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

感受第十二届国际 CC 会议

atsec， 白海蔚 刘岩，2011.10

2011 年 9 月 27 日至 9 月 29 日，第十二届年度国际通用评估准则会议（ICCC：International Common Criteria Conference）如约在马来西亚吉隆坡召开，也是继日本、韩国之后，第三次在亚洲国家召开的国际 CC 会议。atsec 作为全球信息安全领域的领导者共有十余名顾问参见了本届 CC 大会，且有 5 篇专业论文在本次会议上发表演讲并被高度关注，笔者作为 atsec 的一员深感自豪，并且借助 CC 大会这样的平台在信息安全行业与其他专家交流亦是非常难得的机会。

图：部分 atsec 成员在本届 CC 会议的合影

本届 CC 会议在第一天开始阶段的主题讲演和开幕式之后，设有 3 个分会场，分别是 CC 官方正式信息（CC Formalities）、CC 的技术使用（Technical Use of CC）和管理观点/应用层面（Management Views / Application Aspects）。笔者在为期 3 天的会议过程中针对感兴趣的议题进行了学习和积极参与，本文简要阐述笔者经历本届 ICCC 的一些感受。

供应链安全引发的关注

供应链的安全问题是本届 CC 会议最为关注且重要的议题。

会议的关键主题（Keynote）讲演阶段，两篇分别来自 IBM 和 RIM（Research In Motion，更知名的是 BlackBerries）的演讲就不约而同的谈及了供应链安全的问题。随后，来自 IBM、Microsoft,、Intel、NXP、Cisco 和 Your Creative Solutions 的 6 位专家代表以圆桌会议小组讨论（Panel discussion）的形式共同探讨了厂商如何应对供应链安全威胁，以及 CC 如何更好

的协助有效性和整体保障的评估。他们根据自身实际经验，结合 CC 标准及其相关技术方法，各抒己见，为供应链安全和 CC 相关议题提出了建设性的思路。

在此之后，来自微软公司的 Michael Grimm 在第一天发表了题为“New Direction for the Common Criteria: Implications of Supply Chain and Cloud Computing（通用评估准则的新方向：供应链和云计算）”的讲演。该演讲中提出了对于供应链的风险的理解和定义，并以举例的方式谈及了政策结果。比如美国的 NIST IR 7622 起草了一系列针对高影响程度的联邦信息系统采购、开发和操作的实践应对供应链风险；印度在国家计算机安全策略中开发了类似的策略考虑；俄罗斯的认证体制关注于非暴露的功能。讲演还提及了诸多可能的供应链威胁的实例，比如产品源代码、客体代码、可执行文件的篡改；故意的添加设计脆弱性；故意的添加实现的脆弱性；已经废除或者不安全的部分被植入到产品中；伪造产品；伪造部分产品；产品完整性的缺失；产品更新的完整性的缺失；开发站点、物流、存货控制的安全性缺失；缺乏供应链改变的问责制等潜在威胁。同时提出了在 CC 产业内创建工作组，寻求一致方案，为下次 CCDB 会议提交建议，并最终输出 CC 认可的文档的一系列建议，并阐述了其价值和优势。讲演最后提出了云计算的供应链的实例，云服务可能具有供应链类似的属性，并谈及了诸多已有的评估标准，关注于操作安全，可能被参考使用，比如 ISO 9001、ISO/IEC 27001、美国的 FISMA 以及 SSAE 16（之前的 SAS70）。以下将是供应链问题很好的出发点，比如：篡改产品（Tampered products）、假冒产品（Counterfeit products）（CC 中 ALC_DEL/AGD_PRE）、数据披露（Disclosure of data）、不被设计或生产于不可信任的国家、公司、产品、流程和个人（Not designed or produced by distrusted countries, companies, products. processes and/or individuals）、产品质量（Product quality）、业务连续性（Business continuity）、正确的劳务条件（Proper labour conditions）和回收（Recycling）等。

演讲结束后，Michael 号召并组织在会议第二天午餐后围绕供应链安全主题展开进一步的工作组研讨会。近 40 余名会议代表参加了该研讨会，研讨会主题突出，氛围活跃，大家畅所欲言，并形成了此领域的工作组（Working group），完成了初步的题为“CC and Threats to Supply Chain Security（CC 和供应链安全威胁）”论文成果。笔者也非常有幸参加了本次研讨，并将在今后的工作组讨论中积极参与，期待着在供应链安全领域进一步的投入和参与。

会议的第二天，来自 atsec 专家发表了题目为“Evaluating Third-Party Code: How Can It Be Trusted?（评估第三方代码：它如何被信任？）”的讲演。她从过程和技术两个角度的目的提出了问题，“过程”工作单元的目的是建立 TOE 开发者的信任，而“技术”工作单元的目的是验证 TOE 安全功能如所期望的进行工作；而目前所面临的问题来自于组成的第三方的组件，CC 中并没有明确定义建立第三方硬件/软件开发者或第三方代码本身信任的方法。atsec 专家的讲座并提出了所建议的解决方案，提出了从 EAL 2 到 EAL 4 级别的“可信的供应商”保障包，以及在 EAL 3 和 EAL 4 级别所定义的接受方法。

来自 Cisco 公司的 Gene Keeling 发表了“Certifying Trust（认证信任）”的讲演。讲演提出了全球经济的成功要求厂商开发和生产产品更加全球化，政府越来越认可 COTS（commercial off the shelf）产品的价值，因为其具有更大的创新、更短的推动时间、更低的成本以及全球化的互操作性。全球化导致了产品信任层面的关注，而讲演指出 Common Criteria 无疑是解决这些问题的独特的方法。Cisco 提出了其信任产品模型（Trusted Product Model），涵盖了安全硬件、安全软件、价值链安全、以及独立认证，而对于基于标准的、国际互认且实现知识产权保护的独立认证标准，CC 无疑是其所采用的基本标准。谈及认证

信任，产品特定的问题和生产（制造）特定的问题同等重要，缺一不可。讲演的最后，提出了对于技术社区（Community）建立的必要性，且需要建立可行的时间周期和计划。演讲的内容还涉及了站点认证，站点认证在智能卡领域应用广泛，但不局限于该领域。站点认证针对某站点生命周期基于 ALC 执行认证，据此检查站点是否正确执行了版本管理，并针对收到、操作、生成和输出的配置项提供足够的机密性和完整性的保护。

在此，笔者不得不提及重要的开放组（Open group）可信技术论坛（TTF：Trusted Technology Forum）。atsec 于 2011 年 2 月成为 TTF 初始成员之一，参见新闻：http://www.atsec-information-security.cn/cn/news--244.html。目前，该工作组的成员包括了世界范围诸多的大型知名机构，比如 atsec、IBM、CISCO、HP、ORACLE、Juniper、Microsoft 以及来自中国的金蝶（Kingdee）等。TTF 旨在为安全工程和供应链信任制定最佳实践，“Build with Integrity, Buy with Confidence”是 TTF 的宗旨和目标。会议第三天上午，TTF 的代表也发表了“The Open Group’s Trusted Technology Forum: Developing open standards for a more trusted global supply chain（开放组的可信技术论坛：开发针对更加可信的全球供应链的开放标准）”主题讲演，提出了开发更值得信赖的全球供应链的开放标准的思路；讲演介绍了开发组，业界面临的供应链的挑战，以及如何应对该挑战，并结合最佳实践，谈及 TTF 的成果。TTF 计划在 2012 年上半年完成标准初稿，并进行相应授权认可体系的开发，并计划 2013 年开始体系的试运行和产业推广，该标准将完全承认独立的 CC 产品评估。

谈及供应链安全，atsec 于 2011 年初正式获得了授权成为 NASPO 标准的审核机构，且拥有首批中国本土的经过考核的审核员。参见 2011 年 6 月由 atsec 资深顾问张力发表的名为“采用 NASPO 标准进行风险管理”的短文（http://www.atsec-information-security.cn/downloads/documents/NASPO.pdf）。NASPO 需求应用于风险管理（控制），这种风险会潜在的降低或消除安全技术、产品或服务的价值。NASPO 标准并不关注产品或服务的内在功能的安全价值。由于这些原因，NASPO 倾向依赖市场来评估特性，诸如防伪造、防篡改、追踪特性、认证价值与辩论证据价值等。由此可见，诸多信息安全行业标准都潜移默化的与 CC 标准有着联系，本文后面也会提及本届会议中就标准之间关联所展开的热议。

标准的发展和使用

截至目前，CCRA（CC 互认协定：Common Criteria Recognition Agreement）成员国为 26 个，其中包括 16 个证书颁发（Certificate Authorizing）国家和另外的 10 个证书接受（Certificate Consuming）国家。其中马来西亚在本届 CC 会议上正式由证书接受国家成为了证书颁发国家，马来西亚的代表在颁奖会议上正式得到了来自 CCMC（Common Criteria Management Committee）主席 Dag Stroman 的授予的成员证书。

与往届会议一样，会议首日的上午，CCMC（CCRA Management Committee）主席和 CCDB（CCRA Development Board）主席在本届会议上分别就 CC 最新的动态进行说明（“Update from the CCRA Management Committee”和“Update from the CCRA Development Board”）。其中，各个技术社区都在不断的努力和大力推进 PP 和相关产品类型技术领域的 CC 应用和发展，一些国家已经开始制定经过认可的 PP 列表。

会议讨论和专题讲座中，美国、土耳其、英国和日本几个国家体系分别发表主题讲演，阐述本国 CC 评估和认证体系的最新消息和目前状态。其中，美国体系的更新状态依然备受

关注；来自美国 NIAP/CCEVS（ National Information Assurance Partnership/US Common Criteria Evaluation & Validation Scheme）代表 Carol Houck 发表“An Update on the NIAP Evolution（NIAP 发展更新）”。美国计划仅仅接受符合美国政府认可 PP 的产品的认证，并且将建立政府采购清单，弱化 EAL 级别的体现。美国策略的调整更新，对于厂商和 CC 互认领域都会有些许影响，并且带来了诸多的争论。而相对而言，欧洲以及其他各参与国保持了较高程度的互通性和体系策略的一致性。

从产品类型层面，很多业界同仁均在讲演或者讨论中表示赞同且鼓励针对不同产品形成产品社区论坛（Community），加强纵向的讨论和研究。

atsec 德国实验室主任 Gerald Krummeck 在会议第一天发表讲演题为“Fighting the bean-counters”针对评估方法的议题，演讲内容从实际出发，生动有趣，很多听众都纷纷称赞且高度评价该讲演的精彩。Gerald 首先自现实生活的实例（如美国超市买啤酒；飞机手提行李的流体物品要求）出发，说明了完全借助检查单（Checklist）式的评估是不合理的，CC 评估工作更是需要评估师多动脑子，理解真正目标。 “A fool with a tool is still a fool（一个会使用工具的傻子还是傻子）”，检查单可以在满足场景时被使用，可以节省评估时间和投入，最终达到预期目标。检查单仅仅能作为指导，需要考虑如何实现目标的，而为了达到目标，也需要允许其他的形式。Gerald 建议无论是 CC 和 CEM 进一步更新都应该将这点作为主要目的，对于每一个 CEM 工作单元，评估师应理解执行该项评估的意义和重要性。Gerald 的讲演也引来了 CC 和 CEM 标准编写者的热议，在给予该讲演高度肯定和祝贺同时，展开了技术讨论和澄清。

atsec 首席科学家 Helmut Kurth 和评估顾问 Trang Huynh 合作演讲的“An Access Control Model for Applications on Mobile Devices using Common Criteria Certifications（使用 Common Criteria 认证针对移动设备应用的访问控制模型）”关注于较新的 CC 应用领域，讲演提及了移动设备上支付应用和联系人数据库等实例，体现了 atsec 专家们对于新兴技术和领域的研究和关注，特别是如何引入和采用 CC 保障移动设备的安全。

信息安全行业标准与 CC 的关系

CC 标准也其他行业最佳实践和标准的关联一直以来是历届 CC 会议的持续关注点。信息安全行业诸多标准均与 CC 标准有着密不可分的关系。

密码安全是 CC 领域的持续热点话题，其中以美国 NIST 维护的 FIPS 140 标准尤为受到关注，往届 CC 会议就提出了诸多的该领域的论文，比如早在罗马召开的第八届 CC 会议上，Fiona Pattinson（atsec）就曾提出了 CC 和面向信息安全管理体系（ISMS）的标准 ISO/IEC 2700x 系列以及面向密码模块实现的 FIPS 140-2 标准的统一符合性建设思路。本届会议上，atsec 资深顾问毛翊博士发表了题为“From FIPS 140-2 to CC（从 FIPS 140-2 到 CC）”的讲演，分别阐述了从 CC 和 FIPS 140 角度的安全产品的理解，将二者之间公共的安全检查点进行了比对。从某种意义上，FIPS 140 可以被看作一个保护轮廓（PP：Protection Profile）。讲演提出了获得 FIPS 140 密码模块的认证对于 CC 评估和认证的价值。从分析可以看出，FIPS 140 测试和 CC 评估具有很大的关联，FIPS 140 认证具有自身的方法，同时它也是获得 CC 认证的重要基石，特别是对于首次开展安全标准合规的机构而言。同时，笔者也认同 FIPS 140-2 专注于密码领域的测试结果会对 CC 标准评估带来价值和成果积累，在实际 IT 产品进行安全标准合规时，往往先完成 FIPS 认证会为后续开展 CC 认证奠定坚实的基础。且从市场角

度来看，因为 FIPS 较 CC 评估工作的周期短成本低，先行通过 FIPS 认证无疑是可行的方案。

随后，来自 Realia Technologies 和 Epoche & Espri 的两位专家的讲演“HSM Protection Profile：How to CC-evaluate a HSM to meet FIPS requirements（HSM 保护轮廓：如何 CC 评估 HSM 以满足 FIPS 要求）”，也再次涉及这两个标准的相关性。

来自美国 Mitre 的讲演“Secure Content Automation Protocols (SCAP)：how it is increasingly used to automate enterprise security management activities（安全内容自动协议（SCAP）：如何提高自动企业安全管理活动）”讲述了什么是 SCAP，为什么要采用 SCAP，如何针对 CC 推动 SCAP，并提出了将 SCAP 集成到 CC 领域的建议方案。关于 SCAP 更多的信息，也可以参见 atsec 资深顾问张力早先所编写的文章 “SCAP 标准简介”：http://www.atsec-information-security.cn/downloads/documents/SCAP_Standard_introduction_Li.Zhang.pdf

中国对 CC 会议的持续关注

虽然中国目前还没有加入国际 CC 互认，但是中国技术领域的专家对于 CC 会议，及其涉及的标准和技术话题多年来给予了长期的关注。本年度来自中国监管机构、认证机构、测评机构等多位领导和技术专家参加了本次会议，从技术方面在会议上与国际 CC 产业专家展开了交流和探讨。据本届 CC 会议官方统计数据显示，本届会议来自中国大陆的参会人员总数在各个参会国家的数量上位居第二，美国参会代表人数最多。

笔者很高兴看到来自中国的专家将国内的标准和技术介绍呈现给世界，在本次会议上共计 4 篇来自中国的演讲。

atsec 美国资深顾问毛翊、中国信息安全认证中心陈晓桦副主任，以及 atsec 中国资深顾问刘岩共同编写了“Comparative study between the Chinese standards and the Common Criteria（中国标准和通用评估准则之间的比较研究）”，并在本届会议上发表讲演。该讲演精炼性地将中国信息安全标准的现状展示给了 CC 社区，让国际信息安全产业进一步地了解中国的信息安全标准及其相关评估认证体系，并以数据库和操作系统两个具有代表性的产品类型进行了国际 CC 标准的 PP 和中国国家标准的比对，做到了国际技术交流桥梁的作用。

来自中国公安部第三研究所宋好好博士向与会嘉宾分享了中国信息安全标准的应用情况，演讲题目为“Chinese general techniques requirements for important information system（针对重要信息系统的中国通用技术要求）”。来自中国信息安全测评中心 CNITSEC 的 Hongsong Shi 发表了题目为“Quantifying the strength of security functions in vulnerability assessment（在脆弱性评估中量化安全功能强度）”的讲演。

源自中国的知名厂商中兴和华为在本次大会上分别获得 CC 认证证书。此外，华为代表王欣和崔杰博士在会议第二天合作讲演了“CC Certification for Telecom Product（通信产品的 CC 认证）”，介绍了华为公司的信息安全认证战略，以及通信产品的信息安全的总体框架。笔者在此表示衷心的祝贺，同时也期待 atsec 作为全球领先的评测评估实验室能够在中国的 CC 产业做出更多的贡献，将 atsec 在西方国家积累的成功经验以及 atsec 所了解的国际产品评估领域在过去几十年来历经的弯路，在中国进行分享。

在大会第二天进行的欢庆晚宴（Gala Dinner）按照惯例颁发了各个认证机构年度内完成的认证证书。其中，由 atsec 评估完成的 PR/SM on IBM System z196 HE GA1,D86E 产品在

德国 BSI 体系下获得 EAL 4 级认证。

图：atsec 德国实验室主任 Gerald Krummeck 陪同 IBM 领取 CC 证书

本届 CC 会议总结与展望

马来西亚科学技术与创新部（MOSTI：Ministry of Science, Technology and Innovation）下设的 CyberSecurity 组织主办本次会议，他们慷慨地与我们分享自己国家的文化和美食，当然也包括科技的成果

各国采取 CC 标准执行符合性建设的区别也在本届会议上多次被提及和讨论。CC 会议历来具有很多的争论和不同的声音，但是每个与会嘉宾对于构建国际信息安全保障的目标高度一致，且非常高效的达成共识。

CCDB 和 CCMC 的主席分别在结束会议上为本届会议做了总结。今年依然是个忙碌却又与众不同的会议，会议两个关键主题讲演提出了在供应链安全领域非常类似的挑战话题。

大会最后主持人宣布 2012 年 CC 会议的主办城市 -- 法国巴黎。我们将把更多的期待和憧憬交给那个浪漫的国度。