atsec the information security provider
NEWS
04/1013

首届国际密码模块会议(ICMC 2013)

2013年9月24日至26日首届国际密码模块会议（ICMC：International Cryptographic Module Conference）将在美国马里兰州Gaithersburg area召开。该会议目的是汇集来自世界各地的专家共同探讨密码模块的话题，着重于他们安全的设计、实施、保证和使用，参考两个新的且已经建立的标准如：FIPS 140-2 和ISO/IEC 19790。

我们的重点是吸引来自工程和研究领域、测试实验室、政府组织、产品采购者、密码模块的开发和管理员，以及学术界的参与者。我们的活动包含一天的研讨会和课程，随后是两天的30分钟演讲（加上15分钟的问答）。我们征求高质量的论文和相关研讨会的建议，这些将针对密码模块相关的社区感兴趣的主题展开，如:

- 密码模块的管理领域
- 包括 FIPS 140-2、ISO / IEC 19790、FIPS 140-3
- 物理安全和硬件设计
- 密钥管理
- 随机数生成
- 旁信道分析（Side channel analysis）、非侵入性的攻击（non-invasive attacks）
- 密码算法的选择和执行
- 开源中实现的密码模块
- 混合系统、嵌入式系统
- 工具和方法

本委员会支持独立于厂商的演讲者，着重于密码模块的实际的设计、测试和使用。产品厂商将被鼓励去寻求客户和合作伙伴，他们作为讲演者也可能成为前线的执行者。

访问 http://icmc-2013.org/wp/获得更多信息。

请所有有意向的作者使用如下链接提交他们的摘要和研讨会建议：
http://icmc-2013.org/wp/?page_id=35

若有任何关于提交物或会议的一般性问题，请联系我们：info@icmc-2013.org.

atsec 支持供应链认可标准

德克萨斯-奥斯汀，开放可信技术供应商标准(O-TTPS：Open Trusted Technology Provider Standard)的第一个版本由开放群组可信技术论坛（The Open Group Trusted Technology Forum）发表，atsec 提供了支持工作。

该新标准可以在 Open Group 免费获取，该标准使用了 Open Group 所建立的共识过程完成标准开发，汇集了许多生产和使用商业成品组件（COTS）的信息和通信技术的领导机构。这些机构来自行业、政府机构和 COTS 供应链全球性机构的代表。

atsec 被赋予特权致力于 O-TTPS 的开发工作，贡献了在 COTS 产品及其开发、生产和分发过程的评估和测试的丰富专业知识。

O-TTPS 奠定了认证体系的基础，该认证体系目前正在由 Open Group 开发和试运行。

该认证体系将允许 COTS ICT 产品的全球供应商去证明他们遵循行业标准的最佳实践，是与 COTS ICT 产品大多数用户所关心的威胁相关风险减缓的重要因素，即那些假冒产品和恶意污染产品的防范。

atsec 期待支持标准的实际应用，这将会为 COTS ICT 计算机安全宏观发展做出巨大的贡献。

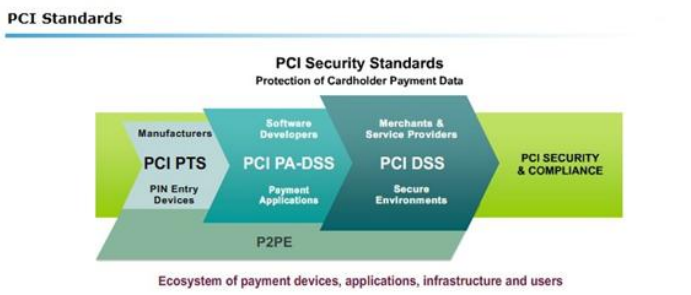
如何有效地实施 PCI DSS 所要求的文件完整性监控措施

高向东，刘岩（atsec 中国）

一、什么是PCI DSS？

为应对支付卡产业（Payment Card Industry）中所面临的各种安全问题，美国运通（American Express）、美国发现金融服务公司（Discover Financial Services）、JCB、全球万事达卡组织（MasterCard）及Visa国际组织五家支付品牌共同建立了支付卡行业安全标准委员会（Payment Card Industry Security Standards Council，英文简称为PCI SSC）。目前为止，PCI SSC主要维护了四个安全标准，即PCI DSS（Payment Card Industry Data Security Standard 支付卡行业数据安全标准）、PCI PA-DSS（Payment Card Industry Payments Application Data Security Standard支付卡行业支付应用数据安全标准）、PTS（PIN Transaction Security PIN传输安全标准）以及P2PE（Point-to-Point Encryption端对端加密标准）。atsec是经过PCI SSC所授权的安全合规评估机构QSA和经过认可的弱点扫描机构ASV。

下图较为宏观的体现了这四个标准之间的关系。



这些标准的目的是为了应对不同层面出现的持卡人数据的安全问题。（关于 PCI-PTS、PCI-DSS、P2PE 和 PA-DSS 更多的介绍，可参见 PCI 官方网站 www.pcisecuritystandards.org 和 atsec 官方网站 www.atsec.cn）。

PCI-DSS标准适用于涉及持卡人数据的处理、传输和存储的系统组件及其相关的管理措施，共包含了物理安全、网络安全、应用安全、人力资源、安全管理体系等6个方面的12大要求。

二、为什么PCI DSS会要求文件完整性监控措施？

基于防范黑客对持卡人环境所产生的破坏，PCI-DSS V 2.0版本在第11.5章节明确提出了对涉卡的服务器系统实施文件完整性监控的要求。内容原文（英文）如下：

11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

对于多数PCI DSS合规机构而言，实施难度较大，实施经验也较为欠缺。对于首次执行PCI-DSS合规的机构而言，则通常需要考虑并搭建文件完整性监控机制与措施。

基于PCI-DSS项目咨询的经验看来，文件完整性要求的根源来自于应对和避免黑客攻击成功后对系统产生的破坏和非法篡改。笔者之所以将PCI-DSS所要求的文件完整性监控要求定位于应对黑客的破坏和非法篡改，主要体现在如下两个方面：其一，文件完整性监控的覆盖范围基本上是按照黑客获得系统控制权后所企图修改和破坏的文件（比如所提及的可执行文件、审计踪迹、配置文件等）来考虑的；其二，通过定期比对发现关键文件异常的方式也主要是发现黑客破坏的痕迹。

由此看来，大家通过一个典型黑客攻击的步骤（搜索、扫描、获得权限、保持连接和消除痕迹）来把握，则文件完整性监控主要避免保持连接和消除痕迹过程中的影响，则11.5的要求就清晰多了。

三、如何实施文件完整性措施？

为避免因对该要求把握不够清晰而做很多无用功的情况，笔者建议从以下角度降低文件完整性监控的实施难度：

1、系统组件范围

文件完整性工具的安装范围主要是服务器。其范围包括了各类的操作系统，如windows, unix, linux等。

2、关键文件的范围

从黑客恶意篡改和破坏的角度，关键文件主要指日志文件，重要的系统可执行文件、应用可执行文件，配置和参数文件等。

a.操作系统级别可执行文件：

此处的操作系统级别的可执行文件主要指的是系统目录下的可执行文件，典型的情况如linux操作系统下的/bin和/sbin目录，windows操作系统下的/windows目录等。其范围建议包含所有重要的可执行文件的路径。如考虑范围的精简，建议基于如下原则进行梳理和简化：

- 破坏该执行文件后，系统的运行环境会被破坏，出现系统的不稳定等情况。
- 文件的执行权限高，一旦被控制，影响的范围大。
- 文件运行频率高，被植入恶意代码后，在很大程度上将得到执行的可能。

b.应用级别可执行文件：

此处的应用级别的可执行文件主要指的是自研程序中的可执行文件。通常建议监控应用程序所在的路径下的相关文件，如可执行文件、程序包文件等。

c.配置和参数文件：

此处的操作系统层面的配置文件主要指处于操作系统层面的配置文件，典型的系统层面配置文件如/etc/hosts。应用层面的配置文件主要指自研程序的配置文件。

d.日志文件：

这里所指的日志文件是指持卡人数据环境内以文件方式存在的日志文件（包括但不限于操作系统产生的日志，应用程序和中间件软件产生的日志，网络设备和安全设备产生的日志），存在数据库内的日志不在文件完整性监控的范围之内。

3、监控机制的选择

文件完整性监控的主要目的是在事后发现黑客的恶意破坏（如删除文件、植入rootkit等），可采用定期比对的方式（推荐比对sha-1哈希结果），对如下文件完整性事件时给出告警信息：

- 文件被未授权访问或者读取（包括成功或者失败的状态）（如果此处的访问读取通过日志监控的实施达到日志记录的要求，则按照标准基线要求文件完整性方案可以不监控针对文件的读取）；
- 文件内容被修改或者未授权篡改；
- 文件被删除；

当然，如果性能上可接受，也可以采用实时的针对关键文件的监控与告警机制。比如通过监控对关键文件读写的I/O,并将改写行为实时告警出来。

四、可考虑的方案

基于PCI DSS要求，有众多方案可选择，如下：

1、使用开源或商业软件

目前可用的软件较多，大家可以基于实际情况进行选择。这些软件通常可以实现单机部署，也可以实现客户端和服务器架构部署。通过Hash算法等比对方法来检测和报告系统中任意文件被改动、增加、删除的详细情况，以用于入侵检测、损失的评估和恢复、证据保存等多个用途。在产生规则不允许的事件后，这些软件通常具有告警机制，以便安全响应人员对异常行为及时做出响应。

无论是开源软件，还是商业软件，均可以通过安装和配置达到合规的要求。开源软件的获取成本较低，但需要实施人员具有较强的实施经验，如果需要atsec可以提供这个领域的协助和支持；商业软件相对易于实施和维护，但通常会产生软件获取方面的成本。

2、自主开发

在对文件完整性监控机制有充分了解的基础上，可以通过开发相应的应用程序来实现。其方法首先是定义关键文件，然后对文件的改动进行识别（如通过截取文件的I/O，或者比对文件的摘要值），最后在集中端对改动的情况进行告警和排除。

其优点在于可基于标准要求和操作系统状态进行灵活的控制，但这需要投入较多的开发资源。

3、使用操作系统自带的工具或脚本

操作系统本身自带的工具或脚本也可以用于达到文件完整性监控的目的，比如windows下的powershell，linux下的sha1sum等。这些均具备对文件完整性的监控，然而对于关键文件的定义以及对完整性被破坏时的告警则需要相应的辅助手段。

在AIX下的audit子系统则提供了一种纪录系统安全方面信息的方法，同时可以为系统管理员在用户违反系统安全法则或存在违反的潜在可能时，提供及时的警告信息。详细的关于配置内容参见http://www.redbooks.ibm.com/abstracts/sg246396.html?Open提供的Accounting and Auditing on AIX 5L。

该方案无需安装额外的软件，但通常需要在维护和定制化方面需要有较多的资源投入。

atsec 中国完成银联商务 PCI DSS 合规性评估

atsec很荣幸地宣布：银联商务有限公司（中文简称“银联商务”，英文简称"ChinaUMS"）通过了atsec基于支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standards）v 2.0版本的符合性评估。

对于银联商务成功且顺利通过此次 PCI 合规建设，银联商务有限公司副总裁张永涛表示：“银联商务通过 PCI DSS 审核认证是国际权威组织对于银联商务的肯定，体现了银联商务在支付行业内技术安全领域的领先地位，同时也宣告银联商务安全解决方案达到国际领先水平。面向未来，银联商务将以更加专业的服务技术，努力为客户提供安全的高品质的综合支付服务，继续为改善银行卡受理市场和国内综合支付环境贡献力量。”

atsec中国项目经理高向东对于本次PCI成功合规表示：“首先感谢在整个项目过程银联商务领导和团队所给予的大力支持和配合。项目之初，双方团队紧密配合，积极沟通，通过梳理业务和系统有效地精简了持卡人数据环境范围，为完成合规建设提供了良好的基础。银联商务充分而合理地利用了虚拟化、双因素控制等安全技术，按照既定计划有效地达到了PCI DSS的基线要求。”

atsec 中国成功完成和融通 PCI DSS 合规性评估

atsec很荣幸地宣布：北京和融通科技有限公司（中文简称“和融通”，英文简称"HRT Payment"）通过了atsec基于支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standards）v 2.0版本的符合性评估。

对于和融通成功且顺利通过此次PCI合规建设，和融通副总经理刘文广表示：“非常感谢atsec和我们的团队紧密配合，共同完成本次高效且高质量的PCI DSS合规建设。PCI DSS合规也进一步提高了我们的安全体系架构和系统安全性，更加有效的保护持卡人数据的安全传输、存储和处理。我们期待与atsec进一步的长期合作。”

atsec中国业务发展总监白海蔚对于本次PCI成功合规表示：“和融通作为国内某些主要收单机构的支付服务提供商，本次PCI DSS合规项目责任重、时间紧，也因此选择具有诸多行业经验且拥有本土强大服务团队的审核机构atsec共同致力于标准的合规建设工作，使得完整的项目在3个月之内高效且高质量完成。项目过程中，atsec凭借多年来丰富的信息安全实践经验，与和融通一起攻克合规中的技术障碍。而和融通的项目团队也在本项目中体现了高度的责任心和专业的技术实力，相信PCI DSS的合规结果将为和融通的业务持续发展以及数据安全保驾护航！”

atsec 2013 年度首次 PCI DSS 培训成功在广州开展

*2013 年 2 月 28 日和 3 月 1 日，atsec 在广州开展了 2013 年度首场 PCI DSS 培训

本期培训中，在 atsec 的组织下，大家针对目前支付产业的一些热点且具有争议的安全问题进行了积极讨论和互动，比如持卡人在信用卡使用时是否需要设置密码、卡背面的最后三位数字（CVV2）是怎么定义的、快捷支付的安全与便捷等等。这些问题虽然并不是 PCI DSS 作为数据安全标准的核心和重点，然而作为抛砖引玉，atsec 的培训也引发了各位支付安全专家针对各类实际工作中遇到的支付安全话题的积极研讨，来自银行和支付服务提供商的专家们给予了专业的诠释分析。同时，来自卡厂的专家们还与大家分享了在物理环境安全方面更高要求的最佳实践。

atsec 在上海成功开展 PCI DSS 培训

*2013年3月28日和29日，atsec在上海开展为期两天的PCI DSS培训。

在本次培训中，atsec首先整体介绍了PCI DSS合规建设的思路和实施要求，把PCI DSS的完整要求按照持卡人数据环境的范围确定、网络架构、安全运维三个方面进行讲解，并以模拟案例分析和研讨的形式进行现场的讲解和讨论，剖析了项目实施中的一些重点和难点，从而更加深入的帮助现场学员们理解PCI合规的要求。

艾特赛克（北京）信息技术有限公司
北京市海淀区上地七街1号
2号楼119室 100085
电话：+86 10 84834011
传真：+86 10 82890017
Email：info_cn@atsec.com