atsec the information security provider
NEWS
11/2010

最近新闻一览

首信易支付于2010年10月成功通过了atsec针对其持卡人数据环境的PCI DSS合规评估

atsec完成皮尔森（Pierson）MIIKOO的五个密码算法的CAVP测评

atsec完成中兴两个模块诸多密码算法的CAVP测评

和往年一样，atsec多位专家顾问于2010年9月底参加在土耳其安塔利亚举行的第十一届ICCC会议，并在会上发表主题讲演
（参见第二页的短 文分享）

atsec于2010年9月参加奥兰多举行的PCI安全标准委员会社区会议

风河公司（Wind River）将第一款嵌入式Linux系统提交美国国家信息安全保障合作组织（NIAP）进行EAL4+认证

BSI和atsec发布操作系统保护轮廓（OSPP）

atsec对两个多功能打印机的IEEE保护轮廓进行评估

IBM’s(R)z/OS(R)Version 1 R. 10系统SSL密码模块获得FIPS 140-2认证

国民技术（Nationz）密码算法于2010年8月实现通过密码算法验证体系（CAVP）的认证

易宝支付于2010年6月成功通过了atsec针对其信用卡还款业务持卡人数据环境的PCI DSS合规性评估

atsec Steve Weingart 在2010年度IEEE VLSI测试研讨会中发表讲话

更多的新闻，请参见我们的网站：
www.atsec.com

在atsec，我们一直努力不断充实我们在信息安全领域的知识和专业技术，并且努力的为我们的客户提供更好更广泛的服务。对员工坚持不懈的培训、与国际信息技术安全标准委员会的投入，以及与业内同仁之间持续不断的交流就是我们所致力于事业的例子。我们现在在这一方面有了进一步的方向：我们很荣幸的宣布标准实验室（Criteria Labs）和atsec信息安全达成合作协议，将标准实验室提供的硬件测试和故障分析的重要资源与atsec提供的安全测试和评估技能整合起来。我们可以针对以基于芯片设备的安全测试提供扩展的服务和先进的美国设备，这些产品诸如智能卡、RFID、ASIC、FPGA和嵌入式系统。Criteria实验室位于德克萨斯州（Texas）奥斯汀（Austin）和科罗拉多州（Colorado）彭罗斯（Penrose），其拥有大量的微电子故障分析处理能力，包括声显微镜（Acoustic Microscopy，CSAM）、扫描电子显微镜（Scanning Electron Microscope，SEM）、实时X射线成像（Real Time X-Ray）、研磨切片（Cross Sectioning）、微细探针（Micro-Probe）、光学显微镜（Light Emission Microscopy）、De-Cap（Wet）、激光打印（Laser Marking）、结构分析（Construction Analysis）、平行抛光（Parallel Polishing）、Front Lapping、闩锁效应（Latch Up）/电荷过载压力（EOS）、静电释放（Electro Static Discharge，ESD）、数码图片抓取（Digital image capture）和焊锡性试验（Solderability Testing）。他们的设施包括无污染的测试间和活动的测试楼层。标准实验室也通过了MIL-PRF-38535/883认证来测试军事和国防电子产品。 atsec信息安全，总部位于德克萨斯州（Texas）的奥斯丁（Austin）（在德国、瑞典和中国分别设有分支机构），提供安全评估和测试服务。atsec在通用评估准则（Common Criteria）评估和FIPS 140-2（密码模块）测试和咨询服务具有多年的历史，针对来自业界领导厂商的各类产品和应用，包括HP、IBM、Microsoft、Red Hat、Honeywell、Apple、Samsung和NationZ等。atsec为包括ISO/IEC 15408以及即将提出的关于物理安全攻击、缓解技术和安全需求的ISO技术规范在内的安全标准作出了重大的贡献。atsec和Criteria实验室展现了针对美国市场的高质量且独立的设备和专业技术。我们也为两个实验室的客户提供了改进和扩展的服务。

- **在atsec成立的第一天我们宣布的原则是：**
- **专业**
- **专注**
- **独立**

最重要的是

- **诚信**

Salvatore La Pietra
CEO

感受第十一届国际 CC 会议

atsec，刘岩(yan@atsec.com)

第十一届国际通用评估准则会议（11ICCC：11th International Common Criteria Conference）如约而至，本届会议于 2010 年 9 月 21 日到 23 日在土耳其地中海畔美丽的城市安塔利亚（Antalya）成功举办。

本文简述了笔者参加会议期间的些许感受。或许诸多的关注通用评估准则（Common Criteria）的厂商、评估机构、信息安全专家同仁并没有直接参加本次会议，且会议期间很多的主题技术讲演是并行进行的，谨此短文作为信息的分享和交流，也欢迎指正和进一步探讨。

技术社区和保护轮廓的推进

历届的 CC 会议技术和标准发展的讨论和争论都是广泛存在的，大家的初衷都是为了改进 CC 标准及其应用。然而本届 CC 会议上对于技术社区（Technical Community）和保护轮廓（Protection Profile）的发展思路得到了极其广泛的共识和认可。

CC 标准作为世界范围公认的信息安全领域的标准，其适用范围涵盖到诸多的产品形态，包括但不限于访问控制设备和系统（Access Control Devices and Systems）、生物识别系统和设备（Biometric Systems and Devices）、边界保护设备和系统（Boundary Protection Devices and Systems）、数据保护（Data Protection）、数据库（Databases）、检测设备和系统（Detection Devices and Systems）、IC、智能卡和智能卡相关的设备和系统（ICs, Smart Cards and Smart Card-related Devices and Systems）、密钥管理系统（Key Management Systems）、网络和网络相关的设备和系统（Network and Network-Related Devices and Systems）、操作系统（Operating systems）、其他设备和系统（Other Devices and Systems）、数字签名产品（Products for Digital Signatures）、可信计算（Trusted Computing）。随着 CC 标准应用广度和深度的发展，业界同仁深刻的意识到在某特定产品类型领域加强技术探讨，以及保护轮廓（PP：Protection Profile）制定和推广的价值，比如在智能卡领域就是很好的成功范例。技术社区的思路就是整合特定产品技术领域的厂商开发人员、最终用户、评估人员，以及认证人员一起共同讨论，从而达成一定程度评估内容和方法的共识，特别是保护轮廓的制定。

这一思路在本届 CC 会议的关键主题讲演（Keynote）、专家座谈（Panel Session）以及诸多主题讲演上被提及并得到了高度统一。来自微软的 Steven B.Lipner 和 Cisco 的 Gene Keeling 作为厂商代表进行了会议的 Keynotes 发言。发言中表示产品的最终用户将是致力于 CC 合规和评估认证的受益者，最终用户希望评估在真实的场景下进行；智能卡领域是 CC 评估较为成功的应用领域，最新的提出的 OSPP 是业界的一大贡献。厂商代表呼吁更多的厂商能够参与到共同的厂商社区进行 CC 及其相关技术的研讨和推动，并加强与最终用户、评估实验室和认证机构的沟通，从而使得最终用户得到更大的收益， Cisco 已经组织诸多的机构成立了技术社区。比如在脆弱性评估，特别是 Attack Resistance（攻击抵御）等方面，需要各个厂商之间合作，以及整个产业的投入和平衡；同时对于特定的产品领域也需要吸取诸多的输入，比如 CVE（Common Vulnerabilities and Exposures）、CWE（Common Weakness Enumeration）、CAPEC（Common Attack Pattern Enumeration and Classification）等脆弱性的业界积累。

大会第一天上午，组委会安排了一项名为“满足用户的需求—PP 和技术社区的力量”的专题讨论，来自不同机构的专家共同探讨 PP 和支持文档的推进，从而更好地表达最终用户的需求，并且表示应该加强最终用户的参与和投入。在专家座谈中，多位专家表示 PP 本身的编写应借助优秀的评估实验室的技术力量，他们可以借助自身对于 CC 标准的深刻理解，通过和诸多厂商的共同努力完成 PP 的制定以及后续的评估和认证工作。

atsec 无疑是该领域的领导者，也是由于近年来在 CC 发展，特别是 PP 编写和评估的贡献，是唯一的在 Keynotes 被提及的评估实验室。atsec 早从 2009 年开始组织了业界诸多的厂商，政府认证机构发起了 Protection Profile（保护轮廓，也可以理解为某类型的产品标准）。首先值得一提的是操作系统保护轮廓（OSPP :Operating System Protection Profile），该 PP 由 atsec 负责编写，并组织了 Argus Systems、惠普、IBM(AIX 小组、z/OS 小组以及 Linux 小组)、Juniper Networks、微软、Novell (SUSE)、Oracle、Red Hat、SUN、Univention、BSI、NIAP 一同参与，组成了专家社区进行讨论，最后通过了 atsec 的评估和 BSI 的认证。在本届 CC 会议上，atsec 德国实验室主任 Gerald Krummeck 和 IBM 的 William Penny 继 09 年挪威 CC 会议的主题讲演之后，进行了联合主题讲演 – 针对操作系统的保护轮廓（Protection Profile for Operating System），来自德国认证机构 BSI 的 Gereon Killian 也发表了主题讲演 - 使用通用评估准则 OSPP 的模块性和灵活性（Operating System Protection Profile Modularity and Flexibility using the Common Criteria）。此外，atsec 代表 IEEE 对两个规定了不同环境下多功能打印机的安全功能和安全保障需求的保护轮廓进行了评估。IEEE 的两个保护轮廓 PP.2600.1 和 PP.2600.2 分别在美国认证机构 NIAP 和德国认证机构 BSI 进行了评估和认证，并且在会议第二天的庆典晚宴（Gala Dinner）上进行了证书颁发的仪式。

来自中国公安部第三研究所的技术专家陆臻进行了主题讲演 - The application of ISO/IEC TR 15446:2004 in the process of compilation of Chinese national standard “GB/T 20279-2006”，这也是整个会议 Protection Profile 部分的重要讲演主题之一。

此外，对于进一步 PP 的开发，将关注在诸多的产品领域，比如 USB 存储设备、企业安全管理、电子证书系统、安全签名等。

来自 atsec 的首席科学家 Helmut Kurth 在会议上发表了题为“提高保护轮廓的灵活性和适用性（Improving the Flexibility and Applicability of Protection Profiles）”，他本人参与了诸多业界 PP 和各个大型厂商 ST 的编写工作，并且对 CC 标准的发展起了重要的作用，如往年一样，他的讲演吸引了诸多业界专家的关注和学习。

最后值得一提的是，PP 的编制和贡献鼓励多个厂商参与，旨在推动同类产品的安全标准发展，而不是某厂商制定技术壁垒的途径，在 PP 中提及的安全功能要求和安全保障要求应该是具有普遍意义且较为通用的，且能够在同类厂商产品中获得实现。

标准技术的整合

CC 会议作为信息安全业界较为重要的会议之一，一向以来关注信息安全领域的诸多的标准和技术，以及其之间的关联和整合。

早在 2007 年罗马的 CC 会议上，atsec 的业务发展总监 Fiona Pattinson 便提出了 FIPS 140-2 和 CC 的相辅相成的合规建设思路。本届 CC 会议上，来自加拿大和美国的评估实验室继续致力于 CC 和 FIPS 140 的相关技术关联和依赖关系，给出了题为“FIPS & CC – How do they get along?”和“FIPS and the Common Criteria: finding the least common denominator”等主题讲演。

支付产业的安全问题得到了越来越多的重视，PCI 标准与 CC 标准关联的主题讲演是本届较新的关注点，同时也是笔者本人较为关注的技术领域。支付终端的安全评估在会议首日的下午便在 CC 社区报告部分给出了讨论，来自德国 BSI 的 Sandro Amedola 作了题为“JTEMS – A community for the evaluation of payment terminals”，无独有偶，随后来自法国的专家也作了“GESTE: a consortium fully supporting the CC adoption by payment terminals industry”的讲演。讲演中，各位专家提及了 PCI 安全标准家族对于支付产业的重要性，以及标准评估和认证的整合思路，同时也提出希望在不久的将来，两个不同标准能够得到在一定意义上的互相接受，比如 CC 领域能够一定程度的接受 PCI 评估实验室出具的 PCI 报告。对于 atsec 而言，atsec 既是国际三个国家授权的 CC 评估实验室，同时也是 PCI 安全标准委员会授权的 PCI DSS QSA 和 PA DSS QSA，我们希望看到相关标准的整合，并一如既往的致力于相关的标准工作。

标准和产业动态

评估实验室在各个国家体系下接受认证机构的监督和管理，同时各个国家的认证机构也需要接受 CC 管理委员会的严格监管。CCMB 通过 shadowing 和 VPA（Voluntary Periodic Assessment）的方式，保证各个国家认证机构的章程和流程和 CCRA 互认协定的要求相一致，也是保障标准互认的重要基础。

2009 年 9 月，针对土耳其认证机构执行了 Shadowing，2010 年 ES（ES :Executive Subcommittee）会提交报告给 MC（MC：Management Committee）主席，并在年底前进行投票。根据大会汇报，2010-2012 年期间，将分别针对加拿大、德国、荷兰、澳大利亚/新西兰、西班牙、挪威等国家执行 VPA。CCRA 成员目前共有 26 个成员国家，14 个国家可以颁发 CC 证书，共计 50 多个授权的评估实验室，对于实验室的监管也将持续严格，比如英国体系取消了之前的某些实验室的授权资格。目前有四个新的国家申请加入 CC 互认，有四个国家正在努力从认证接受国家（Certificate Consuming）申请成为认证颁发国家（Certificate Authorizing）。

Dag Stroman 先生也在会上介绍了 CC 管理委员会的最新任命情况。管理委员会（MC：Management Committee）主席为来自瑞典的 Dag Stroman，执行委员会（ES：Executive Subcommittee）主席为来自德国的 Irmela Ruhrmann，CC 发展组（CCDB：Common Criteria Development Board）的主席为来自英国的 David Martin，CC 维护组（CCMB :Common Criteria Maintenance Board）的主席来自于美国。

如往届一样，各个国家认证机构介绍了各自体系的变更情况。美国体系 NIAP 给出了最新 Policy 的介绍和解读，并得到了 CC 互认各个国家的广泛认同，特别是对于特定产品领域 PP 的开发和推动。

CC Version 4 正在制定过程中，目前已经完成了年度变更的内部版本，将提交给产业和工作组获得更多的反馈和交互。

美国将接管 CC 官方网站的相关工作，并将可能考虑网站的布局的进一步合理性。

从本届会议接受的论文情况来看，美国、德国、法国和西班牙发表论文数量较多，美国共发表了 18 篇论文讲演，德国共发表了 12 篇专题论文讲演，法国共发表了 10 篇专题论文讲演，西班牙共发表了 9 篇专题论文讲演。另外荷兰、英国、日本、土耳其均也在大会上发表多篇论文。来自中国信息安全监管机构、认证机构、评估机构，以及知名厂商的代表出席了本次会议。如前文提及，公安部三所的同仁发表了技术讲演。此外中国合格评定国家认可委员会（CNAS）实验室认可处的曹实处长与 atsec 的毛翊和刘岩合作完成了“成为 CNAS 实验室（Becoming a CNAS Laboratory）”的主题讲演，和各位与会专家分享了 atsec 中国成为 CNAS 认可实验室的意义、目的、过程经历，以及相关心得体会，得到了国际业界同仁的广泛关注。

本届 CC 会议从一开始到结束就展开了正式或者非正式的讨论，许多的参会者都表示希望能够有更多的交流的场所和机会。MS 的主席，来自瑞典 CSEC 的 Dag Stroman 最后给出了结束发言，也再次强调了本次会议的对于技术社区，产品 PP 等领域发展的技术共识，并鼓励大家不断创新，不断接受挑战，共同努力在不同的技术领域不同的地域实现风险管理上的共识。

会议的最后宣布了第十二届国际 CC 会议将在马来西亚的吉隆坡（Kuala Lumpur）举办。

atsec 信息安全成功完成中兴 CAVP 密码算法测评

2010/10/28

中国，北京 - atsec 信息安全荣幸宣布成功完成对于中兴通讯股份有限公司(以下简称" ZTE")两款密码模块 UEPCM（UEP Cryptographic Module）和 UPCL（Unified Platform Cryptographic Library）的诸多密码算法经过了 atsec 信息安全的测评，并通过美国国家标准技术委员会（NIST：National Institute of Standards and Technology）的密码算法验证体系（CAVP ：Cryptographic Algorithm Validation Program）的验证。

本次成功认证的结果已经在 NIST 官方网站上发布。证书编号、产品信息和厂商信息均可 CAVP 的官方网站的验证列表中查到：http://csrc.nist.gov/groups/STM/cavp/validation.html.

UPCL 包括的如下算法和证书编号如下：

- TDES (证书编号 #998, #999)
- AES (#1483, #1485)
- DSA (#468, #469)
- SHA (#1340, #1341)
- RN G(#808, #809)
- RSA (#727, #728)
- HMAC (#873, #874)

UEPCM 包括的算法和证书编号如下：

- TDES (#1002, #1003)
- AES (#1497, #1498)
- DSA (#470, #471)
- SHA (#1348, #1349)
- RNG (#814, #815)
- RSA (#734, #735)
- HMAC(#880, #881)

双方团队将会继续就 FIPS 140-2 密码模块验证体系（CMVP：Cryptographic Module Validation Program）测评和验证进行合作。

密码算法评估体系（CAVP）由 NIST 于 1995 年 7 月建立，针对"FIPS Approved"和"NIST recommended"密码算法展开验证测评。密码算法验证是密码模块验证体系（CMVP）下的 FIPS140-2 验证的先决条件。所有 CAVP 和 CMVP 下的测试都由第三方的实验室进行，这些第三方的实验室被美国国家实验室认可体系(NVLAP :National Voluntary Laboratory Accreditation Program)授权为密码和安全测试（CST： Cryptographic and Security Testing）实验室 ,比如 atsec CST 实验室。atsec 在该领域拥有丰富的经验 ,并且在安全测试和评估领域处于领先地位。

联系我们

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：84834011
传真：82890017
Email:info_cn@atsec.com

atsec 完成皮尔森（Pierson）MIIKOO 的密码算法测试

2010-11-4

中国，北京 - 最近，atsec 信息安全对皮尔森科技（Pierson Capital Technology LLC，PCT）提供的 MIIKOO 密码模块中的密码算法进行了测试。模块实现了 5 项 FIPS 认可的密码算法，在美国国家标准与技术研究所（National Institute of Standards and Technology，NIST）维护的密码算法验证体系(Cryptographic Algorithm Validation Program，CAVP)下全部验证通过。这是对 MIIKOO 进行密码模块验证体系（Cryptographic Module Validation Program，CMVP）测试过程中皮尔森科技取得的一个重要的里程牌。

NIST 证书验证了 MIIKOO 中的算法是严格的遵循 CAVP 准则开发实现的。Frank Psaila，皮尔森科技总经理表示："我们在为高端客户提供安全环境方面的承诺和技术已经成为了推动我们努力通过这次认证过程的动力。我们相信，我们的尖端技术是在各种级别的安全链下提供简单的、可负担的、且依然用户友好的解决方案的先锋。"（原文如下："our commitment and expertise in providing a secure environment for our high profile clients has been the motivation behind all the effort to get us through this certification process. We at PCT believe that our leading edge technology is a pioneer in providing a simple, affordable and yet user-friendly solution at all levels of the security chain."）

密码算法验证是进行符合 FIPS 140-2 标准的密码模块一致性测试的必要条件。所有测试都必须由被经过认可的第三方实验室，也即密码模块测试（Cryptographic Module Testing，CMT）实验室进行。atsec 信息安全，作为被认可的 CMT 实验室，在信息安全评估和信息安全相关产品测试方面具有全球性的成功经验，自然成为了皮尔森的选择。Steve Weingart，atsec 资深顾问，此项目的测试人员，表示："通过对他们密码算法的独立测试和验证过程，皮尔森展示了他们致力于为他们的产品满足更高的质量和互操作性标准。目前密码算法测试已经完成，我们将继续进行 FIPS 140-2 一致性测试并且期待着成功验证。"（原文如下："By going through the process of independent testing and validation of their cryptographic algorithm implementations, Pierson has shown that they are committed to meeting a higher quality and interoperability standard for their products. Now that the cryptographic algorithm tests are completed, we are continuing to move forward on the FIPS 140-2 conformance testing and looking forward to a successful validation."）

证书编号、产品信息和厂商商信息可以在 CAVP 官方网站的验证列表中查到：

http://csrc.nist.gov/groups/STM/cavp/validation.html.