网络安全信息简报

安博士月刊

2014.07（Vol.21）

POS 系统的安全问题，

POS系统面临的安全威胁

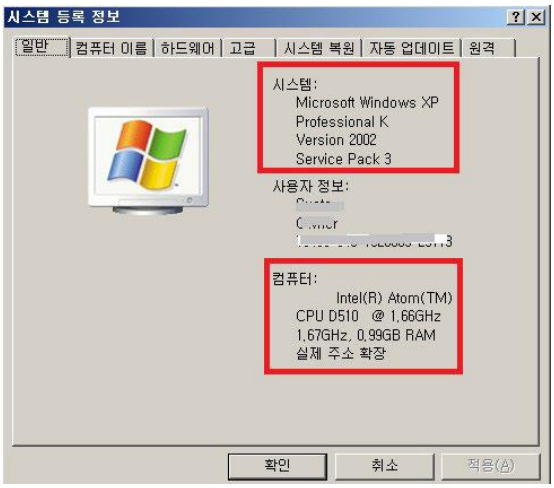
POS系统的安全问题及最近的安全事故

POS系统（Point of Sales，销售点管理系统）的安全问题最近经常在媒体报道。其实，很早以前安全专家曾警告POS系统存在的安全危险性。但是，“安全”这个问题如往常并没有引起人们的广泛注意。直到去年12月，各国发生大规模的POS系统被攻击事件，POS系统的安全问题才开始受到关注。另外，微软中止了Windows XP的支援，这使大多数的还在使用该操作系统的POS系统面临了重大挑战。随着POS系统的广泛应用， POS系统的安全性和保密性越来越受到关注，POS系统的安全问题已成为了社会的问题。

如此，POS系统持续受到多种多样攻击，本刊将叙述有关POS系统的安全问题和其攻击手法。

POS系统即销售时点信息系统，是指通过自动读取设备（如收银机）在销售商品时直接读取商品销售信息（如商品名、单价、销售数量、销售时间、销售店铺、购买顾客等），并通过通讯网络和计算机系统传送至有关部门进行分析加工以提高经营效率的系统。[1]

通常成为“POS系统、POS终端机或销售点管理系统等。大部分的POS系统在内存空间在256MB~1GB之间的低配置的设备中运行。而且大部分的POS系统在 Windows 操作系统下运行，其中还有 Windows XP。最近，部分POS系统已进行了操作系统的版本升级，但是大部分的销售点仍然最广泛使用Windows XP。



【图 2】 POS系统终端机系统配置示例

【图 1】POS系统

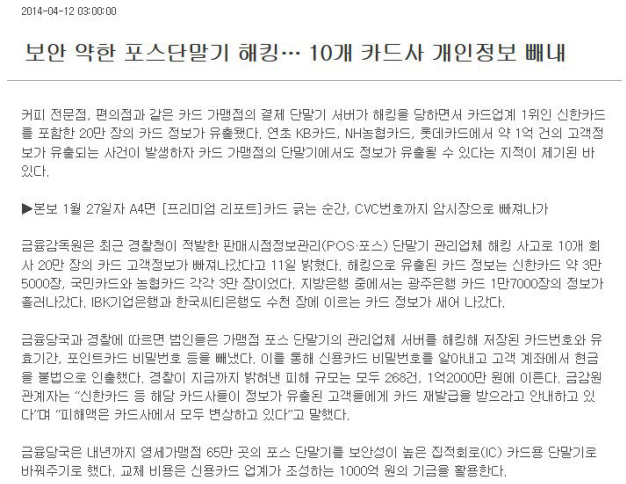
POS系统的入侵事件

最近国内外发生了多数攻击POS系统盗取信用卡信息的事件。对此，各国政府代替容易获取信息的磁卡，推广了内置IC卡的芯片密码(Chip-and-PIN)方式的信用卡。 由于识别IC卡的读卡机的普及不足， 除了欧洲地区使用内置IC卡的方式，其他地区仍然使用磁卡方式。

1 百度百科， http://baike.baidu.com/view/2053724.htm?fr=aladdin

1. 韩国事例

从2000年开始攻击POS系统的事件频繁发生，而大部分黑客没有露出水面。但在去年12月，攻击咖啡点和饭店使用的POS终端机窃取信用卡信息的不法分子被检举。据媒体报道，犯人窃取了全国85家加盟店POS终端机里的20万5000个卡交易信息，利用该信息制造伪造卡，然后在国内外的自动取款机(ATM)机取出了1亿2000万韩元。



2014-04-12 03:00:00

보안 약한 포스단말기 해킹… 10개 카드사 개인정보 빼내

커피 전문점, 편의점과 같은 카드 가맹점의 결제 단말기 서버가 해킹을 당하면서 카드업계 1위인 신한카드를 포함한 20만 장의 카드 정보가 유출됐다. 연초 KB카드, NH농협카드, 롯데카드에서 약 1억 건의 고객정보가 유출되는 사건이 발생하자 카드 가맹점의 단말기에서도 정보가 유출될 수 있다는 지적이 제기된 바 있다.

▶본보 1월 27일자 A4면 [프리미엄 리포트]카드 긁는 순간, CVC번호까지 암시장으로 빠져나가

금융감독원은 최근 경찰청이 적발한 판매시점정보관리(POS·포스) 단말기 관리업체 해킹 사고로 10개 회사 20만 장의 카드 고객정보가 빠져나갔다고 11일 밝혔다. 해킹으로 유출된 카드 정보는 신한카드 약 3만 5000장, 국민카드와 농협카드 각각 3만 장이었다. 지방은행 중에서는 광주은행 카드 1만7000장의 정보가 흘러나갔다. IBK기업은행과 한국씨티은행도 수천 장에 이르는 카드 정보가 새어 나갔다.

금융당국과 경찰에 따르면 범인들은 가맹점 포스 단말기의 관리업체 서버를 해킹해 저장된 카드번호와 유효기간, 포인트카드 비밀번호 등을 빼냈다. 이를 통해 신용카드 비밀번호를 알아내고 고객 계좌에서 현금을 불법으로 인출했다. 경찰이 지금까지 밝혀낸 피해 규모는 모두 268건, 1억2000만 원에 이른다. 금감원 관계자는 "신한카드 등 해당 카드사들이 정보가 유출된 고객들에게 카드 재발급을 받으라고 안내하고 있다"며 "피해액은 카드사에서 모두 변상하고 있다"고 말했다.

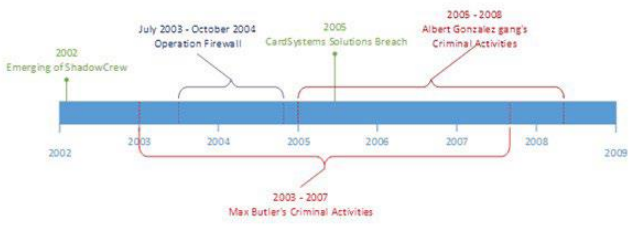
금융당국은 내년까지 영세가맹점 65만 곳의 포스 단말기를 보안성이 높은 집적회로(IC) 카드용 단말기로 바꿔주기로 했다. 교체 비용은 신용카드 업계가 조성하는 1000억 원의 기금을 활용한다.

【图 3】2013年12月发生的 POS 系统黑客攻击事件(来源：东亚经济)

2. 海外事例

惠普(HP)公司通过博客发表了从2002年到目前为止发生的多数有关信用卡的安全事件。其中，最有名的是去年末发生的美国有名大型折扣零售商塔吉特(Target)的信用卡数据泄露事件。该事件发生在美国最大节日 '秋收感恩节' 期间。据悉， 约7,000万个塔吉特消费顾客的信用卡信息在2013年11月27日至12月15日之间通过公司门店销售终端(POS)被盗。

2014年5月末，安全研究人员发现一个全球范围网络犯罪活动，其中感染了36个国家的1500个POS(销售点)终端、会计系统和其他零售后台平台。这些受感染的系统组成了一个僵尸网络，IntelCrawler研究公司将这个僵尸网络称为Nemanja。[2]

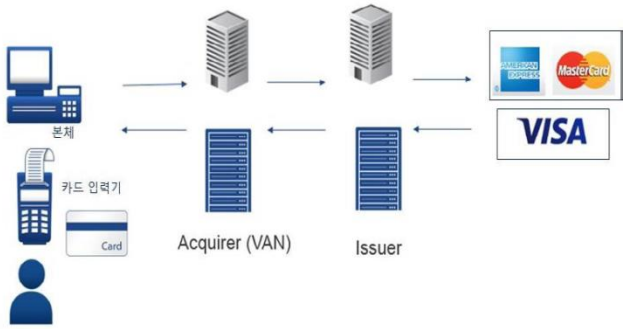


【图 4】 2002-2009 海外信用卡欺诈事例
（来源：HP博客， 'Credit card fraud scene' ）

【图 5】 2010-2013 海外信用卡欺诈事例
（来源：HP博客， 'Credit card fraud scene' ）

POS系统的组成及支付过程

POS机系统主要有下列部分组成：主机、读卡机和收银小票打印机。其中 '读卡机' ，虽然最近也有阅读IC卡的终端机，但是大部分的读卡机只能阅读磁卡，因此被成为磁条阅读机(MSR, Magnetic Stripe Reader)。犯罪分子便利用磁卡易于复制的弱点，司机攻击安全方面比较脆弱的POS系统，窃取大量的信用卡信息。



【图 6】 POS系统的信用卡支付流程

通过POS系统的刷卡支付流程如【图 6】所示。当持卡人在销售处利用信用卡付款，则POS系统的读卡机读取信用卡类型、卡号、有效期间等信息后传送给增值网络(VAN)提供商。增值网络提供商根据收集到的这些信息后，在发卡机关查询该卡的交易限额、可交易与否等信息。如无异常，正常支付，并打出刷卡支付的收据，持卡人检查支付收据上的信息无误后应在此收据上签字。至此，POS机上的刷卡程序完成。银行和发卡机关使用专用网络，具备了较完善的安全系统。因此，攻击者想利用网络攻击银行和发卡机关并窃取信用卡信息是并非易事。相反，大部分的POS系统不具备安全体系，而且还使用Windows操作系统。制作恶意软件攻破该系统，对于攻击者可以说是非常容易的事情。

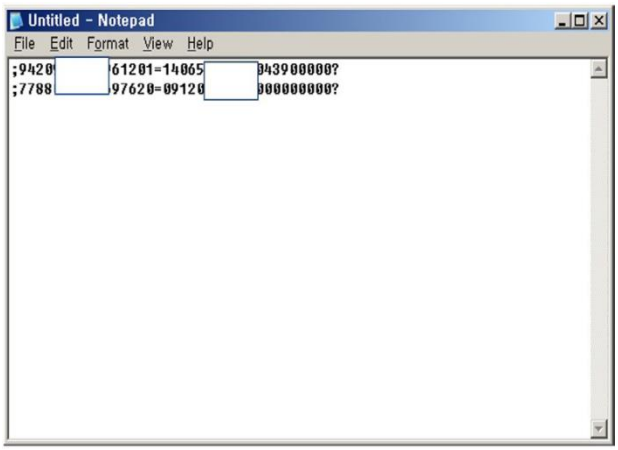
2 http://netsecurity.51cto.com/art/201405/440556.htm

POS系统的威胁因素

1. POS系统

攻击者通过攻击POS系统的磁卡读卡器MSR、内存和硬盘等窃取信用卡信息。

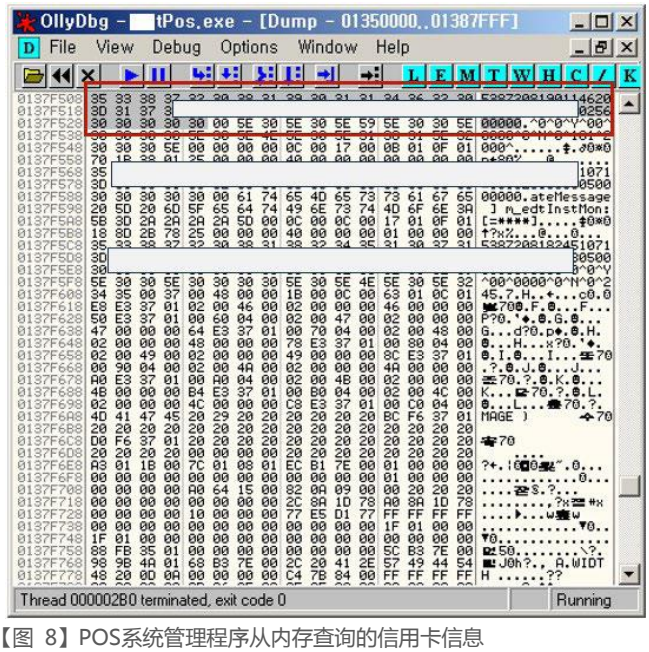
在持卡人刷卡时，通过读卡机就可以泄漏信息。大部分的读卡机可相当于一个键盘，从读卡机读取的信用卡信息输入到POS程序。此时，打开一个记事本【图 7】，可以看到信用卡号等有关信息以文本形式输入到记事本。这说明利用记录用户输入的信息的间谍软件-键盘记录器(keylogger)可窃取信用卡信息。



【图 7】 读卡机读取的磁卡信息

读卡机读取信用卡信息后，数据保存到POS系统的管理程序或内存。因此，查询POS系统的内存也可以确认信用卡信息。

另外，部分POS系统在刷卡的同时将数据进行加密。但是为了打印收据，将译码数据保存在内存，因此信用卡信息仍然处于被泄漏的危险。



【图 8】POS系统管理程序从内存查询的信用卡信息

信用卡信息在得到发卡机关的承认期间，保存在POS系统。此时，如果信用卡信息没有加密的状态下保存，只要知道相关文件，即可容易得到信用卡信息。

攻击者利用“tapping”、“漏洞”和“恶意软件”等窃取信用卡信息。

Tapping是指通过导线物理窃取传送的信息。物理窃取就要物理接近系统，而且内部要有共谋者，这就存在当场被抓的危险。

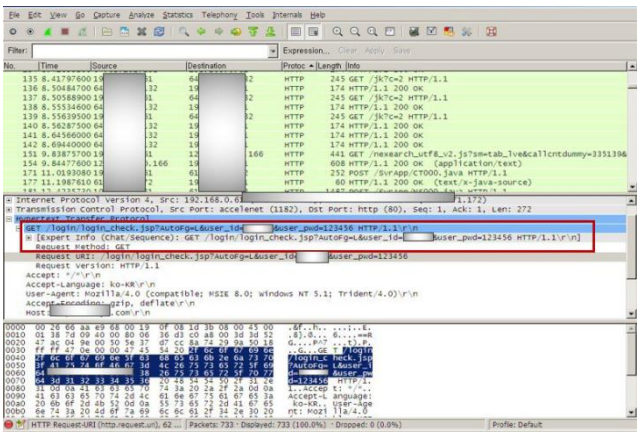
相对来说，攻击者容易窃取信息的方法是利用操作系统或POS系统的管理程序的漏洞来入侵或掌握系统。大部分的POS系统没有应用Windows安全更新。还有，许多POS系统的管理程序包含了远程控制功能。这说明外部也可以访问到POS系统。问题是如【图 9】所示，大多数加盟店的系统登录密码设置得简单，如“1234”或电话号。这使得攻击者很容易破解密码，随即入侵到内部系统。

【图 9】登录POS系统时密码示例

与其他计算机系统一样，攻击者主要利用恶意代码感染POS系统后窃取信用卡信息。因此，展开多种多样的攻击来感染POS系统。

2. 通信网络

POS系统传送的信用卡信息总体上进行加密处理，但是POS系统的管理程序的登录信息(如ID和密码)等没有进行加密的情况也存在。登录信息与信用卡信息泄漏没有直接的关系，但是有些POS运营程序在网络提供服务。因此，只要知道登录信息，外部也可以访问，即存在泄漏的危险。



【图 10】未加密传送的POS系统登录信息

3. POS系统管理提供商

POS系统管理提供商是租赁或销售POS系统或终端机的厂家。管理小规模销售点的厂家中，有些厂家在服务器保管客户的菜单和广告内容等。另外，通过管理厂家的服务器进行POS系统的管理程序的更新。因此，管理厂家的服务器被黑客攻击后程序被更换或伪造的话，与该服务器连接的POS系统也容易被恶意代码感染。

POS系统和恶意代码

1. 感染路径

POS系统基本与电脑相同，因此也可从多种路径感染恶意代码。POS系统感染恶意代码的主要路径有互联网、U盘、应用程序更新和POS系统映像恢复等。

其中，互联网的使用是POS系统感染恶意代码的主原因。很多小规模公司把读卡机和收银小票打印机连接到个人使用的手提电脑，当作信用卡支付系统使用。而且，该手提电脑还用在网上冲浪或网络游戏等，因此，被恶意代码感染的可能性较高。另外，随着社交网络的发展，利用该服务的顾客也随着增加。为了响应此类型的顾客，有时还需要访问社交网络。此时，如果该社交网络被黑客攻击，POS系统也有可能被恶意代码感染。

第二原因是POS系统连接U盘等存储装置而感染恶意代码的情况。如【图 11】所示，POS系统如同电脑一样可以连接键盘和鼠标，还可以连接U盘等存储装置。在现场，为了库存管理等，实际将U盘连接POS系统的情况较多，因此POS系统也有可能通过U盘感染恶意代码。

【图 11】 POS系统的输出入端口

第三，POS系统的管理程序的更新过程中也有可能被恶意代码感染。POS系统的管理程序与通常的应用程序一样，也通过互联网下载更新文件进行更新。如果下载的更新文件包含恶意代码，启动POS系统就有可能被恶意代码感染。

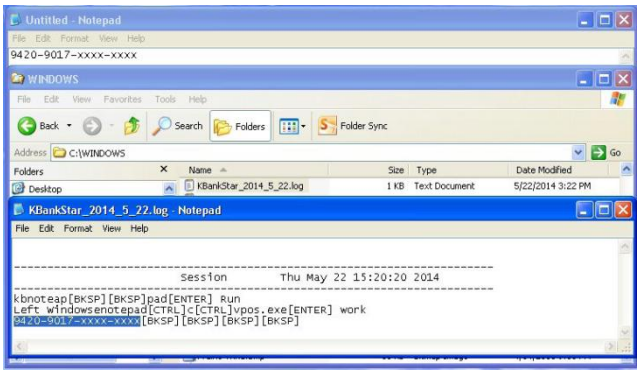
最后，当POS系统发生障碍时，为了复原系统制作的映像恢复文件有可能包含恶意代码。使用被恶意代码感染的映像文件进行系统恢复，导致系统也被恶意代码感染。

2. 攻击手法

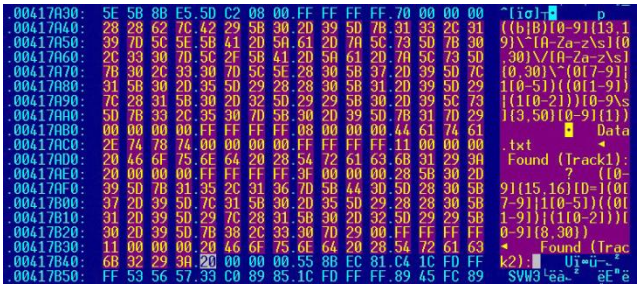
利用恶意代码窃取信用卡信息时使用的攻击手法有键盘记录(keylogging)和内存擦除(Memory Scraping)等。

当通过读卡机刷卡的时候，信用卡信息将输入到POS系统的管理程序。攻击者就在中间截取该信息，利用该信息复制信用卡。在韩国发现的大部分的恶意代码都包含了键盘记录功能。攻击者主要利用商用的键盘记录器或远程控制程序，而不会亲自制作为键盘记录的恶意代码。

美国等国外比起键盘记录方式较多使用内存擦除方式。



【图 12】 利用键盘记录方式的信用卡信息窃取



【图 13】利用内存擦除手法的恶意代码查找的字符

到目前为止，我们了解了POS系统和相关安全问题，尤其是利用恶意代码的攻击手法。有关POS系统面临的主要安全威胁和实际发生的POS系统被入侵事件，我们将在以后的期刊中继续讲述。

<참考网站>
http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/HP-Security-Research-Threat-Intelligence-Briefing-episode-12-The/ba-p/6434420#.U3ceTnIvm1L
http://intelcrawler.com/news-18

http://www.ahn.com.cn
http://global.ahnlab.com
http://www.ahnlab.com

关于安博士（AhnLab,Inc.）

安博士的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

安博士已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号院望京SOHO220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932 / +86 21 6095 6780 | v3site@ahn.com.cn