Persistent Access Control

Protecting & Controlling Primary and Secondary Information Distribution

Marshall D. Abrams
26 September 2000

© Copyright 2000, The MITRE Corporation. All rights reserved.

Persistent Access Control (PAC)—Concept in Brief

- PAC provides a mechanism to ensure that creators of digital information can control redistribution and use
- Commercial concerns
  - Unauthorized redistributed with no compensation to the owner
- National security concerns
  - Inability to control distribution of information
Applicability
National Security/Intelligence Community

- Prevent authorized users from further disseminating sensitive data
- Fine-grained control of data
- Traditional response: physical, administrative, and (limited) technical security
- PAC provides a new level of technical security that complements traditional ORCON and allows complete control over data

Applicability
Commercial

- The system provides a mechanism to ensure that creators of intellectual property (IP) distributed in digital format can control redistribution (piracy) and, also, can control use.

- Without such protection any digital material can easily be redistributed with perfect fidelity (indistinguishable from the "original") with no compensation to the owner.

- The software publishers association estimates that over $7.5 Billion of such redistribution occurred last year.

- The growing availability of networked systems (e.g., Internet) will exacerbate this problem.
The economic disincentives associated with conventional (i.e., non-digital) forms of data (e.g., printed material or audio tapes) do not stand as barriers to copying and distributing digital data.

The “copy” of a digital “original” is indistinguishable from the original. Possession of a “copy” is not associated with loss of status, fidelity, or utility.

### Commercial Illustration

![Diagram of digital data flow]

### Data Structured and Protected

<table>
<thead>
<tr>
<th>Text</th>
<th>Restrictions on use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Still &amp; Motion Pictures</td>
<td>Cryptographic algorithms and protocols</td>
</tr>
<tr>
<td>Audio</td>
<td>Electronic payment procedures</td>
</tr>
<tr>
<td>Other source material</td>
<td>Protected Data</td>
</tr>
</tbody>
</table>

- Encrypted IP body part
- Unencrypted IP body part
- Permission List
- Ancillary information
Operational Concept

Operational Concept Diagram:

- **Originator**
  - Select data inputs, distribution list, permissions & rules
  - Bind data, rules & list
  - Distribute package
    - Data & rules may be distributed together or separately
  - Controlled access to information
    - Enforced by tamper-detecting mechanism
    - Unauthorized access prevented by encryption

- **Protected & Packaged Information**
  - Encrypted Info body part
  - Unencrypted Info body part
  - Permission List - Rules
  - Ancillary Information

- **Recipient**
  - Select package
  - Obtain rules (if separate)
  - Read, print, copy
    - Only as permitted

- **Technical Approach: Access Control**
  - Data sent out of the security boundary are under the control of the access mechanism
    - All I/O requests and interrupts are handled by the access mechanism below the operating system
  - Data encrypted on any non-volatile storage devices so that they remain unavailable in the case of tampering
  - Unencrypted data and cryptographic variables
    - Only present inside the security boundary
    - Destroyed when tampering is detected
At Originator’s Workstation

- Human selections
  - Information, protection
  - Restrictions, policy, distribution list
- Functions in workstation
  - Encryption: data-encrypting key, data, rules & ancillary information
  - Data structuring & packaging
- Trust requirements
  - Integrity: correct functioning & no hidden side effects
  - Protection of cryptographic methods and variables
  - If incorporating protected information
    - Ability to access previously protected information
    - Propagation of restrictions

At Recipient's Workstation

**Setup**
- Information received
- Access mechanism gets & verifies rules
- Information made ready for processing inside protection boundary

**Operation**
- User attempts operation
- Access mechanism mediates
- Permitted or prevented

**Tamper Detection**
- User attempts to violate protection boundary
- Detected
- Erase protected information
- Zeroize keys
How PAC Works: Two High-Level Views

- **Program(s) view**
  - Clear at start
  - "Promote" when opening file(s)
  - Controlled READ/WRITE
  - Rules from opened file(s)
  - Clear at end when file(s) and program(s) closed

- **I/O call view**
  - All I/O controlled by Basic I/O System (BIOS)
  - "Well structured" application call via OS
  - Direct call possible
  - BIOS enforces PAC rules

---

How PAC Works at Recipient's Workstation: A Pictorial View

- Computer Cabinet tamper-detect boundary

- Encrypted distribution
- Encrypted data
- Mother Board
  - Crypto
  - BIOS
  - Key: Changed

- Hard Disk
- Memory
- Display
- Printer
How Encryption Is Used

- Select data, cryptographic algorithms, protocols
- Construct permission lists/rules
- Data-encrypting key $K_D$ & symmetric algorithm selected by the distributor
  - May be different for each part/product
- $K_D$ encrypted using asymmetric rule-encrypting key $K_R$
  - When rules packaged with data, $K_R$ same for all data at specific sensitivity and all embodiments
  - When rules are distributed separately, $K_R$ can be unique
- Keys protected within tamper-detecting mechanism

PAC Key Management Observations

- PAC requires subset of “conventional” Certificate Authority
  - NOT $n^2$ size (any person ↔ any person)
  - Only n size
    - Each “owner” of protected information ↔ set of computers (n)
    - Not fully “managed”
    - Need only confirm association of public key with recipient
      - Serial number
      - User ID (e.g., token)
Rule Distribution Alternatives

* Rules encrypted independently from information
  - Different key, perhaps different algorithm
  - Multiple rule sets possible (e.g., demo, user, developer, level of clearance)
* Rule-decrypting key encrypted under key-encrypting key
  - Key-encrypting key unique per copy
* Key-decrypting key distributed separately
  - On-line interaction
  - From merchant
* Distribution of rules
  - With the IP — same media
  - Separately from IP
    - IP copy identified by serial number

Summary

* Provides fine-grained control of access and distribution
  - Enforced by hardware/firmware mechanism independent of OS (e.g., BIOS)
* Provides new level of technical security that complements traditional ORCON
* Rules bound to information
  - Rules can be distributed with information or separately
* Supports multilevel distribution
* PAC includes
  - Protecting selected portions of the information
  - Protecting information by encryption
  - Determining rules concerning access rights
  - Protecting the rules
  - Packaging protected portions of data and rules
*** Rapid Prototype Screens***
Prototype: Policy Control Editor

Prototype: Selecting Access Controls
Prototype: Selecting Fees

![Fees window](image_url)

- **Copy Cost**: $4
- **Print Cost**: $7.8
- **Read Cost**: $9.778