21st Annual National Defense Industrial Association
Systems and Mission Engineering Conference

Advancing DoD Software Assurance (SwA)

Thomas Hurt
Office of the Under Secretary of Defense for
Research and Engineering
October 24, 2018

84% of breaches exploit the vulnerabilities in the application,
yet funding for IT defense vs. software assurance is 23 to 1.
DoD systems rely on COTS SW for execution of critical mission functionality. Over 107,000 known vulnerabilities have been reported in publicly released SW.
Tools Throughout the System Lifecycle

Through the integration and automation of software assurance tools, throughout the system lifecycle, programs can make informed decisions on the identification and mitigation of risk.

Talent Through Training

Defense Acquisition University (DAU) CLE 081 Software Assurance (SwA) Awareness Continuous Learning Module (CLM)

The CLE 081 SwA Awareness continuous learning module is intended for all DoD acquisition professionals, across all Services and DoD Agencies.

The intent of the module is not to train experts in SwA coding and other implementation techniques, but to provide the DoD acquisition workforce with an awareness of SwA in the development environment and throughout the entire system lifecycle.
**Overview of changes**

- Focus on how to determine what data rights are needed and how to obtain the proper data rights for software assessment.
- Reorganized the document to clarify which sections of the contract we are recommending Software Assurance Language be added.
- Added new sample contract language for use cases.
- Updated existing and added new references.

*Version 2.0 completed September 2018*

---

**Talent through Guidance (continued)**

- Identifies program management (PM) software assurance responsibilities critical in defending software-intensive systems.
- Presents actions a PM must take to ensure that software assurance is effectively addressed throughout the acquisition lifecycle.
- Helps software developers understand expectations for software assurance.
- Summarizes standards and requirements that affect software assurance decisions and provides pointers to key resources that developers should consult.
Technology: Binary Analysis Capabilities

Execution of binary samples in an instrumented virtual environment using a combination of automated and manual testing to identify potentially malicious code

Compute complete control flow and remove dead code that can be used for exploitation

Unpacking of software executable to run static test and examine structural features of the binary sample

Extract structuring and behavioral functions for analysis and include findings in risk report

*Source: AFLCMC TSN Lackland AFB

Summary

Department of Defense security spending continues to increase for cybersecurity instead of fixing the vulnerabilities most commonly exploited by our adversaries.

DoD systems rely on COTS software for the execution of critical mission functionality and must be able to identify and mitigate existing vulnerabilities.

In order to fill the gap, OUSD(R&E) has identified three key areas:

• **Tools:** Software assurance tools selected based on program specific needs and applied throughout the system lifecycle.

• **Talent:** Delivery of training materials and DoD guidance to grow SwA expertise in all assurance related roles.

• **Technology:** Development of assurance processes and methodologies to provide assured software

By building the tools, talent, and technology necessary to identify and mitigate vulnerabilities, future cyberattacks are unsuccessful, because instead of delaying success by mitigating risk at the entry point, the vulnerabilities adversaries typically exploit have been removed.
For Additional Information

Mr. Thomas Hurt
Office of the Under Secretary of Defense for Research and Engineering
571-372-6129
thomas.d.hurt.civ@mail.mil
<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber crime</td>
<td>A criminal or hacker that attacks and exploits your computer system.</td>
</tr>
<tr>
<td>Computer Worm</td>
<td>A worm makes copies of itself and spreads itself to other computers.</td>
</tr>
<tr>
<td>Spyware</td>
<td>A malicious program that looks like a legitimate software.</td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Unauthorized access to company data and systems.</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A malicious program that looks like a legitimate software.</td>
</tr>
<tr>
<td>Malware</td>
<td>A malicious software or website that can harm your computer.</td>
</tr>
<tr>
<td>Phishing</td>
<td>Phishing is a very easy to execute. It consists of fake emails or messages.</td>
</tr>
</tbody>
</table>
| Virus                    | A virus is always hidden in a legitimate software or website and infects your computer.