Publication: Lianhe ZaoBao, Pg 26
Date: 23 March 2017
Headline: How to select certified information security products 如何选 信息安全合格产品

企业 Q&A

如何选择 信息安全合格产品

李迎九

问：产品的信息安全为何漏洞百出?

答：信息安全是一门快速发展并且专业性很强的技术。即使是很有经验的软硬件工程师精心打造的信息技术产品，也可能存在很多信息安全漏洞。

随着时间的推演，有些漏洞会被研究人员或黑客发现。包括笔者在内的业界人士就发现了许多苹果手机和安卓手机系统的漏洞。随着软硬件规模的扩大，潜在漏洞的数目也会随之快速增长。因此，有效的信息安全技术也必须更加专业化。

然而，据笔者观察，市场上许多信息安全产品并非由信息安全方面的专业人士打造。这就好比外科医生的手术器具未经外科医生的设计及评价。

毫无例外，每个信息安全产品的营销团队都声称自己的产品安全、可靠、强大、甚至便宜。这在一定程度上给采购者或消费者造成选择上的困难。

问：如何判断产品的信息安全合格?

答：非专业人士要如何选择合格的信息安全产品呢？笔者在此提出三个建议，包括核心技术透明化、研发团队专业化，以及产品评估标准化。

一、核心技术透明化。信息安全的一个基本原理是“透明化”，即信息安全产品的核心技术应该公开，并且接受专业人士的评估和检验。这一原理被称作Kerckhoffs原理或Shannon原理，长期以来被业界普遍认同，并且极大地促进了信息安全技术的发展。然而市场中许多信息安全产品却没有遵循这一原则，以致不可能对其产品的安全性进行评估。这一类把安全性建立在“秘密配方”基础上的产品，其安全性是可疑的，也是不可靠的。随着时间的推移，其“秘密配方”可能由于种种原因（例如逆向工程和内部人为攻击）泄露，直接导致其产品安全性的失效。

二、研发团队专业化。由于信息安全技术的专业性及复杂度，合格的信息安全产品的研发团队中，应该有信息安全方面的专业人士自始至终地参与。这里所说的专业人士，不仅是指熟悉信息安全方面的标准与工具，还应该了解信息安全研究发展的前沿。

鉴于信息技术的快速发展，笔者建议了解信息安全最前沿技术的专业人士（包括学术界人士）积极参与信息安全产品的研发，或者提供必要的咨询。

三、产品评估标准化。一个合格的信息安全产品需要经过严格、公正的评估。这种评估最好由专业的第三方根据国际标准实行。

例如，国际标准信息技术安全评价通用准则（Common Criteria）可以用来评价电脑安全产品在特定使用环境中的安全属性和等级。对于规模不太大的软件系统而言，可以考虑用严格的形式化方法（Formal Method）来证明其没有安全漏洞。

另外，特别的侵入测试（Penetration Testing）可以用来测试产品的安全属性。这样的测试只能针对当时所知的一部分安全漏洞和侵入方法进行检测，其结果不能适用于当时没有检测到的安全漏洞和侵入方法，以及其后新发现的安全漏洞和侵入方法。因此，侵入测试的适用范围是有局限性的。

作者为新加坡管理大学信息系统学院副教授