Global Information Assurance Certification Paper

A theoretical insider attack on a financial services organisation

E-WARFARE
Certification (GEWF)
Practical Assignment v1.0

Option 2 - Analysis
17th December 2004

Submitted by: Alex Tilley
Location: Brisbane, Australia

Introduction

This Paper will detail a theoretical insider attack on one on of the systems used by financial institutions to transfer large amounts of money between banks. Also detailed will be aspects of the same attack meant to cause confusion and chaos throughout the company in question and a summary of the lapses in security exploited and methods to mitigate these risks.

This paper is not meant to be 100% factually accurate in regards to the end result of the attack (the stealing of a large amount of money). The *"FAST"* system of fund transfer is a fictional system. It is however very similar to several fund transfer systems in use by financial services companies today.

While the incident described in this paper is a stylized and hypothetical result of poor security, this paper is meant to introduce the reader to the "Swiss cheese" theory of root cause analysis and incident evolution and describe how this theory can be applied to IT security risk mitigation.

The Swiss cheese theory

The attack detailed below and indeed most other breaches of security can be viewed as results of successive lapses in security and are best described by the "Swiss Cheese" theory developed by Dr. James Reason to describe how plane crashes happen, it is described below:

> "The Swiss Cheese Theory commonly illustrates successive layers of protection, one behind the other, each guarding against the possible breakdown of the one in front…each layer has weaknesses and gaps akin to a Swiss cheese…
>
> The theory holds that these holes are created by a combination of active and latent failures. The active failure consists of errors or violations committed at the sharp end of the system. A latent failure stems from poor design, shortfall in training, inadequacy of tools and equipment, which are present for sometimes years before these conditions combine with local circumstances and active failures to penetrate the system's many defensive layers.
>
> As such, the rare conjunction of a set of holes in successive defenses allows hazards to come into damaging contact with people and assets, according to Dr. Reason as he defines the accident trajectory…"
>
> -- ***Jean-Pierre Dagon "***Root Cause Analysis with REASON"[i]

Basically while individual security lapses may mean little on their own as they are normally mitigated by other defensive layers, when these lapses are combined they can form a large hole in security through which a successful attack can pass. This theory can also be described by the following slides from the "Safety Risk assessment Newsletter" May-Jun 2004:

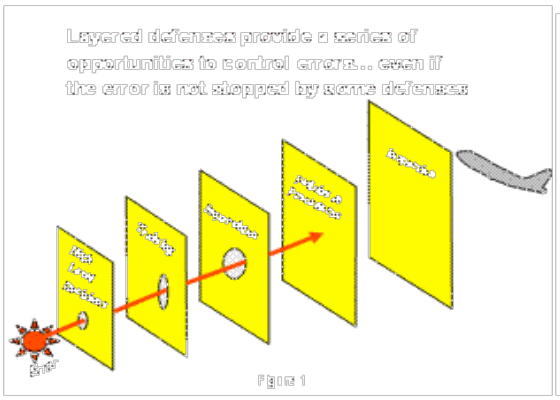

Figure 1

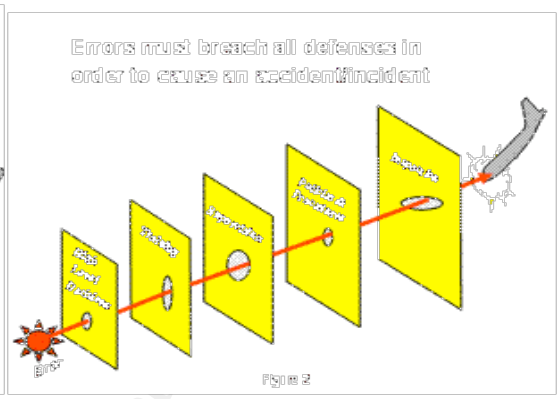

Figure 2

Further reading on Reason's "Swiss cheese" theory can be found at the end of this paper.

Setting the scene.

The subject of this paper will be a medium sized financial services organization "**Fin-Bank**" that is in the middle of major network upheaval due to the takeover and absorption of the networks and firewall infrastructure of a second smaller financial company "**B-Bank**". Due to the nature and speed at which this second company was absorbed the firewall and network infrastructure was simply "bolted together" to get the two systems working side by side with rule cleanups and reviews slated for a future date when the upheaval caused by the absorption has been reduced.

Fin-Bank's Network Security team has just completed the initial melding of firewall rule bases from the two companies. One firewall engineer becomes an insider motivated by financial gain after seeing the awful quality of the firewall rule base inherited from B-Bank. Problems with this rule base are many but the most glaring problems are:

- There is little to no commenting of rules to explain their purpose or to detail any future removal date.
- Due to the takeover resulting in the in-sourcing of the previously out-sourced firewall management for B-Bank there is little to know understanding of what many of the rules are for.
- Many rules are not set to log connections. Perhaps because log reviewing was not high on the outsourcing companies list of priorities.
- There is no higher level oversight on what rules are changed or implemented beyond a 6 monthly rule base audit by an external audit agency; this audit is only

performed so that Fin-Bank can comply with government guidelines that pertain to financial services companies.

The insider has come from a customer support/helpdesk background and due to Fin-Bank's lax policy on removing user's domain rights as they change positions within Fin-Bank's IT department he still has administration access to the company's user administration system and mail system as well as most other critical servers and all user workstations.

The insider is aware of the use of the *"FAST"* system by Fin-Bank to transfer large amounts of money daily between financial institutions all over the world. He chooses this as a possible method of gaining a large amount of money instantly by exploiting the holes in Fin-bank's security policies and his position of ultimate control over the remote access/firewall infrastructure of Fin-Bank.

The attack

Phase one: Reconnaissance

The first step taken by the insider is to locate an unused workstation and place it out of the way in a cupboard in a meeting room, plug it into an active but unused network port and confirm that he can connect to it via terminal services over the internal network. He also confirms that from this workstation he can remote control any workstation in Fin-Bank including the workstations with existing access through the firewall to the *"FAST"* service.

This completed he uses a commonly known service account (that for ease of administration has been assigned domain administration privileges) to connect from this hidden workstation to the User management system and setup a phantom account with domain administration privileges to the entire company including its mail system.

Once this account is setup he installs the company's mail server software on his hidden workstation and uses this account to start cloning the mailboxes of the Investment services mangers and team leaders, He trawls through the emails until he comes upon what he has been looking for:

----------Start Message----------
From: Team Leader Investment services Blue Team (Mary)
To: New Investment team member (Dave)
Subject: Your *"FAST"* access.

Dave, I'm going to be out of the office for a few days so just to get you started I want you to buddy up with Lisa.

Here are the passwords for this month that you'll need to access the FAST system if you're to become a fully fledged trader. I didn't get a chance to give these to you in person as I'm supposed to but I don't think it'll be a big deal:
User-name:Fin-Bank-UK2231
Password1: $e52Dg5%>4 (this one gives you the read access)
Password2: FR)34!@b)d (this one allows you to make transfers etc.)
Lisa has the program on her computer that will authorize your transactions after she looks over them.

Have a great day!
Mary.
----------EOM----------

These user ID's and passwords will be necessary complete the attack.

The next step is to access the IT support team's file server (using the common service account credentials) and copy to a CD and then install on his hidden workstation the "*FAST"* software package and this months encryption keys (kept together for ease of access when supporting demanding users in a time sensitive profession).

The Insider then checks the status of the antivirus software on workstations across the two companies by randomly remote-controlling workstations across both companies networks and finds that a large percentage of workstations in "B-Bank" have out of date virus signatures (some not updated for more than 8 months) and that many have no active antivirus solution at all (AV having been deactivated by users or having been uninstalled by support staff after malfunctioning), the situation in Fin-Bank is not much better with many internal servers being woefully unprotected and due to their out-dated operating system they have not been patched for the vulnerabilities that many worms will exploit. He confirms this by successfully downloading the "eicar.com" antivirus test file on several randomly selected workstations. The "eicar.com" test file is found on www.eicar.com and is described as:

> "A number of anti-virus researchers have already worked together to produce a file that their (and many other) products "detect" as if it were a virus… This test file has been provided to eicar for distribution as the "Standard Anti-Virus Test File"... It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. (However) Most products react to it as if it were a virus"
>
> --http://www.eicar.com/anti_virus_test_file.htm[ii]

To hamper investigations and spread chaos through the network the insider decides to release a number of different viruses and worms on the internal network at the same time with the hope that even though some are not destructive their very presence and replication methods will cause network and server/workstation degradation and in some cases destruction. This portion of the attack could be described as more a "psychological" attack than a destructive one.

After researching on www.virusall.com and www.viruslist.com he decides on the following worms. W32.Blaster.Worm, the SQL slammer worm and the W32.Korgo.U worm. He also chooses a modified version of Opaserv.K an aging but destructive worm that according to www.fireav.com

> "Contains a destructive payload, when executed it will overwrite all the hard disk sectors."
> --http://www.fireav.com/virusinfo/library/opaservk.htm[iii]

Confident that sufficient chaos will be caused to help mask his intrusion and that the ensuing IT nightmare caused by this outbreak will delay any earnest investigation he moves on to phase two.

Phase two: Preparation

The merging of 2 networks and firewall environments has led to many problems that can only be fixed by changing or adding firewall rules and installing new policies on firewalls during business hours.
The engineer takes the opportunity of yet another firewall policy install to add the following innocuous looking rule to the policy of Bank-B's perimeter and internal firewalls.

Src	**Dest**	**Service**	**Log**
Ext-printer-support	Internal-print-monitor	Print_Mgmt	No

At a casual glance this rule looks like it gives access from one external IP to one internal server for purposes of printer management.
The true detail of this rule is only revealed by viewing the contents of the policy objects:

Ext-printer-support	Internal-print-monitor	Print_Mgmt
163.223.12.54	10.23.12.45	TCP port 3389
Subnet Mask: 255.0.0.0	Subnet Mask: 255.255.0.0	

What this rule actually does is give access via terminal services from an entire Internet Class A (/8) address space to an entire internal class B (/16) address range via terminal services.
There is no oversight so no-one notices this rule is included in the policy that is installed.

N.B. The Next phase of the attack could occur from anywhere in the world as long as the attacker had access to a computer on the 163.0.0.0/8 network.
The attack could therefore originate from his home or from an Internet café in the Bahamas.

Phase three: The Attack

From a computer on the 163.0.0.0 network the engineer connects to his hidden workstation via the "Terminal Services" client. This done at a time just after business hours have closed on a Friday and with him being confident that any transfer he makes from the banks account at this time will hopefully not be noticed until business hours commence the following week. By doing this attack at this time it can be assured that only a skeleton IT staff will be working on Saturday when the full force of the worm infection is noticed.

He connects via the helpdesk's remote control software to the workstation with *FAST* access, logging in with the commonly used service account so as to further "hide in the noise" of logins/logouts using this account, he launches the *FAST* application and when prompted he enters the Bank's User-ID and passwords as harvested from the email in the recon phase.

It is now a simple matter of entering the amount, the intermediary and beneficiary banks and using the cipher-key generator installed on his hidden workstation to generate the days authorization code based on this months two passwords and the User-ID, he authorizes the transaction and waits to receive confirmation of the completion of the transfer.

N.B. As stated, the above attack is highly stylized and is not meant to be taken literally. It is presented only as an example of the outcome of holes in the "Swiss cheese" of IT security.

Phase four: The covering of tracks.

His goal reached with the confirmation of the transfer of $1,000,000 to an account of his choosing. He then remote controls several workstations and servers on both companies' networks and executes his worms. Using he "*ping"* command he is able to confirm success as ping reply times elevate and some workstations and servers stop responding as the worms begin to infect, corrupt and wreak havoc throughout both companies.
The insider then turns his attention to the *"FAST"* workstations.

After executing the "Opaserv.K" virus on each of the workstations with "*FAST"* access, the insider then reboots the workstations using the helpdesk's support tool. Again using the simple "*ping"* command he confirms that the workstations did not come back from their reboot as their hard drives are rendered useless.

This done he executes the same virus on his hidden workstation and reboots it. He attempts to reconnect and fails. The workstation being shutdown will make it harder for investigators to track down the physical source of the attack.
With his connection terminated he heads to a branch of the beneficiary bank and makes a withdrawal…

Mitigation measures

Methods to "plug the holes" in the Swiss cheese.

When taken as a whole only two or three of the below (basic) security measures could together have served to make "plug the holes" in the Swiss cheese that lead to this attack, by making this attack more difficult and therefore less appealing to an insider.

Domain and network account mitigations.

- **Removal of domain and network access**

When an employee changes positions, the existing access that he or she has must be removed and they should only be granted access to the systems and functions that their current position requires. This step would have made accessing the mail and user management system much more difficult.

- **Segmentation of common support accounts and rotation of passwords**

If there is a need for generic domain accounts for support purposes these accounts must have the bare minimum of domain access and should be separated into accounts for specific support groups to use for specific purposes. Where possible the passwords for these accounts should change every 30 days and access to these passwords should be tightly controlled and regularly reviewed. This measure would have made gaining attribution a little easier as it would have forced the insider to use a real user account rather than being able to "hide in the noise".

- **Least privileges**

In the scenario presented above we saw how a support person with access to the user management system could leverage that access to great advantage. This could have been avoided if the practice of assigning least privileges was followed.
If a support person needs access to user mailboxes for support purposes he should only have access to do those tasks necessary. It is all too easy to grant support people "Administrator" access. In most cases support people would not need full administration access to any system, elevated support privileges would be all that is needed. That degree of access should be reserved for the individual system administrators only. In addition Administration access should be tightly controlled and regularly audited.

Firewall Environment mitigations

- **Oversight of firewall/network management**

The establishment of an overall "IT security" department staffed with experienced professionals who are removed from the daily "tech work" yet who have had long experience in the technical aspects of security work should be considered.

The purpose of this team would be to have operational and strategic oversight over changes made to the network security infrastructure. This oversight should include (but

not be limited to) access to all logs, firewall policies and audit trails and access to all account activity logs (workstation/server event logs etc.). They should also have accountability for producing and maintaining security policies etc. This type of team is of enormous benefit from a strategic point of view as its members would have the skills and ability to "keep an eye on" operational staff and changes made without getting bogged down in daily detail. Had Fin-Bank had an active oversight team, the firewall rule included by the insider would have been questioned before the policy was installed.

- **Approval of firewall/network changes**

Be it by an "IT security" team, team leader or technical peer; all changes to the firewall policy/Network security infrastructure must be reviewed and approved prior to implementation. If a change escapes review it should be caught in a periodic review of audit logs to determine when a policy was installed and by whom. Questions should then be asked to ascertain the validity and content of this policy install. This would seem like an elementary step in a large organisation but small companies should consider some sort of "peer review" as well, as the lone "IT guy" with full access to the system could very easily be tempted to exploit the trust that is placed in him for personal gain or revenge etc.

- **Periodic review of firewall rules with removal of unused rules and commenting**

Be it by an "IT security" team, team leader or through group consensus, the need exists for formal periodic review of firewall rules and router access lists. The purpose of this review should be:

- To identify unneeded rules and remove them
- To (where necessary) improve the quality of rule comments.
- To identify rules that could have their "granularity" improved (replacing a /24 subnet with a single host or group of hosts for example).
- To "clean up" the rule base by grouping together rules that have been separated as new rules are added and removed. To improve the ease of management.
- To improve the basic understanding of existing rules and their uses.

Many of these steps seem elementary, but in a large company (like the one featured in this scenario) it is very easy for a rule base to become a terrible mess. This lack of review or oversight without a doubt paid a major part in the successful execution of the attack detailed above.

Physical security mitigations

- **Disabling of unused network ports**

Network data ports (such as those in meeting rooms and at unused desks) must be disabled as soon after they stop being used as possible. The threat posed by active but unused networks ports is huge, not only did it make the insider attack described above easier, but the are also very useful to outsiders for purposes like corporate espionage and intelligence gathering. If a port is active, anyone could walk in, sit down and plug in a laptop and start sniffing network traffic, cracking passwords or attempt to access all manner of private and sensitive data.

- **Keeping track of software packages and controlling copies made.**

The implementation of a software register and restriction of access to serial numbers and software keys should be considered for all software packages not only the sensitive type of software featured in this scenario. Support teams often have a central repository for commonly used software packages to speed up troubleshooting and re-installation. This is a hard practice to stop or to recommend stopping as the benefits to real-world situations of this type of repository are huge. However, great care should be taken to vet the contents of these repositories and remove any "sensitive" software packages. Access to licensed software should be restricted as unauthorized copies could expose a company to possible legal action by the software vendor. Companies should tightly control distribution of sensitive and licensed software. Had Fin-Bank had this type of control, the *FAST* cipher-keys would have been harder to come by for the insider.

Software and operating system mitigations

- **Viable and up-to-date antiviral solutions**

The idea of defense in depth should be applied to all antivirus solutions. Properly configured and regularly updated antivirus solutions should be deployed at the perimeter (such as a gateway virus scanner on the proxy servers), at the server level and at the desktop level. Consideration should be given to using different vendors products for different aspects of a company's overall antiviral solution. This is because it is common for one vendor's product to detect threats that another's does not and vice versa. Once implemented Antiviral solutions should be well administered with particular attention being paid to any virus that gets past the first defensive layer (the perimeter layer) and appears on the last layer (the desktop), any holes that are identified through this investigation should be plugged immediately.

Had the antiviral solution of Fin-bank been up to date and properly configured and administered the insertion and spread of the worms would have been impeded or at the very least the amount of damage caused would have been minimized

- **Keeping critical servers/points of failure up-to-date with supported/patchable operating systems and software packages**

In a large company like Fin-bank it would be a major undertaking to upgrade all workstations to a supported operating system version (going from Windows NT4 to Windows XP for example). That is why this type of system upgrade should be scheduled and well planned as soon as an operating system approaches the end of its vendor support period. Servers and other critical systems however should be maintained at a supportable operating system and software version as a matter of basic procedure. Having critical pieces of infrastructure that are unable to be patched against emerging threats should be considered a serious breach of security and moves to mitigate this threat should be taken as soon as possible.

Had Fin-bank had a patchable operating system at least at the server level, the amount of damage caused by the worm released could have been minimized or restricted to non-critical systems.

Conclusion and Lessons Learnt.

As mentioned at the beginning of this paper the scenario presented in this paper is not meant to be 100% possible. It is presented to convey to the reader that seemingly small lapses in a companies security procedures can be used together to form the basis for a massive breach of security and can cause chaos on a company's network.

The idea of the "Swiss-cheese" theory of aircraft accidents was presented to help explain how small problems can combine to form massive holes in safety and security.

Also presented were steps that could have been taken to avoid this costly breach. Some of them were basic procedural changes and some were wider reaching changes that could involve substantial capital outlay and/or hours of work. It could be argued that all are as important as each other.

It is hoped that by reading the fictional account of the "fleecing of Fin-Bank" the reader will become aware that firewalls, Antivirus solutions and Account permissions are next to useless if they are not properly implemented, managed and maintained.

Further "Swiss cheese" theory reading

Detecting threat & error in operational tasks
Hallman Chris Maj Feb, 2003
Combat Edge
http://www.findarticles.com/p/articles/mi_m0JCA/is_9_11/ai_98565515

FAA Safety Risk Assessment Newsletter may/jun 04
Eiff, Dr. Gary
http://www.asy.faa.gov/Risk/newsletter/may-jun04.htm

"Root Cause analysis with Reason"
Dagon, Jean-Pierre
http://www.rootcause.com/AirTranPaper.htm

List of Figures

List of References

[i] "Root Cause analysis with Reason"
Dagon, Jean-Pierre
http://www.rootcause.com/AirTranPaper.htm

[ii] EiCar Test file description
EiCar Creators.
http://www.eicar.com/anti_virus_test_file.htm

[iii] Description of "Opaserv.k" damage
Kalis, Jacob, Oct. 2002
http://www.fireav.com/virusinfo/library/opaservk.htm