atsec NEWS

12/2010

the information security provider

Do your merchant customers expect you to demonstrate PCI compliance for your services or products? Are your government customers asking you for FIPS 140-2 validation (or even Common Criteria certification) of your products? Does your organization need to implement controls in accordance with international data protection laws? We are here to help!

"Let us take care of the certification headache and help you get your product or service certified reliably and fast."

atsec is a globally-recognized leader in information security testing and consulting services. Our independent expertise and our reputation for "getting the job done" are valued all over North America, Europe, and Asia.

We see current trends in the IT security field: There will be more and more interdependence between IT security standards, like PCI and FIPS 140-2, FIPS 140-2 and Common Criteria, Common Criteria and FIPS 140-2.

There is also a push to mandate IT security from the government. From the Department of Defense to local agencies and law enforcement – certified and evaluated IT security solutions will become more and more important.

We know the complexities of IT security standards, as well as the interdependencies – let us take care of the certification headache and help you get your product or service certified reliably and fast.

We look forward to hearing from you!

Regards,

Andreas Fabis
Marketing Director

Please join us for our
Workshop on "Developing a Protection Profile"
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.

Please check our website for more information or send an email to info@atsec.com.

Recent news in short:

- atsec adds side-channel security testing to its hardware testing portfolio
- atsec information security completes the CAVP cryptographic algorithm testing for ZTE
- atsec information security completes two GSA FIPS 201 evaluations for EK Ekcessories, Inc.
- atsec information security at the MILCOM 2010 Conference
- IBM© z/OS© Version 1 R. 10 System SSL Cryptographic Module receives FIPS 140-2 certification
- Two IEEE Protection Profiles for Multi-Function Printers Evaluated by atsec information security
- atsec information security at the 11th ICCC conference in Antalya, Turkey
- Nationz cryptographic algorithms implementations achieve CAVP Certification
- Wind River Introduces First Embedded Linux Operating System to Be Accepted for EAL4+ Certification by NIAP

More news on our website: www.atsec.com
Did you know that atsec has a security blog? Follow our consultants' thoughts and musings at: http://atsec-information-security.blogspot.com/

Highlights of the Changes to the New PCI Standards

by Jeff Jilg

The Payment Card Industry (PCI) Security Standards Council (SSC) has recently released updated versions (v2.0) of the PCI Data Security Standard (DSS) and PCI Payment Application DSS (PA-DSS) standards. This culminates a 24 month release cycle which was used to collect input from customers and vendors, then undergo review and scrutiny resulting in the new standards. The standards are available to the public for download at *https://www.pcisecuritystandards.org/security_standards/updates.php*

The intent of this article is to provide a brief overview of the significant changes to show how they can affect you. Since there are a large number of changes, each change cannot be covered in this article. Interested parties can read the document "Summary of Changes from PCI DSS Version 1.2.1 to 2.0" (and for PCI PA-DSS) found at the web address above. It is worth noting that v2.0 does not include any new major requirements.

How will this affect you?

While some of the changes are cosmetic, there was a good effort to reduce redundancy between the two standards. Previously in the corresponding v1.2.1 versions, the PCI PA-DSS standard frequently referred to PCI DSS, forcing the customer or assessor to have both standards open while accomplishing PCI PA-DSS assessments. More importantly, the remainder of this article highlights the significant changes in the requirements and testing procedures which will affect customers and Qualified Security Assessors (QSAs).

When will this affect you?

For both standards (PCI DSS and PCI PA-DSS) the transition dates are the same, and are reflected in the following table.

Date	Usage
Now – 2010-12-31	V1.2.1 is required for assessments. V2.0 standards may not be used during 2010.
All 2011	V1.2.1 or v2.0 may be used for assessments. V2.0 becomes effective 2011-01-01.
All 2012	V2.0 must be used for all assessments.
2012-07-01	Starting on this date, PCI-DSS requirements 6.2, 6.5.6, and 11.1 are required. Prior to this date, 6.2, 6.5.6, and 11.1 are best practice

For customers currently undergoing assessment under v1.2.1 this means you still have 13 months to complete that assessment. Customers have the option to be assessed against v2.0 starting in 2011. To summarize, during 2011, customers can be assessed against either the new or old version, but in 2012 and 2013 all assessments must use v2.0.

PCI DSS changes

Since the bulk of assessments are focused on PCI DSS, this standard is reviewed first.

Clarification through separated testing procedures:

In some requirements, the testing procedures in v1.2.1 were specified as bullets or multiple sentences in the testing procedures and it was unclear which items were required. In v2.0, many of these procedures are broken out into individually numbered, more obvious requirements. The first example of this is Testing Procedure 1.1.3 which was split into 1.1.3.a and 1.1.3.b, as shown in the following:

V1.2.1 Testing Procedure	Corresponding V2.0 Testing Procedures
1.1.3 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.	1.1.3.a Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.

Clarifications: There are word clarification changes throughout the requirements and testing procedures. These wording changes are meant to better explain items which might have been confusing in v1.2.1. Consider Testing Procedure 1.3.1, where DMZ protocol verification is now focused on inbound traffic.

V1.2.1 Testing Procedure	Corresponding V2.0 Testing Procedure
1.3.1 Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	1.3.1 Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

Additional Guidance: There are content changes to the requirements, some of which include visibility to newer technologies. For example requirement 2.2.1 has a combination of wording clarifications and also expansion to include assessment encompassing virtualization technologies. Previously the wording for the requirement was simply "Implement only one primary function per server".

V2.0 Requirement	Corresponding V2.0 Testing Procedures
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only on primary function per virtual system component.	2.2.1.a For a sample of system components, verify that only one primary function is implemented per server.
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.

The PCI SSC is actively evaluating the impact of different technologies on PCI environments including virtualization. Requirement 2.2.1 directly addresses questions that customers and QSAs had about virtualization since many CDEs now include virtualized servers.

Evolving requirements:
The significantly updated requirements are generally found in the "evolving requirements" category. The most significant change is that a risk-based approach must be used when addressing vulnerabilities. This affects requirements 6.2, 6.5.6, and 11.2. Specifically, 6.2 is a new requirement which states:

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

Requirements 6.5.6 and 11.1 build upon requirement 6.2, by focusing common coding vulnerability prevention and scanning issue resolution on "high" vulnerabilities. Per notes in requirement 6.2, it is not actually required until July 2012, and is a best practice until then. The requirement enables the practice of reducing overall risks by being able to prioritize which issues need to be addressed more urgently, rather than treating them all the same. As mentioned in the requirement, a company can use CVSS scores as one of the inputs into the risk ranking process.

PCI PA-DSS changes

Significant changes in PA-DSS are highlighted here.

Requirement 4.4 is a new requirement to facilitate centralized logging, aligned with PCI DSS #10.5.3. The two associated testing procedures are listed below. The intent of the requirement is to enable integration with centralized logging applications. This is a useful requirement because it is typical to have multiple applications and to collect and filter their logs centrally for review and alerting.

Requirement 4.4 application must facilitate centralized logging
4.4.a Validate that payment application provides functionality that facilitates a merchant's ability to assimilate logs into their centralized log server.
4.4.b Examine the PA-DSS Implementation Guide prepared by the vendor to verify that customers and resellers/integrators are provided with instructions and procedures for incorporating the payment application logs into a centralized logging environment.

The vulnerability risk ranking and handling in PCI DSS Requirement #6.2 (and others) is also incorporated into PCI PA-DSS via requirements 5.2.6 and 7.1. The PCI PA-DSS requirement is required starting in 2011, unlike the PCI DSS associated requirements which are best practices in 2011 and "hard" requirements in July 2012.

Both PCI PA-DSS 5.2 and PCI DSS 6.5 previously referenced OWASP (and OWASP top 10) as the recommended industry best practices coding guide. In the respective v2.0 standards, other guides are mentioned along with OWASP as references – SANS CWE Top 25 and CERT Secure Coding specifically.

Summary

Some of the major highlights from the new PCI v2.0 standards were reviewed in this article. The new standards should be easy to adopt since there are only two new requirements (vulnerability risk ranking and payment application facilitation of centralized logging). The PCI SSC is adapting to current technologies as shown with the incorporation of clarifications regarding some virtualization technologies in PCI DSS. In general the new standards make life easier for vendors, customers, and QSAs since a lot of clarifications and updates were made. atsec has also recently written two other interesting PCI articles:

Cryptographic Algorithms for the Payment Card Industry v2 - http://atsec.com/downloads/white-papers/cryptographic_algorithms_PCI.pdf
What to Expect From a PCI QSA Led Assessment -http://atsec.com/downloads/presentations/What_to_expect_from_a_QSA_assessment.pdf

NEWS

Common Criteria Forum Established

The Common Criteria represents more than just a security standard; it also serves as a global consortium of interested parties including international schemes, labs, and vendors coming together to work on shared goals. As such, communication between these groups has become increasingly reliant on attendance at events like the annual ICCC conference. The need for an additional means of interaction, such as a forum that allows for international participation, was identified at this year's ICCC Conference, and has now been realized as a Google Group.

The forum can be accessed at this address: http://groups.google.com/group/cc-forum

The goal of this forum is to improve the Common Criteria standard by increasing communication and transparency within the broader community, and by enabling active collaboration between schemes, labs, and vendors.

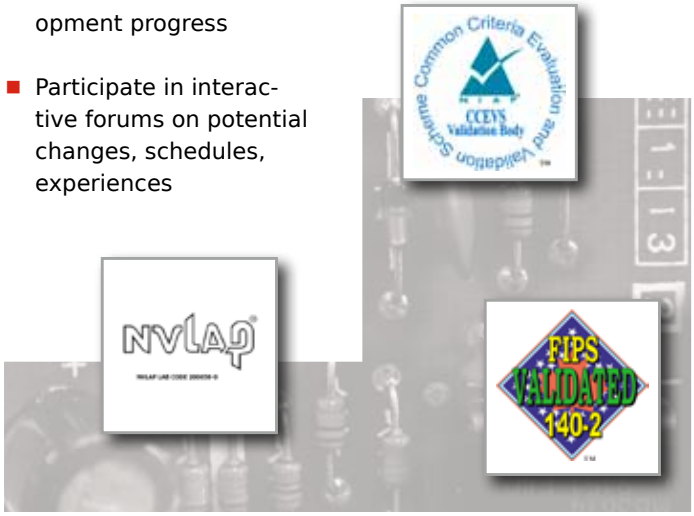
The Common Criteria Forum is set to provide:

- Immediate access to information on a global basis across time zones
- Fast turnaround of input from the Common Criteria community
- A place to launch sub-communities and other related groups

The Common Criteria Forum would bring together interested parties who could:

- Create/access pertinent blog articles and the sharing of ideas
- Post regular updates on Protection Profile development progress
- Participate in interactive forums on potential changes, schedules, experiences
- Have interactive discussions on how to improve the Common Criteria

We invite you to become a member of this group and to take an active role in the Common Criteria community.



2010 MILCOM Conference Experience

We recently visited the 2010 MILCOM (Military Communications) conference and trade show in San Jose, CA. and found it to be a worthwhile experience; the size and flash rivaled the RSA conference. The conference portion of the event was also substantial, with many simultaneous tracks in both unclassified and classified sections. The quality of the presentations that our group attended was excellent, and at conferences, that is not always a sure thing.

A few of the things we learned: while "smaller," "lower power," "faster," and "better" are always the main themes for communications equipment, "security" is taking an even higher-than-usual place in the requirements this year. Many vendors were saying that their DOD customers were really pushing them to meet the FIPS 140-2 Cryptographic Standard for Sensitive but Unclassified Data. Because waivers for this standard have been disallowed since FISMA (Federal Information Security Management Act) came into effect just after 9/11, this is not a surprise. But that it is finally happening is noteworthy. However, the most unusual thing we heard is that the DOD is now requiring CC (Common Criteria) testing for many new purchases of networking equipment. In the future, network devices and appliances -- like routers, firewalls, switches, and intrusion detection and protection devices -- will need to be CC evaluated and certified.

As a side note, the NIST SCAP (Security Content Automation Protocol) folks are moving ahead on standards for XML language communications between network devices. After this is in place, there are going to be some very secure and interoperable network devices available. The purpose for this, in the long run, is the ability to achieve networks that can sense attacks and respond by reconfiguring (or even disconnecting) until the threat is eliminated.

Next year, MILCOM returns to the East Coast at the Baltimore Convention Center, which should bring back the throngs of Beltway folks and raise the attendance to overflowing.

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