atsec the information security provider

NEWS 02/2011

One of the realities of being accredited through a number of government and commercial organizations is the fact that we at atsec are constantly in audit mode. From re-accrediting our Common Criteria and Cryptographic Security Testing Laboratories to having our integrated ISO/IEC27001 and ISO 9001 Information Security Management Systems audited, we know the challenges and headaches that come with compliance and certification. And this is how we want it to be – because we have gone through the same rigorous processes that we help our customers with, we have the advantage of knowing the business from both perspectives.

We also stay on top of new and emerging standards, like the U.S. biometrics program and contribute to existing standards through committee work and editorial contributions.

Even though the audit cycle never stops at atsec, first and foremost we have a business to run. So we became very good at finding ways to make certification and compliance as efficient and easy as possible to achieve and maintain– and we are happy to pass this experience on to our customers. We want IT security to make your business better, safer and more reliable.

How can we help you?

Regards,

Andreas Fabis
Marketing Director

Please join us for our

Protection Profile Developers Workshop

during the RSA Conference in San Francisco. atsec's Chief Scientist Helmut Kurth will be the tutor on

February 15th 2011 from 9am to 5pm

http://atsec-information-security.ticketleap.com/protection-profile-developers-workshop-and-reception/

Recent news in short:

- atsec at the 2011 RSA conference
- Helmut Kurth remembers the KGB hacker affair
- atsec China gains ISO/IEC 27001 certificate issued by ISCCC
- Enterprise Key Management Solution Receives FIPS 140-2 Certification
- atsec information security at the 26th Annual Computer Security Applications Conference in Austin
- atsec tests Pierson MIIKOO cryptographic algorithms
- atsec information security completes the CAVP cryptographic algorithm testing for ZTE

More news on our website:
www.atsec.com
Did you know atsec has a security blog? Follow our consultant's thoughts and musings at: http://atsec-information-security.blogspot.com.
Also join us on Facebook and Twitter (@atsecitsecurity).

Common Criteria (ISO/IEC 15408) ■ FIPS 140-2 ■ CAVS ■ SCAP ■ NPIVP ■ GSA FIPS 201 ■ PCI QSA ■ PCI ASV ■ PCI PA-QSA ■ ISO/IEC 27001 ■ SOX and Euro-SOX ■ FISMA ■ HIPAA ■ VTDR ■ Embedded Systems ■ Hardware Security Testing and Analysis ■ Penetration Testing ■ US Export Control for Cryptography

Let's talk...

by Steve Weingart

As you hopefully know, atsec has a full service Cryptographic and Security Testing (CST) laboratory available to service your certification needs. We are NVLAP [1] accredited to test against the FIPS 140-2, FIPS 201, GSA/PIV, SCAP, and CAVP standards, and we can help you through the certification process. Each of the standards has its own unique requirements, but many of them are complementary.

For example, if you want to validate a PIV card under the GSA FIPS 201 evaluation program, you must first validate the card under FIPS 140-2 for its cryptographic components, and then it must undergo testing in NIST's PIV program before it can be submitted to the GSA for inclusion on their Approved Product List. We can consolidate a significant number of the requirements (especially those related to documentation), to maximize the efficiency of your effort, and thereby minimize the cost and time necessary for certification.

This also holds true for projects that combine Common Criteria with FIPS 140-2 or other NIST standards. The savings resulting from a common knowledge base and documentation repository can be significant.

Where we see the standards going...

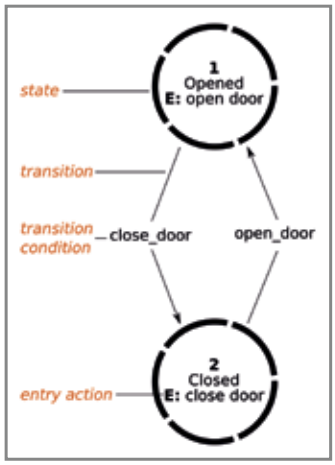
FIPS 140-2 is becoming more important as the government and military seek to reduce costs while keeping high standards for quality and security. Many government and military organizations have made the move to using commercial-off-the-shelf (COTS), FIPS 140-2-validated cryptographic modules. FIPS 140-2-validated cryptographic modules are required under FISMA (Federal Information Security Act) for sensitive but unclassified data, and these COTS FIPS 140-2 validated modules are now also being introduced into battlefield applications, replacing custom and classified equipment, with good security at a much lower price.

Some government organizations will only purchase COTS products that meet their tailored and specific security assurance needs.

In addition, some government organizations require not just one overall level of security assurance, but have more sophisticated requirements, and will only purchase COTS products that meet their tailored and specific security assurance needs. For example, it is becoming more common for the Army to require a FIPS 140-2 Level 2 overall security level, but includes a Level 3 for physical security and design assurance.

Still, the typical requirements are for one specific overall security level. FIPS 140-2 has four security levels. Level 1 is the least secure and level 4 is the most secure. All FIPS 140-2-validated cryptographic modules need to be well-documented and the documentation must match the implementation (this is one of the things that the laboratory checks during validation). In addition, validated modules must use approved functions; this means that the cryptographic algorithms used must be from the NIST-approved list, and they must be used in the correct way. All modules must perform self tests and integrity checks on themselves and the development process must implement configuration control.

Two requirements that are unique to FIPS 140-2 certification are the inclusion of the Security Policy and the Finite State Model documents. The security policy must be a public document that is posted on the NIST CMVP website with the validation listing. It describes the design and the function of the module in a way that addresses its compliance to the standard. The Finite State Model expresses the operation of the module as a state machine and levies certain requirements on the implementation, for example, the module must only be in one state at a time (this can cause compliance problems in modules that perform certain multithreaded operations).



Once the base requirements are met, the requirements specific to each level come next. At level 1, there are not many additional security requirements, and only a few design assurance-related ones. At level 2, users and administrators must be authenticated by their role. In addition, if the module is within hardware, basic physical security requirements apply.

1 NVLAP Lab code 200658

As in level 1, cryptographic keys may be entered in plaintext, however, if the Operational Environment requirements apply then the module must also be evaluated at EAL 2 under the Common Criteria.

The Operational Environment (OE) is one of the most confusing sections of FIPS 140-2 because the OE requirements apply if the user or administrator can modify the environment (beyond upgrading with authorized, authenticated, validated code). If the OE is fixed (i.e. the users cannot modify the OS and runtime code), then the OE requirements do not apply. In many cases, the module can be designed or configured to make the OE fixed, resulting in considerable savings in testing/certification effort and expense.

At security Level 3, the requirements get more rigorous. The physical security becomes relatively substantial; user authentication must be identity-based (i.e. you do not log in as 'admin,' you log in as 'Joe' who is an admin) and all of the keys and critical security parameters must be entered encrypted or use split knowledge techniques.

Finally, at security Level 4, the protection must be essentially without limit. Any attack attempted against the physical security of the module must not permit successful penetration. The software must be formally modeled to show provable security and all of the security requirements are examined at the greatest depth.

In addition to these general requirements, we have found that the CMVP (Cryptographic Module Validation Program at NIST, the owners of FIPS 140-2) is starting to require a deeper level of testing that includes a complete testing of software APIs provided by the software modules, to ensure that cryptographic modules are more secure. A sophisticated CST laboratory, such as atsec, can borrow from experience with other security standards (e.g., Common Criteria) and devise a module testing strategy that meets the letter and spirit of the CMVP requirement, but significantly reduces the time and cost needed to implement it for a given module.

FIPS 140-3, is the long-awaited update to the FIPS 140-2 standard and has undergone two rounds of public comment already. We expect some announcement on the final changes accepted by NIST sometime during 2011. We would also expect a transition period for migration to the new version to be put in place by NIST.

Note that FIPS 140-2 is also becoming more internationally-accepted and has been published as an ISO/IEC standard, which is currently being updated with an eye on the evolving FIPS standard.

SCAP (Security Content Automation Protocol) is becoming more prominent as well. Right now, it is primarily used for configuration and vulnerability scanners. However, in the near future, a network-based version of the SCAP standard may be released which supports communication and interoperability between network devices including routers, switches, firewalls, intrusion detection and protection, and network management systems.

> *The ultimate goal is for all network control devices to be interoperable, secure, and contain sufficient built-in awareness of attacks.*

Overall, we are seeing a move toward requiring network devices to be FIPS 140-2, Common Criteria, and (soon) Network SCAP-validated. This is a part of an orchestrated government effort to make networks, all the way up to the Internet, more aware of nefarious activities.

Hardware testing…

We already do hardware security testing as part of our normal FIPS 140-2 and GSA/PIV work, but this aspect of our security testing work is currently expanding. We are gearing up to perform more involved hardware testing, including chip-level physical security and attack/tamper resistance testing. atsec has partnered with Criteria Labs, a chip-level hardware failure analysis and testing laboratory, so we have access to state-of-the-art microelectronic skills and tools. We bring the security skills and attack methodology to this partnership, for a level of testing that is required now for smart cards and some other specialized security processors, especially single-chip devices. As this type of device becomes more common (and there are a number of them in development right now) this kind of testing will become mainstream.

Let's talk!

Our ultimate goal is to provide our customers with the best standards testing service to help them meet their business objectives by producing the best security product with the optimal use of their precious resources and in full compliance with the security standard(s) their organization aims to meet.

atsec NEWS

Side Channel Analysis

by Steve Weingart

Side Channel Analysis examines emissions from electronic devices to learn secrets that are not supposed to be leaked. The best known methods of SCA are Simple Power Analysis and Differential Power Analysis (SPA and DPA). SPA and DPA are extremely effective ways to extract information from small computing devices, such as smart cards and tokens. SPA and DPA work by sampling and examining the power supply current (Icc) of these devices. By simple inspection, in the case of SPA, or by mathematical processing in the case of DPA, it is often possible to determine the data, and the secrets, that were processed by the device.

When SPA/DPA was first put into use, it was often possible to take a single oscilloscope trace of the Icc as a Smart Card performed an encryption operation and then, with a little practice, read the encryption key from the screen directly. It was pretty scary! Especially since it used no special or exotic equipment and the command that invoked the cryptographic operation was a normal identification command.

Nowadays the attack and defense mechanisms have both become so exotic that it takes very specialized equipment to mount an attack that is likely to be effective. But it is certain that both sides are working harder than ever, and the risk is still there, bigger than ever.

In addition, other avenues of SCA have been explored, such as Electro Magnetic Analysis (EMA). EMA examines the radio frequency emanations from these same electronic devices and can be significantly more effective than SPA/DPA at extracting secrets — despite prevention mechanisms.

What this means to developers of cryptographic devices and tokens is that SCA is an important risk to assess. SPA/DPA risk analysis is becoming required for Smart Cards and tokens used in the credit card and Personal Identity Verification (PIV) industries, and that list of industries is growing. Differential Analysis DPA and Electromagnetic Analysis, EMA) has been identified as one of the new requirements potentially to be added to FIPS 140-3.

atsec's environmental policy

by Andreas Fabis

atsec acknowledges the importance of being a responsible corporate citizen, actively supports the laws in the regions of the world where we operate, and abides by ethical standards and international norms. We strive to reduce and, where practical, eliminate practices that harm the interests of the public and/or the environment in which we conduct our business

We are a consulting firm and have no production environment. As such, the scale of our contributions to conserving energy, reducing pollution, and handling the world's natural resources with respect is comparatively small. Regardless, atsec's management is committed implementing sustainable business practices.

atsec adheres to the following principles in an effort to reduce any negative impact on the environment:

- Supporting our customer's environmental policies and objectives
- Conserving natural resources, such as energy sources, forests, and water
- Reducing emissions and pollution, for example by choosing travel options with the smallest carbon footprint, reducing waste, and recycling materials

atsec specifies corporate and staff policies in support of these principles including:

- Providing a work environment with resources that facilitate good sustainability practices
- Encouraging environmental responsibility in our staff
- Considering environmental impact when specifying our business processes and procedures
- Striving to meet applicable best practice standards, such as ISO 14001
- Conserving natural resources by reusing and recycling materials, purchasing recycled materials, and using recyclable packaging and other materials

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