental printers???

The security perimeter is dissolving

- Computers are brought into the shared workplace
  - Personal computers in open plan offices (cubicles)
- Mobile-/wearable computers (there is an App for that)
  - Access to computing resources anytime, anywhere
    - Working from home, on the move, always-on
  - Changing both virtual and physical locations
- System integration across system boundaries
  - Virtual Enterprises/-Organisations
  - Opportunistic Collaboration and Dynamic Coalitions
- Internet of Things
  - Ubiquitous access to embedded (control) systems (e.g. smart meters)
  - Computers embedded in everyday things (TVs, refrigerators, cars, …)
Ambient Intelligence

- Embedding sensors, actuators & computing capabilities in env.
  - Sensors establishes current context
  - Actuators adapts "environment" to the need of the users
    - Environment may include computer equipment, monitors, etc.
  - Computing capabilities implement smart behaviour
    - Context aware applications, location based services, ...

- Ambient intelligence may provide environmental context to the logical access control mechanism
  - Sensors allow the system to establish location of human users
  - Computing capabilities may determine context of human users
  - Actuators will not be used by security mechanism, but logical access controls may be considered some form of "actuators"

Traditional Security Framework
Identification & Authentication

- The user identity serves three primary purposes
  - It allows the representation of a human user as a system subject
    - Human user claims right to a system identity (subject id)
    - Requires authentication of subjects (validation of claimed id)
    - Human (real world) identity is difficult/expensive to change
      - Reduces probability of White-washing and Sybil attacks
  - It allows different permissions to be granted to different subjects
    - Defined in the access control policy
    - Ultimately based on the identity mapped to the subject
  - It allows accountability
    - Record the identity mapped to the subject performing an action
    - Log serves as evidence if something goes wrong

Access Control in Practise
Enforcing Computer Security Policies

• Security enforced by logical and physical security mechanisms

• Granularity of security mechanisms
  – Logical Security is fine-grained (individual records/files/...)
  – Physical Security is coarse-grained (buildings/rooms/...)

• Computer Enforced Security Mechanisms (logical security)
  – Restricted to consider the state of computer system entities
    • Human users are not directly part of computer systems
    • Data must be rendered physically to be consumed by users
      – Displayed on monitor, printed, played on speakers
    • Access to rendered data is constrained by physical security
      – Confidentiality by restricting access to output devices
      – Integrity by restricting access to input devices

The Granularity Gap in Access Control

• Granularity of physical access control (room, floor, building, ...)
  – Defines the context for logical access control
  – Granularity of physical security dominates
    • \( \min(\text{physical, logical}) = \text{physical} \)

• Trust in subject fills the granularity gap
Authentication in 3D

- Discrete Authentication
  - Login is a discrete event (login + password, biometrics,...)
  - Authentication is extended in time through a session
    - Re-authentication is explicit and rare (Kerberos)
    - What happens if person leaves device with session open?

- Continuous Authentication
  - Authentication is extended in time
    - Token-based (Zero Interaction Authentication)
      - Presence of token is continuously required
      - Secure location services
    - User-centric
      - Biometrics (laptop webcam confirms user is still present)
  - Authentication is extended in time and space
    - Persistent Authentication
Persistent Authentication

- Persistent Authentication provides a calm approach to continuous authentication, using sensors from the smart environment to associate the initial authentication with users moving around.

**Authentication Confidence**
Access Control in Practise

Sensor Enhanced Access Control

• Motivation
  - To extend logical access control with context awareness
  - Allows logical access control to be enforced in the physical env.

• Defines two models
  - Logical access control
    • In principle any access control mechanism
    • Mandatory access control mechanisms are natural candidates
  - Environmental access control
    • Establish the context of subjects and objects
    • Defines authorization zones for location based services
      - Visibility zones for output devices (monitors)
    • Enforces logical access control policy in authorization zones
      - Continuous enforcement based on context
SEAC Model

Environmental access control

Logical access control

SEAC Prototype Architecture

Environment

User space

Kernel space

File

Window

Visibility manager

Process

read/write

draw graphics

Environment

Sensors

Context manager

Person

view

event notification

read/write

event notification
SEAC Prototype Implementation

- Proof of concept prototype developed for standard Linux system
- Simple mandatory access control model (based on Bell & LaPadula)
  - Simple security property (no read up)
  - *-property (no write down) – not implemented in prototype
- Security Labelled file system (and open file monitor)
  - Associates security labels with all files + processes that open files
  - Implements logical access control
- Context Manager
  - Derives context from sensors
    - Issues events when users enter/leave visibility zone
- Visibility manager
  - Subscribes to events from context manage
  - Maps/unmaps X-windows based on subject clearances
    - Considers all persons in the visibility zone (minimum rule)

Summary
Conclusions and Perspectives

• Logical access controls are not enforced in the real world
  – Who has access to physical representation of logical object?

• Smart Environments provides context for logical access control
  – Environmental access control enforces logical AC in the real world

• Environmental access control policies
  – Multiple subjects and continuity of enforcement
  – Policy specification requires an aggregated subject (new challenge)
    • Simple minimum rule, relative importance rule, ...
  – Policy specification requires context definition (new challenge)
    • Confidentiality rule, integrity rule, ...
  – Allows community access control policies (new opportunity)
    • Simple separation of duty
      – Two (authorised) people present to pay a bill
    • Declassification of sensitive information
      – Two (authorised) people are needed to declassify information