atsec the information security provider
NEWS 12/2011

最近新闻一览

atsec完成握奇数据WatchKey USB Token的FIPS 140-2 第2级测试

atsec在“2011移动支付产业年会”发表演讲

atsec为Pierson MIIKOO完成FIPS 140-2测试和验证

Jeremy Powell在2011年度计算机安全应用会议提供Java安全研讨会

atsec信息安全参加在巴尔的摩举行的2011年度Milcom会议

atsec中国与中国信息安全认证中心推出安全软件开发课程

Steve Weingart在日本奈良的非侵入式攻击测试研讨会上发表演讲

IBM ® z/OS®版本1 R. 12系统SSL 密码模块完成了FIPS 140-2 认证

点对点加密解决方案已发布初始版本

更多新闻，请浏览我们的网站
www.atsec.com

中国产品迎来 FIPS 140-2 合规认证丰收年

今年（2011 年）是中国厂商获得基于国际密码模块安全性相关的 FIPS 140-2 标准合规认证大获丰收的一年，atsec 先后与中兴通讯（ZTE）、皮尔森科技（Pierson）、握奇数据（Watchdata）等公司合作完成了 FIPS 140-2 的密码模块测试，并最终为这些公司的相关产品获得了由美国国家标准与技术委员会（NIST：National Institute of Standards and Technology）和加拿大通信安全局（CSEC：Communication Security Establishment of Canada）共同创建和维护的密码模块验证体系（CMVP：Cryptographic Module Validation Program）所颁发的合规证书。我们高度赞赏这些公司敢于尝试与开放严格的国际性标准的合规性检查，勇于接受第三方实验室基于标准的公正客观的测试和验证，研发团队勤于学习吸收标准精髓，善于改进产品安全性能，乐于做出不懈努力直至最终获得认证。通过认证的产品证书编号依次为#1586、#1589、#1634 和#1640，详细的验证结果可在如下链接查看：http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm

通过认证的四款产品既具有典型性又具有广泛性，产品形态涉及硬件和软件，产品类型包括用于网络设备以及管理软件中的提供密码支持的软件包、智能卡以及结合生物识别和令牌技术的硬件等，被认证的级别覆盖了 FIPS140-2 中规定的四个等级中的前三个。

在 FIPS 140-2 标准下获得密码模块的验证在许多行业和政府部门中越来越重要，目前世界上很多国家机构的采购和招标要求中也明确地提出具有密码模块的产品 FIPS 140-2 的合规要求。不仅仅是美国和加拿大，还包括全球很多国家。截至 2011 年 12 月 15 日，NIST 网站公布的已经获得 FIPS 140-2 认证证书的密码模块有 1655 个，而在 2011 年一年间 atsec 与中国厂商紧密合作使得在这些证书中包含了 4 个重要的来自中国大陆的产品。这对于我国国内的商业密码安全产品是一个里程碑似的跃进，特别是为其进一步打开国际市场提供了必要且重要的安全保障。

皮尔森的总经理 Frank Psaila 先生评论道：“该证书的获得对于皮尔森而言是一项巨大的成就，致力于该项目的工程师团队创造了前所未有的 FIPS 140-2 验证的记录，结合生物识别和令牌硬件，使其具有能力同时为 OTP 和 PKI 技术工作。对于在非常合理的项目周期内获得该项成功，在此对我们双方团队的专家表示感谢。该成功将毫无疑问地为远程身份验证及其适用性设定新的标准，这也是该项目中我们的主要目标。”

ZTE 美国首席执行官 CEO Lixin Cheng 在项目结束后这样说道：“ZTE 相信满足国际标准的要求是交付给来自客户要求的最为安全和可靠的解决方案的关键，获得 FIPS 140-2 标准的认证进一步展示了我们的工作，确保我们的研究和研发（R&D）战略映射了这些标准的重要性，使我们产品的质量和可靠性逐步赢得客户的信心。”

握奇数据副总裁高翔先生在项目结束后表示：“感谢 atsec 以及他们的辛苦工作，同时也感谢握奇数据的产品团队。该证书为握奇数据的 USB Token 迈向国际市场开辟了新的道路，但是这只是一个开始。未来将有更多的成功。”

正如来自厂商的声音，FIPS 140 认证的结果不但提升了客户对产品质量和可靠性的信心，而且为我国的产品走向国际市场开辟了新的道路。与此同时，atsec 密码和安全测试（CST：Cryptographic and Security Testing）实验室也因为成功完成这些首批来自中国大陆的产品的 FIPS 140-2 认证而骄傲。毫无疑问在整个测试和认证过程中，双方团队均面临着巨大的挑战，一方面这是国际上最为严格的、高质量的，且是广大中国的产品开发者所可能不是特别熟知的密码领域的信息安全标准，另

一方面来自中国的前几个不同领域的产品认证申请得到了 NIST 较高级别的关注和非常高的审查要求。比如，在皮尔森 MIIKOO 设备评估过程中，因为产品采用的生物识别安全技术对于 NIST 认证是全新的，因而双方团队完成了独一无二的挑战，来证明其符合了 FIPS 140-2 安全级别为 3 级的标准要求。这些项目不仅要求广泛的技术知识和理解，atsec 测试人员必须全面探究 FIPS 140-2 标准的广度和深度，以展示其在这样高级别保障下的合规性。

经历了 FIPS 140 测评项目的洗礼，各个开发人员确实地体会到了该标准的实践为产品的信息安全和质量带来的提高，每一个合作的技术人员都深深地体会到了 atsec 对于致力于高质量和严格的信息安全保障要求的产品的专注和专业。针对此巨大成果以及与 atsec 的成功合作，我们也来听一下来自产品开发人员的声音：

FIPS 140-2 认证终于取得了圆满的结果，这个和大家共同的努力是分不开的。在合作的过程中，atsec 实验室的贡献是有目共睹的，无论是熟练扎实的专业技能，严谨求实的工作态度，还是项目过程中对产品的每个细节不遗余力的反复推敲和确认，都体现出 atsec 作为一家业内领先的实验室在安全领域方面的的前瞻性和专业性。我们在认证过程中也都受益匪浅，对产品的安全性有了更进一层的认识。--握奇数据曹海涛

得到 Watchdata USB FIPS 140 认证通过的消息非常高兴！也非常感谢你们 atsec 团队在这一过程中的每一份帮助、支持与努力！虽然我是中途加入该项目组，但是已经能很好地体会到 atsec 在方案的分析评估、审查、修改建议等方面的高效与负责，争取到了很多时间以配合我们尽早完成测试与认证。在与 atsec 测试人员的配合中，我们也都深深感受到其认真、细致、高效、严谨，这也是我们在项目完成过程中提升 WatchSafe 产品的同时所学到的 atsec 令人佩服的工作态度，而且这个感受很深。这些因素都是帮助我们顺利获得认证的保证！我们也从中对产品的安全、文件结构的完善有了更多的改进和思考~谢谢！--握奇数据吕晓燕

回顾与我们与 atsec 共同完成的 FIPS 140-2 CAVP 与 CMVP 认证过程感触颇多，其中有几点仍记忆犹新。首先，站在产品设计的角度来说，使用 FIPS 140-2 认证标准来重新审视一款产品，这个体系标准从逻辑层到应用层，方方面面都有有法可循的具体要求，从而保障了产品的安全性能。其次，对于工程师来说，这套标准就是一套详细的设计大纲，从概要设计到详细模块设置，甚至到后期的功能，压力边缘测试都有具体的实施方案。所以个人感觉，工程师严格遵照认证标准实施下来，想设计出一个不安全的产品都很难。最后，真心的感谢 atsec 的同事们对我们项目的支持，没有你们的帮助，我们不能如此顺利的与远在地球另一边的美国实验室合作和沟通。--皮尔森李畅

感谢 Yi Mao 女士，在我印象中，她是一个非常忙碌的人，但纷繁复杂的事务并没有扰乱她的思维，在每周的例会中，她总是能做到思路清晰表达清楚，对 UEPCM FIPS 认证的进展和遇到的问题了如指掌，使我们能够非常清楚地知道当前要做的事情和下一步的工作计划。感谢 Trupti Shiralkar 女士，她主要负责 UEPCM FIPS 认证的相关文档审核以及测试的工作，她是一个非常专业而且严谨细心的人，对我们文档中不恰当的地方给出了详细的修改意见，减少了我们修改文档的次数，在进行 CMVP 远程测试的过程中，她经常工作到深夜，对不能满足要求的测试脚本进行修改，直到全部通过测试。感谢其他 atsec 的工作人员，虽然我们没有直接接触过，但你们科学的工作方法、严谨的工作作风以及坚持不懈的努力，为 UEPCM FIPS 认证成功做出了不可缺少的贡献，非常感谢！我期待与 atsec 的专家们再次合作！--中兴通讯胡江辉

早自 2007 年以来，atsec 已协助国民技术（原中兴集成电路）、杭州晟元芯片、时代今典、握奇数据、皮尔森等完成近 40 个算法的密码算法验证体系（CAVP ： Cryptographic Algorithm Validation Program）的测试和验证，详细证书信息请查看如下链接：

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

除此以外，atsec CST 实验室与全球诸多的大型厂商长期合作，开展基于 FIPS 140-2 标准的测试和认证，这些厂商包括但不限于三星、IBM、惠普、Red Hat、 Wind River 、Patrick Townsend Security Solutions、Quantum Corporation、Data Locker、Secuware 等。2011 年以来，在智能手机领域的密码算法和密码模块的测试得到全球诸多手机厂商的重视和投入，atsec 也期待着在这些新兴领域的更多的贡献。

atsec，白海蔚

从研发角度来理解 CC

atsec 资深顾问张力

CC（Common Criteria）给研发人员提供了一套完整且清晰的方法描述产品的安全，但对研发人员来说，如果你不能够真正理解其内在的含义的话，很难用CC“语言”来描述产品的安全。

本文档的目的是帮助研发人员更好地理解 CC 评估，在此基础上对 CC 标准中一些晦涩、难懂的概念进行了深入的探讨与阐释，以帮助大家更好地理解标准，希望对今后参与 CC 评估工作的研发人员起到一定的指引作用。

1 产品研发与 CC 评估的关联概述

每个产品都有自身的安全功能需求，不同的产品安全功能可能会有所不同，但对安全功能的保障方式依据 CC 则有着相同的预定义准则，CC 标准中提出了评估保障级别（EAL：Evaluation Assurance Level）的概念，分为 EAL1~EAL7，EAL1 为最低保障级别，EAL7 为最高保障级别，每一级 EAL 要比其下的所有 EAL 有更多的保障要求，下面以 EAL4（商业互认的最高级别）为例来说明产品研发过程与实际评估过程的对应关系。

对一个产品做安全评估，首先需要基于该产品用户的安全问题形成安全需求描述，然后针对这些安全需求，确定评估范围和被评估范围的安全功能，之后通过审核产品的开发流程（即生命周期）、开发（产品设计）、测试与脆弱性分析以及产品交付等方面评估产品是否符合了相应的保障级别要求。下图说明了 CC 的整个评估流程，重点描述了产品研发过程的各个环节与评估保障类的对应关系。

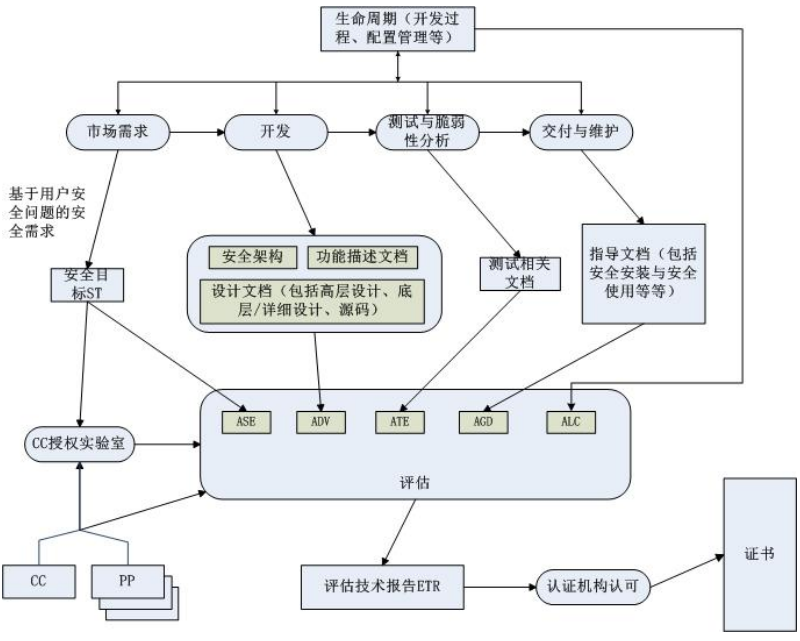


图 1 产品研发与CC评估的关联关系

由上图我们可以看出，对产品的评估主要关注在下面五个层面：

1） 安全目标（ST：Security Target）
2） 生命周期
3） 产品开发
4） 测试与脆弱性分析
5） 产品交付

下面从研发角度对这5个方面给出详细的阐述。

1.1 ST

ST是针对一款特定产品的安全需求描述，是开发人员、评估人员以及产品（TOE：Target Of Evaluation）的最终用户在产品的安全特性与评估范围方面达成一致的基础。ST基于用户的安全问题来描述产品的安全需求，包括产品的安全功能、产品抵御的安全威胁以及环境的支持。

一个实际的评估项目首先要确定评估的范围，即哪些安全功能需要评估，被评估的安全功能要求按照特定的格式在ST中给出描述。ST中必须包含的内容如下：

- 需要解决的安全问题描述，包括：产品抵御的威胁列表，产品实现或遵从的安全策略列表（比如国家的法律或法规），功能实现所需要的预期环境描述（包括人员安全意识的培训）。
- 针对安全问题的解决方案的高层描述，由一套抵御威胁与在预期环境中实现策略的安全目标组成。
- 运用CC标准来明确描述产品的安全需求。
- 产品怎么实现所选的安全需求。
- 论证安全功能如何实现安全需求、安全需求如何实现安全目标、安全目标如何抵御威胁，以及这些方面描述的一致性。

1.2 生命周期

生命周期贯穿于产品从市场需求、研发到最终交付实施与使用的整个过程，关注产品的开发流程，包括配置管理、审核流程、项目管理控制、变更控制过程、测试方法、办公场所安全、开发工具与交付使用等方面。

配置管理系统，必须对产品的每个版本与配置项分配唯一的标识，必须阻止未授权的更改，支持添加或更改配置项的过程。配置管理系统必须管理所有的设计描述、测试文档、用户与管理员指导手册、配置管理文档、所有发现与报告的安全缺陷信息。

办公场所安全需要关注开发与设计过程的人员安全，是否安装了摄像监控系统，开发环境是否连接到了公共网络，外部人员的进出访问控制等等。

1.3 产品开发

产品开发需要有产品设计文档描述，针对EAL4，至少应该包括功能说明文档、安全架构文档、TOE设计文档（高层设计文档、底层设计/详细设计文档），源码实现等等。

功能说明描述产品的所有外部接口，针对每个接口，需要详细描述它的目的、使用方法、参数、相关的行为与错误处理。功能说明必须描述与安全相关的所有部分，必须能够证明它与ST中描述的安全需求是一致的。

TOE设计可以按照子系统、模块的划分来描述，必须描述每个子系统或模块提供的安全功能和所有的接口，每个接口需要详细描述它的目的、使用方法、行为与错误处理。必须说明产品必需依赖的底层硬件、软件与固件，描述由他们提供的保护机制。必须也能证明TOE设计与ST中描述的安全需求是一致的，并且能正确且完整地映射到功能说明。

安全架构需要证明产品不能被篡改，安全机制不能被迂回。下一章节我会对这一部分进行深入的探讨。

源码是设计的最终体现，要能正确、完整地映射到TOE设计。

1.4 测试与脆弱性分析

CC评估中所说的测试侧重于测试产品的安全方面，需要审核的信息包括测试计划、测试流程描述、期望的测试结果与实际的测试结果。要求功能说明中的每一项至少被测试一次，并且测试要求深入到产品设计的每个子系统级别。评估人员需要通过一系列脆弱性分析来证实产品的安全机制足以抵制每种攻击。

1.5 产品交付

在对产品的研发版本经历了严格的测试与脆弱性分析后，将形成一个稳定的可以发布的版本，但在安全交付客户使用前需要注意两个问题，一个是安全交付，一个是安全安装。

安全交付需要有相应的交付流程描述，其中描述了安全的交付方式，以及辨别真伪的方法。

安全安装需要有相应的安装向导文档，描述用户怎样创造一个安全的操作版本，这包括安装软件与硬件的过程，包括配置、个性化设置、生成密钥，创造一个安全的物理环境、等等。

除了安装向导文档外，EAL4还需要提供操作指南，包括安全操作、错误与警告、带特权用户的处理、操作模式，安全事件等等。

整个评估过程，最为重要的部分即为开发与测试的评估，这两部分也与我们的产品研发人员最为密切，当然这并不是说其它部分的评估不重要，而是其他部分在CC标准中的描述要相对容易理解，而对于开发与测试，CC保障需求（ADV：Assurance of Development 与ATE：Assurance of Tests）的描述包含了更多的专业术语，也比较难于理解，下面主要就ADV与ATE中一些难点进行深入的探讨。

2 CC 标准的难点解析

2.1 安全架构

CC标准中的安全架构需要保护三个要素信息的描述，即自保护、域隔离与防迂回。下面分别进行说明。

- 自保护

TOE实现的某种安全功能以阻止未信任的用户或进程干扰安全功能。TOE需要保证没有非信任的用户能篡改TSF功能。以Redhat Linux为例，内核与应用程序的分离即为一种自保护的机制，应用程序对内核的访问仅能通过系统调用完成。内存管理（限定应用程序对内存的使用），以及对配置文件和其他关键数据的自主访问控制（DAC: Discretionary Access Control）也是自保护的一部分。

- 域隔离

域隔离是支持自保护的一种机制。还以Redhat Linux为例，Linux通过页表、页读写保护、内存虚拟化等方法建立不重叠的地址空间来实现内存保护；带不同特权级别的不同处理器模式（仅在特权模式能更改内存保护），无特权进程禁止I/O操作；存放核心代码在管理状态域（即内核），存放信任程序的代码在独立的用户状态域（即程序），存放未信任的程序代码在其它用户状态域（不同于拥有信任程序代码的用户状态域），域之间仅能通过友好定义的接口来交互；应用进程间仅能通过内核提供的通信机制通信；这些方面都实现了域隔离机制。

包过滤防火墙并不实现域隔离机制，这是因为防火墙仅有一个域就是防火墙自身，防火墙通常不拥有未信任的实体，它仅分析网络数据。防火墙可以拥有不实现安全功能的非信任实体，仅提供方便的功能。例如允许远程监视防火墙设置的应用（不更改设置），周期性的复制审计日志到外部实体的应用。

大多数应用类型TOE实现的域隔离，是借助底层的操作系统建立的不同域或分布式环境来完成的。

- 防迂回

防迂回是TOE保护用户数据与TSF（TOE Security Functionality）数据的机制，以用户通过友好定义接口的方式访问它们。防迂回确保非信任的实体能做关键性的安全操作，如仅通过友好定义的接口（如Redhat Linux中IPC、命令行或配置文件）访问被保护的对象，所有这些接口能确保安全功能被正确执行。防迂回是针对TOE所有的安全功能，而不是针对TOE的部分安全功能，因为如果部分安全功能没有实现防迂回，这部分安全功能将会给TOE带来安全威胁，比如迂回认证能潜在地迂回所有用户基于安全功能的识别，迂回审计可以允许用户尝试违反策略而没有被监测，迂回加密可能泄露数据，等等。

2.2 SFR-enforcing、SFR-supporting 与 SFR-no-interfering 含义

在对TOE设计部分进行评估时，评估人员通常会将TOE系统划分为SFR-enforcing（Security Functionality Requirement执行）、SFR-supporting（SFR支撑）与SFR-non-interfering（SFR不相关）子系统或模块，然后再按照子系统或模块所完成的功能进行进一步的评估。

SFR-enforcing是直接实现SFR的部分，比如自主访问控制DAS、用户管理、用户认证。

SFR-supporting是SFR执行功能依赖的部分，比如设备驱动、内存管理。

SFR-non-interfering是不实现TSF的TOE其他软件部分，或SFR执行或支撑依赖的其他软件部分，

为了帮助大家理解，下面以防火墙与Linux为例来阐述一下这三个概念的区别与含义。

- 防火墙

SFR-enforcing：包过滤功能。

SFR-supporting：防火墙的操作系统内核。

SFR-non-interfering：日志分析器（如果日志检查功能没有声称在SFR中）。

- Redhat Linux

在Redhat Linux操作系统中，通常仅部分内核实现安全执行机制（如DAC、审计等），而在内核域的设备驱动程序虽然不直接实现安全功能，但它们可能会导致产品的安全功能失效，因而，贡献于安全执行的设备驱动程序为SFR-supporting部分，内核中也存在没有实现SFR的其他功能（例如，优化调度策略的负载管理器），也没有安全功能依赖于它，因而这些机制是SFR不相关的。针对应用程序也是相同的，“passwd”应用实现了更新用户口令的安全执行机制，这个应用包含了解析文件“/etc/passwd”的逻辑，它应属于SFR-supporting部分，当这种解析逻辑失败时，更新用户口令的安全执行功能也会失败。

2.3 产品安全功能接口（TSFI：TOE Security Functionality Inferface）

在产品的功能说明描述中，需要详细阐述所有TSFI的目的与方法，以及每个TSFI所有参数的描述，并且要对每个TSFI依据其所完成的功能来划分为SFR-enforcing TSFI、SFR-supporting TSFI或SFR-non-interfering TSFI。下面以Linux 操作系统与防火墙为例来进行说明。

- Linux操作系统

SFR-enforcing TSFI：系统调用（open, msgctl），应用的命令行（passwd, login），配置文件（/etc/passwd, /etc/shadow）。

SFR-supporting TSFI：非执行 TSFI 的系统调用。

SFR-non-interfering TSFI：应用的命令行（ls, rm），配置文件（vimrc）。

- 防火墙

SFR-enforcing TSFI：网络接口。

SFR-supporting TSFI：检验日志的接口。

SFR-non-interfering TSFI：N/A

2.4 针对自保护、域分离与防迂回的脆弱性分析

自保护、域分离与防迂回是TOE的特性。评估人员在做脆弱性分析时不仅要看直接支持这些特性的功能，而且还要以所有可能的方式与TSF交互以检查破坏与自保护、域分离与防迂回相关的安全目标的潜在方式。

在自保护实例中，评估人员检查影响TSF行为的潜在方式，这种潜在方式可能会导致TSF不执行部分安全策略。举例来说：TOE的TSF为每个用户进程包含一个数据结构，其中包含了用户的特权级别，紧邻特权级别的元素是一个用于统计进程已分配资源的32位计数器，通常进程不会分配超过2^{16}的资源，因而计数器是足够大的，从而会存在这样的假定：在TSF内没有检查是否计数器达到了它的限制，那么用户能够通过导致进程分配资源数的内存溢出而潜在地操纵特权级别。

域分隔允许在一个域中存储域管理关键数据，这些数据应该被保护以禁止其它域的访问。举例来说，操作系统为所有激活用户存储关键用户数据（如密钥或口令）在一个特定域中，其它域的用户不可直接访问，仅能通过这个特定域提供的域间接口同步函数进行查询与修改操作，比如查询是否这个用户的数据已经存在这个特定域中，或者将一个新的用户数据加入这个特定域中。脆弱性分析时需要考虑这个域间同步函数是否进行很好的安全保护，比如是否仅在特权模式才能执行修改操作，而查询可以在任何模式，如果没有进行很好的保护则有可能导致用户口令或密钥的泄露。

3 结束语

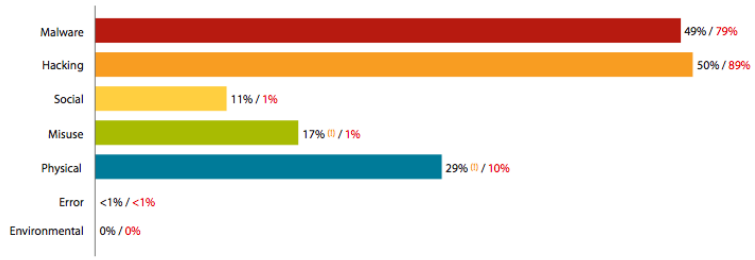
CC 标准是最为全面和公认的面向产品评估的信息安全评估标准，它已经被世界上诸多的国家所完全采用成为自己的信息安全评估标准，它可以用于评估任何具有安全功能的 IT 产品，包括智能卡产品、操作系统、数据库、无线通讯设备、数据通讯设备等等。 我国虽然还没有加入 CCRA（Common Criteria Recognition Agreement），但对产品的信息安全评估工作越来越重视，越来越多的厂商也认识到产品安全的重要性，为了更好的进入国际市场，很多产品的 CC 评估也势在必行，希望有更多的研发人员投入到 CC 的研究中来，为今后顺利完成相应产品的评估工作做出贡献。

借助优秀业界实践经验，提升应用开发的安全性

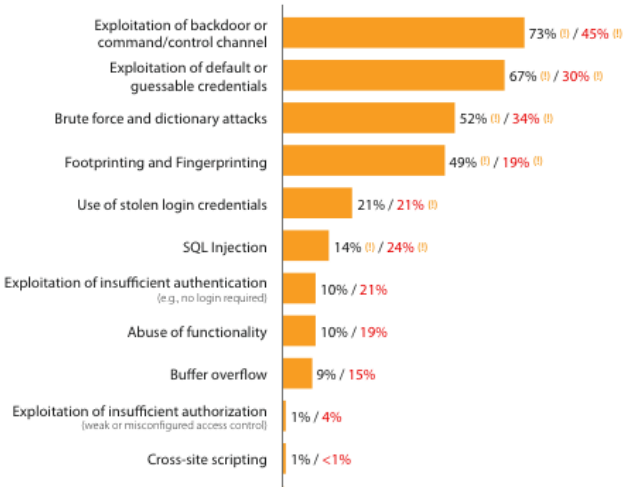
atsec 高级咨询顾问 高向东

一、实现应用安全开发的意义

当前越来越多的互联网应用通过 B/S 架构来实现，使得互联网的开放程度不断扩展，尤其是随着 web2.0 技术（如 Blog、twitter 等）的迅猛发展和普及，应用和内容的开放性得到空前的扩展。然而，不断开放的互联网应用也面临着越来越多的安全问题，如下图所示。



从上图来看，黑客攻击占据了相当大的比例。而基于黑客攻击的具体手段进行分析后发现，使用控制通道和探测密码等手段成为明显的薄弱点。具体如下图所示：



诚然现在有很多的安全设备以及加固手段，可以在确定安全隐患的前提下解决发现的安全问题，但通常是基于已知的安全问题，因而容易出现“头痛医头，脚痛医脚”的情况。更为严重的是，随着互联网本身应用价值的膨胀，攻击行为所带来的影响和损失也越来越大。

从应用的整个生命周期过程来看，产生安全弱点的源头在于应用的实现阶段，即软件开发过程。那如何从根本上解决应用本身的安全性问题呢？有效地将安全开发的方法和实践落实到开发过程。如果得到有效地实现，软件的安全开发将从根本上提升应用本身的安全性，从而将投入收益最大化，并将安全问题的影响最小化。

二、通过业界的最佳实践，构建安全开发的技术体系

除了与安全开发相关的业界安全标准（如通用评估准则 Common Criteria, PCI PA-DSS 等）以外，还有很多业界的最佳实践关注于安全开发的不同方面，如 OWASP（open web application security project）实践、微软的 SDL 软件生命周期计划、CERT 的 secure Coding 安全编码规范等等。OWASP 计划是一个开源项目，可在很大程度上节省组织在安全方面的资金投入。目前，该项目专注于 web 应用所提出的众多实践和指导，覆盖了规范指导、编码接口、测试工具等多个方面，这对于从根本上解决应用的安全问题有很强的实用价值。主要体现在：

1. 完善应用开发生命周期的安全管理

OWASP 所提供的指导性文档，如“development guide”,“code review guide”,“testing guide”等，这些具体的规范分别对于开发过程、代码审核过程和软件测试过程中如何提升软件的安全性提出了具体的指导，推荐用于改进整个开发生命周期过程中的安全性。

另外，top 10 项目总结了当前最主流的 web 应用威胁，cheat sheet 则简明扼要地提出了针对 top 10 威胁的防范要点。这些无疑对开发安全的体系和规范具有很强的借鉴意义。

2. 融入并建立应用开发的安全实践

首先，通过安全编码接口减少编码过程中产生的安全隐患。OWASP 计划提供了针对 Web 应用安全编码过程中的接口，其应用价值和参考意义在于提升编码实现的安全性。典型的安全编码接口编码如下：

- AntiSamy：AntiSamy 项目提供了编码过程中的过滤规则，这将有效降低来自客户端输入的安全风险，降低由跨站脚本等应用层面攻击带来的影响；
- ESAPI（Enterprise Security API）：此项目提供了一组安全控制的接口，可用于降低代码编写过程中的安全问题；
- EnDe：针对开发过程中的编码接口，避免因编码问题导致的安全事件，如不安全的对象引用等；

其次，通过工具化的方法实现有效的代码安全性审核。有效的代码安全性审核也是目前的一个难点，OWASP 项目提供的 LAPSE（Lightweight Analysis for Program Security in Eclipse）安全代码审核工具可在很大程度上帮助代码审核人员有效地完成任务。

最后，通过软件安全性测试工具，使安全问题在未产生影响之前得以发现和修复。软件生命周期过程中的测试阶段，除了进行功能性和性能性测试外，安全性的测试也非常重要。OWASP 项目中也有多款实用的安全性测试工具，这对于尽早并有效地发现软件的安全漏洞具有很重要的现实意义。其中，典型的安全性测试工具如下：

- w3af：一款针对 web 应用 top 10 漏洞的渗透工具；
- ZAP（Zed Attack Proxy）：一款用于发现 web 应用中的安全漏洞的渗透测试工具；
- WTE(Web Testing Environment)工作包：集中提供了大量的应用安全测试的工具。

有关 OWASP 计划的详细信息，请参见：http://www.owasp.org

三. 助力开发过程中安全性的合规建设

上述提及的应用安全开发实践指南和工具除了有助于提升软件开发过程的安全性外，对于组织在安全开发方面的合规性也有非常大的帮助。在此以支付卡行业数据安全标准（PCI-DSS）的合规建设为例，简要谈一下业界最佳实践对于安全性合规的意义。众多安全规范和实践（如 OWASP 实践、微软的 SDL 软件生命周期计划、CERT 的 secure Coding 安全编码规范等），在与符合 PCI-DSS 合规的组织充分融合后，将为开发安全的生命周期管理方面提供非常有力的支撑。

笔者在此谈一下理想化的组合，希望对组织的安全性合规建设思路有一些参考意义:

1. 安全软件开发的体系合规

对于 PCI-DSS 要求的整个开发生命周期管理（详见 PCI-DSS Requirement 6.3-6.5.9），整个生命周期过程安全管理流程，如 NIST 的 SP-800-64 等具有较强的指导意义。而如何将安全管理流程和安全目标落实到应用安全开发的关键阶段中呢？如果组织自身进行实践并总结安全的具体方法，则需要极其大量的投入。CERT 所提供的 Secure Coding 编码规范以及 OWASP 计划中的“development guide”、“code review guide”以及“testing guide”等指导性文档则是业界最佳实践的总结，将极大地节省组织进行总结和归纳的资源投入，并为达到合规提供有力的支撑。

2. 应用开发生命周期过程的合规

对于 PCI-DSS 针对生命周期过程各个阶段的要求，归纳的实践方法具体如下：

编码阶段(PCI-DSS Requirement 6.5.1-6.5.9)。OWASP 中 antiSamy、ESAPI 和 EnDe 等编码接口的使用，可较好地满足开发过程中的编码规范的要求。

代码审核阶段（PCI-DSS 6.3.2）。通过引入 OWASP 的 LASPE 工具，则可有效地应对并符合对具体代码进行检查和审核的要求。

测试阶段（PCI-DSS 要求 6.5.1-6.5.9）。通过使用 OWASP 计划中的测试工具，如 W3af，可有效地展开基于标准要求的 OWASP top 10 漏洞的测试工作。

生产阶段（PCI-DSS 要求 6.2）。通过使用 CVSS（通用脆弱性评分系统），可有效地对生产阶段所发现的漏洞进行评级，并确保关键的应用安全问题及早得到修复。

四. atsec 与安全开发

作为专注于信息安全领域的安全咨询和评估机构，atsec 一直关注于软件开发过程的安全性。除了为多家业界一流的厂商，如 IBM、HP、Microsoft 等提供基于标准的软件安全咨询和测评服务外，atsec 关注于涉及应用开发的厂商以及机构在安全开发方面的能力提升。在此有一个消息与大家分享，atsec 已于近期与中国信息安全认证中心（ISCCC）合作共同推出 CISAW 安全软件开发课程，并预计于 2012 年第一季度开展第一期培训。

编后语：作为应用安全性方面的一个问题，即如何有效地将安全问题在未产生影响前得以识别和应对。而通常的情况是，作为开发人员来讲，通常很难把主要的精力投入到考虑软件的安全性本身，而专业的安全人员通常不会被分配完成代码的编写工作，软件的安全性提升并非一朝一夕，也并非一己之力所能解决。在此也希望与业界的各位同仁一道，共同为提升软件开发过程中的安全而努力！

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：+86 10 84834011
传真：+86 10 82890017
Email: info_cn@atsec.com