DEFENSIVE CYBER SECURITY
PROCESSES AND POLICIES
How long can you wait for
CMMI® Compliance?

Manage your software and systems engineering projects
in guaranteed compliance with the CMMI NOW!

processMax 2i and 3i include all the necessary policies, procedures, guidelines, criteria, templates, and forms in role-based, step-by-step instructions, ready for use—everything you need for compliance with the CMMI-DEV at Level 2 and Level 3 respectively. Integrated with robust document management, workflow, and automated measurement and reporting, processMax is the intranet web-based solution for effective and efficient management of your software and systems engineering projects. processMax enables you to start operating in compliance with the CMMI immediately! We guarantee that organizations using processMax will not fail a formal appraisal led by an independent SEI-licensed appraiser.

pragma SYSTEMS CORPORATION
www.pragmasystems.com
877.838.PMAX
info@pragmasystems.com

GSA Schedule Contract No. GS-35F-0559S. processMax is a registered trademark of pragma SYSTEMS CORPORATION. Although processMax makes use of portions of "CMMI" for Development, Version 1.2, CMU/SEI-2006-TR-068, copyright 2006 by Carnegie Mellon University, neither the Software Engineering Institute nor Carnegie Mellon University have reviewed or endorsed this product.

Copyright © 2008 pragma SYSTEMS CORPORATION.

This is a paid advertisement.
Cyber security, with a concentration on defensive practices, processes, and policies, is the theme of this issue of the Software Tech News. Assuring a software system is at minimal risk from intrusions is not only about developing and maintaining software without weaknesses and vulnerabilities in a properly configured environment. Assurance also requires being able to demonstrate that desired properties of the system and its environment hold. Furthermore, a secure system should provide such Information Assurance functionality as confidentiality, integrity, availability, authentication, and non-repudiation.

Cyber security professionals have developed a variety of distinctions, understandings, practices, and policies to support their mission. This issue provides an overview of selected elements of cyber security, with a focus on software issues.

In “Today’s Cyber Environment: Where Does Software Fit?”, Terry Roberts, (Software Engineering Institute), argues for the need for cyber security concerns to be integrated through software and system engineering, not compartmentalized. She takes a comprehensive view of the cyber environment and calls for the development of a new discipline, cyber science. Cyber science would include parts of computer science, system and software engineering, electrical engineering, mathematics, and social sciences.

Steve Welke (Trusted Computer Solutions, Inc.) describes “Certification and Accreditation (C&A) Basics”. The C&A process examines demonstrations that an information system implements approved safeguards in its environment. The C&A process is described in terms of roles, activities, and documents. C&A regulations applicable to United States government platforms include the DoD Information Assurance Certification and Accreditation Process (DIACAP), Intelligence Community Directive 503 (ICD 503), the IA Risk Management Framework from the National Institute of Standards and Technology (NIST), and their predecessors, emerging successors, and adaptations to Cross Domain Solutions (CDS).

In “Information Security in Software and Technology Reliant Environments”, Salvadore Paladino (ITT) provides ten points to assist organizations in implementing cyber security programs. These points address practical concerns, such as the potential for the introduction of weaknesses and vulnerability through Commercial Off-The-Shelf (COTS) and other software developed by third parties.

Subair Hafez Amer (Southeast Missouri State University) and John A. Hamilton Jr. (Auburn University) provide an “Intrusion Detection Systems Taxonomy – A Short Review.” Network Operations Centers (NOCs), for example, operate Intrusion Detection Systems (IDSes) to identify vulnerabilities and weaknesses that attack might exploit, to identify intrusions as they occur, and to perform forensic analysis after an intrusion has occurred. The authors’ taxonomy builds on previous work and classifies IDSes among twelve dimensions. Taxonomy dimensions account for modern developments in the networks monitored by IDSes, such as the varieties of wireless networks, and the evolution and expansion of IDSes.

Ron Ritchey, Gene Tyler, and Karen Mercedes Goertzel (Booz Allen Hamilton), in “IATAC’s Critical Role in Cyber Security”, provide an overview of selected contributions from the Information Assurance Technology Analysis Center (IATAC). IATAC, like the DACS, is a Department of Defense (DoD) Information Analysis Center (IAC). IATAC helps spread Information Assurance (IA) and cyber security information, thereby providing access for government, industry, and academia to the knowledge and tools essential for effective computer network defense. The authors provide some examples where the community served by IATAC has found IATAC products and services particularly effective. The article concludes with some reflections on the future direction of the IA and cyber community.

About the Author

Robert L. Vienneau is a senior analyst at the DACS. He has published articles on formal methods, on financial analysis techniques in software cost modeling, and on a real-time Synthetic Aperture Radar (SAR) demonstration of High Performance Computing (HPC). He has participated in projects developing and demonstrating a controlled experiment for constructing a performance baseline for systems delivering Net-Centric Enterprise Services (NCES), an Identification and Authentication architecture, and an Automated Intrusion Detection Environment. Mr. Vienneau holds a BS in mathematics from Rensselaer Polytechnic Institute and a MS in Software Development and Management from the Rochester Institute of Technology.

Author Contact Information

Robert Vienneau: rob.vienneau@itt.com
Today’s Cyber Environment: Where Does Software Fit?

Cyber security concerns need to be integrated through software and system engineering, not compartmentalized. A comprehensive view of the cyber environment calls for the development of a new discipline, cyber science.

by Terry Roberts

Many of us have studied, worked, and made a profession in either software/system engineering or software architecture, or as program managers of software-reliant systems. Yet to many of us, the Cyber Environment seems disconnected from our daily work. We think of “that cyber stuff” as being limited to current Cyber Operations and Cyber Security, to vulnerabilities, hackers, and intrusions. That is a narrow and dated view of the Cyber Environment.

In the spring of 2009, I joined the Carnegie Mellon® Software Engineering Institute after more than 30 years of working within the government. In that time, I have been struck by the technical stovepipes that linger throughout our engineering and scientific communities. This working model was once appropriate during the days of primarily proprietary and hardware-centric capabilities, systems, and architectures. But in today’s netted world—in this Cyber Environment—we can’t afford to be compartmentalized. Those outdated models are limiting and prohibit us from leveraging our respective skills, technical backgrounds, and mission-centric insights.

In this article, I’ll propose an expansive view of the evolving Cyber Environment.

How Should We Define the Cyber Environment & Where Does Software Fit?

With input from the International Telecommunications Union1 and building upon the National Military Strategy for Cyberspace Operations, we define the term Cyber Environment as the conditions that are present when interacting with computing and networking resources. The Cyber Environment encompasses users, networks, devices, systems, software, hardware, data in storage or transit, applications, services, and processes. In summary, when you refer to the Cyber Environment, you refer to anything foundational to it, connected with it, that resides in it, and that is accomplished via this global netted arena.

The Cyber Environment is the entire connected framework and more; it is the people, work, missions, and functions that are performed within and rely upon the environment. Thinking in an all-encompassing manner like this can sometimes stretch the limits of our imagination and comprehension, but should that keep us from working to understand this new operational space and how our work fits within it and is impacted by it? If we don’t expand our thinking and understanding of how everything interrelates in cyberspace, we have to wonder what we will miss. Without that...

---

shift in focus, will we negate all that we are trying to achieve in our respective mission areas?

To many, it is fairly self-evident that software is foundational to the majority of systems, systems of systems, and ultra-large systems. Our architectures are run by software products and applications, truly performing our discrete missions and functions throughout Cyberspace. This has resulted in a dramatic growth of software lines of code within the majority of our systems today, mirroring the growth of system functionality and complexity. Now that systems are netted, these complexities are compounded. In fact, most netted architectures today increasingly rely on supply chain software from global developers and vendors. I like to say that software has truly become the heart and the mind of today’s systems; take software away or have it malfunction, and the system is no longer mission capable.

Where Do the Disciplines of Software and Cyber Engineering Fit?

I gave a presentation recently to an audience of roughly 400 system/software engineers and program managers. I asked how many of them would define their work as being part of the Cyber Arena—interestingly, only about a dozen people raised their hands. Perhaps the reason for this is the current state of our related sciences and fields of study. To exploit the interdisciplinary nature of the Cyber Environment, we must link key areas from the science and engineering disciplines to construct an integrated, higher level, and comprehensive Cyber Science. These disciplines should include key aspects of computer science, system engineering, software engineering, electrical engineering, mathematics, and the social sciences. We must undergo this foundational work collectively. We need to derive the competencies and establish the curriculum to develop Cyber Scientists and Engineers. In this emerging field, Cyber Scientists would ideally think and work seamlessly within these continuously evolving disciplines and within the global netted environment, while remaining fully aware of its inherent capabilities, limitations, and dynamics. Only in this way will we be able to take our body of work and knowledge to the next level—to one of game changing insight, high-end performance, and innovative solutions.

What Impact Does Software Have on the Cyber Environment?

Software is critical to the Cyber Environment; without it, there is no environment. Without assured software, the environment is unstable and at risk. The stakes are high since the vast majority of security issues and vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>PHYSICAL SCIENCE</th>
<th>BIOSCIENCE</th>
<th>COMPUTER/SOFTWARE/CYBER SCIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Origins/History</strong></td>
<td>Begun in antiquity</td>
<td>Begun in antiquity</td>
<td>Mid-20th Century</td>
</tr>
<tr>
<td><strong>Enduring Laws</strong></td>
<td>Laws are foundational to furthering exploration in the science</td>
<td>Laws are foundational to furthering exploration in the science</td>
<td>Only mathematical laws have proven foundational to computation</td>
</tr>
</tbody>
</table>
| **Framework of Scientific Study** | Four main areas: astronomy, physics, chemistry, and earth sciences | Science of dealing with health maintenance and disease prevention/treatment | • Several areas of study: computer science, software/systems engineering, IT, HCI, social dynamics, AI  
|                               |                  |            | • All nodes attached to/relying on netted system |
| **R&D and Launch Cycle**      | 10-20 years      | 10-20 years | Significantly compressed; solution time to market needs to happen very quickly |
result from the exploitation of software weaknesses. We face many challenges as our dependence on large-scale, highly distributed technologies such as SOA, cloud computing, and multi-core systems and architectures continues to increase with no end in sight. Because of these interdependencies—this interconnectedness of the Cyber Environment—the results of software failure are often catastrophic.

**How Should Software Architects and Engineers Think Differently About the Cyber Environment and Why Should They Care?**

To align ourselves effectively within the Cyber Environment, we need to shift not only our mindset but our methodologies. As we develop, evolve, and implement our software-centric approaches, models, technologies, and tools, we must take into account the added dynamics and complexities of the Cyber Environment. Which is not to say that we should abandon the foundational software practices and frameworks; adhering to software coding standards and software quality protocols is ever more important in this interconnected arena. In fact, assured software has a profound impact on the performance and security of the cyber environment—it remains a key secret ingredient to Cyber Assurance.

If we fail to acknowledge the interdisciplinary nature of the Cyber Environment, we risk it all—our financial institutions, our social networking, our critical infrastructure, and our national and global security. It is like driving a car in outer space and expecting it to perform as if it were on a traditional highway. Imagine how surprised you will be when your car begins to catapult to the ground instead of responding to your commands behind the wheel. Interestingly Cyberspace shares several qualities with outer space—the very environment and the operational dynamics are uniquely their own. Technology must be specifically designed for this arena, little responds as anticipated and to perform effectively - man must be one with the technology. With Cyberspace we are seeing an entirely new science and operational space. So in the Cyber Arena, expect the unexpected. Take nothing for granted. Explore, connect, collaborate, research, prototype, create, and fast track solutions. Operationalize and circle back once more. We are on a never-ending journey to establish and maintain an assured, high-performance Cyber Environment, upon which we can build and expand our future. Each of you and your work are foundational to the Cyber Environment.

**About the Author**

**Terry Roberts** is the Executive Director of Carnegie Mellon, Software Engineering Institute, leading all customer support for the U.S. Department of Defense, the U.S. Intelligence Community, and the rest of the US Interagency, with a special focus on network security and acquisition excellence in today’s cyber environment. Before coming to the SEI, Terry Roberts was the Deputy Director of Naval Intelligence (DDNI). Prior to being the Navy DDNI, Ms. Roberts served as the Director of Requirements and Resources for the Office of the Under Secretary of Defense for Intelligence (USDI).

An intelligence professional since 1979, Ms. Roberts has held many senior intelligence positions, including Director of Intelligence, Commander Naval Forces Europe and Commander-in-Chief NATO AFSOUTH; Director, Defense Intelligence Resource Management Office (manager of the General Defense Intelligence Program); Director, Naval Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Scientific and Technical Intelligence (S&TI) analysis at the Office of Naval Intelligence; special assistant to the Associate Director of Central Intelligence for Military Support and the Chief of Staff for the Director Military Intelligence Staff.

**Author Contact Information:**

twroberts@sei.cmu.edu
Satisfy Your Quality Obsession

Software quality and reliability are mission critical. The size, pervasiveness, and complexity of today’s software can push your delivery dates and budgets to the edge. Streamline communication, improve traceability, achieve compliance, and deliver quality products with Seapine Software’s scalable, feature-rich application lifecycle management solutions:

• **TestTrack Pro**—Development workflow and issue management
• **TestTrack TCM**—Test case planning and tracking
• **Surround SCM**—Software configuration management
• **QA Wizard Pro**—Automated functional and regression testing

Designed for the most demanding software development and quality assurance environments, Seapine’s flexible cross-platform solutions adapt to the way your team works, delivering maximum productivity and saving you significant time and money.

Visit [www.seapine.com/gsa](http://www.seapine.com/gsa)

© 2009 Seapine Software, Inc. All rights reserved.

This is a paid advertisement.
Certification and Accreditation (C&A) Basics

THE C&A PROCESS EXAMINES DEMONSTRATIONS THAT AN INFORMATION SYSTEM IMPLEMENTS APPROVED SAFEGUARDS IN ITS ENVIRONMENT. THE C&A PROCESS IS DESCRIBED IN TERMS OF ROLES, ACTIVITIES, AND DOCUMENTS.

by Steve Welke

The arena of certification and accreditation (C&A) is like alphabet soup. There are so many acronyms and so many entities, that it can be very difficult to understand. This paper sorts through the confusion to identify which terms, approaches, and processes apply in a given situation. It starts by describing the foundational C&A principles that apply to any C&A effort. It then provides an overview of C&A approaches being used by the Department of Defense (DoD), the Intelligence Community (IC), and Civilian government. Finally, it provides an overview of the cross domain solution (CDS) C&A processes being used by the DoD and the IC. It also provides insight to the following questions:

- What are the temporal relationships among C&A components?
- What is the scope of each C&A component?
- How do all of the C&A components fit together?
- What is required right now?
- What has replaced (or is replacing) what?
- What is the C&A flow from the perspective of a software development organization?

C&A Principles

Why Conduct C&A?

C&A is performed because threats to and vulnerabilities in information systems affect people’s lives and/or the ability to perform missions. Threats are active entities that attempt, maliciously or unintentionally, to do harm to a system and its users. Vulnerabilities are weaknesses in a system that can be exploited to potentially allow harm to the system and its users. The combination of threats and vulnerabilities creates risk. If there are no threats, there is no risk; if there are no vulnerabilities, there is no risk. The reality is that threats and vulnerabilities are always present. Any active entity poses a potential threat to a system, and a system that has no vulnerabilities is so limited that it cannot do useful work. It is prudent to cost-effectively mitigate risk to protect lives and missions. The risk that cannot be mitigated cost-effectively, called residual risk, must be assessed before approving a system for operation.

What is C&A?

C&A is the process of comprehensively evaluating technical and non-technical features of an information system [in its environment] so that a Designated Approving Authority (DAA) can determine whether or not the system is approved to operate at an acceptable level of [residual] risk based on the implementation of an approved set of technical, managerial, and procedural safeguards. Safeguards are implemented to mitigate risk in a cost-effective manner, and then the DAA has to decide whether to accept the residual risk.

It is useful to compare and contrast C&A with a related assessment process – evaluation. Evaluation is “an assessment of [a product’s claims] against defined [information assurance (IA)] criteria.” Evaluation is conducted on a product by a licensed laboratory against the Common Criteria (CC). The product is assessed independent of its environment. At the conclusion of a CC evaluation, a certificate is issued for the product.

C&A, on the other hand, is an assessment of one or more products, in a particular environment, associated with specific policies and procedures, designed to meet a specific mission. Evaluation of a product can feed into the “certification” portion of C&A for a solution at a particular site. C&A, however, takes more factors into account and ultimately requires the approval of a DAA. Thus, C&A is an approach to managing risk that enables a DAA to make an informed decision about using particular information systems with cost-effective safeguards to accomplish a mission in a specific environment.

---

1 See [CNS06] for the definition of C&A and other information assurance terms.
2 The official definition of evaluation is “an assessment of a Protection Profile (PP), a Security Target (ST) or a Target of Evaluation (TOE), against defined criteria.” [CC09] Explaining these CC terms is beyond the scope of this paper, so the terms have been replaced with their intent. For more information about CC terms as they relate to C&A, see [WEL05].
3 See [CC09] for the definition of evaluation and a description of the CC assessment process.
Components of C&A

All C&A efforts involve three basic components: roles, activities, and documents. This section introduces these foundational components. Later sections will elaborate on these fundamentals as they apply in different environments. The roles and activities are essentially the same in all environments. The content of the documents is essentially the same, but the names of the documents are different depending on the environment.

Roles

As we start to introduce the roles involved in a C&A effort, it will help to think of the participants in a courtroom as an analogy. In a courtroom, the Judge is the person who has the authority to make a decision based on weighing the balance of evidence presented by a Lawyer to a Jury on behalf of Interested Parties. Interested Parties include those who are responsible to Produce and Implement the best result for their constituents, and those constituents who are left to Manage and Use the result.

A C&A effort has similar participants. Every C&A effort consists of four key roles:

- The Designated Approving Authority (DAA) grants approval to use a system prior to its operation. The DAA is the official who has the authority to formally assume responsibility for operating a system at an acceptable level of residual risk. This is the person that everyone needs to convince (i.e., make “warm and fuzzy” in C&A terms) to achieve the appropriate result.

- The Certification Authority (CA) is the expert responsible to the DAA for ensuring that security is integrated into the system. The CA makes a judgment of the system’s compliance with IA requirements, identifies and assesses the risks associated with operating the system, participates in certification activities, reviews the C&A evidence, and provides a recommendation to the DAA.

- The Program Manager (PM) ensures that security measures are implemented to adequately satisfy the security specification and that any residual risks are identified. The PM is ultimately responsible for the overall production (i.e., procurement, development, integration, modification, operation, and maintenance) of the system.

- The User Representative (User Rep) provides the user voice in identifying the users’ roles, responsibilities, and capabilities. The User Rep represents the user or user community in the definition of system requirements.

To complete the set of C&A participants, TCS recommends that three additional roles also be included:

- The Information Assurance Officer (IAO) or the Information Assurance Manager (IAM) ensures site security policy compliance and manages the system on a day-to-day basis. The IAO/IAM reports security incidents, provides user training, and identifies changes that may require reaccreditation.

- The Developer or Integrator implements the system and assists with user training.

- The C&A Facilitator coordinates all of the C&A activities, oversees production of C&A evidence, and presents evidence to the CA on behalf of the PM, User Rep, and IAO/IAM.

As shown in Figure 1, the PM, IAO/IAM and User Rep work to satisfy the DAA that the residual risk is acceptable. They coordinate with the C&A Facilitator to identify the appropriate IA requirements, interact with the Developer/Integrator during the software development process to implement a system that satisfies those IA requirements, and coordinate with the C&A Facilitator to produce C&A evidence. The C&A Facilitator presents appropriate C&A evidence to the CA at the right time to demonstrate that the system safeguards satisfy the IA requirements while meeting the mission need. The CA interacts with the DAA as C&A evidence is provided to ensure that the IA requirements are sufficiently met to achieve an acceptable level of residual risk.

Figure 1. C&A Roles
Activities

As shown in Figure 2, C&A activities are grouped into four phases:

- **Phase 1 (Pre-Certification)** is the longest phase. The objective of this phase is to agree on the intended system mission, environment, architecture, IA requirements, certification schedule, level of effort, and resources required to achieve accreditation. It also includes preparation for testing by analyzing the software design and developing test plans. The first phase culminates with a documented agreement (i.e., the initial C&A documents) of the approach and the results of the above activities.

- **Phase 2 (Certification)** includes activities that verify compliance of the system with previously agreed upon IA requirements (i.e., execution of test plans). Lab-based testing, called Certification Test and Evaluation (CT&E), evaluates security properties of the software to be implemented. On-site testing, called Security Test and Evaluation (ST&E), evaluates specific software configurations and the environment (i.e., people, processes, facilities) where the software will be installed. The second phase culminates with a set of test results and proposed mitigations for identified risks.

- **Phase 3 (Accreditation)** includes activities that evaluate the fully-integrated system (i.e., analyzing test results and proposed mitigations) to validate software operation in a specified environment has an acceptable level of residual risk. The third phase culminates in an accreditation decision – an approval to operate (ATO).

- **Phase 4 (Post-Accreditation)** includes activities that continuously monitor software management and operation to ensure that an acceptable level of residual risk is preserved.

The first step in getting started with any C&A effort is to bring the stakeholders together to identify the DAA, identify the approach/process to be used, clarify what the DAA cares about most, set timelines, and set responsibilities. All of this information is documented in a C&A Plan. The timeframe for completing a C&A effort depends on the following factors:

- Whether the DAA is risk-tolerant or risk-averse
- The number of C&A efforts the DAA and CA are working
- The number of nodes in the system undergoing C&A
- Prior C&A efforts on the current system
- The criticality of the mission (e.g., nice-to-have future process support vs. analytical products supporting warfighters currently in-theatre)
- The criticality of the system in supporting the mission (e.g., back-end administrative support vs. front-line command and control)
- The quality of the system/software engineering process (e.g., is a sound software engineering process in place? was IA considered early or late in the software engineering process?)

With a sound software engineering process, a DAA who understands risk management, available C&A resources, and a reasonable number of nodes, an initial C&A effort can be completed within 1-2 months of the software development/integration being finalized. Once the initial C&A effort is completed, the system moves into a “continuous monitoring” mode.

Documents

C&A documentation should add value, not simply be thrown together to satisfy the C&A process and then become “shelfware” when the process is complete. To that end, TCS has streamlined the set of C&A documents and developed an approach to making each C&A document a value-added asset. In particular, TCS puts all of the required content into an appropriate C&A appendix and views the System Security Authorization Agreement (SSAA) or the System Security Plan (SSP) as an executive summary of the content in the
appendices. Table 1 summarizes the audience and purpose for each C&A document.

<table>
<thead>
<tr>
<th>Document</th>
<th>Audience</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSAA / SSP</td>
<td>DAA</td>
<td>Executive summary of key information in the appendices.</td>
</tr>
<tr>
<td>C&amp;A Plan</td>
<td>DAA, CA, PM, User Rep</td>
<td>Primarily boilerplate, but it identifies the key players (its audience), lays out the typical C&amp;A activities/deliverables/responsibilities, and contains the C&amp;A schedule.</td>
</tr>
<tr>
<td>Concept of Operations (CONOPS)</td>
<td>All</td>
<td>High-level document that identifies the mission need, describes the existing system, identifies its shortcomings, and presents the concept to overcome those shortcomings.</td>
</tr>
<tr>
<td>Security Policy</td>
<td>DAA, CA, PM</td>
<td>Based on the CONOPS, high-level IA properties (typically in government regulations) plus site-specific IA needs.</td>
</tr>
<tr>
<td>Security Requirements Traceability Matrix (SRTM)</td>
<td>CA, Testers, PM, Developers</td>
<td>Based on the Security Policy, specific &quot;what&quot; statements that drive the software design/system architecture. The matrix is a mapping between security requirements and test procedures that are filled in as tests are developed to ensure testing is necessary and complete.</td>
</tr>
<tr>
<td>Architecture</td>
<td>Developers, Testers</td>
<td>Based on the CONOPS and Security Requirements, detailed &quot;how&quot; design information that leads to system implementation.</td>
</tr>
<tr>
<td>Test Plans &amp; Procedures</td>
<td>CA, Testers</td>
<td>Based on the Security Requirements and the Architecture, the specific tests (e.g., CT&amp;E and ST&amp;E) that verify the system and its environment meet their security objectives.</td>
</tr>
<tr>
<td>Test Results and Plan of Action &amp; Milestones (POA&amp;M)</td>
<td>CA, PM, Developers</td>
<td>Based on implementation of the Test Procedures, these two documents capture the residual risk of operating the system in its particular environment and the plan for addressing those risks.</td>
</tr>
<tr>
<td>Site Security Management Plan</td>
<td>IAM</td>
<td>Based on the CONOPS, the Security Policy, and the Security Requirements, site-specific procedural information for implementing a secure environment.</td>
</tr>
<tr>
<td>Administrator's and User's Guides</td>
<td>IAO</td>
<td>Based on the Architecture, technology-specific information for installing, configuring, and maintaining the system.</td>
</tr>
<tr>
<td>Memorandums of Understanding (MOUs) / C&amp;A Letters</td>
<td>DAA, CA, PM</td>
<td>Official statements from the DAA(s) and CA.</td>
</tr>
</tbody>
</table>

Once the C&A Plan is developed as an agreement between the four key C&A roles, the CONOPS is written as a resource for everyone involved with the system. The CONOPS drives the Security Policy and security requirements (i.e., in the SRTM) that apply, and the Architecture must meet the applicable requirements. The SSMP and Administrator's/ User's Guides provide direction to the IAO/IAM on how to operate the environment and the resident software. The Test Plans are developed to demonstrate that the system, as architected and operated, meets the security requirements. The Test Results capture the results of testing, and the POA&M captures mitigations for failed test results. MOUs and C&A Letters are collected as the C&A effort progresses. The SSAA/SSP is an executive summary of all of this C&A evidence that is updated throughout the C&A process to focus the DAA on important information.

While C&A evidence is always required, it does not have to be newly created. In fact, most of the evidence that goes into a C&A effort should already exist if the site is following a sound software engineering process. If done correctly, the C&A process mirrors the software engineering process.

**C&A and the Engineering Process**

As shown in Figure 3, C&A roles, activities, and documents are natural parts of a sound software engineering process. Software engineering starts with the PM and User Rep identifying what is currently taking place, what is not sufficient/working, and how the obstacles are going to be overcome (i.e., in a CONOPS). The CONOPS drives the PM and IAO/IAM to develop requirements and site policies/procedures, which lead the Developer/Integrator to design and develop the actual system. During the software development process, the Developer/Integrator documents the architecture and develops administrator/user guides.
Developers/Integrators create test plans and testers (e.g., the CA) conduct test events to ensure that the software, as designed and operated, meets its intended requirements. Testers capture and analyze test results, which leads to identifying risks and how they will be addressed (i.e., in a POA&M). All of this evidence is summarized and presented to the person (e.g., DAA) with the authority to approve system operation.

If a sound software engineering process is not in place, C&A will be quite painful because it will highlight the missing pieces.

**Which C&A Approach and Which CDS C&A Process?**

Now that we have covered the fundamental principles of C&A, the foundation has been laid to present an overview of the three C&A approaches and the two CDS C&A processes. Figure 4 illustrates which C&A approach and which CDS C&A process applies depending on the site environment.

For a local area network (LAN) used by the IC (e.g., connected to a Top Secret/Sensitive Compartmented Information (SCI) network like JWICS), the Intelligence Community Directive (ICD) 503 approach applies. For a LAN used by the DoD (e.g., connected to a Secret network like SIPRNET or an Unclassified network like NIPRNET), the DoD Information Assurance Certification and Accreditation Process (DIACAP) approach applies. For a LAN used by a Civilian government organization, the C&A approach created by the National Institute of Standards and Technology (NIST) applies.

**Figure 3. C&A and the Engineering Process**

**Figure 4. Applicable C&A Approach and/or CDS C&A Process**
For a CDS, there is a separate CDS C&A process that builds on the applicable C&A approach. The CDS is always added to the “high side” LAN. A CDS connected to a Top Secret/SCI LAN on the high side follows the Top Secret/SCI and Below Interoperability (TSABI)/CDS C&A process building on the ICD 503 approach. A CDS connected to a Secret LAN on the high side follows the Secret and Below Interoperability (SABJ)/CDS C&A process building on the DIACAP approach.4

Overview of C&A Approaches

The DoD, IC, and Civilian government have each developed a C&A approach for their community. This section provides an overview of the C&A approaches used by each community, including some history and some information on how the C&A approaches relate to one another. It concludes with an overview of an effort led by the Committee on National Security Systems (CNSS) to bring these three C&A approaches together.

DoD – DITSCAP to DIACAP

In 1997, the DoD created the first C&A approach, called the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).5 DITSCAP established the concepts of four key roles, four phases of activities, and a set of C&A documents headed by an SSAA.6 DITSCAP formed the foundation for all future C&A approaches.

In 2007, the DoD created a new C&A approach to replace DITSCAP. This new approach, called the DoD Information Assurance Certification and Accreditation Process (DIACAP),7 clarifies the starting point for identifying IA controls8 and expands the awareness of what must be considered to make an accreditation decision in today’s net-centric world. DIACAP introduces a different set of C&A documents: the System Identification Profile (SIP), the DIACAP Implementation Plan (DIP), the DIACAP Scorecard and the Information Technology (IT) Security POA&M. DIACAP also provides two useful tools, the DIACAP Knowledge Service and the Enterprise Mission Assurance Support Service (eMASS).9

IC – DCID 6/3 to ICD 503

In 1999, the IC documented their original C&A approach in Director of Central Intelligence Directive (DCID) 6/3. DCID 6/3 introduces the concept of Protection Levels to describe different security environments (e.g., PL2 for single-level environments, PL4 for multi-level or cross domain environments). DCID 6/310 followed the DITSCAP foundation, but changed the set of documents to be headed by an SSP.

In 2008, the IC created a new C&A approach to replace DCID 6/3. This new approach, documented in Intelligence Community Directive (ICD) 503, points to guidance produced by the CNSS and NIST while minimizing the amount of IC-specific guidance. Although ICD 50311 is now official, it is not fully ready and most customers are still using DCID 6/3.

Civilian – NIST C&A

In 2004, NIST created a C&A approach for Civilian government organizations.12 As mandated by the Federal Information Security Management Act (FISMA) of 2002,13 NIST developed an IA risk management framework (RMF)14 that includes C&A as a component. NIST changed the name of the approval authority official from DAA to an Authorizing Official (AO). Although the NIST C&A approach was the last one to be developed, it is becoming the foundation for bringing the three communities together.

Bringing the Three C&A Approaches Together – CNSS

In 2006, a C&A Revitalization effort was initiated to bring the DoD, the IC, and NIST together to discuss harmonizing the three C&A approaches.15 One of the results of the C&A Revitalization effort is that the CNSS was tasked to create a

---

4 There is a fourth C&A approach and a third CDS C&A process. For a LAN used by the Special Access Program/Special Access Required (SAP/SAR) community, the Joint Air Force – Army – Navy (JAFAN) 6/3 [JAF94] approach applies – JAFAN 6/3 is essentially identical to the Director of Central Intelligence Directive (DCID) 6/3 approach (the precursor to ICD 503). A CDS connected to a SAP/SAR LAN on the high side follows the SAP/SAR CDS C&A process building on the JAFAN 6/3 approach – the SAP/SAR CDS C&A process is essentially identical to the TSABI process.
5 For official DITSCAP guidance, see DoDI 5200.40 [DoDD97] and DoD 8510.1-M [DoDD00]. For a brief history leading to the creation of DITSCAP, see Security C&A: DITSCAP vs. DCID 6/3 [WEL02].
6 For information on streamlining DITSCAP documentation, see Streamlining DITSCAP Documentation [WEL00].
7 For official DIACAP guidance, see DoDI 8510.01 [DoDD07].
8 See DoDD 8500.1 [DoDD02] and DoDD 8500.2 [DoDD03].
9 For more information on the transition from DITSCAP to DIACAP, see Moving from DITSCAP to DIACAP [WEL09].
10 For official DCID 6/3 guidance, see DCID 6/3 [DCI99] and DIMD DS-2610-142-01 [DIM01]. For a brief history leading to the creation of DCID 6/3, see Security C&A: DITSCAP vs. DCID 6/3 [WEL02].
11 For official ICD 503 guidance, see ICD 503 [ICD08].
12 For official NIST guidance, see NIST SP 800-37 [NIS04].
13 For official FISMA guidance, see Title III of PL 107-347 [PL02].
14 For more information on the NIST RMF, see NIST SP 800-39 [NIS08].
15 For more information on the status of the C&A Revitalization effort, see Certification and Accreditation Transformation [DNII88].
set of C&A guidelines for national security systems (NSS).16 The NIST C&A approach was the starting point for the CNSS C&A guidance. More recently, CNSS has been coordinating with the DoD, the IC, and NIST to incorporate feedback from all three communities. As a result, the current direction is that NIST guidance will be the foundation, CNSS guidance will be added to address any areas that are specific to NSS, and DoD- or IC-specific instructions will only be added to the NIST and CNSS guidance if necessary.

**Overview of CDS C&A Processes**

The DoD and IC have each developed a CDS C&A process for their community. This section provides an overview of the CDS C&A processes used by these two communities. It concludes with an overview of an effort led by the Unified Cross Domain Management Office (UCDMO) to bring synergy to these two CDS C&A processes.17

**DoD – SABI/CDS**

The Secret and Below Interoperability (SABI)/CDS process follows the basic principles in the DIACAP approach to C&A, but requires several extra activities shared between many additional organizations. These organizations then use a tailored documentation approach to gain approval for a CDS to be used at a particular site.

The SABI/CDS process involves three primary organizations: the National Security Agency (NSA), the Cross Domain Technical Advisory Board (CDTAB), and the Defense IA/Security Accreditation Working Group (DSAWG). NSA provides personnel to perform lab-based CT&E testing of CDS products – this is the group that is being referred to when customers ask, “Has NSA looked” at the CDS?” The CDTAB is a board that provides a recommendation to the DSAWG, and the DSAWG makes the ultimate decision to approve operation of a CDS at a site.

SABI/CDS testing is performed against a set of nine NSA guard Security Requirements (SR 1-9) and the NSA’s Risk Decision Authority Criteria (RDAC). SABI/CDS documentation involves creating a Cross Domain Appendix (CDA), which addresses the particulars of the CDS as implemented at the site and is added as another appendix to the existing high-side network’s SSAA/SSP.

**IC – TSABI**

The Top Secret/Sensitive Compartmented Information (SCI) and Below Interoperability (TSABI) process follows the basic principles in the DCID 6/3 approach to C&A, but requires a few extra activities shared between four additional organizations. These organizations then use a tailored documentation approach to gain approval for a CDS.

The TSABI process involves four primary organizations: the Defense Intelligence Agency (DIA), the Independent Test Authority (ITA), the Compliance Assessment Team (CAT), and the Principal Accrediting Authority (PAA). DIA provides certifiers to support overall assessment of a CDS at a particular site. The CAT provides personnel to perform lab-based CT&E testing of CDS products. The ITA maintains a repository of TSABI documentation and issues a Certificate to Field once a CDS has successfully completed TSABI CT&E testing. The PAA makes the ultimate decision to approve operation of a CDS at a site.

TSABI testing is performed against DCD 6/3 PL-4 requirements and additional requirements in the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSIISSS). TSABI documentation involves creating a Short Form SSAA/SSP, which addresses the particulars of the CDS as implemented at the site and is reviewed in conjunction with the “baseline” set of C&A documents for the CDS.

**Synergy Between the Two CDS C&A Processes – UCDMO**

As an outgrowth of the C&A Revitalization effort18 started in June 2006, the UCDMO was established in July 2006 “to address the needs of the DoD and the IC to share information and bridge disparate networks. The UCDMO was created to address the duplication, inefficiencies and resulting ineffectiveness resulting from years of uncoordinated activities in the CD arena.”19

The UCDMO has already achieved some significant success. For example, they have created a CD Baseline list20 that focuses resources on a set of mature CDSs. Also, they have worked with NIST to overcome the duplication of DoD and CDS processes.

---

16 As defined in FISMA [PL02], an NSS is “any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency; or other organization on behalf of an agency, the function, operation, or use of which: involves intelligence activities; involves cryptologic activities relating to national security; involves command and control of military forces; supports a weapon or weapons system; or is critical to the fulfillment of military or intelligence missions.”

17 For more information on SABI/CDS, TSABI, and the UCDMO’s efforts, see Working Toward Synergy Between the Two Cross Domain Solution (CDS) Certification and Accreditation (C&A) Processes [WFL10].

18 See [DNI06] for a description of the C&A Revitalization effort.

19 See [BAI08] for more details on the early activities of the UCDMO. See [UCD09b] for current information on the UCDMO.

20 See [UCD09a] for details on the CD Baseline list.
IC security controls by including CDS security controls in a single source that the entire federal government is moving to adopt – NIST Special Publication 800-53. Some difficult challenges still remain, however, as the UCDMO pursues its mission. Those challenges include:

- Bringing cohesion to the SABI/CDS and TSABI cultures,
- Fostering agreement on lab-based CT&E testing,
- Significantly reducing the time and cost to meet SABI/CDS mission needs,
- Clarifying reciprocity, and
- Educating customers on CDSs, SABI/CDS, and TSABI.

**Summary**

C&A is an informed approach to managing risk that results in an acceptable level of residual risk. All C&A efforts involve three basic components: roles, activities, and documents. C&A roles include a DAA, CA, PM, and User Rep – and should also include an IAO/IAM, Developer/Integrator, and C&A Facilitator. C&A activities are grouped into four phases. C&A evidence should be placed into an appropriate C&A appendix, with the SSAA/SSP serving as an executive summary of the content in the appendices.

The DoD, IC, and Civilian government have each developed a C&A approach for their community. CNSS is working to bring these three C&A approaches together. The NIST C&A approach is becoming the foundation for bringing the three communities together.

The DoD and IC have each developed a CDS C&A process for their community. Additional activities and organizations play a part, using a tailored documentation approach to gain approval for a CDS. The UCDMO is leading an effort to bring synergy to the two CDS C&A processes.

**References**


---

21 See [NIS09] for details on NIST SP 800-53.
About the Author

Steve Welke is a Principal Consultant with Trusted Computer Solutions, Inc (TCS). He has over 24 years of industry experience in the information assurance field, with a specific focus on trusted operating system (TOS) and cross domain solution (CDS) requirements, analysis and implementation. Mr. Welke provides thought leadership in assurance policy and standards. Among his other duties, he works closely with customers to help them achieve their risk management goals. Mr. Welke specializes in certification and accreditation (C&A) of computer systems, leading efforts for large systems, targeted applications, and cross domain products. In addition, he continuously works with the accreditation communities and authorities and has contributed to the Unified Cross Domain Management Office’s (UCDMO) efforts to bring key process assessments together including Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) / Cross Domain Solutions (CDS). Prior to TCS, Mr. Welke worked for the Institute for Defense Analyses (IDA) performing cutting-edge computer security research and supporting the National Security Agency (NSA) in defining and executing information assurance product evaluation methodologies.

Author Contact Information
Email: swelke@TrustedCS.com
Ft. Belvoir, VA (May 25, 2010) – On May 24, 2010, the Defense Technical Information Center (DTIC) awarded nine indefinite delivery, indefinite quantity (ID/IQ) contracts under a multiple award contract (MAC) covering Software, Networks, Information, Modeling and Simulation (SNIM). Awardees of Prime Contracts for SNIM are as follows:

- Alion Science and Technology Corporation (Alion)
- Battelle Memorial Institute (Battelle)
- Booz Allen Hamilton, Inc. (BAH)
- ITT Corporation, Inc. (ITT)
- L-3 Communications, Inc. (L3)
- MacAulay Brown, Inc. (MacB)
- Science Applications International Corporation (SAIC)
- Wyle Laboratories, Inc. (Wyle)

With a maximum value of $2 billion over the next 5 years, SNIM serves as an efficient contracting vehicle to quickly get information assurance, software data and analysis, modeling and simulation, knowledge management and information sharing services into the hands of DOD components, other Government agencies, industry and academia.

“The purpose of SNIM is to leverage the best and the brightest in order to solve the Government’s toughest problems and ultimately satisfy the needs of our nation’s Warfighter,” explained Terry Heston, Program Manager for the Information Analysis Centers (IACs).

SNIM provides a unique and symbiotic relationship for both customers and the science and technology community. Customers fund Technical Area Tasks (TATs), which yield new Scientific and Technical Information (STI). Under SNIM, all newly created STI will be added to one of the following IACs, thus becoming readily available to the entire scientific community: Modeling and Simulation Information Analysis Center (MSIAC), Information Assurance Technology Analysis Center (IATAC) or Data and Analysis Center for Software (DACS).

“Customers who use SNIM not only save federal resources by not duplicating work that’s already been performed, but also strengthen our scientific community by adding new pieces of STI for others to use,” Heston explained. “In a time of shrinking budgets and increasing responsibility, IACs are a valuable resource for accessing evaluated STI culled from efforts to solve new and historic challenges.”

For more information on SNIM, please visit the IAC Web site at, [http://iac.dtic.mil/snim.html](http://iac.dtic.mil/snim.html)
Information Security in Software and Technology Reliant Environments

FOR ANY ORGANIZATION THAT RELIES ON SOFTWARE, INFORMATION SECURITY MUST BE A CONCERN. THIS ARTICLE EXPLAINS TEN SECURITY ACTIVITIES AN ORGANIZATION SHOULD EMBRACE.

by Sal Paladino

A great deal of attention has been paid recently to security through better software, and rightfully so. As a result, organizations are becoming increasingly committed to security through sound software development practices. The shift in thinking that has turned software security into a priority rather than an afterthought has done much to limit the buffer overflows, string format problems, cross-site scripting bugs, and race conditions that have made SQL injections, data validation attacks, stack smashing, and countless other attacks possible for far too long. Those who develop software have adopted formal development models such as Capability Maturity Model Integration (CMMI) in order to refine processes and improve quality and the (ISC)², a respected authority in certification, even announced a certification program called the Certified Security Software Lifecycle Professional (CSSLP).

These changes all send a positive message; however, while a great deal of entities develop software, nearly all organizations acquire, implement, use, or otherwise rely on software in executing their critical operations. As a result, the secure design of software has to be viewed as just one of many steps on the ladder of information security.

This article presents a collection of ten important security points for organizations that rely on software in any form or fashion. It speaks to the fact that many must acquire their software from third parties and may have little control over its design. It acknowledges that the insecure implementation of an application, whether inherently secure or not, will ultimately lead to compromise. It concedes that people will make mistakes, and without proper training, will undoubtedly expose their employers to an array of security threats by using software in a manner for which it is not intended.

Establishe an Information Security Awareness Program

User error and abuse is still a major cause of adverse incidents, and organizations are doing very little to educate employees about security. According to the Computer Security Institute’s Computer Crime and Security Survey, 42% of respondent agencies reported that awareness and education comprise less than 1% of their security budget. Further, the percentage of agencies reporting significant losses from insider abuse has hovered around 50% since 2004, and is much higher when insider error or negligence is factored in.

To effectively respond, organizations need to educate all of their employees in the proper use of information systems, software, and networks. This program should not only raise awareness of contemporary threats, but identify the location of relevant policies, discourage high-risk behaviors, and clearly define the consequences for non-compliance. The best programs provide both general and role-based (software developers, system administrators, or anyone with elevated access rights) training and deliver mandatory refresher sessions at least once per year. Many organizations are even encouraging employees to pursue third party security certification and education programs. If anyone is not sure which certifications pass muster, he or she can review the Department of Defense Directive (DoDD) 8570, which includes a list of certifications deemed appropriate for enhancing information assurance aptitude among government employees and contractors.

Virtualization Software is Not a Total Security Solution

Many professionals have looked to virtualization software to boost their security posture, claiming that while virtual environments are capable of emulating an array of hardware and software technologies, they do not carry with them the same set of vulnerabilities. Others have even elected to use virtual machines as firewalls. While it is true that virtual machines can offer cost savings, flexibility, and an added layer of security, these systems have recently come under attack by several creative analysts. The primary focus of their testing is measuring detectability and escapability; that is, how easily attackers can determine which virtual technology is being used and whether or not they can effectively escape from it into another operating system. The results of some of these assessments are not overly...
positive⁴. Further, implementing virtual systems can inhibit redundancy and availability if multiple virtual machines are running on the same physical hardware. The bottom line is, while virtual machines can be secure, they should not be viewed as a security panacea or as a substitution for a layered security approach.

Beware of Transitive Trust Issues in Acquired Software

Regardless of whether you are developing software or purchasing it, proper steps must be taken to avoid transitive trust issues. Transitive trust is a trust relationship that develops beyond the two parties that are directly interacting with one another. It becomes problematic when one party obtains code from a second party, only to find out it was developed by a third party or perhaps multiple unknown parties⁵. Transitive trust first got the attention of the DoD in 2004 when the Government Accountability Office (GAO) published a report citing concerns that DoD was not doing enough to prevent the use of code acquired from unknown or foreign developers⁶. The primary audience was the software development community, but the lesson is relevant in the acquisition and use of all software applications. From payroll systems to office suites to Web 2.0 technologies, employees may

Control Downloads and Filter Web Traffic

Organizations have generally become better about blocking access to websites believed to be obscene, offensive, or otherwise inappropriate for their employees. The common belief is that sites containing such material are a source of malicious code. While these sites certainly pose a threat, the fact remains that malicious code is frequently downloaded from sites believed to be wholly legitimate. In fact, a 2009 Websense report indicated that 70% of the most popular websites hosted some form of malicious code or contained links to known malicious sites⁸. While commercial web filtering solutions offer the capability to block nearly all of these pages, blocking is typically scaled back to bare minimum levels.

The solution is for organizations to take a more aggressive approach, blocking any content deemed unrelated to normal business operations. Further, policies should prohibit the download and/or installation of content not explicitly approved by management. This can be enforced technically through desktop management systems, web proxies, and even anti-virus solutions. Management can then periodically formulate and distribute lists of acceptable applications based on sound risk analysis.

Test Early, Often, and Using Different Methods

Testing is a priority of software developers and engineers and has its rightful place in all phases of the development process, but what kind of testing are most organizations performing on third-party applications? Acquisition personnel can make the mistake of placing too much faith in the quality control efforts and security-mindedness of vendors or suppliers. The National Institute for Standards and Technology (NIST) tells us that third party applications must be tested just as rigorously (or more so) that those developed in-house. Applications should be tested for coding errors, malware insertion, and backdoors. If the source code is not made available, then static binary analysis tools should be utilized to test compiled code. (NOTE: You may have to add a provision to contracts with suppliers in order to avoid violating the Digital Millennium Copyright

---

⁴ Liston and Skoudis. Thwarting VM Detection. 2006.
Test web apps, and a thorough review of security capabilities should be executed against the original stated requirements. Integration testing must be done to determine how the software will work in your environment. Lasty, some form of acceptance testing should be done to determine how users will interact with the software. This can go a long way in predicting otherwise unexpected or unintended behaviors that can lead to various security vulnerabilities. Also, it can serve as food for thought in putting together application training programs for end-users.

Focus Patching on Applications as well as Operating Systems

The number of vulnerabilities associated with applications has grown substantially and now exceeds the number of network and operating system vulnerabilities. This is, in part, attributed to the fact that while organizations have automated the process of patching operating systems, applications are often patched manually and sometimes overlooked entirely. The result is that hackers are crafting more exploits designed to target applications. Specifically, those with malicious intent are targeting browsers and other client-side applications.

Organizations can minimize the risk of running applications by instituting a formal patch management policy by developing manual patching strategies. It is also prudent to install web application firewalls and other specialized application firewalls when possible. Further, all in-house or third party software should have filtering capability based on white-lists. White-lists offer greater security than black-lists because they define only the data and/or applications that are expressly permitted, rather than forcing the administrator to compile a list of everything that is not. This can go a long way considering the number of attacks attributed to the passing of malformed data. For an even higher level of assurance, the organization should employ (or contract with third party suppliers who do so) the services of penetration testers with specialized experience in testing web and other applications against the Common Weakness Enumeration’s (CWE) collection of vulnerabilities. Particular attention should be paid to “The 2010 CWE/SANS Top 25 Most Dangerous Programming Errors list”.

Use Security Templates to Configure the Environment

IT administrators struggle mightily with configuring the hundreds of settings that will ultimately have implications on their organization’s information security posture, and even more importantly, what employees can or cannot do on their systems. In dynamic environments, administrators may quickly lose control of computer and network settings and find it daunting to harden systems to an acceptable level.

One solution is the use of security templates. These templates allow administrators to configure settings such as password policies, event logging, user rights, file system and registry permissions, and services in a centralized manner. Moreover, they provide the opportunity for technical staff to streamline the process of getting baselines approved by upper management and referring back to those baselines when users seek out exceptions. Microsoft allows IT professionals to utilize Active Directory and Group Policy Objects (GPOs) to quickly and effectively deploy security templates. It even offers a default set of templates to find a logical starting point.

Enforce Least Privilege on the Desktop

IT security administrators will tell you that far too many users demand administrative privileges on their local machines, leaving those machines much more vulnerable to malware infection. Requests for these privileges may be particularly common among highly technical people as they may need to run certain programs or install applications in the course of their duties. Once given, it can be difficult to take these rights away, resulting in serious privilege creep. IT professionals may also have difficulty in deciding who legitimately needs elevated rights and who is abusing the system. An incorrect decision, they fear, could lead to a program not running properly or perhaps an angry call to the boss. The solution is twofold. First, a privilege audit should be conducted in order to ensure that only those who absolutely need administrative rights are granted them. Second, the IT staff should provide employees with user accounts that are utilized for ordinary operations and local administrator accounts that can be utilized when elevated rights are necessary. In Windows XP, this can be accomplished using the “Run as…” feature. Windows 7 makes things a bit easier with User Account Control, and in nearly every Unix implementation, the “sudo” command negates the need for a second account altogether.

Control the Use of Mobile/Portable Devices for Storage and Transfer

With storage capacities getting larger and form factors getting smaller, flash drives and other portable media are becoming a favorite of users looking to store or transfer a lot of data, or even run portable software. The problem lies in the fact that these devices are more susceptible to theft, easier to surreptitiously transport in and out of security zones, and can be used as an effective vehicle for propagating viruses and other forms of malware. Policy should dictate the types of devices that are authorized as well as mandate encryption for data classified at appropriate levels. Policies should cover issues such as portable software to ensure that users are not running unauthorized operating systems or applications from their mobile devices. Users should be made aware of the implications of using the same devices on their work and home systems, as well as basic physical safeguards such as not leaving items unattended in public places. Lastly, policy must instruct employees never to connect abandoned or lost devices in order to identify their contents. This could be an attack referred to by the hacker community as the “USB Switchblade,” whereby a storage device is intentionally left unattended with the hopes an employee will use it. This is fast becoming a common technique for reconnaissance and malware propagation14.

Look Before You Dive into Cloud Computing and Web 2.0 Technology

In the interest of cutting costs and reducing the need for hardware, many organizations are purchasing services such as cloud computing, thereby entrusting some of their critical operations to third parties. These decisions may be good for the immediate bottom line, but bring about some serious and potentially costly security vulnerabilities. For one, service providers may not guarantee customers an exact location where potentially sensitive data will be stored. This presents some jurisdictional issues in the event that a cybercrime is perpetrated against the service provider or the data owner. Second, as Cisco CEO John Chambers admitted in 2009, cloud computing entirely contradicts many proven security principles such as security perimeters, zones, and data compartmentalization. This requires those offering cloud computing services to rethink their security design—something that may take some time15.

There is also a push among managers of information-based organizations to move to Web 2.0 and social networking sites for knowledge management and even collaboration on projects. These technologies bring about an array of vulnerabilities to XML poisoning, cross-site request forgeries, and authentication attacks. Worst of all, they afford users the opportunity to post sensitive or inappropriate content without proper review, leading to a series of problems with data aggregation or disclosure. As such, a thorough review of Web 2.0 technologies should be executed prior to their implementation. Considerations of who will be using the system need to be made and appropriate user access levels need to be decided upon. Someone needs to be charged with managing the system and removing content that is not appropriate for consumption. Presenting the system to users as a mechanism for less formal communication and project planning, as opposed to a platform for exchanging technical information, can go a long way in avoiding data management issues.

About the Author

Salvatore C. Paladino is a Cyber Security Analyst with ITT Corporation’s Information Protection and Sharing Department in support of both the Department of Homeland Security’s Science & Technology Directorate and ITT’s IT Security Operations Center. His areas of expertise include technology evaluation, transition, and deployment, information security policy development, information assurance training and awareness, and the identification of emerging cyberthreats. He has authored numerous technical papers and has testified before the New York State Commission of Investigation as an expert witness specializing in cybercrime.

Mr. Paladino holds a BS with a concentration in Computer Security from Utica College of Syracuse University and an MBA in Technology Management from the State University of New York. In addition to being a Certified Information Systems Security Professional (CISSP), he is a Network+, Security+ and A+ Certified Professional. He is also an Adjunct Lecturer in the School of Business and Justice Studies at Utica College.

Author Contact Information

Email: Sal.Paladino@itt.com

14 Hak5.org. USB Switchblade. 2010.

rity_nightmare_says_cisco_ceo.html
The DACS Gold Practice Initiative:

• Promotes effective selection/use of software acquisition & development practices
• Defines essential activities/benefits of each practice
• Considers the environment in which each practice is used
• Addresses the timeliness of practice benefits
• Recognizes interrelationships between practices that influence success or failure
• Contains quantitative and qualitative information
• A continually evolving resource for the DoD, Government, Industry and Academia
• Free to use/free to join

Learn More About the DACS Gold Practice Initiative:
http://www.goldpractices.com

Current Gold Practices:

• Acquisition Process Improvement
• Architecture-First Approach
• Assess Reuse Risks and Costs
• Binary Quality Gates at the Inch-Pebble Level
• Capture Artifacts in Rigorous, Model-Based Notation
• Commercial Specifications and Standards/Open Systems
• Defect Tracking Against Quality Targets
• Develop and Maintain a Life Cycle Business Case
• Ensure Interoperability
• Formal Inspections
• Formal Risk Management
• Goal-Question-Metric Approach
• Integrated product and Process Development
• Metrics-Based Scheduling
• Model-Based Testing
• Plan for Technology Insertion
• Requirements Management
• Requirements Trade-Off/Negotiations
• Statistical Process Control
• Track Earned Value
Intrusion Detection Systems (IDS) Taxonomy - A Short Review

MOST EXISTING IDS TAXONOMIES ARE HIGHLY ABSTRACT, NOT COMPLETE, AND ARE MISSING SIGNIFICANT IMPORTANT CHARACTERISTICS (ITEMS). THE AUTHORS HAVE DEVELOPED A TAXONOMY FOR IDS THAT IS COMPREHENSIVE.

by Suhair Hafez Amer and John A. Hamilton Jr.

When network based technologies are being utilized by different parties, they become more vulnerable to security threats. With the increasing number of computer-related security incidents, more intrusion detection systems are being developed. Both host-based and network-based protection is becoming important. A single IDS is one important solution for protecting systems and networks; however, a single one may not be totally effective in protecting an organization. Traditionally IDSs are classified according to two characteristics: detection method and protected system type. The detection method can be anomaly or misuse. The protected system type can be host-based or network-based. Although such a distinction is essential when building an IDS, other characteristics, as explained in this paper, are as important. A complete secure solution cannot be achieved by considering one aspect of the IDS taxonomy. Both IDS developers and organizations employing IDSs need to understand and study IDS taxonomies in order to choose the best IDS characteristics. Such characteristics need not be limited to protected system type or detection method. When investigating the different aspects of the taxonomy and applying different options, better security can be achieved.

Table 1 below provides a brief history of IDS taxonomies.

<table>
<thead>
<tr>
<th>Taxonomy by Author(s) and Year of Publication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Debar, Dacier and Wespi 1999)</td>
<td>This taxonomy is considered one of the first attempts of classifying IDSs and the authors incorporate aspects of security monitoring such as vulnerability assessment. They classified IDSs according to five concepts: detection method, behavior on detection, audit source location, detection paradigm and usage frequency. The detection method partitions IDSs into behavior-based and knowledge-based systems. Behavior-based systems maintain a database of the behavior of the monitored system during normal operation rather than a database of attack signatures which needs to be kept up-to-date. Knowledge-based systems use a database to store the signatures of known attacks. An alarm is generated whenever an activity matches a signature in the database.</td>
</tr>
<tr>
<td>(Debar et al. 2000)</td>
<td>This revised IDS taxonomy takes into account the detection paradigm implemented by the IDS. In the state-based paradigm, the IDS attempts to recognize a given system state as either an error state or a failure state. A transition-based IDS monitors a system for any state transition that could represent an intrusion. The audit source location concept was also modified by adding the categories application log files and IDS sensor alerts, which take into account differences in the granularity of log data generated on a host.</td>
</tr>
<tr>
<td>(Axelsson 1999; Axelsson 2000)</td>
<td>This taxonomy provides intrusion detection features. Several IDSs were surveyed and classified according to this taxonomy. He used different terms to identify detection methods and regrouped and extended the remaining categories by providing “a taxonomy of system characteristics.”</td>
</tr>
<tr>
<td>(Cachin et al. 2001)</td>
<td>In this taxonomy, the capabilities of IDS were analyzed and tested with respect to the activities performed. They indicated that by only classifying IDSs into behavior-based or knowledge-based systems, the precise type of attacks and the amount of false positives generated cannot be drawn. They identified two main classes of information sources that are raw data sources and log data sources. Raw data sources are a non-transformed view of the data as it is sent by an activity; whereas, log data sources provide a view on the manner the received data was interpreted by the monitored system.</td>
</tr>
<tr>
<td>(Kazienko and Dorosz 2004)</td>
<td>This revised classification indicates that an IDS can operate as standalone centralized application or an integrated application that create a distributed system. Distributed systems employ autonomous agents that are able to take preemptive and reactive measures and move over the network.</td>
</tr>
</tbody>
</table>

Table 1. History of IDS Taxonomies
Revised IDS Taxonomy

The taxonomy provided in this paper (Figure 1 on next page) extends the previous attempts described in Table 1. This paper presents an up-to-date IDS taxonomy with a short explanation of each characteristic in the taxonomy. To achieve greater security, a combination of intrusion detection systems and tools should be incorporated in the overall solution. In the revised taxonomy, for example, the authors found it important to extend the detection technique to not only include anomaly and misuse – as historically distinguished – but also to include target monitoring, vulnerability scanners, integrity mentoring, log file monitors, honey pot, stealth probes and specification based IDS. The protected system should also include application based IDS and not only network, host or hybrid-based IDSs.

The authors expanded the taxonomy by indicating that layout technology is important when deciding on an IDS. The system layout can be either wired or wireless. Wireless communication can be further expanded to be fixed or mobile. This paper provides a more comprehensive list of the source of audit data, which is not limited to host log files or network packet processing. Also, we found it important to include intrusion prevention systems which are believed to be an extension to IDSs. Finally, to make the revised taxonomy comprehensive and complete, the following characteristics were included: response type, usage frequency, data collection, data processing, structure or arrangement, detection paradigm, and time of detection.

In this section, different elements appearing in the expanded IDS taxonomy (Figure 1) are briefly explained.

Source of audit data

Intrusion detection systems detect intrusions by analyzing
Intrusions can be detected in real-time or non-real-time. Real-time detection is achieved as the system is being monitored during execution (Axelsson 1999). Data Collection

Audit data can be collected in a distributed fashion from several different locations or sources, or they can be collected in a centralized approach from one single source (Axelsson 1999).

Table 2. IDS sources of audit data

<table>
<thead>
<tr>
<th>Source of Audit Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host log files</td>
<td>Host log files gather information about user activities on a given machine. In case of a successful attack, they are vulnerable to alterations which make it important to process such data before the attacker can alter the logs. The system of (Debar, Dacier and Wespi 2000) Syslogs is easy to use in audit trails. The processing engine receives a text string for an application, then prefixes it with a time stamp and system name, and archives it. Since security audits are used to record all security-significant events that occur on a system, their system records instructions executed by the processor in the user space and instructions executed in the trusted computing base space C.</td>
</tr>
<tr>
<td>Network packets</td>
<td>Network sniffers are popular for gathering information about the events that occur on the network architecture. Sniffers can be application level gateways or filtering routers. Analysis of packets can be performed quickly if it is carried out at a low level by performing, for example, pattern matching or signature analysis. A more thorough analysis can be performed by analyzing each packet with respect to the application or protocol being employed which is expensive (Debar, Dacier and Wespi 2000).</td>
</tr>
<tr>
<td>Application log files</td>
<td>Application log files are a good source for obtaining data since they are more accurate and more complete, as the file contains all relevant information and does not require re-assembling such as with network packets. When using application log files, the application has the choice of selecting what information to log according to what is relevant to its security purposes. However, some attacks go undetected because attackers are able to prevent writing their actions to the log file, and such incidents cannot be discovered when log files are checked. Furthermore, some attacks target the lower levels of the system software and therefore, they will go undetected (Debar, Dacier and Wespi 2000).</td>
</tr>
<tr>
<td>IDS sensor alerts</td>
<td>IDS sensor alerts are a new generation of IDSs that do not detect attacks directly, but will correlate the information gathered from several intrusion detection tools using correlation techniques and data-mining techniques. Such a technique retains the number of events that needs to be processed. It is also beneficial when the activity spans multiple users, machines or networks (Debar, Dacier and Wespi 2000).</td>
</tr>
<tr>
<td>System state analysis</td>
<td>An IDS utilizing system-state-analysis models attacks as a series of state changes starting from an initial state that is secured to a target state that is compromised. The diagrams are used to model the critical events that must occur to successfully penetrate the system. State transition analysis is based on the concept that all penetrations have two features: 1) penetrations require the attacker to possess access to the target system. 2) Penetrations lead to the acquisition of some ability or resource such as unauthorized access to data or other user’s privileges. The intermediate states that lead from the initial state to the comprised final state are actions that if omitted will prevent the attack from finishing (Ilgun and Kemmerer 1995).</td>
</tr>
</tbody>
</table>

Table 2. IDS sources of audit data

Data Processing

Audit data can be processed either in a central or in many distributed locations. Both types are not affected by the way data was collected, which could have been from one single site or from many different locations or sources (Axelsson 1999).

Structure of IDS

The arrangement of an IDS can be either centralized or distributed. A central arrangement of all IDSs is achieved by physically integrating it within a firewall. A distributed IDS consists of multiple IDSs over a large network, all communicating with each other. More sophisticated systems follow an agent structure principle, where small autonomous modules are organized on a per-host basis across the protected network (Kazienko and Dorosz 2003).

Layout technology

When deploying an IDS it is important to know what type of network layout technology is used. Wired networks, versus wireless networks, employ different and specific secure transmission techniques, such as encryption. Therefore, it is important to understand the characteristics of the layout technology of the network employed and to successfully use the correct measures to secure it. Table 3 on next page provides a brief description of network technology layouts for which IDS can be employed.
Intrusion Prevention System (IPS)

An IPS is any hardware or software device that has the ability to detect and prevent known attacks. Currently there are two types of IPSs: host-based and network-based. The IPS’s software for host-based systems will be installed directly on servers that host the monitored applications. All IPS for network-based systems is specifically targeted at detecting and then preventing publicly known application-specific attacks (IPS 2003).

### Detection Paradigm

The detection paradigm describes how the IDS evaluates intrusions and can be of two types. The first type evaluates states to know if they are secure or insecure. The second type evaluates transitions while moving from a secure state to an insecure state (Debar, Dacier and Wespi 1999). Both state and transition analysis can be carried out in two ways:

- **Non-perturbing observation performs a vulnerability assessment** by requesting application versions and banners and then comparing them with a table of known vulnerabilities. If found in the table, then the system is tagged as vulnerable, otherwise it will be tagged as secure.
- **Pro-active analysis triggers events** on the environment to determine states or create transitions. The vulnerabilities are actively exploited to determine the state of the system. These attempts are almost indistinguishable from actual intrusions (Debar, Dacier and Wespi 1999).

### Intrusion Prevention System (IPS)

An IPS is any hardware or software device that has the ability to detect and prevent known attacks. Currently there are two types of IPSs: host-based and network-based. The IPS’s software for host-based systems will be installed directly on servers that host the monitored applications. All IPS for network-based systems is specifically targeted at detecting and then preventing publicly known application-specific attacks (IPS 2003).

### Detection Method

The detection method is also referred to in other taxonomies as the detection technique, principle, or approach. IDSs are historically classified to basically anomaly-based or signature-based. In the revised taxonomy more methods or types have been included, such as anomaly, signature, hybrid, target monitoring, vulnerability scanners, integrity monitoring, log file monitors, honey pot, stealth probes and specification-based. Table 4 provides a brief description of IDS detection methods.

---

### Table 3: Network Layout Technology Employing IDS(s)

<table>
<thead>
<tr>
<th>Layout Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Network</td>
<td>Wired networks, once connected, are usually faster and less expensive than wireless networks. Some utilize the existing phone line wires in homes while others need special network cabling. Some of the network features, such as, traffic behavior and network topology, can be utilized to identify intrusions (Estevez-Tapiador et al. 2004).</td>
</tr>
<tr>
<td>Fixed Wireless Network</td>
<td>Fixed wireless networks refer to wireless devices or systems that are situated in fixed locations. Fixed wireless devices usually obtain electrical power from utility mains and their point-to-point signal transmissions occur through the air. One advantage of employing fixed wireless networks is the ability to connect with users in remote areas without the need for laying new cables (<a href="http://www.stratexnet.com/products/fixed_networks/">http://www.stratexnet.com/products/fixed_networks/</a>).</td>
</tr>
<tr>
<td>Mobile Wireless Network</td>
<td>A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes that automatically self-configure without the help of a fixed infrastructure or centralized management. A Mobile Agent has the ability to move through a large network, is assigned to perform only one specific task, and is distributed in the network. Different agents are assigned different functions which reduces consumption of power. If the network is partitioned or some agents are destroyed, the remaining agents are still able to work. Mobile Agents are also scalable and are independent of platform architectures (Anantvalee and Wu 2006).</td>
</tr>
</tbody>
</table>

Stand-alone IDSs run on each node independently to determine intrusions. They base their decision only on the information collected at their own nodes, and no cooperation exists among nodes in the network. Nodes do not exchange data, and they don’t know anything about the remaining nodes (Anantvalee and Wu 2006). Distributed and Cooperative IDSs have every node participate in intrusion detection and response by having an IDS agent running on them. An IDS agent detects and collects local events and data to identify possible intrusions (Anantvalee and Wu 2006). Hierarchical IDSs are for multi-layered network infrastructures where the network is divided into clusters. The cluster-head of each cluster usually have more functionality than other members. For example, they are responsible locally for their nodes, they route packets across clusters, they are globally responsible for their clusters, and they initiate a global response when a network intrusion is detected (Anantvalee and Wu 2006).
Anomaly detection

In anomaly-based detection, the normal behavior of user activities is kept in profiles. While in detection mode, the system compares the current monitored data with these profiles, and any deviation is reported to the administrator as being an attempted attack (Anantvalee and Wu 2006). In general, since anomaly-based systems are based on regular behavior, which is different for different networks because working conditions vary, the degree of freedom for the problem is large. This is why it is important to make the IDS adaptable by monitoring and recording network behavior after deployment (Kabiri and Ghorbani 2005). However, one dangerous characteristic of such technique is that the system may learn to accept dangerous behavior as normal (Axelsson 1999).

Signature detection

Signature detection systems update a database of known attack signatures each time a new attack is launched. The system keeps signatures of known attacks and uses them to compare with the current data, and any matched signature is considered an intrusion (Anantvalee and Wu 2006). Signature detection systems are very efficient with known attacks and produce a small number of false positives. However, they are unable to detect novel attacks, even if they are slightly altered from a known pattern (Kabiri and Ghorbani 2005).

Hybrid

A hybrid technique is a combination of anomaly and signature based detection systems. It requires two processing elements and two sets of configuration and data storages. Triggering an alarm is based on performing a simple decision by weighing several factors in an equation that identifies the relation between both systems (Axelsson 1999).

Target monitoring

Target monitoring systems look for modifications in specific files. It is designed to identify an unauthorized action after it occurs in order to reverse it. For example, cryptographic hash for files are kept on regular desired intervals. To check if a file has been edited or modified, the cryptographic hash for the file is re-calculated. If there is a difference between these two values then an intrusion is identified. Such systems are easy to implement because they do not require constant monitoring by the administrator (http://www.securityfocus.com/infocus/1520).

Vulnerability scanners

System vulnerability scanners run against a network, and scan it, and then report identified vulnerabilities. For example, Internet Security Systems' Internet Scanner (ISS) is a security product that assesses devices on a network for vulnerabilities. It performs many checks and tests, and gathers appropriate information, and then reports such vulnerabilities (Pfleeger and Pfleeger 2002).

Integrity monitoring

An integrity monitor watches key system structures for change, for example, using registry keys to track changes by an intruder. Although it has limited functionality, an integrity monitor can add an additional layer of protection to other forms of IDSs. Pfleeger and Pfleeger (2002) discuss the importance of this technique.

Logfile monitors

Logfile monitors are the simplest form of IDS, which attempt to detect intrusions by checking system event logs. This technology is limited because it detects only logged events which, sometimes, could have been altered by attackers. In addition, intrusions caused by low-level system events will be missed because event logging is a relatively high-level operation (http://www.samspublishing.com/articles/article.asp?p=29601&r=1).

Honeypot

A honeypot is an artificial environment intended to lure an attacker. It can be considered an IDS, in the sense that the honeypot may record an intruder's actions and sometimes trace the attacker's identity. It performs such tasks by recording actions, packet data, or connections (Pfleeger and Pfleeger 2002). A honeypot is usually used as a supplement to an IDS to detect an intrusion where IDS was unable to do so. In general, honeypot resources are supposed to be unused; therefore, any attempt to use those resources is expected to be malicious and should be monitored (Kabiri and Ghorbani 2005).

Stealth probes

This technique attempts to detect any attackers that choose to carry out their attack over prolonged periods of time. Stealth probes collect a wide-variety of data and perform a wide-range sampling to discover any correlating attacks over a long period of time. For example, an attacker may check for system vulnerabilities and open ports over a two-month period and then wait another two months to actually launch his attack (http://www.securityfocus.com/infocus/1520).

Specification-based detection

With specification-based detection, the system defines a set of constraints that describe the correct operation of a program or system. The detection system then monitors the execution of the program or the system against these constraints (Anantvalee and Wu 2006) and then flags any deviations.

### Table 4: IDS Detection Methods

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly detection</td>
<td>In anomaly-based detection, the normal behavior of user activities is kept in profiles. While in detection mode, the system compares the current monitored data with these profiles, and any deviation is reported to the administrator as being an attempted attack (Anantvalee and Wu 2006). In general, since anomaly-based systems are based on regular behavior, which is different for different networks because working conditions vary, the degree of freedom for the problem is large. This is why it is important to make the IDS adaptable by monitoring and recording network behavior after deployment (Kabiri and Ghorbani 2005). However, one dangerous characteristic of such technique is that the system may learn to accept dangerous behavior as normal (Axelsson 1999).</td>
</tr>
<tr>
<td>Signature detection</td>
<td>Signature detection systems update a database of known attack signatures each time a new attack is launched. The system keeps signatures of known attacks and uses them to compare with the current data, and any matched signature is considered an intrusion (Anantvalee and Wu 2006). Signature detection systems are very efficient with known attacks and produce a small number of false positives. However, they are unable to detect novel attacks, even if they are slightly altered from a known pattern (Kabiri and Ghorbani 2005).</td>
</tr>
<tr>
<td>Target monitoring</td>
<td>Signature detection systems update a database of known attack signatures each time a new attack is launched. The system keeps signatures of known attacks and uses them to compare with the current data, and any matched signature is considered an intrusion (Anantvalee and Wu 2006). Signature detection systems are very efficient with known attacks and produce a small number of false positives. However, they are unable to detect novel attacks, even if they are slightly altered from a known pattern (Kabiri and Ghorbani 2005).</td>
</tr>
<tr>
<td>Hybrid</td>
<td>A hybrid technique is a combination of anomaly and signature based detection systems. It requires two processing elements and two sets of configuration and data storages. Triggering an alarm is based on performing a simple decision by weighing several factors in an equation that identifies the relation between both systems (Axelsson 1999).</td>
</tr>
<tr>
<td>Target monitoring</td>
<td>Target monitoring systems look for modifications in specific files. It is designed to identify an unauthorized action after it occurs in order to reverse it. For example, cryptographic hash for files are kept on regular desired intervals. To check if a file has been edited or modified, the cryptographic hash for the file is re-calculated. If there is a difference between these two values then an intrusion is identified. Such systems are easy to implement because they do not require constant monitoring by the administrator (<a href="http://www.securityfocus.com/infocus/1520">http://www.securityfocus.com/infocus/1520</a>).</td>
</tr>
<tr>
<td>Vulnerability scanners</td>
<td>System vulnerability scanners run against a network, and scan it, and then report identified vulnerabilities. For example, Internet Security Systems’ Internet Scanner (ISS) is a security product that assesses devices on a network for vulnerabilities. It performs many checks and tests, and gathers appropriate information, and then reports such vulnerabilities (Pfleeger and Pfleeger 2002).</td>
</tr>
<tr>
<td>Integrity monitoring</td>
<td>An integrity monitor watches key system structures for change, for example, using registry keys to track changes by an intruder. Although it has limited functionality, an integrity monitor can add an additional layer of protection to other forms of IDSs. Pfleeger and Pfleeger (2002) discuss the importance of this technique.</td>
</tr>
<tr>
<td>Logfile monitors</td>
<td>Logfile monitors are the simplest form of IDS, which attempt to detect intrusions by checking system event logs. This technology is limited because it detects only logged events which, sometimes, could have been altered by attackers. In addition, intrusions caused by low-level system events will be missed because event logging is a relatively high-level operation (<a href="http://www.samspublishing.com/articles/article.asp?p=29601&amp;r=1">http://www.samspublishing.com/articles/article.asp?p=29601&amp;r=1</a>).</td>
</tr>
<tr>
<td>Honeypot</td>
<td>A honeypot is an artificial environment intended to lure an attacker. It can be considered an IDS, in the sense that the honeypot may record an intruder's actions and sometimes trace the attacker's identity. It performs such tasks by recording actions, packet data, or connections (Pfleeger and Pfleeger 2002). A honeypot is usually used as a supplement to an IDS to detect an intrusion where IDS was unable to do so. In general, honeypot resources are supposed to be unused; therefore, any attempt to use those resources is expected to be malicious and should be monitored (Kabiri and Ghorbani 2005).</td>
</tr>
<tr>
<td>Stealth probes</td>
<td>This technique attempts to detect any attackers that choose to carry out their attack over prolonged periods of time. Stealth probes collect a wide-variety of data and perform a wide-range sampling to discover any correlating attacks over a long period of time. For example, an attacker may check for system vulnerabilities and open ports over a two-month period and then wait another two months to actually launch his attack (<a href="http://www.securityfocus.com/infocus/1520">http://www.securityfocus.com/infocus/1520</a>).</td>
</tr>
<tr>
<td>Specification-based detection</td>
<td>With specification-based detection, the system defines a set of constraints that describe the correct operation of a program or system. The detection system then monitors the execution of the program or the system against these constraints (Anantvalee and Wu 2006) and then flags any deviations.</td>
</tr>
</tbody>
</table>

### IDS Placement

The protected system or the monitored environment and the placement of the IDS can be network-based, host-based or a hybrid of both network and host-based devices. Table 6 provides a brief description of IDS placements.

### Usage Frequency

Usage frequency of IDS corresponds to how often collected data is analyzed or processed. Table 7 provides a brief description of IDS usage frequency types.

### Conclusion

Most of the previous taxonomies were highly abstract, not complete, and missed significant important characteristics (items). The authors have developed a taxonomy for IDS that is comprehensive. The taxonomy enables organizations to draw precise conclusions on the type of IDS to be employed according to its security standards and type of systems currently employed. The comprehensive taxonomy included the following: detection method, response type, protected system, usage frequency, data collection, data processing, layout technology, structure, source of audit data, detection paradigm, intrusion detection system, and time of detection. Furthermore, the revised taxonomy in this paper would facilitate developing an intrusion detection system by highlighting the characteristics that are important for an organization. For example, an organization may choose to employ a hybrid detection method where anomaly and signature-based detection are used. It may
### Table 5: IDS Response Types

<table>
<thead>
<tr>
<th>Response Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>Passive systems do not mitigate the damage done by the intrusion or try to defend against the attacker, but notify the proper authority that will confirm the attack and then perform the required steps (Axelsson 2000).</td>
</tr>
<tr>
<td>Active Controlling attacked system</td>
<td>The system has control over the attacked system by modifying the state of the attacked system or by mitigating the effect of the attack. Such control can be performed by terminating network connections, or killing suspicious processes (Axelsson 2000).</td>
</tr>
<tr>
<td>Active Controlling attacking system</td>
<td>The system has control over the attacking system. This is achieved by attacking the attacker and removing his platform from operation. However, such a method may be difficult to defend in court and as a result is not recommended (Axelsson 2000).</td>
</tr>
</tbody>
</table>

### Table 6: IDS Placement

<table>
<thead>
<tr>
<th>IDS Placement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-Based</td>
<td>In the Monolithic Approach, the central intrusion detection server and any associated host audit programs run on several local hosts. Audit trails for the local hosts are collected and then sent to the intrusion detection server that analyzes the data. Such a technique has scalability, robustness and configurability problems (Kim and Bentley 1999).</td>
</tr>
<tr>
<td>Network-Based</td>
<td>The Hierarchical Approach is designed to monitor large-scale networks having more than several thousand hosts. This can be achieved by defining a number of hierarchical monitoring areas and having different IDSs monitoring different areas. Each single IDS performs local analysis and sends its local analysis results up to the IDS at the next level in the hierarchy to perform further analysis. However, one of the challenges is that when the topology changes, the network hierarchy must be changed. Also if a high level monitor is attacked, all lower level monitors escape detection (Kim and Bentley 1999).</td>
</tr>
<tr>
<td>Host-Based</td>
<td>In the Co-operative Approach, the responsibilities of a single central server are distributed to a number of cooperative host-based IDSs. Each IDS is responsible for monitoring only a small aspect of a local host. Then a global decision is made using a coherent inference engine (Kim and Bentley 1999).</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Host-based IDSs refers to systems that reside on and monitor a single host machine. They are beneficial because they discover, for example, changes related to file systems. They can also identify network related attacks. This is because the IDS can intercept all network communications after they have been processed by the network stack and before they are passed on to user-level processes in the same form seen by the process. Host based intrusion can also be performed by monitoring the system’s kernel where system calls indicate the behavior of the program (<a href="http://www.cs.ucsd.edu/classes/fa01/cse221/projects/group10.pdf">http://www.cs.ucsd.edu/classes/fa01/cse221/projects/group10.pdf</a>).</td>
</tr>
<tr>
<td>Hybrid</td>
<td>A hybrid system that incorporates both network-based and host-based IDSs will be advantageous if the network IDS filters alerts and notifications in an identical manner to the host-based portion of the system. In such hybrid systems the IDS mainly rely on the host-based components and uses the network-based IDS to complete the defense (<a href="http://www.securityfocus.com/infocus/1520">http://www.securityfocus.com/infocus/1520</a>).</td>
</tr>
<tr>
<td>Application based</td>
<td>An application-based IDS concentrates on events occurring within some specific application. It often detects many types of attacks by analyzing the application log files. It can by use application-based encryption/decryption services to monitor encrypted data. However, application-based IDSs are known to consume significant application (and host) resources (<a href="http://www.windowssecurity.com/articles/What_You_Need_to_Know_About_Intrusion_Detection_Systems.html">http://www.windowssecurity.com/articles/What_You_Need_to_Know_About_Intrusion_Detection_Systems.html</a>).</td>
</tr>
</tbody>
</table>
also choose to employ a honeypot as an extra precaution. The organization may choose to have a reactive type over its system (the attacked system). They may also choose to protect their systems on the network level and not on the host level by employing network-based IDS. In addition to processing the collected data in real time, the organization may choose to perform periodic processing to do an after-the-fact assessment of the situation. Depending on the organization layout, it can perform data collection and data processing either in a centralized or distributed fashion. Layout technology employed plays an important role when choosing the suitable IDS because wired and wireless technologies have different approaches that are better suited for them. A newly adapted approach is an intrusion prevention system which is assumed not only to detect intrusions but also to prevent them. In addition to being able to identify the different intrusion detection characteristics employed by an organization, the taxonomy can help new organizations in tailoring an IDS that fits their needs. For example, when the budget is limited, the taxonomy can aid in identifying different components that can, when grouped together, produce better security.

### Table 7: IDS Usage Frequency Types

<table>
<thead>
<tr>
<th>Usage Frequency Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real time Or Continuous</td>
<td>With real time processing, a stream of network packets is constantly monitored and compared against a database or the knowledge of current activities of the monitored network to identify attack attempts. The algorithms to be used should be quick, efficient, and algorithmically simple. It also requires a large amount of RAM and, therefore, reduce network throughput especially in the segment on which the IDS sits. They can detect inherent security holes and they consume less system resources than using audit trail processing (Kazienko and Dorosz 2004).</td>
</tr>
<tr>
<td>Periodic</td>
<td>Periodic non-real time assessment is desirable, especially after an attack has been completed. This is known as after the fact assessment, to better understand the attack (Axelsson 2000).</td>
</tr>
</tbody>
</table>

References


About the Authors

Suhair H. Amer, Ph.D. is an Assistant Professor in the Department of Computer Science at Southeast Missouri State University. She received her Ph.D. degree in Computer Science and Software Engineering from Auburn University in 2008, a Master of Science in Computer Science from The American University in Cairo in 2000, and Bachelor of Science in Computer Science from The American University in Cairo in 1998. Previously she served on the Computer Science Faculty of the Applied Science University and Ajman University of Science and Technology. She also served as an IT Technical/Training Specialist at the University Research Corporation.

John A. “Drew” Hamilton, Jr., Ph.D. is a professor of computer science and software engineering with a joint appointment as a professor of management at Auburn University and is director of Auburn’s Information Assurance Center. Dr. Hamilton was responsible for Auburn University being designated an Information Assurance Center of Academic Excellence in Research as well as Education by the National Security Agency. He is the Past President of the Society for Modeling & Simulation, International (SCS), Vice-chair of ACM’s Special Interest Group on Simulation (SIGSIM) and is on the Board of Directors of the Alabama Modeling & Simulation Council and Director of Auburn University’s branch of the McLeod Institute of Simulation Science (MISS). Previously he has served on the Electrical Engineering & Computer Science Faculty at the United States Military Academy and as Director of the Ada Joint Program Office.

Author Contact Information

E-mail: samer@semo.edu, hamilton@eng.auburn.edu
IATAC’s Critical Role in Cyber Security

MOVING FORWARD, IATAC WILL REMAIN FOCUSED ON COLLECTING, ANALYZING, AND DISTRIBUTING THE INFORMATION AND INSIGHTS NEEDED TO ENSURE A SECURE CYBER INFRASTRUCTURE FOR GOVERNMENT, DEFENSE, AND OUR NATION’S CRITICAL INFRASTRUCTURE.

by Dr. Ron Ritchey, Gene Tyler, and Karen Mercedes Goertzel

The security of our nation depends on the survivability, authenticity, and continuity of Department of Defense (DoD) information systems. These systems are vulnerable to external attacks, due in part to the necessary dependence on commercial systems and the increased use of the Internet. Security of DoD information systems is also of supreme importance to the warfighter in defending our national security. With the increasing amount of concern and Information Warfare (IW) activities requiring rapid responses, it is difficult to ensure that all appropriate agencies and organizations are given the knowledge and tools to protect from, react to, and defend against IW attacks. The Information Assurance Technology Analysis Center (IATAC) is DoD’s institution for facilitating the sharing of Information Assurance (IA) and cyber security1 information throughout government, industry, and academia so that individuals can gain access to knowledge and tools essential for effective computer network defense.

IATAC was formally created in 1998, and is one of ten Information Analysis Centers (IAC) administered by the Defense Technical Information Center (DTIC). As defined in the IATAC charter, its mission is to, “provide the DoD a central point of access for information on IA emerging technologies in system vulnerabilities, research and development, models, and analysis to support the development and implementation of effective defense against IW attacks.” Though IATAC’s mission focuses on DoD’s IA and cyber security needs, its scope extends across government, industry, and academia.

IATAC’s Products and Services Strengthen IA and Cyber Security2

DTIC recognizes the importance of sharing and reusing information specific to critical topics that improve our nation’s defense. Like all of DTIC’s IACs, IATAC provides several products and services that enable greater information sharing, including:

- **Information Resources:** The scientific and technical information (STI) IATAC collects is loaded into information databases that allow authorized DTIC customers3 access to IA and cyber security resources;
- **Training:** IATAC offers several IA training courses on topics such as Law in Cyberspace, Network Operations, and Certification and Accreditation;
- **State of the Art Reports (SOAR):** IATAC has published nine SOARs (and is currently developing its tenth), each of which provides in-depth research and analysis into a specific topic of interest within IA and cyber security;
- **Tools Reports:** Each Tools Report IATAC publishes provides a compendium of commercial solutions and their specifications so that IA practitioners can find the tools for their respective organization;
- **IA newsletter:** IATAC publishes this free quarterly magazine so that the IA community can learn about emerging trends and technologies in IA and cyber security;
- **Subject Matter Expert (SME) Program:** This program unites IA SMEs from government, industry, and academia so that they can continually share best practices with one another;
- **Technical Inquiry (TI) Service:** IATAC provides authorized DTIC customers4 with four hours of free research for any IA-related question they may have. Oftentimes, IATAC engages its SMEs so that customers receive information from the experts themselves.

---

1 For the purposes of this article, we use IA and cyber security interchangeably. However, there is an ongoing debate in DoD and other areas of the federal government about whether or not these terms are synonymous.

2 For more information about any of IATAC’s products and services, please visit: http://iac.dtic.mil/iatac/

3 Some of IATAC’s products and services are restricted to authorized customers who are registered with DTIC. To register with DTIC, please visit: http://www.dtic.mil/dtic/registration/

4 To become an authorized customer, by registering with DTIC, please visit: http://www.dtic.mil/dtic/registration/
Information Resources

In 2009, IATAC processed more than one million requests for information from DoD, non-DoD Government agencies, industry and universities. These requests were primarily for STI that IATAC collects and disseminates, and covered a wide range in IA and cyber security subjects, including policy and governance and mission assurance, to market intelligence, technology, and operations.

Training

In addition, IATAC trained over 7,000 people by conducting over 350 training activities in 2009. This training was comprised of Security Officer, Certification and Accreditation, Cyber Security, Hands-on Hacking, Encryption, Cyberlaw, and Network Operations courses. IATAC provides expert training that addresses organization-specific needs by conducting training for groups rather than for individuals; we send mobile training teams out to requesting organizations.

State of the Art Reports

Perhaps the most valuable resources IATAC develops are its SOARs. In 2009, IATAC produced the Measuring Cyber Security and Information Assurance SOAR, which provides a broad picture of the current state of cyber security and information assurance (CS/IA), as well as a comprehensive look at the progress made in the CS/IA measurement discipline. Currently, IATAC is finalizing its newest SOAR, Security in the Information Technology Supply Chain. The focus of this SOAR is security over the entire lifecycle and maintenance of the supply chain to address threats during development, delivery, and maintenance for DoD’s information technology (IT) hardware, firmware, software and commodity IT services. This SOAR will be published and available for distribution in August 2010.

Of all SOARs published to date, one in particular has had a significant impact on IA and cyber security. In summer 2006, IATAC’s government Steering Committee tasked IATAC with developing a SOAR on software assurance practices and technologies. IATAC engaged SMEs in software reliability from the Data and Analysis Center for Software (DACS) to contribute to the SOAR development effort. The resulting Software Security Assurance SOAR provides:

- An overview of the current environment in which defense and national security software must operate;
- Surveys of current and emerging activities and organizations involved in promoting various aspects of software assurance;
- Descriptions of the variety of techniques and technologies in use in government, industry, and academia for specifying, acquiring, producing, assessing, and deploying software that can (with a justifiable degree of confidence) be said to be secure.

Released in July 2007, this SOAR was the first publicly available SOAR in IATAC’s history. Since that time, over 625,000 copies have been distributed, making it the most widely read product ever produced by an Information Analysis Center. Additionally, this SOAR has been implemented into IA and cyber security curriculum at four universities and at the IA certifying organization, International Information Systems Certification Consortium [(ISC)2].

Tools Reports

IATAC compiles open source product information in its Tools Reports, which provide IA practitioners with a consolidated, vendor-neutral, objective list of various products critical for IA implementation along with their specifications. These reports allow IA practitioners to easily compare and contrast tools so that they can more easily decide upon which solutions to implement in their respective networks. IATAC recently updated three Tools Reports and produced one new report:

- Intrusion Detection Systems
- Firewalls
- Vulnerability Assessment
- Malware (new)

IANewsletter

In order to provide snapshots of emerging technologies and share information about relevant IA topics regularly, IATAC publishes a quarterly magazine, the IANewsletter.
This newsletter is a free publication that remains vendor-neutral and is distributed to over 8,000 subscribers. The spring 2010 edition, “Cloud Computing: Silver Lining or Storm Ahead?” featured arguments for and against the implementation of cloud computing resources. IATAC has been commended for publishing articles on cutting-edge topics like cloud computing, which is mainly due to the reputable authors featured to date. Authors have included SMEs from the National Security Agency (NSA), North Atlantic Treaty Organization, Department of Veterans Affairs, Air Force Institute of Technology, Naval Postgraduate School, MITRE, and the Institute for Applied Network Security as well as many others from government, academia and industry.

Subject Matter Expert Program

The IATAC SME Program unites over 400 volunteer IA SMEs from across government, industry, and academia. These SMEs have significant educational and practical experience in specific IA specialties, and they volunteer their expertise by contributing to the IAnewsletter, vetting the SOARS and collaborating to address questions IATAC receives through the Technical Inquiry Program. IATAC’s SMEs are instrumental in ensuring that IATAC’s products and services provide up-to-date and accurate IA and cyber security information.

Technical Inquiry Service

Through this program, IATAC provides four hours of free research for authorized users on any IA-related questions they may have. Instead of consuming critical resources—time, manpower, and funds—to find answers to questions that have most likely been answered previously, IATAC customers can simply submit an inquiry and gain quick access to the information they need most. In turn, these inquiries help IATAC gauge what the IA community is interested in, and can then tailor its products and services so that they meet its customers’ ever-changing needs.

IATAC Provides the Government Critical IA and Cyber Security Analysis

Of course, DoD and the federal government have far-reaching IA needs that cannot be met by the aforementioned IATAC products and services. To meet these needs, IATAC provides organization-specific IA research and analysis on a contractual basis. From embedding IA into Combatant Command (COCOM) exercises, to harmonizing network operations, the following examples provide snapshots of research and analysis IATAC provides the government at large.

Example 1: DoD Information Assurance (IA) Policy Chart

In June 2009, the Defense-wide Information Assurance Program (DIAP) was asked by the Deputy Assistant Secretary of Defense (DASD) for Cyber, Identity, and Information Assurance (CIIA) to create a chart that captured and organized all IA policy at the DoD level, along with related federal policies and authorities. A decision was made to organize the policy under the CIIA’s new IA Strategy goals. Approximately 200 policies were identified and aligned under the organizational structure. Each publicly available policy listed in the chart is hyperlinked to the actual policy, thus helping IA professionals get easy access to often hard-to-find policies. Drafts of the chart were vetted among IATAC SMEs, key IA personnel in DoD, and within other IATAC entities. IATAC continues to keep the chart updated with the latest policy changes and also continues to publicize it to the broader IA community.

Example 2: National Institute of Standards and Technology (NIST)

NIST conducts research and develops test methods and standards for emerging and rapidly-changing information technologies. NIST focuses on technologies that improve the usability, reliability and security of computers and computer networks for work and home. Customer organizations include federal, state, and local governments, the healthcare community, colleges and universities, small businesses, the private sector, and the international community. IATAC has provided significant research and analysis to NIST in several key work areas. These include:

1. The Security Content Automation Protocol (SCAP) and National Vulnerability Database (NVD), which is a repository of security checklists, security related software flaws, misconfigurations, product names, and impact...
2. Electronic voting system security, including the ability to secure these machines against tampering/corruption, and to provide an audit trail while maintaining voter anonymity;

3. Special Publications (SP) (800 series): To date, IATAC has provided analysis in the publication of 63 of the more than 120 SPs that NIST has developed. Specifically, IATAC’s analysis has focused on NIST’s 800 series SPs, which are developed for the computer security community. These topics include:

   • e-Authentication
   • Cryptography
   • Identity
   • Metrics
   • Automated Test Equipment
   • Security in the System Development Life Cycle (captured in NIST Special Publication 800-37 Revision 1)
   • Information Security with Privacy
   • Secure Cloud Computing
   • Security Awareness, Training, and Education
   • Mobile, MANET, and Sensor Network Security
   • Physical Access Controls (Biometrics and Smartcards).

**Example 3: IA Research and Analysis for Combatant Commands**

IATAC has been involved in providing IA-focused research and analysis to various Combatant Command (COCOM) missions. IATAC SMEs have been instrumental in ensuring that the COCOM IA initiatives further the Office of the Director of Defense Research and Engineering (DDR&E) Strategic Imperatives to: 1) accelerate delivery of technical capabilities to win the current fight; 2) prepare for an uncertain future; 3) reduce the cost, acquisition time, and risk of our major defense acquisition programs; and 4) develop world class science, technology, engineering, and mathematical capabilities for the DoD and the nation.

The following list illustrates a few areas of focus in which IATAC provides IA analysis critical for improved IA and cyber security across DoD:

   • IATAC provides U.S. Pacific Command’s (PACOM) Commander Operational Test and Evaluation Force with IA and Interoperability Assessments, which allow USPACOM to identify and correct its IA and cyber security deficiencies in simulated wartime scenarios;
   • IATAC assesses the impact and utility of emerging technologies for U.S. Joint Forces Command’s (USJFCOM) Joint Transformation Command for Intelligence (JTC-I). This effort provides the foundation for JTC-I’s robust secure and IA compliant network architecture;
   • Additionally, IATAC performs gap and conflict analysis to determine where significant joint IA, interoperability and information exchange capability issues exist within USJFCOM, which ultimately strengthens IA and cyber capabilities for joint warfare;
   • IATAC provides IA research and analysis essential to solving the most challenging problems for the institution of DoD-wide network operations policies and concepts for U.S. Strategic Command (USSTRATCOM). Essentially, this analysis helps eliminate IA and cyber “stovepiping” that prevents effective, seamless network operations from occurring across DoD;
   • IATAC also reviews current and developing IA and cyber tactics, techniques, and procedures for USSTRATCOM, ensuring that DoD evolves to meet current and future threats.

**Example 4: CND Net-Centric Data Standards and CND Proof-of-Concept Demonstration**

For the DoD Computer Network Defense (CND) Architect, IATAC SMEs and analysts helped define uniform criteria and processes for the secure, seamless, and accurate exchange of CND data and Web services for net-centric CND activities that enable DoD to defend against IA and cyber threats. The analysts also helped develop the proof-of-concept demonstration to validate and showcase functional implementations of the new standards. For the CND proof of concept demonstration, data on network vulnerabilities, physical components of the network, and occurrences of IA and cyber threats were input into the application from multiple sources. They were then correlated, and used to generate a common operational picture of the IA posture of the network. The success of the proof-of-concept led to IATAC developing a follow-on pilot to test the implemented standards in an operational environment.
Example 5: Joint Task Force Global Network Operations

IATAC provides analysis, research, and development, and deployment strategies for the Joint Task Force Global Network Operations (JTF-GNO), which is the USSTRATCOM component Command responsible for directing the operation and defense of the DoD’s Global Information Grid (GIG).

IATAC supports two key initiatives that are critical to the unit’s mission: the NetOps program and DoD’s top enterprise security initiative, Host Based Security System (HBSS):

• **NetOps:** NetOps is the framework used by USSTRATCOM to operate and defend the GIG. IATAC provided the JTF-GNO with critical NetOps technical analysis and training, enabling key personnel to develop usable skills and experiences necessary for facing the IA and cyber security environment. IATAC also provided the Combatant Commands with this essential NetOps analysis and training.

• **HBSS:** IATAC tested and developed deployment strategies for HBSS, effectively piloting the security tool within the operational environment supporting the JTF-GNO itself, assisted in identifying network and security policies that directly impact the deployment and ability of HBSS to access infrastructure systems, and assisted with implementing an HBSS pilot at the JTF-GNO. IATAC analysts helped deploy the system within the JTF-GNO and identified solutions to correct any technical challenges that occurred. IATAC continues to provide refinement in development of HBSS deployment and communications in support of the JTF-GNO to direct and defend the GIG.

Example 6: TEMS and DoDTechipedia

IATAC developed the Total Electronic Migration System (TEMS) for DTIC, which allows IACs the capability to store, search, retrieve, and reuse STI in the performance of their IAC missions. As of May 2010, the IACs had over 400,000 full documents and over 1.2 million document citations stored in TEMS.

Most importantly, TEMS provides DTIC users access to the newest, most current information regarding emerging technologies and research. The importance of immediate access to STI cannot be overstated, especially for IA and cyber security professionals. By making STI available, users benefit by reusing STI; they can immediately access reports relevant to their IA and cyber security challenges and can utilize the information right away.

Similarly, DoDTechipedia provides IA and cyber security experts a secure forum to share critical information with each other. It allows users to utilize social networking technologies in a manner that solves pressing cyber security problems.

DTIC funded IATAC to provide the required research and analysis for three of the initial fifteen technology areas of DoDTechipedia, which was brought on line in October 2008: Information Warfare, Information Assurance, and Networking Technology. IATAC provided the content management for DoDTechipedia’s IA/IW/Networks components’ first phase (internally facing) and promoted awareness of each of the three technology areas through adding content, informative blogs and current event postings.

Future Direction

Moving forward, IATAC will remain focused on collecting, analyzing, and distributing the information and insights needed to ensure a secure cyber infrastructure for government, defense, and our nation’s critical infrastructure. This is now more important than ever given the rapidly rising threats that we face combined with the continually evolving nature of cyber technologies.

From the threat viewpoint, our nation has many different types of adversaries who have discovered that cyber attacks are a powerful way of accomplishing their goals. Because of this, attacks are increasing in number, sophistication, and immediacy, and we can expect this to continue into the foreseeable future. Attack methods that were once the sole province of well-funded nation-states are now being used daily by cyber criminals. This has become big business for our adversaries who are reaping huge benefits by taking advantage of the U.S.’s strong reliance on information technology. This has created a large asymmetric advantage for them.

The IT community’s insight into the vulnerability of our cyber infrastructure is also increasing. Since the creation of IATAC, vulnerabilities reported per year in the NIST National Vulnerability Database have increased 500%. The good news, though, is the rate of increase has flattened significantly with virtually no change in vulnerability discovery rates over the past three years. This is the result of a lot of hard work by...

---

7 Readers may access TEMS at: https://tems-iac.dtic.mil/. Readers may learn more about DoDTechipedia at: http://www.dtic.mil/dtic/announcements/DoDTechipedia.html. Both resources require DTIC registration. To register with DTIC, please visit: http://www.dtic.mil/dtic/registration/

8 Immediacy results from zero-day attacks. Zero-day attacks exploit vulnerabilities that remain unknown or undiscovered by software developers and/or IA and cyber security practitioners.
the infrastructure software providers such as Microsoft to improve the quality of their software development processes. IATAC’s 2007 SOAR on Software Security Assurance documented work that is still ongoing in this area. The efforts that are described in that report now need to make their way further into the development approaches of individual organizations because the attackers have now moved away from compromising infrastructure software and instead are targeting the applications that organizations are building for themselves. This is a difficult challenge and will remain a focus for IATAC moving forward.

The evolution of cyber technologies will also drive future security challenges. Innovation within the IT world has always occurred at a breakneck speed. This will not change and is a key strength of our country. Our willingness to embrace technology-driven change is a double-edged sword, though. Efforts to secure new technologies and even to understand what the security challenges are with new technologies can lag behind their implementations by years. IATAC is working hard to get ahead of this problem.

Some of the key IT movements that IATAC is currently tracking are cloud computing, social networking, and mobile computing. Each of these offers the potential for large benefits to our government and our nation while each also offers unique challenges. These challenges could easily undermine the benefits if left unaddressed due to the fact that our adversaries have become so sophisticated at leveraging new technologies against us.

Social engineering provides a good example of this. Web-based communities such as Twitter, Linked-in and Facebook, and even Intellipedia9 and DoD Techipedia, have enabled new ways for people to connect both personally and professionally. These systems allow their users to rapidly create communities of shared interest, which can facilitate anything from discovering long lost friends to the rapid creation of ad-hoc project teams to solve difficult challenges. The Defense Advanced Research Project Agency just ran an interesting experiment in this area where they hid ten tethered balloons in parks spread across the U.S. and then challenged individuals to use a social networking approach to locate them. This type of geo-location tracking is cloud computing, social networking, and mobile computing. Each of these offers the potential for large benefits to our government and our nation while each also offers unique challenges. These challenges could easily undermine the benefits if left unaddressed due to the fact that our adversaries have become so sophisticated at leveraging new technologies against us.

Social engineering provides a good example of this. Web-based communities such as Twitter, Linked-in and Facebook, and even Intellipedia9 and DoD Techipedia, have enabled new ways for people to connect both personally and professionally. These systems allow their users to rapidly create communities of shared interest, which can facilitate anything from discovering long lost friends to the rapid creation of ad-hoc project teams to solve difficult challenges. The Defense Advanced Research Project Agency just ran an interesting experiment in this area where they hid ten tethered balloons in parks spread across the U.S. and then challenged individuals to use a social networking approach to locate them. This type of geo-location tracking is cloud computing, social networking, and mobile computing. Each of these offers the potential for large benefits to our government and our nation while each also offers unique challenges. These challenges could easily undermine the benefits if left unaddressed due to the fact that our adversaries have become so sophisticated at leveraging new technologies against us.

Social engineering provides a good example of this. Web-based communities such as Twitter, Linked-in and Facebook, and even Intellipedia9 and DoD Techipedia, have enabled new ways for people to connect both personally and professionally. These systems allow their users to rapidly create communities of shared interest, which can facilitate anything from discovering long lost friends to the rapid creation of ad-hoc project teams to solve difficult challenges. The Defense Advanced Research Project Agency just ran an interesting experiment in this area where they hid ten tethered balloons in parks spread across the U.S. and then challenged individuals to use a social networking approach to locate them. This type of geo-location tracking is cloud computing, social networking, and mobile computing. Each of these offers the potential for large benefits to our government and our nation while each also offers unique challenges. These challenges could easily undermine the benefits if left unaddressed due to the fact that our adversaries have become so sophisticated at leveraging new technologies against us.

However, these networks also provide a detailed window into the lives and relationships of their participants, which our adversaries are actively targeting. If you participate in a site like Facebook, it is often easy for anyone to discover who you are, where you are, your political and religious beliefs, and who your friends and colleagues are. This is an intelligence gold mine. More insidious is that, even if you do not participate, you can still be exposed. For example, last year substantial amounts of personal details concerning John Sawyers, the new head of the British MI6 intelligence service, were discovered on Facebook. This information came from his wife’s account, since she had posted details about their family vacations and residence. While innocently posted, the information could potentially compromise their personal security. The main concerns surrounding social media usage have to do with users’ own awareness, judgments about how and why they use social media, skepticism about what they consume, and the ability to protect privacy and national security information in the face of the temptations presented by this easy disclosure environment. More than ever, information assurance needs to expand its vision to include elements of privacy, information quality, operational security, and user psychology. IATAC is tracking these challenges, and the trends and solutions that emerge to address those challenges, to help IA practitioners understand and develop strategies for using social media effectively, yet safely and securely.

This duality of information technology, both as beneficial and potentially threatening, is what makes the IATAC mission so important. As a nation, we will continue to embrace change, and we will continue to innovate. But we must also respond to the threat that has emerged to subvert these endeavors. To that end, IATAC will continue to be a preeminent provider of information, guidance and services that enable the safe use of both existing and emerging information technology.

---

About the Authors

Gene Tyler is a Booz Allen Hamilton employee and is the IATAC Director. He is a retired U.S. Army combat veteran having served over 35 years. He has extensive combat and operational deployment experience with two tours of duty supporting U.S. initiatives in the Republic of Vietnam and the Bosnian peace efforts, and an operational and command deployment as a Combined Joint Task Force commander in the Middle East. Gene has extensive staff and command experience both overseas and on the Office of Secretary of Defense (OSD) staff. In his last military assignment, Gene served on the OSD staff as the Director of the Defense-wide...
Information Assurance Program (DIAP) office. He holds multiple graduate degrees and is a distinguished graduate of the national level Senior Service College – the Industrial College of the Armed Forces.

Dr. Ron Ritchey is a Booz Allen Hamilton employee and is a leading technologist specializing in information assurance (IA) with over 20 years experience working within the IT industry. He is an active researcher in the IA field and is widely published on network security topics including co-authoring recent books on Software Assurance and Insider Threat. He has authored courses on computer security that have been taught across the country and is a faculty member of the SANS Institute, the Institute for Applied Network Security, and George Mason University (GMU). Dr. Ritchey holds masters and bachelors degrees in computer science from GMU and a Ph.D. in Information Technology from their School of Information Technology and Engineering. At Booz Allen, he leads a team dedicated to the development and maintenance of state-of-the-art information assurance capabilities. His focus is on the identification and elimination of the root causes of information assurance weaknesses.

Karen Mercedes Goertzel leads Booz Allen Hamilton’s Security Research Service. She is a SME in software assurance, cyber security, IA, and supply chain assurance, providing support to U.S. government, including Naval Sea Systems Command, the Department of Homeland Security Software Assurance Program, IATAC, the Office of the Director of Defense Research and Engineering, the NSA Center for Assured Software, the NIST Computer Security Resource Center, and the Defense Information Systems Agency IA Executive, Global Information Grid Enterprise Services Engineering Directorate, and Application Security Program. Ms. Goertzel has been widely published on software safety and security, the insider threat to information systems, malicious code, Web services and Cloud computing security, cross-domain information sharing, autonomic computing, and computer immunology. She was a lead author of the past five IATAC SOARs, and a contributing author to several NIST special publications. Her articles have appeared in CrossTalk: The Journal of Defense Software Engineering, The Journal of System Safety, the International Council on Systems Engineering’s Insight, the Anewsletter, and other publications; she is also a frequent conference and workshop presenter and panelist. Before joining Booz Allen, Ms. Goertzel was a requirements analyst and architect of high-assurance software and cross-domain solutions for defense and civilian government organizations in the U.S., NATO, Canada, and Australia.

Readers may contact all IATAC authors at iatac@dtic.mil.

The DACS website has been updated with new research information.

The DACS is a central distribution hub for software technology information sources. The DACS offers a wide-variety of Technical Services designed to support the development, testing, validation, and transitioning of Software Engineering technology.

Visit us at https://www.thedacs.com/
**An assurance case** is “A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system’s properties are adequately justified for a given application in a given environment.” (Ankrum and Howell 2006, as quoted in Goertzel et al. 2007)

**An attack** is “An attempt to gain unauthorized access to a system’s services or to compromise the system’s required properties (integrity, availability, correctness, predictability, reliability, etc.). When a software-intensive system or component is the target, the attack will most likely manifest as an intentional error or fault that exploits a vulnerability or weakness in the targeted software.” (Goertzel et al. 2007)

**Authentication** is “The process of determining whether someone or something (such as a computer or software process) is, in fact, who or what it is declared to be. Methods for human authentication typically include something you know (a password), something you have (a token), or something you are (fingerprint).” (Allen et al. 2008)

**Availability** is “The degree to which the services of a system or component are operational and accessible when needed by their intended users. When availability is considered as a security property, the intended users must be authorized to access the specific services they attempt to access, and to perform the specific actions they attempt to perform. The need for availability generates the requirements that the system or component be able to resist or withstand attempts to delete, disconnect, or otherwise render the system or component inoperable or inaccessible regardless of whether those attempts are intentional or accidental. The violation of availability is referred to as Denial of Service or sabotage.” (Goertzel et al. 2007)

**Confidentiality** is “The extent to which the characteristics of a software component, product, or system – including its relationships with its execution environment and its users, its managed assets, and its content – are obscured or hidden from unauthorized entities.” (Allen et al. 2008)

**Integrity** is “The property of a system or component that reflects its logical correctness and reliability, completeness, and consistency. Integrity as a security property generates the requirement for the system or component to be protected against intentional attempts to do one of the following:

- Alter or modify the software in an improper or unauthorized manner. (Note that attempts to destroy the software in an improper or unauthorized manner are considered attacks on the system’s availability, i.e., Denial of Service attacks)
- Through improper or unauthorized manipulation to cause the software to either perform its intended function(s) in a manner inconsistent with the system’s specifications and the intended user’s expectations, or to perform undocumented or unexpected functions.” (Goertzel et al. 2007)

**Non-repudiation** is, “For software entities that act as users (e.g., proxy agents, Web services, peer processes), the ability to prevent the software-as-user from disproving or denying responsibility for actions it has performed.” (Allen et al. 2008)

**Software security assurance** is “The basis for gaining justifiable confidence that software will consistently exhibit all properties required to ensure that the software, in operation, will continue to operate dependably despite the presence of sponsored (intentional) faults. In practical terms, such software must be able to resist most attacks, tolerate as many as possible of those attacks it cannot resist, and contain the damage and recover to a normal level of operation as soon as possible after any attacks it is unable to resist or tolerate.” (Goertzel et al. 2007)
A threat is “Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service.” (Goertzel et al. 2007)

A vulnerability is “A development fault or weakness in deployed software that can be exploited with malicious intent by a threat with the objective of subverting (violation of integrity) or sabotaging information handled by that software. Vulnerabilities can originate from weaknesses in the software’s design, faults in its implementation, or problems in its operations.” (Goertzel et al. 2007)

A weakness is “A flaw, defect, or anomaly in software that has the potential of being exploited as a vulnerability when the software is operational. A weakness may originate from a flaw in the software’s security requirements or design, a defect in its implementation, or an inadequacy in its operational and security procedures and controls. The distinction between ‘weakness’ and ‘vulnerability’ originated with the MITRE Corporate Common Weaknesses and Exposures (CWE) project.” (Goertzel et al. 2007) See http://measurablesecurity.mitre.org/ for the CWE and related MITRE projects.

References


The STN is a theme-based quarterly journal. In the past DACS has typically solicited specific authors to participate in developing each theme, but we recognize that it is not possible for us to know about all the experts, programs, and work being done and we may be missing some important contributions. In 2009 DACS adopted a policy of accepting articles submitted by the software professional community for consideration.

DACS will review articles and assist candidate authors in creating the final draft if the article is selected for publication. Note that DACS does not pay for articles published. Note also that submittal of an article constitutes a transfer of ownership from the author to DACS with DACS holding the copyright.

Although the STN is theme-based, we do not limit the content of the issue strictly to that theme. If you submit an article that DACS deems to be worthy of sharing with the community, DACS will find a way to get it published. However, we cannot guarantee publication within a fixed time frame in that situation. Consult the theme selection page and the Author Guidelines located on the STN web site (see https://www.softwaretechnews.com/) for further details.

To submit material (or ask questions) contact news-editor@thedacs.com

Recent themes include:
• Earned Value
• Software Testing
• Project Management
• Model Driven Development
• Software Quality and Reliability
• Cyber Security
The first 50 people to send in a completed survey will receive a FREE DoD/IT Acronym CD from the DACS.

This valuable CD-ROM contains over 28,700 Department of Defense and Information Technology acronyms. There are hundreds of acronym lists available but none are as well done as this CD AND specifically targeted towards DoD and Information Technology. This unique-shaped CD-ROM plays in your computer’s regular, hub-mounted, CD drive. You’ll use this great resource over and over again. It’s FREE, just for filling out our brief survey on the next page!

Data & Analysis Center for Software (DACS)

http://thedacs.com
1. Which volume of the Software Tech News did you receive?  STN Vol 13, No. 2

2. When did you receive the newsletter? (month/year)

3. How satisfied were you with the CONTENT of the newsletter? (Article Quality)
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

4. How satisfied were you with the APPEARANCE of the newsletter?
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

5. How satisfied were you with the OVERALL QUALITY of the newsletter?
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

6. How satisfied were you with the ACCURACY of the address on the newsletter?
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

7. Approximately how much of the newsletter do you read?
   - The entire issue
   - Most of the content
   - About half the content
   - Briefly Skimmed
   - Didn’t Read

8. Would you read this newsletter in an E-mail newsletter format?
   - Definitely
   - Probably
   - Not Sure
   - Probably Not
   - Definitely Not

9. How did you request the product or service?
   - Phone Call
   - E-mail
   - DACS Website
   - Subscription Form
   - Other

10. Would you recommend the Software Tech News to a colleague?
    - Definitely
    - Probably
    - Not Sure
    - Probably Not
    - Definitely Not

11. What topics would you like to see this newsletter devoted to?
    -
    -
    -
    -
    -

Comments (optional)

REGISTER FOR THE FIRST TIME | UPDATE CURRENT SUBSCRIPTION

Name: _________________________________  Position/Title: _________________________________

Organization: _______________________________  Office Symbol: _______________________________

Address: ___________________________________  City: _________________________________

State: ___________________  Zip: _______________  Country: ________________________________

Telephone: ______ - ______ - ______  Fax: ______ - ______ - ______  Email: _______________________

Functional Role: _________________________________

Organization Type:
   - Air Force
   - Army
   - Navy
   - Other DoD
   - Commercial
   - Non-Profit
   - Non-US
   - US Government
   - FFR&D
   - Other

*Note: You must give us your address to receive the CD.
ABOUT THE SOFTWARE TECH NEWS

STN EDITORIAL BOARD

Ellen Walker  
Managing Editor  
ITT Corporation, DACS

Dan Ferens  
Co-Editor  
ITT Corporation, DACS

Philip King  
Production Editor  
ITT Corporation, DACS

Wendy Butcher  
Graphic Designer  
ITT Corporation, DACS

Paul Engelhart  
DACS COR  
Air Force Research Lab

Morton A. Hirschberg  
Editorial Board Chairman  
Army Research Lab (retired)

Dr. Kenneth E. Nidiffer  
Software Engineering Institute

Dennis Goldenson  
Software Engineering Institute

John Scott  
Mercury Federal Systems

ADVERTISEMENTS

The Software Tech News is now accepting advertisements for future newsletters. In addition to being seen by the thousands of people who subscribe to a paper copy, an electronic version is available at the DACS website, exposing your product, organization, or service to hundreds of thousands of additional eyes every month.

For rates and layout information contact: news-editor@thedacs.com

COVER DESIGN

Wendy Butcher  
Graphic Designer  
ITT Corporation, DACS

ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

“This article was originally published in the Software Tech News, Vol.13, No.2 June 2010. “

Requests for copies of the referenced newsletter may be submitted to the following address:

Philip King, Production Editor  
Data & Analysis Center for Software  
P.O. Box 1400  
Rome, NY 13442-1400

Phone: 800-214-7921  
Fax: 315-838-7130

E-mail: news-editor@thedacs.com


In addition to this print message, we ask that you notify DACS regarding any document that references any article appearing in the Software Tech News.

ABOUT THIS PUBLICATION

The Software Tech News is published quarterly by the Data & Analysis Center for Software (DACS). The DACS is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC). The DACS is technically managed by Air Force Research Laboratory, Rome, NY and operated by ITT, Information Systems Division.
STN 13-2 June 2010: Defensive Cyber Security; Processes and Policies

IN THIS ISSUE

Tech Views
by Robert L. Vienneau, DACS Senior Analyst ................................................................. 3

Today's Cyber Environment: Where Does Software Fit?
by Terry Roberts, Executive Director, ASP/Interagency and Cyber, Carnegie Mellon, SEI ........................................ 4-7

Certification and Accreditation (C&A) Basics
by Steve Welke, Trusted Computer Solutions, Inc. .......................................................... 8-16

Information Security in Software and Technology Reliant Environments
by Sal Paladino, ITT Corp. .................................................................................................. 17-20

Intrusion Detection Systems (IDS) Taxonomy - A Short Review
by Suhair Hafez Amer, Ph.D. and John A. Hamilton, Jr., Ph.D. Southeast Missouri State Univ. and Auburn Univ........ 22-29

IATAC's Critical Role in Cyber Security
by Dr. Ron Ritchey, Gene Tyler, and Karen Mercedes Goertzel, Information Assurance Technology Analysis Center (IATAC) ......................................................................................................................... 30-36

Definitions
by Robert L. Vienneau, DACS Senior Analyst ................................................................. 38-39