Structural vulnerabilities

What are they and why do they matter?

The foreseeeti white paper series
Structural vulnerabilities - What are they and why do they matter?

Vulnerability scanners often report large numbers of vulnerabilities in corporate IT systems. For the IT security manager, prioritising remediation activities is a problem. Prioritising by vulnerability scoring systems such as the Common Vulnerability Scoring System (CVSS) is simplistic because it does not fully take into account other defences or vulnerabilities. Attempting more detailed analysis quickly becomes very time consuming. As a consequence, structural vulnerabilities\(^1\) caused by combinations of component vulnerabilities\(^2\) can readily remain unresolved.

Furthermore, compliance with IT security standards is generally a poor guide on whether component vulnerabilities combine to create structural ones. The most commonly used standards do not require attack path analysis, the key technique for distinguishing between component and structural vulnerabilities. This creates a problem for data owners and security policy makers; mandating compliance with existing standards is seldom sufficient for their needs.

In this article, we show that determining whether vulnerabilities are structural requires a detailed knowledge of the system configuration. For all but the simplest systems, human analysis alone is a poor solution. However, new techniques and tools make detailed attack path analysis viable for corporate IT

\[^1\] https://en.wikipedia.org/wiki/Structural_vulnerability_(computing)
\[^2\] https://en.wikipedia.org/wiki/Component_Vulnerability
security managers. This creates new options for standards developers and policy makers.

The diagram below illustrates the need for attack path analysis. It represents a simple IT system with a conventional layered security architecture to control access across the Internet to 2 applications. The proxy servers, PS1 and PS2, aim to minimise the attack surface on the application servers (AS1 and AS2) exposed to attackers.

Our vulnerability scanner shows that there are unpatched vulnerabilities in PS2 and AS1 such that an attacker that gains user operating system privileges will be able to escalate these to administrative privileges. The IT Security Manager wants to know how urgent it is patch either or both servers to protect the bulk personal data accessible from AS2. Prudence says ‘patch both immediately’ but real life often requires security managers to choose between multiple urgent and important actions.

The short answer to the IT Security Manager's question is 'it depends' upon the details of the system configuration. Small changes in security related settings can make substantial differences to the most vulnerable attack paths. We can illustrate this by building a model of the system in Figure 1 using a suitable Computer Aided Design (CAD) tool and then measuring its overall security as configuration details vary.

Figure 1 - Simple IT system diagram
Figure 2 shows some of the attack steps identified by securiCAD for a model consistent with Figure 1. The attacker’s entry point is the red circle at the left-hand side. The attack steps shown are drawn from the most vulnerable attack paths. The nodes represent privileges obtained by an attacker after completing the preceding attack steps represented by the arrows between nodes. The green shields represent defence attributes that could be set to increase attack step difficulty.

**Figure 2** - *Initial attack steps from attacker’s entry point. The model is consistent with the system in Figure 1*

SecuriCAD generates the diagram in Figure 2 by:

1. Identifying every possible attack step through the model to create an attack graph.
2. Assigning to each attack step the probability of completion after a given amount of effort by a skilled attacker. The probability functions are derived from statistical analysis of vulnerability databases, applied and practical research, and structured consultations with experienced penetration testers.
3. Exhaustively searching through the attack graph to identify the most vulnerable attack paths based upon the probable time for completion.

Table 1 below illustrates how the probability of compromise changes with each security configuration that builds on top of the other. Each model is consistent with Figure 1.

<table>
<thead>
<tr>
<th>Model</th>
<th>Attack Path</th>
<th>Probability of compromise</th>
<th>Change (percentage points)</th>
<th>Total reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initial configuration</td>
<td>Poorly configured web app on PS2 enables user operating system privileges; o/s vulnerability enables privilege escalation on PS2; connection to AS2 followed by find &amp; deploy an exploit to escalate AS2 privileges.</td>
<td>67%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2. Reduce privilege level of applications running on PS2 &amp; AS2</td>
<td>Increased difficulty of privilege escalation on PS2 and AS2. Critical attack path shifts to exploit http connection from PS1 to AS1.</td>
<td>46%</td>
<td>-21pp</td>
<td>-21pp</td>
</tr>
<tr>
<td>3. Change protocol for dataflow between PS1 &amp; AS1 from http to https</td>
<td>Prevents man-in-the-middle attack on http. Critical path shifts back to privilege escalation from AS2 service</td>
<td>34%</td>
<td>-12pp</td>
<td>-33pp</td>
</tr>
<tr>
<td>4. Improve tuning of PS2 web application firewall</td>
<td>Increases difficulty of gaining o/s user privileges on PS2.</td>
<td>29%</td>
<td>-5pp</td>
<td>-38pp</td>
</tr>
<tr>
<td>5. Remove unnecessary services on AS2</td>
<td>Increased difficulty of privilege escalation on AS2.</td>
<td>19%</td>
<td>-10pp</td>
<td>-48pp</td>
</tr>
</tbody>
</table>

Table 1 - Probability of personal data compromise after 50 days’ attacker effort. Changes from initial configuration are cumulative.
The changes in probability of compromise in Table 1 illustrate the complexity of analysing the security of even very simple IT systems. In a typical corporate IT system there may be thousands of devices with a myriad of protocols, dataflows, defence mechanisms and possible attacker entry points. However, securiCAD aids the user when analysing by presenting chokepoints of the attack paths and mitigation actions that the user should consider. Simplifying and narrowing the scope of where to apply mitigations and in which order.

The model is a simplification of reality, but it helps humans prioritise the remediation of component vulnerabilities in terms of the difference they make to structural vulnerabilities and hence the probability of system compromise.