atsec
the information security provider
NEWS
7/2010

At atsec, we always strive to expand our knowledge and expertise in the field of IT security, and to offer better and broader services to our customers. Constant education of our employees, involvement on international IT security standard committees, and continuous exchanges with our peers in the industry are examples of this commitment. Now we have taken another step in this direction:

> *The principles that we articulated on our very first day as atsec:*
>
> - *Know the business*
> - *Stay focused*
> - *Be independent*
>
> *and above all,*
>
> - *Act with integrity*

We are very pleased to announce that Criteria Labs and atsec information security have agreed to collaborate, bringing together the significant resources for hardware testing and failure analysis provided by Criteria Labs, and the security testing and evaluation skills and resources provided by atsec. Together, we can provide extended services and advanced US facilities for security testing of chip-based devices such as smartcards, RFID devices, ASIC, FPGA, and embedded systems.

Criteria Labs, based in Austin, Texas and Penrose, Colorado, has extensive microelectronic Failure Analysis process capabilities, including Acoustic Microscopy (CSAM), Scanning Electron Microscope (SEM), Real Time X-Ray, Cross Sectioning, Micro-Probe, Light Emission Microscopy, De-Cap (Wet), Laser Marking, Construction Analysis, Parallel Polishing, Front Lapping, Latch Up/Electrical Overload Stress (EOS), Electro Static Discharge (ESD), Digital image capture, and Solderability Testing. Their facilities include a clean room and raised test floor. Criteria Labs is also MIL-PRF-38535/883 certified for testing military and defense electronic products.

atsec information security, based in Austin, Texas (with additional offices in Germany, Sweden, and China), provides security evaluation and testing services. atsec has an extensive history in Common Criteria evaluation and FIPS 140-2 (cryptographic module) testing and consulting for a variety of products and applications from leading companies including HP, IBM, Microsoft, Red Hat, Honeywell, Apple, Samsung, and NationZ. atsec has contributed to security standards including ISO/IEC 15408, and the forthcoming ISO technical specification for Physical Security Attacks, Mitigation Techniques, and Security Requirements.

Together, atsec and Criteria Labs present high-quality independent facilities and expertise for the US market. We also provide improved and extended services to the customers of both laboratories.

Salvatore La Pietra
CEO

Recent news in short:

- Wind River Introduces First Embedded Linux Operating System to Be Accepted for EAL4+ Certification by NIAP
- Operating System Protection Profile Published by BSI and atsec information security
- atsec‘s Steve Weingart presented “Considering Security Standards While Designing Devices and Systems“ at IEEE VLSI Test Symposium 2010
- Upcoming conferences atsec will attend include: TRISC 2010, 11th ICCC, 2010 US PCI Community Meeting, it-sa 2010 and ACSAC 2010
- atsec‘s Auston Holt speaks on GSA FIPS 201 Smart Card Evaluations at ISSA Austin
- PBS Professional Achieves Common Criteria EAL3+ Certification
- More news on our website: **www.atsec.com**
- Did you know that atsec has a security blog? Follow us with some of our consultants’ thoughts and musings at: *http://www.atsec-information-security.blogspot.com/*

Independent Security Analysis

One of atsec's core business principles is that we are independent. This includes our financial independence – we are privately owned and atsec does not have any loans or venture capital that might cause any conflict of interest. We do not form commercial alliances with partners selling particular products or services, nor do we play a role in large integration projects.

We know that our independence is highly valued, because we have been allowed and trusted to provide independent security analysis in areas where existing standards and schemes (such as Common Criteria or FIPS 140-2) did not meet a customer's need for demonstrating assurance.

There are many motivators for such a scenario. It could be that a formal scheme does not yet exist. Sometimes, an independent demonstration of the assurance provided by a certain-product provides our customers with an excellent opportunity to both educate and inform their customers.The following are some examples of projects we've undertaken, which demonstrates the versatility of atsec's consultants and serves as a testament of our unique knowledge of the industry.

Voting Systems Analysis

In this project, atsec was asked to assist a customer, Freeman, Craft, McGregor Group, Inc, a well-respected and notable consultancy group that provides services to many states on electoral systems, in performing an analysis of InkaVote Plus system, a voting system marketed by Election Systems & Software (ES&S). The analysis was for the "Top to Bottom Review", which was commissioned by the California Secretary of State to qualify the machine for use in the elections that were managed by the State of California.

The project was intense, performed on a relatively short timescale, and involved coordination and careful liaison with the multiple parties involved. Our consultants had to quickly learn about some of the intricacies of not just the voting system itself, but also the voting processes and procedures that form the environment in which the system would be used. We also had to know the 2002 Voluntary Voting Systems Standards as well as several coding languages, coding conventions, and have a good working knowledge of the IEEE, NIST, ISO, and NSA standards and guidelines.

The review included emphasis on security and integrity of the voting system and aimed to identify any security vulnerabilities that could be exploited to alter vote recording, vote results, critical election data such as audit logs, or to conduct a "denial of service" attack on the voting system. With all projects of this nature, there are no guarantees that each and every vulnerability in such a system will be found. However, we did our best!

We were required to help produce two reports: a detailed source code analysis, and a red team report which included a hardware analysis and penetration test.

These reports were made public and can be found at:
http://www.sos.ca.gov/voting-systems/vendors/ess/inkavote-public-source.pdf
http://www.sos.ca.gov/voting-systems/oversight/ttbr/inkavote-plus-public-red-team-report.pdf

Vendor Test Data Report

On this project, the customer asked us for help in creating the mandatory Vendor Test Data Report in preparation for the conformance testing that was required for their product to appear on the GSA Approved Products list which is managed by the FIPS 201 Evaluation Program.

The product in question was an electromechanically-opaque sleeve. The sleeve was designed to help ensure that smartcards used in the personal identity verification program cannot be polled and relinquish private information while being worn or carried by the user during normal activities.

atsec's consultants quickly got to the root of the problem – which was with the standard itself. The specifications made were those for measuring RF emanations in co-axial cable, not for flat material such as that typically used in smartcard sleeves. The project evolved to include working with the program and standards developers to implement a more appropriate standard. Of course, the project suffered some delay as a result in the initial change of direction, but the customer was happy with the results.

Virtual Machine Analysis

Red Hat approached atsec to help them produce a report comparing the security-relevant functionality of Red Hat's KVM with other virtual machine monitor implementations that also support the basic concept of virtualizing a physical computer to allow concurrent execution of multiple operating systems. The analysis was performed by Stephan Mueller, an atsec expert consultant in the field. His analysis was based on attack vectors and usage scenarios, and explains how various virtual machines monitor implementations, mitigate potential attacks, and support different usage scenarios.

The technical report was completed and published by Red Hat at
http://www.redhat.com/f/pdf/rhev/kvm_security_comparison.pdf.

Others

We have provided a wide variety of help to customers on an array of challenging projects. Not all of which are public and can be described in detail. Some examples include: providing expert testimony on compliance with German e-commerce and signature law, audits of source code compiled in accordance with company-provided procedures, analysis of Chinese Security Regulation for Databases helping establish national schemes for evaluation, audits of device configurations to check whether they comply with the requirements of FIPS 140-2 Security Policies, mainframe penetration testing for the financial sector, and many more special projects.

An Introduction to Physical Security for Computing Systems

Traditionally, the term ‘physical security’ has been used to describe protection of material assets from fire, water damage, theft, or similar perils. However, ongoing concerns in computer security have caused this term to take on a new meaning: technologies used to safeguard information against physical attack.

In this new sense, physical security is a barrier placed around a computing system to deter unauthorized physical access to the system itself. This concept is complementary to logical security, the mechanisms by which operating systems and other software prevent unauthorized access to data. Both physical and logical security are likewise complementary to environmental security; which is the protection a system receives by virtue of location, such as guards, cameras, badge readers, access policies, etc.

The reason for separating physical and environmental security is partly due to the change in the nature of the assets being protected. In the past, the assets to be protected were nominally physical items: cash, jewelry, bonds, etc. Now the asset is often information, which can be stolen without being physically removed from the location where it is stored. If information can be seen, it can simply be copied. This information can be anything from a spreadsheet to a cryptographic key. It may be reasonable for an individual to have access to a location (environmental security) but not to have access to the information stored on a computing system that is in that environment (physical security).

Physical security is also becoming more important because computing systems, to a great extent, have moved out of environmentally-secure computer rooms and into less environmentally-secure offices and homes. At the same time, the value of the data on these computing systems is increasing as centralization decreases. Logical security has also been improved so that a physical attack may become more easily performed than a logical attack. Additonally, the motivation to attack computing systems is increasing because the rewards for doing so are increasing.

Many different kinds of physical security attack and defense mechanisms have been developed by both the attackers and the defenders. Since this is largely an empirical field (no hard science has been identified, or likely exists to prove the physical security of a system), the state-of-the-art advantage seesaws back and forth between the attacker and the defender.

Additionally, techniques used in these attacks are not always obvious. For example, an air-spray can, turned upside so that it expels freezing gas is a very effective method of stealing hidden information from a PC or laptop. Equally odd mechanisms are used for many other techniques.

For a detailed description of many of the known methods of both attack and defense, please see: Physical Security Devices for Computer Subsystems: A Survey Of Attacks and Defenses 2008 (http://atsec.com/downloads/pdf/phy_sec_dev.pdf).

Operating System Protection Profile Published by BSI and atsec information security

The need for a second-generation, certified Operating System Protection Profile (OSPP) becomes apparent when you take a look at the current reality of networked systems and the few general-purpose OSPPs that specify industry-agreed functional and assurance requirements that are applicable to them. The OS paradigm has evolved from single isolated systems to more complex, distributed and networked, multi-machine environments. Thus, several of the original protection profiles, including the much-cited Labeled Security PP (LSPP), Role-Based Access Control (RBAC), and Controlled Access (CAPP) PPs are rendered obsolete. In addition, applications that execute on operating systems are dependent on a secure platform. The security assurance that is provided by many of today's modern operating systems has been raised during the last decade since EAL4 is the typical level of evaluation for this technology. And, leading vendors are expectd to continue raising the bar further.

The OS Protection Profile was developed by the OSPP forum, including atsec experts with many decades of security experience, and security architects from leading vendors that are working with key operating systems. Bringing such cooperation to OS security standards provides an exemplary model for consolidating the improvements of recent years into the overall security posture of modern operating systems.

For more information, please see the news section on our website:

http://atsec.com/us/news-operating-system-protection-profile-200.html

Overview of Current CCEVS Policies

Understanding the rules for submitting a product for evaluation to the US scheme, operated by NIAP, can be difficult. The policies and intricacies surrounding this process have changed several times during the last few years and confusion in the IT evaluation community. This summary provides an overview of the current policies, and steps that need to be taken to begin an evaluation under the NIAP scheme.

The acceptance policy for CCEVS evaluations has recently been changed. NIAP will only accept into evaluation products that can claim compliance with a US-approved Protection Profile (and your product can not have a higher EAL than the claimed Protection Profile specifies). Without an approved Protection Profile, NIAP requires a Letter of Intent and, depending on validator availability and customer need, NIAP will only consider accepting an EAL 2 evaluation.

The Letter of Intent is a prerequisite that states the explicit requirements for an evaluation from a government agency (details can be found in Policy Letter #12). This can be obtained from a US or NATO organization that has a need for an evaluated product. The recommendation is to get this letter before any other evaluation activities are started.

When it is time to begin work on a Common Criteria project, keep in mind that CCEVS has limited resources. Therefore, Final and Test VORs (Validator Oversight Reviews) take precedence over Initial Validator Oversight Reviews (IVORs). If there is a bottleneck, the start of your evaluation might get moved into the next month (Policy Letter #12 explains this in detail). You should also be aware that there are very stringent requirements regarding the quality of the read-ahead documentation for the IVOR: for example, a clear and complete TOE description.

Another issue that needs to be closely adhered to is the time limits that NIAP has put in place. If a vendor repeatedly fails to adhere to the milestones set at the beginning of the project, the CCEVS will terminate the inactive evaluation. All evaluations have to be concluded within a 12-month period. A realistic project plan and constant communication of possible delays is very important if the project is to be successfully concluded.

The goal of the CCEVS policies is to make better use of the validator resources and to assure higher- quality evaluations. Knowing these policies and their implications is essential to a successful evaluation. atsec information security has been involved in the CCEVS for years and thoroughly understands the complex nature of Common Criteria evaluations. Let us help you with your project.

All current CCEVS policy letters can be found at http://www.niap-ccevs.org/policy/ccevs/

CONTACT US

atsec information security corporation
9130 Jollyville Road, Suite 260
78759 Austin, TX
USA

Phone: +1 512 615 73 00
Telefax: +1 512 615 73 01
eMail: info@atsec.com