Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security for Online Transaction Processing in a White Label Financial Switch

White label financial switches have introduced automatic banking machines (ABMs) in niche markets by taking advantage of cheap modern network and PC technology. However, the use of such technology in ABMs and white label switch data-centers makes these systems susceptible to the same attacks as a common office computer network. The white label market and component organizations are described briefly to set the business context, and the security threats to its network environment are cataloged. The focus is on online tr...

Copyright SANS Institute
Author Retains Full Rights

AD

Security for Online Transaction Processing in a White Label Financial Switch

Fabian Soler

GSEC Practical Assignment V1.4b, Option 1
December 17, 2002

Abstract

White label financial switches have introduced automatic banking machines (ABMs) in niche markets by taking advantage of cheap modern network and PC technology. However, the use of such technology in ABMs and white label switch data-centers makes these systems susceptible to the same attacks as a common office computer network. The white label market and component organizations are described briefly to set the business context, and the security threats to its network environment are cataloged. The focus is on online transaction processing including remote access, wired networks, and wireless networks. Standard industry security mechanisms help to provide protection for financial transactions, but do little to protect the network itself. Threat vectors, security measures, gaps and solutions are outlined for each component of online transaction processing, with particular reference to such systems in Canada. The conclusions point to a Defense-In-Depth architecture built on a step-by-step analysis of the threats and threat vectors in online ABM networking. Recommendations for ABM design, and future subjects for investigation are offered.

Introduction

White Label Financial Switches are organizations that connect privately owned ABMs and POS devices to larger financial networks. Originally they started in the United States, Canada and the rest of the world to respond to niche markets where banks and other traditional financial institutions could not afford to place automatic banking machines (ABMs) due to low customer traffic and therefore low profits. White label switches and their client-partners are able to place ABMs in low traffic areas [1] by levying a surcharge but also due to advances in cheap, powerful, and scalable computer systems that can be used for both network centers and end-point ABM terminals. Today, lower costs and flexibility have allowed these younger organizations to compete effectively to place ABMs in merchant venues traditionally serviced by banks and other large financial institutions (e.g. malls, high-traffic corner stores, and gas stations). As of November 2001, white label switches managed more than one third [1] of the 35,000+ ABMs on the Canadian Interac Network [2].

White Label ABM Switching is often in the news due to the controversy over the practice of surcharging. Regardless of such social controversy, White Label ABMs are now a normal artifact of life throughout much of the modern world. The security concerns of a white label switch are therefore interesting to examine.

Furthermore, white label switches can be considered a focused, quickly evolving model of financial service delivery over electronic networks. The latest networking technologies used by white label switches today for ABM driving are likely the technologies used by the banks and other traditional financial institutions tomorrow. Security analysis of transaction processing in a white label switch may therefore be applicable to any financial institution with ABMs.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Part of the reason for the success of white label switching is inexpensive ABM technology, which has advanced dramatically since its introduction. ABMs have gone from being task-specific appliances (1st generation) to multipurpose, highly configurable devices based on the latest PC technology (4th generation). This has also resulted in growth in the ABM manufacturing sector from two or three large manufacturers to over a dozen manufacturers in the North American market alone. Each of these ABM manufacturers implement the latest and most ubiquitous PC hardware and operating system technologies to make ABMs at lower prices and with more capabilities than their competition. Unfortunately, these ABMs are therefore susceptible to the same attacks as a networked PC.

The Business Environment

The security concerns faced by a small and necessarily flexible business like this one are significant and in some ways may actually be more complicated than for a corporate network. Specifically, a white label switch has the constraint of having a business that is completely reliant on giving numerous and diverse remote computing devices (ABMs) easy, fast access to its network. Every single external connection attempt means revenue, so constant availability of the Switch is a primary objective, but it also means there is significant pressure to provide ABMs with uncomplicated access to the Switch Hosts.

The white label market is composed of a number of organizations working together to build a complete network. These will be covered very briefly here, but only to establish a background of information for understanding this paper:

- The White Label Switch is the service provider that runs a host or hosts compatible with one or more ABM types. A Switch Host is the combination of application software and computer hardware that together forms a transaction processing and routing system. The Switch acts as an access point, connecting these various ABMs into a larger financial network.

- National Financial Networks (e.g. Interac, Nyce, Star) and International Financial Networks (e.g. Visa, MasterCard) carry card-based transactions from the card "Acceptor" to the card "Issuer". The latter is the institution that gave a card with a magnetic stripe to a banking customer and tied it to the customer's account.

- An ISO in the context of this industry refers to an "Independent Sales Organization". This organization buys ABMs and places them at Merchant locations. The merchant locations could be anything from a small corner store, to malls, to casinos. The ISO and the Switch establish a relationship so that any ABMs belonging to the ISO can be connected quickly to the Switch, process financial transactions through the Switch, and receive other services like monitoring from the Switch.

There are also other people involved in the network at arm's length from the White Label Switch. They are important to the security architecture because they have legitimate access to the ABM and the computer inside the ABM:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- the Merchant, on whose premises the ABM is located, may in some cases replenish the cash or printing supplies in the ABM

- a Cash Owner may have access to the ABM in order to replenish the cash

- ABM Technicians employed or subcontracted by the ISO may have access to the ABM in order to load supplies into it (e.g. paper, ink, ribbons), or they may be required to perform maintenance on the ABM hardware or software

As you can see just from the definitions given here, a number of organizations and their staff have legitimate electronic and physical access to the ABM and the Switch's network. For completeness, we'll also define an "Outsider" as someone who does not have a legitimate role in the business model outlined above.

For a more extensive glossary of terms for financial transaction processing in Canada, see [3]. More information about the white label industry is available at http://www.atmmarketplace.com.

Communications Architecture

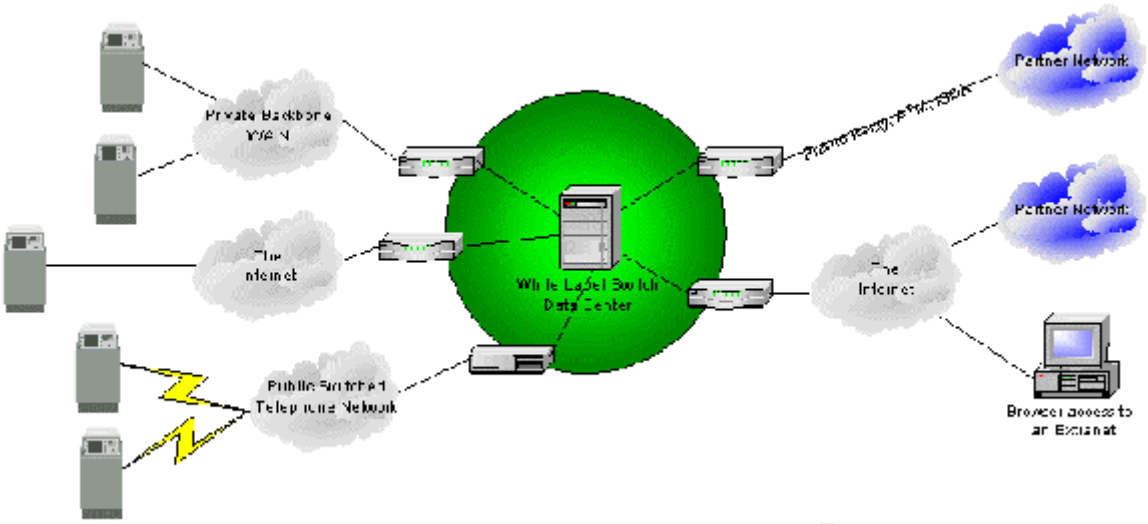
The White Label Switch can take advantage of simple dialup asynchronous communications, private WANs, Internet VPNs, or national wireless networks. In short, it might use any of the latest telecommunication systems to connect ABMs. In Canada, large telecom providers like Telus, Primus, Sprint and Bell Canada Enterprises offer many of these WAN technologies.

As with any business network, there are numerous threats and threat vectors to the Switch that can be catalogued. Any of the above telecommunication systems could be a vector for an attack.

Vectors for confidentiality attacks are of particular concern for the Switch, since an attacker might attempt to capture card-customer information. It is arguable what an attacker could gain from transaction information (customer name, bank balance, account numbers, merchant location, etc.) or whether or not it could be used for fraud. However, a confidentiality attack would certainly be harmful to the credibility of the Switch and its ability to sell services.

The following diagram presents a simple overview of the communications architecture around a white label switch.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



From this overview, we can identify several areas where security may be a concern:

- **Remote Access for transaction processing**
  How do you make the Switch Hosts in the data center easily accessible to remote computing devices (ABMs) for legitimate traffic, but resistant to attacks on confidentiality, integrity, and availability which may originate at those devices? In an electronic funds transfer system, any of these attacks may be related to fraud and are therefore dangerous to the continuation of normal business.
- **Wired Telecommunications**
  A white label switch relies on telecom providers for WAN technology to reach its clients and its partners for 7/24 transaction processing. How do you protect these areas from prying eyes amongst potentially hundreds or thousands of telecom employees with knowledge and access to your telecom lines? How do you protect yourself from threats created when you add Internet-based devices to your network?
- **Wireless Telecommunications**
  A white label switch can take advantage of national radio or microwave-cellular networks to acquire transactions. Networks based on CDPD (Cellular Digital Packet Data) and iDen (Integrated Digital Enhanced Network) are examples. Protecting the financial information flying through the air and through the carrier is critical if a financial institution is to take advantage of the reach, short setup time, and relatively low costs of these networks.
- **Partner Networking**
  A financial network may need partners to provide online transaction services that it cannot provide alone or cannot provide efficiently on its own. How do you connect to your partners to assure speed and availability without exposing your internal systems?
- **Batch Processing and EFT File Transfer**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A financial institution must be able to transfer funds to clients and partners at the end of the day to settle the day's business. How to you protect the files that dictate EFT residing on a computer or in transit to prevent fraud (threats to integrity and confidentiality) and assure settlement (integrity and availability)?

- **Information Extranets**

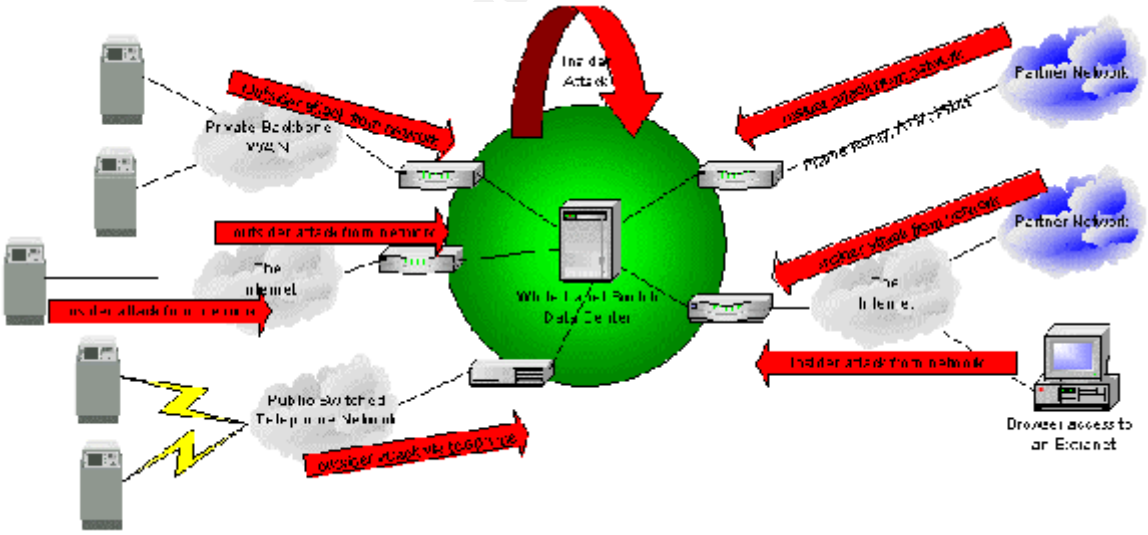
  Clients of a white label switch demand easy access to live information about the status and activities of their ABMs. Consider that a regular banking customer may access their accounts online a few times a week to get up-to-the-minute information about their accounts and transactions. The clients of a white label switch, however, may need to access information about any of their ABMs a dozen times per day to ensure each ABM is working and to assess maintenance needs remotely.

  A browser-based Extranet, for example, is a convenient and efficient method for a white label switch to share this information with its clients. However, how do you secure the information systems that provide this sensitive data to so many individuals?

- **Internal Threats**

  What protects the central network from internal fraud? Fraud can be accomplished by the misuse or altering of information, which are confidentiality and integrity threats. Internal threats to availability are a concern as well since the Switch is expected to provide 7x24 service.

By including the threat vectors within the communications network, our environment now looks something like this:



These areas have been presented to provide context for the electronic security concerns of a white label switch. The complete list is too broad to examine within this paper so, to perform a practical investigation and provide recommendations, the scope

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

of this paper will be limited to the security of online financial transaction processing for a white label switch. Specifically this paper will:

- examine current technology, then assess the threats and threat vectors
- identify gaps not handled by existing security measures
- propose solutions

Each of these tasks will be performed across the following areas:

- Remote Access
- Wired Networks
- Wireless Networks

Now, why should we worry so much about the Switch network, when there are ABMs full of cash out there that are much more lucrative targets? Here are some points to consider:

- **The Switch wants to stay in business**
  A white label switch network that is compromised looses the confidence of its customers, and may come under regulatory review [4], likely in a very political public forum. The consequences to the line of business could be devastating. From the Switch's point of view, this is far more serious than the compromise of an individual ABM.
- **The Switch must provide 7/24 service**
  The ISO clients of a Switch expect near 100% uptime, as do the larger national and international networks a Switch must connect to. Security problems that make the network unavailable could cause loss of clients for both the ISO and the Switch. It could also result in significant financial penalties levied by the larger networks against the Switch.
- **The Switch may be liable for losses**
  If an attack on an ABM was related to, or resulted from, an attack on a poorly protected Switch network then the Switch could face legal problems as well as loss of customers or financial penalties from larger financial networks.
- **The Switch must help maintain consumer confidence in the industry**
  Again, if ABMs are compromised due to attacks on a poorly protected network operated by a white label switch, then the entire EFT industry could loose consumer confidence and may even face legislation to force improvements in security planning [4]. The sensitivity of consumer confidence in financial networks is exemplified by events chronicled in [5].

Financial transactions already have some encryption and authentication security built-in as demanded by industry standards and regulatory bodies. Note that such security is designed on the premise that the PIN and transaction are all that need to be protected and that secrecy is the solution.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If we want to protect the network itself, then we must define at least part of a policy as to what must be protected. In some cases unfortunately, legal and regulatory bodies have not caught up to the technologies, or only provide general guidelines about networking security (e.g. they may state "The network must be secure and private"). The White Label Switch may not have specific higher level policies to guide the Switch's own security policies.

While the focus of this paper is not to define a complete security policy around online transaction processing, we will have to identify some of the elements that can be used to make a policy later on as a follow-up to this paper. Specifically, when we identify the threats and threat vectors in the three selected areas, we will also identify what we must protect, why, and how we're going to protect it.

Once we understand what we are protecting and why, we can propose methods and technologies that mitigate the risk to a white label switch's online networks within the constraints of this business model.

Existing Security Mechanisms

There are a handful of procedures and technologies already in place that protect the financial transactions moving through almost every financial network in the world. These should be understood before we proceed into analyzing threats and threat vectors against the White Label Switch.

Each debit transaction carries the customer-entered PIN as well as some account information in a form called the Encrypted PIN block. The data is encrypted at the ABM using the symmetric DES algorithm, and then transmitted to the Switch host, which decrypts the data using the same key used to encrypt it. The data is then re-encrypted with a key for the destination issuer or network where the transaction will be routed. More information on this subject can be found in [4]. All decryption and re-encryption is performed in one step within a tamper-proof Host Security Module, therefore no one can directly compromise the customer-entered PIN in the transaction as it moves through the various financial switches in a network. All of this is meant to ensure the confidentiality of the customer-entered PIN, and therefore the integrity of the transaction and the customer's bank account.

The debit transaction may also be secured using a Message Authentication Code (MAC) algorithm. The MAC is a cryptographic hash [6] calculated from part or the entire transaction message using a secret MAC key. The resultant code is appended to the end of the transaction message, and then the whole message is sent to the Switch. When the message arrives at the Switch, the MAC is recalculated from the message content using the same secret MAC key and hash algorithm, and compared to the MAC that arrived with the message. If the message has been altered or replayed from an earlier transaction, the MAC codes will differ and the Switch will detect and reject the compromised message. This protects the integrity of the financial transaction [7]. The secrecy of the MAC key prevents an attacker from providing a valid MAC for an altered message. Replaying the MAC'd transaction without alteration (for example to get an ABM to dispense cash) is also ineffective because the Switch Host will recognize the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

transaction as a duplicate and drop the transaction before it can be sent for authorization.

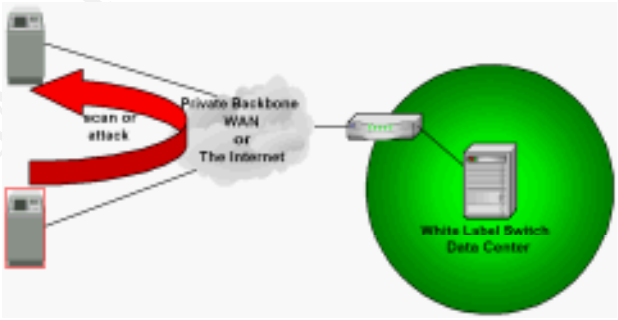
We should also briefly mention how financial institutions keep ABM, MAC, and other keys secret. For any PIN or MAC key injection process at the ABM or at the Switch, there are (normally) two key custodians. Each custodian holds one component of the key. Combining the components in a secure manner using tamper-proof security hardware produces the complete key. The complete key is actually stored within the security hardware, and is never transmitted outside of it. This scheme is intended to prevent any individual from knowing the complete key[8]. This is a very simplified review of key handling; more information about this and other key handling methods can be found in [8]

Now that we've identified the basic security present in financial switching networks, we'll take a look at the threats and threat vectors. We'll identify how the existing security mechanisms affect the threats, identify the gaps ("what" and "why"), and offer countermeasures ("how") to mitigate the risks to the Switch.

Threat Vector: Remote Access ABM Network

The ABM must have remote access to the Switch network to process transactions and possibly perform other functions like uploading an electronic ABM journal (the machine's transaction and event log), diagnostics reports, or graphics used for the ABM display. If the ABM computer can be compromised, an attacker could use it and the communications link to attack the Switch or even try to gain control of Switch hosts or other components in the Switch network.

A Windows virus or Trojan could also be introduced to the ABM since many of these ABMs run on one of the varieties of Microsoft Windows OS and include an unsecured diskette drive. The unsecured diskette drive is the vector for introducing malicious code into the ABM. The ABM network is then the vector that could introduce the malicious code to the Switch. A number of insiders have legitimate physical access to the ABM computer (the Merchant, ISO, Cash Owner, and ABM technical staff) and have the potential to do this, so this is an insider attack via the network.

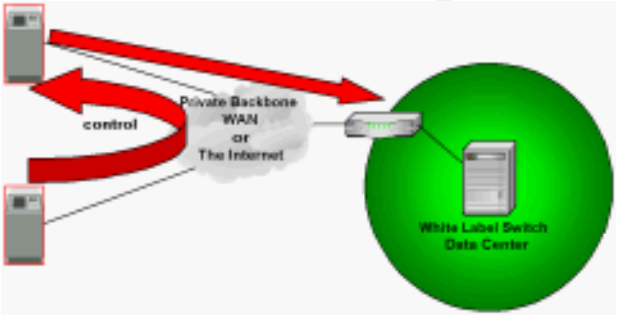


If one ABM computer is compromised, other PC-based ABMs on the WAN could be compromised. No ABM has any reason to be talking directly to another ABM through the Remote Access WAN, as illustrated below.

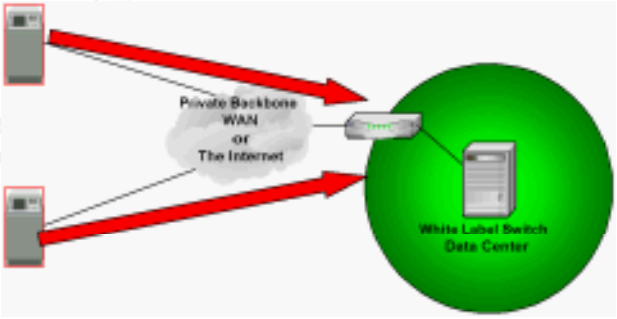
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If they can, then an attack abusing Remote Access privileges through a WAN could allow an attacker to scan other ABMs on the WAN. If open ports or services can be found, especially in the operating system, then the attacker can identify the operating system with tools like nmap and Queso. The attacker can then lookup the CVE list at www.mitre.org or hacking oriented web sites for corresponding attacks. The attacker might be able to install Trojans to take control of the target ABM. Alternatively, the attacker might introduce a virus to compromise the ABMs behavior (an integrity attack) or worms to take advantage of ABM OS vulnerabilities and spread the damage as quickly as possible to other systems in the WAN.

That in itself is a serious threat to the individual ABMs, but as far as Switch security is concerned, it could multiply the threat by giving the attacker greater resources to use in their attacks on the Switch. The secondary ABM or ABMs could scan the Switch host system for known vulnerabilities using tools like Queso or Nessus. To avoid detection the attacker could even use a tool like hping with addresses of other ABMs in the Remote Access WAN as the source of the scan packets. The attacker could then attempt to compromise the Switch Host based on the results of the scans, safely hidden away in case the scan is detected.



The attacker could even launch distributed denial of service attack.



Alternatively, if the attacker can gain control of enough ABMs, he could use them to perform DDOS attacks against other remote ABM nodes on the network that cannot be directly compromised. The net result is still an availability attack against the Switch Network, and would likely be seen by the ISO and Merchant clients as a fault at the Switch, or the WAN, but not their ABMs. Since today's ABMs do not have IDS, or system administrators nearby, such attacks would be difficult to identify quickly. By

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

directing attacks at the weaker points (the remote components) instead of the strongest points (the Switch hosts), an attacker would be employing a very effective principle of information warfare [9].

We should also note that the ABM computer does not have to be compromised at all to attack the Switch through the Remote Access network. Any computer connecting to the WAN from any access point using valid login credentials could enter the network. ABM technical staff or other ISO staff would have this information since they generally setup or maintain the remote site telecommunications equipment that use these credentials with automatic login. It does not matter if the WAN is a private backbone or an encrypted Internet VPN for this attack to be effective.

Furthermore, if procedures are not followed for the secure handling and storing of the login credentials, then Outsiders could also gain knowledge of the credentials through simple social engineering methods. Once they have the credentials, accessing the WAN with a PC is trivial. This would allow an Outsider attack on the Switch Host via the network.

Gap Analysis and Countermeasures

We've examined various scenarios but the Threat Vectors related to ABM Remote Access can be categorized as:

- Insider attacks from the Network (the WAN)
- Attack from malicious code
- outsider attack from the network

PIN encryption and transaction MACing do nothing against any of these.

This is not a surprise since those security measures are directly aimed at protecting PIN confidentiality, transaction integrity, and ultimately the integrity of the card customer's financial account but not specifically the EFT network. The situation is even less certain if the ABM is connected to the Switch by a modern TCP/IP network. In that case you have a well-known multifunction network that could carry a lot more than transactions upstream to the Switch.

We can not do much about securing the diskette drive and hence the computer in an individual remote ABM. That is at the mercy of the ABM design. We can however mitigate the risk to other ABMs comprising the White Label network by ensuring that the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

WAN architecture does not allow remote ABM nodes to talk to each other at all. This will be discussed in more detail under the sections on Private Backbone IP Networks and Internet-based ABMs, but for now we simply state that we must isolate the ABMs from each other.

If the WAN is Internet-based, then there are no ACLs out in the WAN to prevent ABM nodes from accessing each other. In this case, using encrypted VPN connections to the ABMs would be a good idea. It would provide confidentiality of the data, and prevent attacks by Outsiders on the Internet and Insiders at other ABM locations. However, there's a problem with trying to implement VPNs in this environment. We can understand this problem by comparing remote access for a telecommuter to remote access for an ABM.

A telecommuter using a company laptop or home PC to connect to their corporation's network could be forced to use all-in-one software packages that provide secure SSH or VPN connections as well as prevent unintended links to other systems. Without such protection at the remote computer, unintended links could allow an attacker to access the corporate network via the client. A system like Checkpoint VPN-1 SecureClient is an excellent example of a solid-state personal firewall and VPN client that allows the remote computer to communicate securely (over a VPN tunnel) with host servers but also prevents attacks through unintended links at the remote computer [10]. Anti-virus or anti-malware software could be added to the remote laptop to protect the network from the introduction of malicious code which could be more successful at attacking the central host if up to date defenses are not employed against them [11].

Now think about the ABM-Switch connection. The ABM and all related equipment at the site is owned by the ISO, and ABM manufacturer will not support their product if someone else installs new software on the ABM's computer. The manufacturer could argue that such software is not part of their design and may not be compatible with the ABM application and interfere with it. This precludes the use of Switch-deployed VPN software, anti-virus, or anti-malware tools. Therefore, software solutions for remote access are not viable in this business environment.

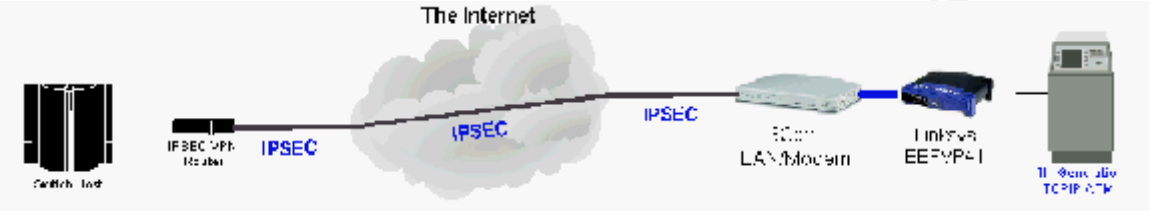
IPSEC VPN solutions like those offered by Cylink Corporation in [18] are also interesting but not viable in this business since we cannot modify the software inside the ABM. On the other hand, we could look at pure-hardware VPN solutions, like a Cisco PIX 501/506 Client [12]. This device could sit inside the ABM and allow setup of an end-to-end 3DES IPSEC VPN between the ABM and the Switch Hosts. Unfortunately, this unit is in the range of $600 US which is too expensive for ISO's to install in each ABM just for communications. It also does not address communications for legacy ABMs that may not support TCP/IP and Ethernet.

At this point, the author presents a VPN solution that was developed from off the shelf SOHO networking devices. The following VPN hardware solution is simple to configure and allows an ABM to communicate securely to the Switch Host server over an IPSEC tunnel with strong encryption and authentication. This combination of devices is easy to configure and only costs about $250 US, an acceptable cost for placing a multi-function TCP/IP ABM in a remote location where other telecom options are too costly. The point of presenting this solution is to show that with a little creativity, a viable, cost-effective

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

solution can be found to meet a security need not fulfilled by standalone commercial products.

The diagram below shows the proposed solution. A 3Com Lan-Modem provides Ethernet-to-PPP communications. Behind it, a Linksys BEFVP41 router configured with a simple IP address on the WAN port, provides the IPSEC VPN endpoint. This combination has been tested by the author and proved compatible with CheckPoint VPN-1 and CISCO PIX VPN products at the Host end.



In this scenario, an attacker could not launch a successful confidentiality attack via the network on the message or its DES Pin block. The entire transaction is protected from exposure with strong encryption using 3DES IPSEC.

Finally, let's look at the next layer of our defense: a firewall. A stateful packet inspection firewall could detect improper access attempts from the ABM population, in either a private WAN or an Internet-based WAN. Note that if we are using VPN tunnels as in the previous diagram, the firewall must be placed between the demarcation point of the VPN tunnel and the local Switch network or Switch Hosts, otherwise the VPN tunnel may carry scans or attacks right into the local network.

With the firewall we can limit incoming traffic to only financial transaction TCP ports, whose contents are only data and do not contain crafted packets. FTP access can be allowed outbound-only from the Switch to allow the retrieval of journal files from ABMs and download of marketing graphics to the ABM. If we use a stateful packet inspection firewall that should help reduce the risk by filtering out some of the traffic trying to exploit any weaknesses in the TCP/IP stack of the Host application [13]. Such packet traffic could at least cause the application software to crash. The firewall could also provide early warning of problems if it detects crafted packets or scanning attempts from an ABM (or a computer using the ABM's valid credentials). In a closed network, no such traffic should exist, so it is a clear sign of improper use of the network.

Finally, we need to protect the Host Switch against the common threats of Trojans, worms, and viruses. Secure communications technology and firewalls will not help us very much with these kinds of threats. If an attacker or malicious code has managed to get into the network and past our firewall, then we will need another layer of defense to protect the Switch or at least generate an alert. Host-based Intrusion detection systems are therefore a natural addition to our defense strategy.

Besides host-specific tailoring, the greatest advantage of deploying host-based intrusion detection at the Switch is that HIDS matches the business model of a white label switch.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As stated earlier, the Switch evolves quickly to take advantage of new technologies and take on new opportunities, which means it may be susceptible to new threats faster than the Switch's IT administrators can plan against them. Detecting and possibly blocking previously unknown threats is a strength of a well-tuned HIDS[14]. Since HIDS works best on systems that are fairly static, HIDS is a good choice for the Switch Hosts responsible for transaction processing. Such servers should not change except for scheduled upgrades. To support the HIDS, we can also implement anti-virus software on all computer systems in the Switch's data center, not just the static servers. This adds protection against viruses and in some cases against known Trojans and worms using a different mechanism.

Finally, we must consider our applications on the Switch hosts. The financial application as well as any TCP/IP capable software used for interacting with the ABM should be tested with a tool like Nessus to ensure they are not vulnerable to TCP/IP stack or buffer overflow attacks. For example, a Ping of Death attack could be sent through the network over the TCP port used for Online Financial Transactions. If such fragmented packets get past our firewall and reach the Switch Host, we need to be sure our Host would not just crash or allow a buffer overflow exploit. The same needs to be done of course with any software at the Switch Host data center that may interact with the ABMs.

We have started to build a plan for our defenses against abuse of Remote Access privileges. We have an inexpensive and easy to configure VPN solution for any Internet based ABMs and a firewall to filter out and report some illicit traffic. We also have HIDS and anti-virus software in the Switch Host computers should all these other measures fail, and we will harden our Switch Host applications to prevent simple well-known exploits against our TCP/IP stack.

To complete this discussion of security for Online Transaction Processing, we need to take a closer look at the communications network itself. The Switch network may actually consist of several different telecommunications technologies, so we will examine a few mediums for ABM traffic to see if our defenses protect us there, and what other measures we need to take.

Wired and Wireless Telecommunications

A white label switch must support a small, attractive mix of wired and wireless WAN systems to carry transactions into the Switch hosts. This is intended to keep costs low where possible with modern networks, but attract clients who need support for older ABMs and protocols.

Earlier generation ABMs support protocols such as SNA, X.25, and TC500. Fourth Generation, PC-based ABMs may support those protocols as well as asynchronous dial-up, and TCP/IP. There are also translation devices available which convert older protocols into TCP/IP to allow the ISO's to use their legacy ABMs with modern TCP/IP networks [15].

Furthermore, not all communications methods are suitable or available for all areas. For example, an ABM at a rural fair would need to use a wireless protocol since

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

installation of permanent phone lines or other wired WAN technologies would be expensive, time-consuming, and inappropriate for a temporary venue.

We'll consider a sample of four WAN technologies that meet various combinations of ABM abilities and needs. Each could potentially be a vector for threats against the White Label Switch hosts:

- Legacy X.25 networks
- Private Backbone IP VPN
- Internet-based VPN
- Asynchronous dialup over a public switched telephone network
- regional or national wireless IP networks

Threat Vector: X.25/3201 Networks

The X.25/3201 protocol is still used in networks such as Canada's Datapac service, which is used extensively by white label switches and traditional financial institutions for ABM and POS terminal driving. 3201 protocol, which is encapsulated within X.25, is used for communicating with terminals.

Datapac and similar 'public' X.25 networks are not difficult to access. While it is not as open and accessible as the Internet, you still only need to buy an account (called a "Network User Interface" or NUI) to get into Datapac. Much like an organization working hard to secure their Internet links while forgetting all their dialup modems, there are many organizations still running systems with unsecured, unmonitored, and perhaps even unknown X.25 modems. According to some discussions on the Internet, North American financial institutions in particular have not yet phased out their X.25 WANs in favor of modern IP networks or IP VPNs[16], making this network an attractive target for hackers. Unfortunately, hackers are very much aware of this network and its use. There are currently a dozen documents describing Datapac and how to hack it on the "Hack Canada" site http://www.hackcanada.com/canadian/hacking/. One document in particular extols the virtues of this attacking via this hidden network, and includes scan results dated as recently as July 2001[17]. Combine this network with the dangerous information still available on the web for probing and attacking it, and we have found another threat vector for any business using this network.

An X.25 WAN is also susceptible to physical probing. X.25 network lines have the same physical vulnerabilities (known circuit locations, easy access at multiple points, etc) as outlined for ATM and Frame Relay lines in [18]. Telecom staff, many with legitimate reasons to access the physical X.25 lines, could execute a confidentiality attack on the Switch's network by grabbing private information from transactions. Further, Information Integrity is protected by using MACing, but Availability attacks are still possible by disrupting the right circuits.

It is interesting to note that mitre.org has only one CVE candidate for X.25, which can be found at http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0648. While X.25 is not as well known these days as TCP/IP, security by obscurity is not an adequate countermeasure to protect the Switch from the X.25 WAN, so it is still a threat vector.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Gap Analysis and Countermeasures

X.25 can be secured by auditing the computer system's process list for listening X25 services or active sessions. Any open X25 ports should be tracked down and if possible deactivated. Further, all legitimate hosts and ABMs in the network should be defined as members of a Closed User Group or CUG. In Canada, Datapac implements a CUG upon request. Only circuits identified as members of the CUG can access other members in the CUG. Note that new members can only be added to the CUG by offline written authorization sent to Datapac from the 'owner' of the CUG.

This is effective against outsider attack through the physical network, however, since there is no layer of encryption, there is no protection against physical attacks on the network wiring. Encrypted IP over X.25 is not possible because there are no software or hardware solutions that could be deployed at the remote ABM end of the communication.

Considering the availability of information for X.25 hacking, and the lack of updated tools to prevent hacking, then a better method of securing an X.25 network is to get rid of it and close the X25 circuits at the Switch. If feasible based on business requirements, there are technologies on the market which can translate X.25/3201 to TCP/IP, thereby allowing clients to keep using older machines while eliminating the need for an X.25/3201 network for the White Label Switch [15].

Threat Vector: Private Backbone IP Networks

In the last few years some telecom companies have started to roll out managed WANs or private IP networks for business users [19] [20]. These networks are designed mainly to allow remote clients to access their corporate networks, but can be easily adaptable to the needs of the White Label ABM market. The remote ABM complex just needs to support dialup PPP to access one of the network's Points of Presence (POPs). The most advanced private networks give the organization using the network the ability to directly manage their own login credentials [19]. These credentials are used during the PPP authentication sequence for authorized users to get into the Switch's segment of the overall private WAN.

An ABM supporting Ethernet TCP/IP could use a device like a 3Com OfficeConnect LAN-Modem or Netgear LAN-Modem to perform PPP dialup into one of these private IP WANs. A legacy ABM could use the previously mentioned 3201-to-IP converter to accomplish the same thing.

Gap Analysis and Countermeasures

Without encryption at the edges (from the ABM to the Switch) a private IP Network is vulnerable to examination at the wiring level much like the Frame Relay and ATM lines discussed in [18]. A confidentiality attack by Insiders is possible. Unfortunately, since the network is private, the cost of extra encryption hardware at the ABMs is harder to justify against the perception that the network is already perfectly secure.

The firewall and the HIDS from earlier however, are already present and do not raise the site cost. The best way to use the firewall with this private backbone WAN is to put it on a separate NIC on the firewall, which should allow us to use simple rules to control

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

its traffic [21]. The firewall and HIDS provide a significant defense against the private backbone network as a threat vector, and also provide the excellent opportunities for incident handling.

Consider that there is no reason for an ABM to scan the private backbone network or perform anything but file transfers or online transactions to the Host, so identification of an attack is easy using the firewall or HIDS alerts. Containment of the offending ABM (or computer using stolen ABM credentials) is also easy since Switch staff can immediately disable the login credentials used by the attacker and force them off the network. The ISO can be contacted immediately to begin eradication and recovery procedures in cooperation with Switch staff.

There is one final note about security of the private backbone network. Earlier we stated that we must prevent ABM nodes from talking to each other. We do this to prevent an attacker from compromising or silencing ABMs that are the life-blood of the Switch, and to prevent an attacker from using compromised ABMs to further attack the Switch Hosts. We also do this so that we do not perform an availability attack on an ABM wrongly implicated of improper behavior thanks to IP address spoofing. We therefore make it a contractual business requirement that the network carrier's Access Control Lists and authentication architecture must prevent connections between the remote nodes. The ACLs should also perform strict egress filtering to prevent source address spoofing. Switch staff can (with written permission) set up a PC with remote-access credentials to scan the IP address space on a regular basis with a tool like nmap to ensure the ACLs are doing their job.

We have now added ACLs on the private WAN (for strictly controlled communications and egress filtering) to our list of defenses.

Threat Vector: Internet-based ABMs

ABM manufacturers generally leave telecommunications security up to the Switch network, and assume the ABMs are on a sufficiently secure communications link of some kind. This becomes a real problem however if you want to connect an ABM that only supports DES through the public Internet. DES has not been considered a secure encryption method for the Internet since 1997 [22], so we could not ensure reasonable safety of PINs from a brute force attack. Not to mention that there is absolutely no protection for personal information like the card magnetic stripe, account number, client name, bank balance, etc that are in the clear in the transaction request or response.

A financial institution or white label switch must above all else be able to protect and prove their network's availability, and confidentiality, and integrity otherwise they may not be allowed to process transactions through larger networks, or at the least may not be able to attract and keep clients. Combining the significant confidentiality vulnerabilities listed above with the high threat of the Internet attacks results in a high risk (Risk = Threat x Vulnerability) [23].

However, the Internet may often reach remote areas that private WANs and wireless networks either do not reach or cannot reach in a cost-effective manner. Satellite IP networks for example, while available virtually anywhere, may not be useful in indoor venues, and are too expensive for most ABMs in this market. If we can lower the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

confidentiality vulnerabilities (not covered by PIN encryption and MACing measures) then we can lower the risk to an acceptable level. Once that is done, we can reassure ISO clients that such ABMs can be secure.

We can use the VPN solution identified earlier (combining an IPSec router with a dialup LAN-modem) to connect an ABM to the Internet inexpensively, and provide secure communications between the ABM and the Switch Hosts. Using standards (IPSEC and ISAKMP) recognized by the security and networking community as effective and resistant to attack, and by implementing them according to best practices (careful management of shared secrets, using strong authentication and encryption, etc [24][25]), we can backup our confidence in the solution.

The VPN solution protects message confidentiality, and in combination with the firewall (only allowing VPN traffic through) at the host it protects the Switch. Note that we should also pass network traffic through the firewall both before and after it has been decrypted to ensure the information within the VPN tunnel does not contain illicit traffic. In this configuration, confidentiality and integrity of the transactions and the Switch network are protected since only VPN traffic with authentication can properly pass through the firewall to the Switch. Unfortunately, even if we implement a packet filtering router on our Internet link, an availability attack is still possible and very difficult to protect against.

Unlike the private backbone WAN, with Internet-based ABMs we are limited to ignoring the incoming scans or tuning and checking our defenses against specific attacks that we detect. We might also enlist the help of our ISP in blocking traffic from a given host or domain if we decide that is safe to do and won't block legitimate users. Beyond that, the most we could do would be to report the attacker to the offending ISP and hope they are considerate Internet neighbors and do something about the traffic, or we report the problem to legal authorities

Threat Vector: Dialup Modems

Many ABMs send transactions to the network via asynchronous dialup connections. The Switch may have dozens of open modem ports waiting for such connections. Furthermore, many ABMs can also dial into manufacturer-provided monitoring and management software installed at the Switch site. The capabilities and security of these applications may not always be fully known. The following URLs identify some of these ABM manufacturer products:

http://www.tritonatm.com/public/products/tritonconnect/main.htm

http://www.tidel.com/products_aimsoftware.asp

http://www.tranax.com/products/webrms/

Although these modems on the Switch Host do not run TCP/IP, or a login shell, availability attacks are still possible. An attacker may attempt to send data to overwhelm the modems or the host application's communication buffers and thereby crash the software.

There is greater risk if the Switch is running third party software whose full operation is not well understood. Such systems could be placed in a segment of the network

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

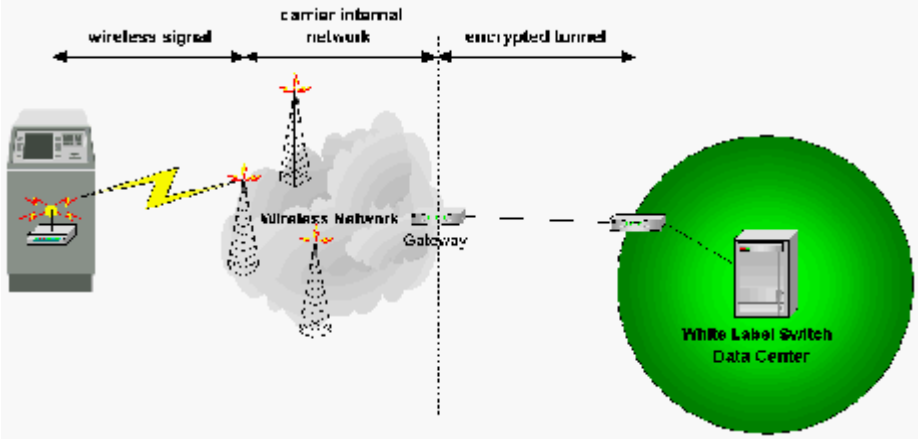
isolated by a firewall so any behavior or problems with the software could be contained. If the third party software does not actually need to be on the network for file backup or other purposes, it could be run without a network connection.

In both of the above cases, open modems on the dialup Switch Host or the third party monitor, occasional audits using a commercial phone scanner like PhoneSweep would be prudent. It may also be necessary to create custom attacks to crash the modems and applications by sending large or improperly formatted data streams to see if the applications are coded well enough to defend themselves against such threats. An alternative would be to ask the application software providers to state as part of the purchase agreements whether or not their software is susceptible to such attacks so the risk can be assessed.

Threat Vector: Wireless Telecommunications

There are a number of competing wireless technologies trying to gain dominance in the wireless data arena. Most of these like CDPD, 1X, CDMA, TDMA, GPRS and so forth [26] specify how bits are delivered over wireless signals and most include some level of security. CDPD for example incorporates encryption and authentication into each packet. CDPD has already been used extensively in the US to network mobile ABMs. In Canada, however, CDPD has very limited coverage and is being replaced by other newer technologies with much larger coverage like the proprietary iDEN system from Motorola, and 1X which was co-developed and supported by various technology companies [27] [28]. For this discussion we will focus on iDen.

iDen is not an encrypted protocol by default, but is purportedly secure due to the complexities of the protocol [29]. From the carrier to the Switch, communications may occur over a traditional Frame Relay line or a VPN over the Internet.



Gap Analysis and Countermeasures

The risk of confidentiality attacks on the wireless signal is low since it would take specialized test equipment to find, parse, and decode an individual communication from the iDen wireless signal[30]. However, if the risk is deemed sufficient to warrant extra precautions, devices like Precidia Technologies' "CellDial" do provide IPSEC tunneling end-to-end to the Switch host. More information about CellDial is available at http://www.precidia.com/products/celldial.html.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

It is a straightforward matter to use a VPN tunnel with strong encryption from the carrier's network gateway to the Switch's perimeter router. It is also obvious from the diagram above that there is no explicit use of encryption between the wireless demarcation point and the gateway at the carrier. The possibility exists for legitimate telecommunications staff or subcontractors to physically access the network in this zone, just as with Frame Relay [18] as noted earlier. This is therefore a threat vector for an insider attack via the network.

Unless the carrier enforces encryption within their infrastructure, then only end-to-end encryption implemented by the Switch and ISO could guarantee total confidentiality within the network. Unfortunately there is no software or hardware solution for end-to-end encryption at this time. PIN encryption and MACing do mitigate the risk against integrity of the financial transactions and therefore the integrity of the Switch network, but private customer information might still be tapped within the telecom carrier's perimeter.

The specific defenses against abuse of remote access (firewall, IDS, Anti-Virus at the Switch data center) are just as applicable to wireless technologies and do mitigate the threat of malicious code, integrity, and confidentiality attacks at the Switch. As with the private WAN solution, if any of the above three systems detect unusual traffic from the wireless carrier, it is very likely that the Switch is being attacked or its defenses are being examined. Since the segment of the wireless WAN where ABMs reside effectively 'belongs' to the Switch, it is a simple matter for Switch staff to deactivate access for the offending node, and initiate an investigation with the carrier and the ISO that owns the ABM. If we elect to use an HIDS with dynamic response (and spoofing is not possible in this network), then the offending wireless connector can be blocked even faster.

With wireless networking for our ABMs then, we have established that existing measures (firewall, HIDS, and Anti-Virus systems at the Switch) help mitigate the threat by protecting the Switch against probing and attack. Improper access will stand out easily and can be dealt with quickly. Further, encryption can be employed in the wireless zone, and encryption is easy to implement in the zone between the carrier and the Switch. Unfortunately, the zone between wireless and the carrier's external gateway, is open to confidentiality attacks, though integrity attacks are not possible thanks to transaction MACing and PIN encryption.

Conclusions

We have examined three areas of Online Transaction Processing where vulnerabilities and limitations of the ABM systems and networks can allow hackers or malicious code to launch attacks against the Financial Switch. These areas are Remote Access, Wired Networking, and Wireless Networking.

While 4th generation ABMs may be vulnerable to the same kinds of attacks in these three areas as a regular network PC, the countermeasures available for a normal PC may not always be suitable for an ABM. Normal defensive measures can be employed such as firewalls, port scanning, and anti-virus software but such measures are one sided; they can only be employed at the Switch. In other areas, such as the use of VPN

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

technology with strong encryption, neither inexpensive software solutions nor expensive hardware solutions are suitable for the unique needs of the White Label Switching market.

VPN connectivity with strong encryption and authentication is still desirable for the resistance it can provide against brute force attacks on customer PINs, and for the extra protection it provides to confidential customer information such as bank balances, account numbers, and names in the transaction message. For VPN connectivity then, the author has proposed a simple, effective hardware system that could be assembled from inexpensive networking devices. This combination of VPN and dialup technology fits well into the networks used by an average white label switch while maintaining simplicity and low cost as required by the ISO's in this market.

By combining these common and purpose-built security measures, we have proposed a viable and effective Defense-in-Depth architecture to protect the White Label Switch. Furthermore, by selecting the particular security technologies based on a step-wise assessment of threats and threat vectors, we have provided the elements of a security policy and basic business case that could be used to justify the costs of implementing these technologies. Note as well that such measures could extend to the networks of traditional financial institutions.

Future Investigations for Financial Switching Security

There are a number of areas of risk in the White Label Switch's network that were identified but not pursued within this paper. These include:

- Partner Networking,
- Batch Processing and EFT File Transfer,
- Information Extranets, and
- Internal Threats

These are topics that could be pursued in other papers.

Another, perhaps more interesting area of investigation is the implementation of security within the ABM. ABM manufacturers could endeavor to put easily maintainable, inexpensive Firewall, IDS, and VPN software in their ABMs as countermeasures for threats like viruses, malicious code, and network hacking.

Since ABM software does not change except for scheduled upgrades, both IDS and small/personal firewall software could be setup with very simple configuration in the ABM. Such systems would provide warning and defense against most integrity attacks with potentially no reliance on regular updates. This of course is considering "what could happen" vs. "what is likely to happen". Up until now, there is no published incident of an ABM being compromised through a network or having malicious code introduced directly via physical loading of programs from diskette or other removable media. However, the market and its technologies are constantly evolving and growing, so it may just be a matter of time before such an incident occurs.

The use of VPN technology within the ABM would be particularly beneficial since it would standardize security for confidentiality and integrity right from the ABM to the Switch, regardless of the communications medium. Remember that the consumer

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

using these ABMs is likely to continue using them as long as their confidentiality is assured and the integrity of their personal accounts is not compromised. Standards-based software of this kind could easily advance the ABM's defense against malicious code and other attacks through the WAN. We've said all along that neither the Switch, nor the other players in the White label market could implement such measures in the ABM, but the ABM manufacturers certainly could.

References

[1] Financial Consumer Agency of Canada. "CONSUMER INFORMATION: White-Label ABMs and Point-of-Sale Terminals" October 4, 2002. URL: http://www.fcac-acfc.gc.ca/eng/publications/cgb/abm.asp#abm (Oct. 24, 2002)

[2] Interac Association. "Connecting Canadians" URL: http://www.interac.org/pdfs/connectingCanadians_en.pdf (Oct. 1, 2002).

[3] "Canadian Code of Practice for Consumer Debit Card Services" URL: http://strategis.ic.gc.ca/SSG/ca01581e.html (Oct. 20, 2002).

[4] Anderson, Ross. "When Cryptosystems Fail." University Computer Laboratory, University of Cambridge. 1993. URL: http://www.cl.cam.ac.uk/users/rja14/wcf.html (June 15, 2002)

[5] Appleby, Timothy. " Chilling debit-card scam uncovered." December 10, 1999. The Globe and Mail. URL: http://insight.mcmaster.ca/org/efc/pages/media/globe.10dec99.html (Oct. 21, 2002).

[6] National Security Agency, "Information Assurance Technical Framework Release 3.1." September 2002. URL: http://www.iatf.net/framework_docs/version-3_1/pdffile.cfm?chapter=ch06s7 (Oct. 21, 2002)

[7] Verifone. "Understanding Pins & Pin Pad Security In Debit Transactions." May 19, 1997. URL: http://www.usamerchant.com/PINPAdUND.pdf (Oct. 21, 2002).

[8] KPMG. "Key Management Policy and Practice Framework." February 15,2002. URL: http://www.ip3seminars.com/download/kpmg.pdf (Nov. 10, 2002).

[9] SANS Institute. "Track 1 - SANS Security Essentials; 1.2 SANS Security Essential II: Network Security." January 12, 2002.

[10] Gibbons, Ryan. "VPN-1 SecureClient - Check Point's solution for secure Intranet extension." Sans Institute Information Security Reading Room. April 9, 2002. URL: http://rr.sans.org/encryption/secureclient.php (July 29, 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[11] Maslowski-Yerges, Al. "Securing the enterprise from the dangers of remote access: Analysis of new options available for personal firewall management in comparison with other established and emerging remote access solutions." Sans Institute Information Security Reading Room. March 27, 2002. URL: http://rr.sans.org/telecom/dangers.php (July 29, 2002).

[12] Cisco. "Configuring the VPN Hardware Client on PIX 501/506 Version 6.2 for Use With a VPN 3000 Concentrator." URL: http://www.cisco.com/warp/public/471/pix501506_vpn3k.html (Oct. 21, 2002).

[13] SANS Institute. "Track 1 - SANS Security Essentials; 1.1 SANS Security Essential I: Information Security, The Big Picture." January 16, 2002.

[14] SANS Institute. "Intrusion Detection FAQ - Why is intrusion detection required in today's computing environment?" Oct 16, 2002. URL: http://secinf.net/intrusion_detection/Intrusion_Detection_FAQ/Intrusion_Detection_FAQ__Why_is_intrusion_detection_required_in_todays_computing_environment.html (Dec. 9, 2002)

[15] Precidia Technologies. "Low cost IP solutions for the retail payments industry." URL: http://www.precidia.com/products/product6.html (Oct 21, 2002).

[16] Gadaix, Emmanuel. "Penetration Testing: Re: [PEN-TEST] X25, all but forgotten?" Insecure.Org. URL: http://lists.insecure.org/pen-test/2000/Aug/0208.html (Oct. 21, 2002).

[17] Che, Doktor. "Datapac Scan - A very large Datapac scan." July 3, 2001. URL: http://www.hackcanada.com/canadian/hacking/the-d-files.txt (Oct. 21, 2002).

[18] Cylink Corp. "Leading provider of security solutions hails industry analyst group for exposing vulnerabilities of wide area networks." Cylink Corp. September 2000. URL: http://www.cylink.com/news/press/pressrels/30700.htm (Aug. 8, 2002).

[19] Meyer, David. "Sprint IP Backbone Network and MPLS" August 7, 2002. URL:http://www.sprintbiz.com/business/resources/resource/SprintCiscoMPLS.pdf (Sep. 15, 2002)

[20] Bell Canada. "Bell Canada Introduces First Internet Protocol-Virtual Private Network to Offer Bandwidth and Level of Service on Demand." April 17, 2001 URL: http://www.bell.ca/en/about/news/releas/2001/pr_20010417.asp (Oct. 1, 2002).

[21] Mackey, Richard. "Layered Insecurity." Information Security Magazine June 2002 (2002). URL: http://www.infosecuritymag.com/2002/jun/insecurity.shtml (Aug. 12, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[22] Electronic Frontier Foundation. "RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)" January 19, 1999 URL: http://www.eff.org//Privacy/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html (Sept. 15, 2002)

[23] SANS Institute. "Track 1 - SANS Security Essentials; 1.2 SANS Security Essential II: Network Security." 2002.

[24] Browne, Brian, et al. "MANAGEMENT STRATEGIES: Best Practices For VPN Implementation." Business Communications Review March 2001 (2001). URL:http://www.bcr.com/bcrmag/2001/03/p24.asp (Nov. 13, 2002)

[25] Microsoft TechNet. "VPN Best Practices." 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/sag_vpn_us02.asp (Dec. 3, 2002)

[26] Chaplin, Kevin. "White Paper: Wireless Network Technologies" Sierra Wireless Inc. June 2, 2002. URL: http://www.sierrawireless.com/news/docs/2130209.pdf (Oct. 20, 2002).

[27] "Wireless Carriers Overview." FutureQuest Wireless Inc. July 8,2002. URL: http://www.futurequest.biz/carriersoverview.htm (Oct. 4, 2002).

[28] "Digital PCS." Telus Mobility. 2002. URL: http://www.telusmobility.com/on/1X/index.shtml (Oct. 4, 2002).

[29] "Fact Sheet: Digital Security in the iDen System." Nextel Communications Inc. March 2001. URL: http://www.nextel.com/about/corporateinfo/iden_security.pdf (Dec. 10, 2002)

[30] Veeneman, Dan. "Wireless Overview: Protocols and Threat Models." Black Hat Briefings. July 31, 2002. URL: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-veeneman-wireless.ppt (Dec. 10, 2002)

Alternson, Gary. "Comparing BGP/MPLS and IPSec VPNs." Sans Institute Information Security Reading Room. January 9, 2002. URL: http://rr.sans.org/encryption/MPLS2.php (July 29, 2002).

Bayley, Robert. "Configuring a NetScreen Firewall: Best practice guideline for the basic setup of a NetScreen firewall using the command line configuration options." Sans Institute Information Security Reading Room. April 14, 2002. URL: http://rr.sans.org/firewall/netscreen.php (July 29, 2002).

Collin, Barry C. "Extranet Security: what happens if your partner turns against you?" Computer Security Institute. October 1997. URL: http://www.gocsi.com/extranet.htm (July 10, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Egorov, Andrew. "Implementing Virtual Private Networks - observations from the field." Sans Institute Information Security Reading Room. April 29, 2001. URL: http://rr.sans.org/encryption/implement_VPN.php (July 29, 2002).

Grance, Tim, Joan Hash, Steven Peck, Jonathan Smith, and Karen Korow-Diks. "Security Guide for Interconnecting Information Technology Systems" National Institute of Standards and Technology Special Publication. 800-47. August 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf (Oct. 4, 2002).

Interac Association, "Interac: Changing for the Future." October 1997. URL: http://finservtaskforce.fin.gc.ca/pdf/Interac1e.pdf (October 1, 2002)

Klavsen, Klavs. "Securing remote users VPN access to your company LAN." Sans Institute Information Security Reading Room. July 29, 2001. URL: http://rr.sans.org/encryption/sec_remote.php (July 29, 2002).

Levine, Mark. "Telecommuting safely - Remote node or remote session?" Sans Institute Information Security Reading Room. February 19, 2001. URL: http://rr.sans.org/encryption/telecom.php (July 29, 2002).

Pedersen, Stephen. "Corporate remote access VPN: Issues and a solution." Sans Institute Information Security Reading Room. January 29, 2001. URL: http://rr.sans.org/encryption/corp_vpn.php (July 29, 2002).

Schaefer, Norma Jean. "Knock, knock… who's there? Do you know who is accessing your VPN?" Sans Institute Information Security Reading Room. December 1, 2001. URL: http://rr.sans.org/encryption/knock.php (July 29, 2002).

Torello, John. "Implementing remote access: Security, usability and management." Sans Institute Information Security Reading Room. June 11, 2001. URL: http://rr.sans.org/encryption/remote_access.php (July 29, 2002).

Yankee Group, The. "Frame Relay and ATM: Are they really secure?" New Architect. February 1, 2001. URL: http://research.newarchitectmag.com/data/detail?id=992377020_897&type=RES&x=132156494 (Aug. 8, 2002).

Younker, Eddie. "IP Security protocol-based VPNs." Sans Institute Information Security Reading Room. October 9, 2001. URL: http://rr.sans.org/protocols/IPsec.php (July 29, 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced