atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

迎接支付安全的挑战，期待支付安全的春天

atsec，刘岩、陈谨运，2011 岁末

谈及支付方面的信息安全问题，支付产业的机构通常都会马上考虑到应对措施，比如加密技术、日志管理、网络优化、主机加固，甚至机构自身的安全意识教育。而笔者认为，支付相关机构的信息安全工作应以保护客户的帐户安全作为首要出发点，而不是仅仅考虑保护卡片信息。针对信用卡的用卡安全，我们都知道任何情况下在授权交易完成之后，商户、服务提供商、收单机构均不允许存储敏感的认证数据，然而，设想如果机构由于用户的体验原因，违规的存储了诸如 CVV2/CAV2/CVC2/CID 等敏感的认证数据，即使部署了 IDS、聘请资深的安全专家、且短期业务发展迅速，但是你的客户将可能遭受由于公司行为而导致的信用卡盗用的危害，且由此可能对其他的合作机构的利益带来损害，这样的风险又怎能接受呢？可以看到，国内的信用卡持卡人的用卡安全意识越来越强，作为持卡人的广大用户是不会介意由于保护个人的用卡安全和隐私而再次交易时提供 CVV2 的。故而笔者认为，支付的整体信息安全需要各个机构针对数据保护给予共同重视的态度。

笔者谨以此文分享来自支付安全产业会议对于全球范围的一些数据统计，随后将重点关注新的技术和趋势，特别是 EMV、支付应用安全和移动支付等，最后笔者分享 PCI DSS 信息安全合规工作中所需要关注的重点和难点的部分心得。

PCI 社区会议

2011 年欧洲社区会议于 2011 年 10 月 17 日至 19 日在伦敦召开，北美社区会议于 9 月 20 日至 22 日在美国亚利桑那州斯科特斯德召开。2012 年度的北美社区会议将于 2012 年 9 月 12 日至 14 日在佛罗里达奥兰多举办。

五大信用卡组织共同成立支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）至今已有五年，今年（2011）和去年（2010）PCI 年度社区年度会议（Community Meeting）参与总人数均已分别超过了 1000 人，与早先 2007 年度的 343 参会者比较，有了较大幅度的增长。这些参与者来自于世界范围 40 多个国家的 600 多家大型银行、商户和处理者。涉及的行业包括但不限于航空、教育、金融服务、政府、医疗、IT 硬件和软件、IT 服务以及零售等行业。全球范围的参与者一同为 PCI 标准的发展和支付安全出谋划策，共同改进提高对持卡人数据的安全保护措施。在 PCI DSS 和 PA DSS 标准的三年生命周期内，最终也是主要环节就是广泛的征求支付卡产业内的反馈意见和建议。

据统计，目前 PCI DSS 合规状态并不理想，整体来讲全球范围参与统计的机构中约 89% 的机构还没有达到 PCI DSS 的合规建设。然而值得鼓励的是这些参与统计的机构大多已经开始致力于 PCI DSS 的合规工作。

新趋势和发展

2011 年，支付产业在安全领域特别给予了以下几个方面的最新指导： EMV、基于电话线路的持卡人数据的保护、虚拟化技术、Tokenization、无线、支付应用和移动支付。下面笔者将逐一简要介绍其趋势和情况。

EMV

EMV 和 PCI DSS 均是应对支付卡欺诈和数据泄露的重要基础，EMV 降低了针对现场面对面交易环境的伪造卡片的风险，而 PCI DSS 依然是 EMV 环境中降低欺诈风险的必要要求，故而 EMV 和 PCI DSS 的有效结合将是减少欺诈并提高安全的有力途径。PCI SSC 在 2010 年 10 月份已率先发布了 EMV 指导的初步版本。

基于电话线路的持卡人数据的保护要点

针对基于电话线路的持卡人数据，需要识别持卡人信息获取的位置和方式，制定明确的方法禁止存储语音记录中的敏感认证数据，针对禁止/消除数据存储的控制措施应进行文档化记录，并进行验证。

作为商户，应该对其合作的呼叫中心进行监管，查看其如何实现 PCI DSS 的合规。

虚拟化

今年 6 月份，PCI SSC 发布了虚拟化指导。PCI SSC 提出了虚拟化技术的指导，识别了针对 PCI DSS 控制领域特殊相关的虚拟化技术的特性。

总体来讲，目前并没有一个单一的方法或者解决方案可以安全地进行虚拟化环境的配置。虚拟化技术具有诸多的应用，适用于某一个实现的安全控制可能不能够很好的满足其他应用的要求。每一个环境将需要根据特定的设计和配置，进行单独地评估。

该指导给出了一系列针对虚拟化环境的安全考虑，并识别了在同一主机范围内和范围外的组件合理分隔维护工作的挑战。由于这些挑战的存在，我们鼓励机构可以考虑在整个虚拟化环境内使用 PCI DSS，因为该标准提供了针对整体保护环境的安全基线和分层方法。

针对云架构，根据不同的云服务和/或实现，职责将会有所不同。公共的云环境需要关注复杂度的增加、动态边界、底层架构受限的可见性或控制。

Tokenization

Tokenization 技术解决方案的主要目的是将敏感的 PAN 数据替换为非敏感的 Token 值。Tokenization 技术可能无法从根本上规避 PCI DSS 合规的需要，该技术能够帮助减少 PCI DSS 合规建设范围的系统数量，并能简化 QSA 验证的工作量。Tokenization 解决方案根据不同的实现可能具有非常大的差异，比如不同的开发模式、Tokenization 方法和技术。

如果机构考虑使用 Tokenization 的解决方案，我们鼓励机构针对该方案彻底地执行业务影响分析的评估和持卡人数据环境引来变更的风险评估，从而确定特定的环境需要和特性，包括支付过程。该技术对于持卡人数据安全的分层实现方法具有价值。

机构应考虑 Tokenization 部署的类型是否能够最好的满足其精简持卡人数据环境和业务运转的要求，并且决定方案管理职责的相关细节。

Tokenization 解决方案提供商（TSP：Tokenization solution provider）应比较其方案如何满足 PCI SSC 提出的指导，并确定如何帮助其客户实施方案以满足 PCI DSS 的合规要求。

总体来讲，TSP 应负责设计有效的 Tokenization 解决方案，商户最终负责确保其环境满足 PCI DSS 的要求，而且范围内所有的组件都是年度 PCI DSS 合规评估的一部分。

某个系统如果仅仅包括了 Token，它并不是自动地会被排除于持卡人数据环境（CDE）范围之外。机构必须合理的分隔 Tokenization 系统和 CDE，且必须确保 Tokenization 系统不具有从 Token 到 PAN 的转换能力。

PCI SSC 和评估机构 atsec 均鼓励机构能够尽可能的精简持卡人数据环境范围，比如在尽可能多的位置使用 Token 替换 PAN 的存储；对现有 PAN 的捕获点和数据值进行限制；将 Tokenization 与 P2PE 相结合，使得商户任何情况下都看不到持卡人数据；确保所有 PAN 数据在源系统上安全删除；选择解决方案确保商户一旦获取 Token，不能抽取出 PAN 的信息。

最后，当我们审核 Tokenization 解决方案时，机构应充分考虑该方案是否满足适用的 PCI DSS 的要求，这有助于机构 PCI DSS 的合规建设，且生成 Token 之后可以消除机构存储或者访问持卡人数据的需要。

无线

谈及无线安全，无线特别工作组（Wireless SIG）和 PCI SSC 早在 2009 年就发布了针对于该领域的补充说明，并于近日进行了更新。更新的版本更好的与 PCI DSS v2.0 版本相一致，且包括了针对安全蓝牙技术的额外指导。

出于物理层面对无线访问点的安全性考虑，机构应特别关注维护相关的最新硬件资产清单。

该更新指导也给出了一系列的方法，从而满足 PCI DSS 的要求 11.1，包括自动扫描工具（如无线扫描和分析、无线 IDS 和 NAC 控制），详细组件和网络的物理和逻辑审查，以及恶意设备检测的建议。

人员培训和安全意识教育对于识别恶意无线设备是非常重要的环节，根据环境的大小和复杂度、授权的无线技术以及其他环境特定因素和检测的方法可能有所不同。

支付应用以及移动支付

支付应用（PA：Payment Application）和移动支付的安全性一直是笔者所关注的领域。

针对 PA DSS 标准，和 PCI DSS 类似，2011 年 12 月 31 日 PA DSS 旧版本 v1.2.1 正式过期而不在使用（针对新的评估验证），对于已有的已经通过 PA DSS v1.2.1 验证的支付应用将于 2013 年过期需要进行重新评估。

2011 年 6 月，PCI SSC 发布了针对 PA DSS 和移动支付安全相关的指导。

该指导识别了目前针对不同类型的移动应用支付产业的接受情况。简而言之，目前移动支付接受类别 1 或类别 2 的应用进行 PA DSS 的评估，包括 PTS 认可设备上设计的应用和其他专有 POS 功能的设备。而类别 3 的应用（一般目的的智能设备）目前还不能被 PCI 产业接受，也不能执行 PA DSS 验证。而 PCI 标委会和产业也正在积极调研这类应用支持 PCI DSS 合规环境的能力，相关设备、指导和潜在的标准也正在研究。

对于移动支付，PCI 标准委员会设置了一个任务组进行该产业专项的协调和调研工作，并推动相关产业指导的发展，比如 OWASP 移动项目、Global platform、GSMA、BITS、NIST 和 ANSI/ISO。

atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

PCI DSS 合规经验分享

atsec 基于业界和产业的积累，将整体 PCI DSS 合规工作依据实现目标的优先级分为六个里程碑（Milestone，以下简称 MS）。大体来讲，MS1 的目标为删除敏感认证数据并限制数据的存储；MS2 的目标为保护边界、内部和无线网络；MS3 的目标为安全的支付卡应用；MS4 的目标为监控和控制系统的访问；MS5 的目标为保护存储的持卡人数据；MS6 的目标为完成所有的剩余合规工作，并确保所有的控制措施到位。对于初次致力于 PCI DSS 合规工作的机构，可以参考该里程碑涉及的要求分阶段进行整改。

而从实现的难度来讲，不同的机构根据现状的不同需要解决不同的技术难点和整改内容。如下的要点是笔者根据以往项目经验，简要提炼出现实持卡人数据环境实施整改中需要较为关注的层面：

- 持卡人数据的保护（可以考虑采用加密系统以及与之相关的密钥管理流程，或者产业认可的补偿措施来实现对持卡人数据的保护）。
- 安装的最新补丁。这个貌似基本的要求，真正在生产环境实施时却可能具有一定的难度和压力。从安全角度的考虑以及 PCI DSS 的标准要求，严重级别漏洞补丁的安装是必须的。建议在安装补丁之前先对其测试，在补丁安装的时候如果是 windows 系统平台可以采用自动化的方式完成补丁的分发控制，比如采用 WSUS 系统等。
- Linux 防病毒系统的安装，通常可能是致力于 PCI DSS 之前被忽略的环节。
- 密码复杂度的正确实施。
- 测试环境中不允许使用真实卡号。
- 非法无线热点的监测，可以部署无线 IDS/IPS，然而也可以考虑定期的使用工具进行监控。
- 完善的工作职责和权限记录，人员安全意识培训和技能培训等。
- 制定并完善加固手册，并对持卡人数据环境之内的系统组件实施加固。
- 物理安全，如机房的访问控制系统，系统组件的物理保护，持卡人数据环境监控系统的部署等。

参考 PCI 年度会议上来自 British Airways 自身 PCI DSS 合规经验分享，如下几个要点值得其他致力于 PCI DSS 合规建设的机构借鉴：

- 考虑保护客户的用卡安全，而不是关注在卡片本身；类似笔者在本文之初所引出的保护客户的用卡安全，机构应重视信用卡欺诈为客户带来的严重后果；
- 寻求正确的合格安全评估机构 QSA，好的 QSA 可以帮助机构解决实际困难，而不是仅仅重复标准的要求，好的 QSA 将成为你的朋友；
- 参加 PCI 培训；
- 识别威胁；
- 得到高层支持；

- 创建良好的沟通；
- 尽可能自己找寻解决方案；
- 正确实施技术解决方案，解决方案可以更好的满足机构自身的要求，同时达到 PCI DSS 合规的要求。atsec 积累了完整的 PCI DSS 的解决方案，其中相当一部分是免费开源工具的采用，可以在满足要求且稳定应用的基础上，节省投入；
- 激励系统、数据库、应用等管理员，使其更好的协同工作，达到最终的 PCI DSS 合规建设；
- 正确实施对于持卡人数据环境以及内部的访问控制；
- 尽可能的分割和优化网络，其主要目的不是为了减低审核费用和时间，而是为了降低机构的风险；
- 关注人员的问题，包括机构的员工、客户、供应商等，这些都是重要的因素，不能仅仅关注技术层面；
- 评估第三方，确保机构的第三方合同包括合理的 PCI 合规要求条款；
- 合规工作应深入到业务正常运转，不断地持续改进，满足年度审核的要求。

伴随着整个支付产业的繁荣发展，支付安全的相关问题也越来越严峻地展现在业界面前，而诸多新兴的技术和趋势也增加了支付安全的复杂度。atsec 希望通过自己的贡献为支付行业信息安全的发展和提高尽自己的微薄之力。