Detecting and Countering Insider Threats: Can Policy-Based Access Control Help?

Jason Crampton\(^1\)  Michael Huth\(^2\)

\(^1\)Information Security Group
Royal Holloway, University of London

\(^2\)Department of Computing
Imperial College London

STM 2009
The terms **insider**, **insider threat** and **insider attack** are understood by most people, albeit in an informal way.

- Traitors and moles are obvious examples of insiders who can inflict damage on the host organization.

Insider attacks are very common and can be extremely damaging.

- The FBI estimated that they cost approximately 50 times more on average than external attacks.

There is no real consensus about how to define an insider.

- Makes it difficult to provide a satisfactory formal approach to the insider threat.
Introduction

We explore the insider threat from the perspective of access control

- Many enterprise security requirements are enforced using access control systems
- Most access control systems assume that authorized users are trusted

How can we build access control systems for which this assumption might be relaxed?

- We examine how recent advances in policy-based access control may be used to build systems that are responsive to insider threats
Introduction

Insiders and the Insider Threat

Trust and Trustworthiness

Access Control and Trustworthiness
Illustrative Scenarios

There are many examples in the literature...

- A system administrator has write access to the directories containing Company A’s intellectual property
- Urgent building work leads to external contractors working in security-sensitive parts of Company B’s headquarters
- The personal assistant to the chief financial officer (CFO) of Company C has access to the CFO’s diary and personal email account
What is an Insider?

Insiders

- “someone with access, privilege, or knowledge of information systems and services” [Brackney and Anderson]
- “anyone operating inside the security perimeter” [Patzakis]
- “someone with authorized access who might attempt authorized removal or sabotage of critical assets or who could aid outsiders in doing so” [Dagstuhl seminar on countering insider threats]

When is an “outsider” an “insider”?
A system administrator has write access to the directories containing Company A’s intellectual property

**Threat** The administrator may encrypt all the IP and extort money from Company A

**Assumption** The administrator won’t encrypt the IP in this way
Threats and Assumptions

Urgent building work leads to external contractors working in security-sensitive parts of Company B’s headquarters.

**Threat**  A contractor could be a hacker working for Company B’s competitor.

**Assumption**  The contractors are vetted thoroughly.
The personal assistant to the chief financial officer (CFO) of Company C has access to the CFO’s diary and personal email account.

**Threat** The PA could divulge details of confidential negotiations between Company C and Company D to a mutual competitor.

**Assumption** The PA is trusted by the CFO.
Introduction

Insiders and the Insider Threat

Trust and Trustworthiness

Access Control and Trustworthiness
Some Observations

- Organizations have many employees
- Each employee has certain responsibilities and duties
- An employee must be given access to resources to enable her to discharge her responsibilities and perform her duties
- An organization assumes that an employee does not abuse the access she has been granted
Some Observations

- Organizations have many employees
- Each employee has certain responsibilities and duties
- An employee must be given access to resources to enable her to discharge her responsibilities and perform her duties
- An organization assumes that an employee does not abuse the access she has been granted
- Therefore, the “insider threat” is unavoidable and we can only hope to mitigate its effects
Trust and Insiders

The term “insider” does not appear to be very useful

- All authorized users of a computer system are trusted to a greater or lesser extent
- Authorized users are (indeed, have to be) trusted not to abuse any access for which they are authorized
- Any authorized user represents a threat if the trust placed in her is not appropriate
Trustworthiness and the Insider Threat

The distinction to be made is between trusted users that are trustworthy and those that are not

- A trustworthy user does not abuse the trust that has been invested in her
- We must identify those users that are trusted but who are not trustworthy
- An outsider that impersonates an authorized user renders that user untrustworthy (from the system’s perspective)
Trustworthiness and Insiders

Problem

How do we decide who is trusted but not trustworthy?

Problem

What do we do, in terms of access control, about such a user?

We focus on the second of these questions in this paper.

- Nevertheless, a comprehensive solution requires that the first question be addressed.
Introduction

Insiders and the Insider Threat

Trust and Trustworthiness

Access Control and Trustworthiness
Access Control

User → PEP → Resource

- User: interaction
- PEP: authorization request, authorization decision
- Resource: resource information
- PDP: user information, authorization policy
- PR: authorization decision

Access Control and Trustworthiness
Access Requests

We model attempted user-resource interactions as access requests.

- Requests are determined by (attributes of) users and resources, the type of interaction, and the context in which the attempted interaction occurs.
- The request space is defined by the sets of users, resources, interaction types, and contexts.
Access Control Policies

An access control policy may be as simple as “allow all requests in this subset of the request space”

- XACML rules have this form

A policy may be formed by combining other policies

- XACML policies and policy sets are obvious examples
- We need ways of computing a single decision from the multiple decisions returned by constituent policies

Policies should be re-usable
Our Policy Language

- A policy may return one of four values

\[ \{\emptyset, \{0\}, \{1\}, \{0, 1\}\} \equiv \{\bot, 0, 1, \top\} \]

Deny \equiv 0 \text{ and Grant} \equiv 1

- Specify sets of requests using predicates ranging over variables in the request space

\[ \text{Manager} \land \text{PersonnelFile} \land \neg \text{Weekend} \]

- Specify policies from sets of requests

\[ \text{grant if} \ (\text{Manager} \land \text{PersonnelFile} \land \neg \text{Weekend}) \]

- Specify sets of requests from policies

\[ p@\text{grants} \quad \text{and} \quad p@\text{denies} \]
Applying the Language

We can construct parameterized policies using predicates and policy operators

```plaintext
pol insdrThrt(abnmlBhv: reqs, authzUsr: reqs)
{
    (grant if !(abnmlBhv) && authzUsr) >
    (deny if abnmlBhv || !(authzUsr))
}
```

- The request predicates `abnmlBhv` and `authzUsr` identify subsets of the request space
- The (policy) operator `>` is a precedence operator
- The policy `insdrThrt` allows only those requests that originate from authorized users and do not represent abnormal behavior
We can “harden” a policy $P$ so that it only allows if the request is authorized by $P$ and originates from a trustworthy user:

```plaintext
pol grantOnlyInsdrs(P : pol, trstwrthyUsr: reqs)
{
  (grant if P@grants && trstwrthyUsr) > deny
}
```

This suggests the need for a trustworthiness evaluation system.
Applying the Language

We can modify a policy $P$ to incorporate a risk-based stance

```plaintext
pol denyTooRsky(P : pol, tooRsky: reqs)
{
    (deny if tooRsky) > (grant if P@grants) > deny
}
```

- The request predicate `tooRsky` identifies those requests that, if granted, represent a risk greater than some threshold value
- `tooRsky` could, for example, be evaluated according to the trustworthiness of the user and the value of the resource
Architectural Modifications

<table>
<thead>
<tr>
<th>TEP</th>
<th>Trustworthiness evaluation point</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEP</td>
<td>Context evaluation point</td>
</tr>
<tr>
<td>ADS</td>
<td>Anomaly detection system</td>
</tr>
<tr>
<td>CAS</td>
<td>Context acquisition system</td>
</tr>
</tbody>
</table>

Introduction
Insiders and the Insider Threat
Trust and Trustworthiness
Access Control and Trustworthiness
Future Work

- Further investigate how trust and reputation systems can be fused with our policy language
- Examine case studies of insider attacks to evaluate whether our approach could have helped prevent those attacks
- Identify and specify requirements for access control architecture