We thought we had this stuff figured out back in the 1970s. What went wrong?

Jerome H. Saltzer, MIT
<Saltzer@mit.edu>

ISSSE 2006

What I’m planning to say...

• What we thought we knew
• What happened next (PC’s and the Internet)
• What went wrong (neglect of complete mediation)
• What happened in UNIX (buffer overflows)
• What went wrong (neglect of complete mediation)
• Analysis: Why? (more trouble ahead…)

Two models

• Discretionary

<table>
<thead>
<tr>
<th>objects</th>
<th>permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>actors</td>
<td></td>
</tr>
</tbody>
</table>

• Mandatory

Read:

\[
\text{level} \_\text{classification} \leq \text{level} \_\text{clearance} \\
\text{hwm} \leftarrow \text{MAX} (\text{hwm}, \text{level} \_\text{classification})
\]

Write:

\[
\text{level} \_\text{classification} \geq \text{level} \_\text{hwm}
\]

(where \text{hwm} is a high-water mark)

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHRÖDTER, MEMBER, IEEE

Invited Paper
Progress report…

√ What we thought we knew
⇒ What happened next
  *(PC's and the Internet)*

- What went wrong
  *(neglect of complete mediation)*
- What happened in UNIX
  *(buffer overflows)*
- What went wrong
  *(neglect of complete mediation)*
- Analysis: Why?
  *(more trouble ahead…)*

Complete Mediation
Always ask three questions…

1. Authentication:
   *Who made the request?*

2. Integrity:
   *Has anyone tampered with it?*

3. Authorization:
   *Is this request permitted?*
Why was this design principle, which is so fundamental to security, neglected?

1. Rapid rise of the PC
2. Rapid rise of the Internet
3. Government interference

next...

√ What we thought we knew

√ What happened next (PC’s and the Internet)

√ What went wrong (neglect of complete mediation)

⇒ What happened in UNIX (buffer overflows)

• What went wrong (neglect of complete mediation)

• Analysis: Why? (more trouble ahead...)

Buffer overflow exploitation
next...

√ What we thought we knew

√ What happened next
   (PC’s and the Internet)

√ What went wrong
   (neglect of complete mediation)

√ What happened in UNIX
   (buffer overflows)

⇒ What went wrong
   (neglect of complete mediation)

• Analysis: Why?
   (more trouble ahead…)

Return instruction:

load program_counter from return_point;

Complete Mediation
Always ask three questions…

1. Authentication:
   Who made the request?

2. Integrity:
   Has anyone tampered with it?

3. Authorization:
   Is this request permitted?

next...

√ What we thought we knew

√ What happened next
   (PC’s and the Internet)

√ What went wrong
   (neglect of complete mediation)

√ What happened in UNIX
   (buffer overflows)

⇒ Analysis: Why?
   (more trouble ahead…)
The future…

Is security going to improve?

No!

1. Technology change:
   \[
   \frac{d(\text{technology})}{dt}
   \]
   is too large!

2. Can’t keep up with all of the elves.
The real security challenge:

How do you keep people from doing stupid things?