atsec
the information security provider

NEWS
04 / 2012

Recently atsec celebrated its 12th birthday. As always, our best wishes and thanks to all of the contributors: our customers, our partners, and our employees.

This year R.G. "Jerry" Converse of Fulbright & Jaworski L.L.P. took up the pen and sent us this birthday greeting:

"Happy Birthday, atsec!

You are not an ordinary 12-year-old! Your knowledge and wisdom extend well beyond your years. Some of the best people in the world work at atsec and make it what it is today. We at Fulbright & Jaworski LLP are honored to list atsec information security corporation among its clients.

Our best wishes to you for many more years of success."

R.G. "Jerry" Converse
Fulbright & Jaworski L.L.P.

In this newsletter we want to share with you our opinions on trends and developments in the CST area. Apostol Vassilev and Steve Weingart contributed the main article about this topic.

I would also like to bring our publications section to your attention, where you will find white papers on a variety of subjects: *http://www.atsec.com/us/publications-white-papers.html*

Regards,

Andreas Fabis
Marketing Director

Recent news in short:

- IBM's® z/OS® Version 1 R. 13 System ICSF PKCS#11 Cryptographic Module Receives FIPS 140-2 Certification
- Industry-Leading Enterprise Java Application Platform Earns Common Criteria EAL4+ Certification
- atsec information security at the 2012 RSA
- Stonesoft Firewall/VPN product family awarded Common Criteria EAL4+ Certification
- atsec completes PCI DSS compliance assessment for ShengPay
- atsec Provides Common Criteria Evaluator Course for ISCCC
- Fiona Pattinson to Present at ISSA Austin: "FRITSA: Do you understand how all of your IT security assurance efforts fit together?"

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

Common Criteria (ISO/IEC 15408) ■ Cryptographic Algorithm Validation Program ■ FIPS 140-2 FIPS 140-2 ■ FISMA ■ NASPO ■ SCAP ■ NPIVP ■ ISO/IEC 27001 SOX and Euro-SOX ■ HIPAA ■ VTDR ■ Embedded Systems ■ Hardware Security Testing and Analysis ■ GSA FIPS 201 ■ U.S. Export Control for Cryptography

CST Trends

One of the important observations is that the trends that we saw last year are continuing, at least from a security standards standpoint.

One of the important observations is that the trends that we saw last year are continuing, at least from a security standards standpoint.

There are no more waivers under FISMA for validation of cryptography to FIPS 140-2. Following the FISMA rules isn't just a good idea, it's the law. Thus, formal validation is now the norm for all non-classified uses of cryptography. Similarly, many defense applications require FIPS 140-2 validation for the Suite B ciphers. In addition, government and military customers are also starting to require the security of operating systems and network devices to be evaluated via the Common Criteria.

What does all this mean? To be able to compete in the federal government and military markets, all systems and devices that perform non-classified cryptography need to be tested against the standard and validated. Similarly, if your product implements Suite B ciphers for classified applications, performing FIPS 140-2 validation on it is a significant and, in most cases, a sufficient step towards satisfying the prerequisites for these markets.

It's interesting to note that companies whose primary product is bandwidth, whether via copper, fiber, or satellite, who have said in the past that cryptography is the customer's responsibility are now having to secure their control channels. Cryptography is now their responsibility too. A similar shift of responsibility is also happening for all remotely piloted devices' data and control systems, especially in the light of video data from RPVs being tapped and controls being taken over.

The message is clear: if you use cryptography in your product, a great deal of the market requires it to be validated under FIPS 140-2.

From what we are hearing, the Department of Defense (DOD) is still moving towards requiring FIPS 140-2 and Common Criteria for all smart network devices (managed switches, firewalls, routers, IDS, etc.). Security Content Automation Protocol (SCAP) will be coming too, but is still new and moving along less quickly than originally thought.

The acceptance of FIPS 140-2 goes beyond the federal government and the military. More and more state governments and customers in other sectors of the economy, such as banking, health care, and insurance (i.e., anywhere personal information is used) are also beginning to require that cryptographic devices be FIPS 140-2 validated. On one hand, this helps to ensure interoperability because all validated devices have had the cryptography itself verified for correctness. On the other hand, it increases the potential for higher return on investment in FIPS 140-2 validations because it opens the doors to markets not just within the federal government and the military, but also in several other important large markets.

All-in-all, the security standards climate for U.S. government and military customers is continuing to move in the same direction that we have seen it going in for the last year or so. We also see that the commercial markets are following suit as validated cryptography is becoming required more often under specific-industry requirements and/or inter-industry standards where financial, medical, or personal data is handled.

The message is clear: if you use cryptography in your product, a great deal of the market requires it to be validated under FIPS 140-2.

Security Levels Overview
Levels of FIPS 140-2 validation established by NIST:
Level 1: The lowest level of security; typically used for products that perform software encryption
Level 2: Tamper resistance is an added requirement; mostly addresses products that perform hardware encryption
Level 3: Requires robust cryptographic protection and key management, as well as physical protection of the device against disassembly; also mandates hardware that automatically overwrites critical security parameters in case of a physical attack or tampering
Level 4: Highest level of security; requires advanced tamper protection; typically used for products that are used in physically unprotected environments

IBM’s® z/OS® Version 1 R. 13 System ICSF PKCS#11 Cryptographic Module Receives FIPS 140-2 Certification

Austin, TX – IBM’s® z/OS® Version 1 R. 13 Integrated Cryptographic Service Facility (ICSF) PKCS#11 Cryptographic Module recently received FIPS 140-2 Level 1 certification. The successful certification is listed on the National Institute of Standards and Technology’s (NIST) website (http://csrc.nist.gov/groups/STM/cmvp/validation.html, certification number 1672).

The security of information assets is an ongoing problem of increasing importance for many companies in view of the constant rise of threats. IBM® z/OS® - one of the world’s most advanced operating systems – has shown persistent commitment to their customers by providing solid means for securing valuable data: having undergone numerous Common Criteria evaluations at high assurance levels and corresponding FIPS 140-2 validations of the critical cryptographic components within.

Apostol Vassilev, CST laboratory manager for atsec, commented: “The ICSF module is a fundamental component into the security services framework on the IBM z/OS v1 R13. It enables scalability and performance of cryptographic services on z/OS, aimed at enhancing the security of the operating system and the applications on it, with strong cryptography. It combines software, hardware, and firmware within the module cryptographic boundary on the z/OS architecture and delivers a wide array of cryptographic services backed by the security assurances of the FIPS 140-2 standard. The validation of this new version of the module demonstrates IBM’s commitment to the development of advanced technologies that meet the modern real-life computational challenges and compliant with established standards for the benefit of the federal user communities. It also demonstrates the ability of the atsec CST lab to perform this challenging project leading to a successful validation of a fast-evolving module in its second and more advanced validated edition.”

For more information about the FIPS 140-2 standard, please visit our website at http://www.atsec.com and the NIST website at http://www.nist.gov

atsec Completes FIPS 140-2 Testing for MIIKOO at Security Level 3

Austin, TX - atsec information security is proud to announce that its customer, Pierson Capital Technology LLC (branded as “Pierson”), received a FIPS 140-2 validation certificate #1634 for their MIIKOO product.

The security technology employed by the MIIKOO device was subjected to rigorous testing by atsec’s Cryptographic and Security Testing (CST) laboratory and subsequently validated by the CMVP at the National Institute of Standards and Technology (NIST) in the U.S. and the Communications Security Establishment Canada (CSEC) in Canada. This deliberate and meticulous process resulted in the successful validation of Pierson’s MIIKOO device, published as FIPS 140-2 certificate #1634.

Frank Psaila, Pierson’s general manager, commented, ”This certification is a great achievement for Pierson Capital Technology and its dedicated team of engineers, setting an unprecedented record for the FIPS 140-2 validation, combining biometrics and token hardware, capable of working with both OTP and PKI technologies. Thanks to the expertise of both teams, we managed to succeed in a very reasonable time frame. This success will without doubt set new standards for remote authentication and its applicability, which is our main goal for this project.”

Apostol Vassilev, atsec's CST lab manager, noted, ”The combination of security technologies employed by the MIIKOO device presented a unique challenge for our lab and Pierson’s engineering team to demonstrate compliance to FIPS 140-2 at Security Level 3. This project required understanding of not only a wide range of technologies, but equally as important, a knowledge of the FIPS 140-2 standard. The atsec testers had to explore the full breadth and depth of the FIPS 140-2 standard to demonstrate compliance at such a high security assurance level. I am very proud that the atsec CST Lab successfully completed this challenge, which shows the high professionalism and dedication of our staff. I also applaud Pierson’s commitment to rigorous testing and validation under open international standards, such as FIPS 140-2.”

For more information about the FIPS 140-2 standard, please visit our website at www.atsec.com and the NIST website at www.nist.gov

Industry-Leading Enterprise Java Application Platform Earns Common Criteria EAL4+ Certification

RALEIGH, N.C. - Red Hat, Inc., the world's leading provider of open source solutions, announced today that JBoss Enterprise Application Platform 5.1.0 and 5.1.1 have been awarded CC certification at Evaluation Assurance Level 4 (EAL4+) under the Common Criteria Evaluation and Certification Scheme (CCS). Common Criteria is a set of internationally approved criteria for evaluating and certifying the information security of IT products and information systems. EAL4+ is the highest assurance level that is recognized globally by all signatories under the Common Criteria Recognition Agreement for this category of solutions. This certification also marks the highest level of Common Criteria certification for the JBoss Enterprise Middleware portfolio.

“Security remains one of the most important considerations for security-conscious industries like government, financial services, and healthcare considering new technology solutions, and achieving Common Criteria certification gives customers the added confidence that our solutions meet specific, internationally recognized benchmarks for security performance,” explained Paul Smith, general manager and vice president, public sector operations, Red Hat. “We made the commitment to upgrade our Common Criteria certification for the JBoss Enterprise Application Platform from EAL2 to EAL4+, and achieving the highest available certification level is a testament to our ongoing efforts to meeting the needs of security-conscious government organizations and businesses.”

To facilitate this certification, Red Hat worked with atsec information security, a government accredited laboratory in the United States and Germany, that tested and validated the security, performance, and reliability of the solution against the Common Criteria Standard for Information Security Evaluation at EAL4+. Their tests, and the resulting certification, validate JBoss Enterprise Application Platform as one of the most trusted platforms for building, deploying, and hosting enterprise Java applications and services.

“We are proud that Red Hat chose atsec as the laboratory for the Common Criteria evaluation, as this project continues our successful business relationship with Red Hat,” said Ken Hake, Common Criteria laboratory manager for atsec U.S. “Red Hat’s completion of this Common Criteria project will result in more assurance for customers who run JBoss Enterprise Middleware in business critical environments.”

TRAINING

atsec offers both regularly scheduled and customized, on-demand education and training courses at our facility or on-site at your location. We have held country-specific trainings in Korea, Taiwan, Turkey, as well as other countries.

Our training offerings include:

- **Overview of Common Criteria Evaluations for Business Decision Makers**
- **Necessary Skills for Product Developers Preparing for Common Criteria Evaluations**
- **Beginning Common Criteria Evaluation Skills for Future Evaluators**
- **Introduction to Common Criteria for Developers**
- **Protection Profile Development Workshop**
- **Workshop for IT Security in the U.S. Health Industry**
- **FIPS 140-2 Validation Requirements**
- **FIPS 140-2 Workshop**
- **Physical Security Workshop**
- **Introduction to FIPS 140-2**
- **Penetration Testing Seminar**
- **NASPO Certification Workshop**

We can develop trainings for any other IT security topic to meet your company's needs.

For more information, please visit:
http://www.atsec.com/us/trainings.html

CONTACT US

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

Phone: +1 512 615 7300
Telefax: +1 512 615 7301
Email: info@atsec.com