Cash Bank

Network Security Review

conducted 15-November-1999

1 ABSTRACT AND SUMMARY

This document summarizes a network security review conducted for Cash Bank the week of 15-November-1999. I had previously visited Cash Bank and reviewed security in November, 1998. The goals of this audit were to examine the Cash Bank network areas which had not been fully examined in 1998. Two secondary goals were also given: to verify the results of the Cash Bank reactions to my 1998 report, and to see if additional problems had crept in to the same areas. As always, the audit was strictly time limited. Based on the observations made, I have provided some suggested solutions or courses of action which Cash Bank could consider for possible implementation.

To conduct this review, I used a variety of standard techniques and tools. I was given access to restricted areas and was allowed to have privileged access on all systems and servers. My personnel access was limited to the IS team at Cash Bank. This limits the integrity of the audit (since the team providing the information is the one I was supposed to be auditing); however, given the time constraints and the enormous breadth of systems involved, there was no other practical approach. Because I was more familiar with the network this time, I spent more time by myself and less working directly with Cash Bank staff. Where possible, I have tried to state only directly observable facts and to verify these facts directly. However, there are places where I report configuration information for which I have no direct verification (i.e., second-hand information).

One of the major potential security problems at Cash Bank is the proliferation of dozens of Windows NT servers. It was not possible for me to look at more than one or two of these servers. Because the servers which I looked at may not have been representative of all of the Windows NT servers, I have included additional material on Windows NT auditing which Cash Bank staff should use to audit **all** of the Windows NT servers.

To save time, I did not look at OpenVMS systems at all.

2 Key to Terms

Each issue identified in this report is assigned a risk, rated as "Low," "Moderate," or "High." All issues are rated subjectively.

High risk items: These represent serious issues which should be remedied immediately. Failure to act on these could open the organization to severe compromise of information systems. Resolution of these items will offer greatest immediate benefit and reduce exposure.

Moderate risk items: All of these represent important issues. However, resolution of these issues is of lower importance than those listed previously. Issues identified here may also represent industry consensus which is not in synchronization with the organization's own policies, procedures, or corporate philosophy.

Low risk items: Although these are called "low" risk, this does not mean that they can or should be ignored. Each issue should be explicitly addressed, either with a solution, a decision to explicitly ignore or dismiss the issue, or with acknowledgment that a solution is being postponed until additional resources are available.

3 Issues and Solutions

The following items list a set of issues identified during the security analysis and some suggested solutions. I have classified these into categories based on Network Infrastructure, Windows NT, and Unix.

1. Issue: Staff is not matched to task.

Risk: High
Affects: All areas

The security staff at Cash Bank needs additional expertise, training, and support. In working with the three staff (Debbie Dollars, Phil Funds, and the Unix system manager) who had primary responsibility for security in NT, Unix, and the network, I found enthusiasm and a good grasp of the basic issues. However,

enthusiasm itself is not sufficient to build and maintain a secure network. Cash Bank also lost (the day I arrived) its primary security architect, and it was very clear during the week I was there that there was insufficient knowledge transfer from outgoing staff to existing staff.

I was also disappointed to discover that the one staff member with the greatest insight into both security issues and the Cash Bank security architecture, Mr. Don Deposit, had no real direct responsibility for security.

Solution: Hire additional staff. Train existing staff to much greater depth.

Cash Bank must identify and hire a senior security architect at the earliest opportunity. This new staff member should have responsibility for design of the network security architecture. They would work with specific staff responsible for network infrastructure, NT, and Unix security, and would be responsible for designing security in all three environments.

It is inappropriate for me to make personnel recommendations based on only 4 days of on-site contact. Nevertheless, I offer the following three observations.

The work of Mr. Funds in managing the network and network security implementation should be split between Mr. Funds and a new, additional, staff member. This new staff member could also be responsible for the existing Altavista firewall, or this responsibility could be given to Ms. Dollars.

Ms. Dollars's role should be redefined for at least the next 12 months to focus on Windows NT security; this is a full-time job itself and one where Cash Bank has the greatest need for a large-scale strategy and implementation. The current split of responsibilities across operating systems is keeping Ms. Dollars from delving sufficiently in-depth into any one area.

A staff member should be identified as specifically responsible for Unix security. There appears to be mixed experience within the Unix system staff with security, but there is no centralized strategy person.

2. Issue: PC DUO is used extensively, but is not encrypted.

Risk: Moderate
Affects: Windows NT

Cash Bank staff use a package "PC DUO" extensively for remote control and management of Windows PCs. However, PC DUO does not encrypt

communications, which means that PC DUO sessions are vulnerable to eavesdropping (including theft of sensitive passwords) and hijacking.

PC DUO also does not use any type of strong authentication; it relies on simple user-password pairs from the Windows NT SAM (Security Accounts Manager) database.

Solution: Replace PC DUO with an application which supports encryption

Competing products such as PC Anywhere have supported encrypted sessions for several years. If a PC DUO upgrade is not available which will support strong encryption for remote control sessions, then PC DUO should be replaced with PC Anywhere (or similar product with encryption).

A product which integrates with the strong authentication system at Cash Bank is desirable.

3. Issue: Internal Network is Not Fully Switched

Risk: Moderate
Affects: Network Infrastructure

I was told that the network within the organization is fully switched; this was used as the justification for certain other security decisions. However, it is not true that the network is entirely switched. There are several locations, including the network operations center floor, where sensitive traffic is sent on a shared medium.

This, itself, is not a security risk. Many networks are not fully switched. However, it is a serious security risk if decisions are being made about what is and what is not a risk based on the assumption that the network is fully switched.

These assumptions are what form the risk: there were several times I was told that a particular security risk was minimized because of the switched nature of the network---when the network was not really switched.

Solution: Replace any shared-medium hubs with switches

Although Cash Bank has largely a switched network, there are places where hubs are used for end-user systems and servers. With the dramatic drop in cost

of switches and switch technology, these can be inexpensively replaced with low-end switches and should be.

4. Issue: Wide-Area Links are encrypted using proprietary technology

Risk: Low
Affect: Network Infrastructure

All wide-area links out of the Bank to other Bank sites are encrypted using proprietary Gretacoder Data Systems hardware. These use either a proprietary encryption mode or the triple-DES encryption algorithm. New York staff were unaware of whether these units were in proprietary or triple-DES mode.

More importantly, these units used manual distribution of keying material and an unknown re-keying algorithm.

This technology was considered very advanced at its introduction, but advances in cryptography and, more importantly, cryptographic standardization, have brought units to market with three important characteristics:

1) secure (public-key-based) development of keying material eliminates any possibility of subversion of key material during manual dissemination

2) standardized re-key algorithms and re-key protocols allow for "perfect forward secrecy" and very short key lifetimes along with multiple key streams over the same transmission line

3) triple-DES CBC mode encryption has had extensive public and private analysis and has been shown to be secure against even brute-force attacks

Solution: Ensure Gretacoders support non-proprietary, standards-based (IPSEC) encryption

The Gretacoders themselves can be upgraded (if the vendor will support this) to include much safer key distribution systems, or they can be replaced with widely available COTS (commercial-off-the-shelf) hardware from vendors such as Cisco, Nortel, and 3COM.

5. Issue: CiscoSecure + ACE Server together do not support sufficient security granularity

Risk: Low

Affects: Network Infrastructure and all servers (NT/Unix/VMS)

The combination of the ACE Server and CiscoSecure software, especially with TACACS+, do not support good security granularity. In essence, any user who is authenticated with ACE Server will be "passed through" by CiscoSecure to any service requesting authentication via TACACS+. There is no mechanism to specify which users are authenticated for which services without laboriously re-entering users for each service being supported by the SecurID cards.

As a result of this, SecurID cannot be used for authentication for sensitive services, since devices cannot tell the difference between users who have different security profiles. This begins to defeat the purpose of SecurID itself, and contributes to a fragmentation of authentication and logging databases.

This problem is exacerbated by the relatively low functionality of the TACACS+ protocol, which does not allow the distribution of user-specific information (AVPL, attribute-value pair lists) between requesting services and the server.

Both of these problems are only starting to become obvious to Cash Bank staff, but as wide-scale implementation of SecurID and secured services begins, they will restrict full implementation or cause unnecessary work.

Solution: Replace CiscoSecure with an authentication server; use RADIUS

A variety of authentication servers are available which integrate larger sets of user information and SecurID authentication. Any of these would better meet the long-term needs of the Cash Bank.

The TACACS+ protocols is also fairly weak in this area. RADIUS has greater functionality and allows for stronger ties between the authentication servers and authentication service requesters. RADIUS also has stronger internal security (using MD5 hash algorithm) and is designed not to lose accounting information.

6. Issue: SecurID too cumbersome for system staff to use

Risk: High

Affects: Network Infrastructure and all Servers (NT/Unix/VMS)

The SecurID security system is well-designed from a security point of view, but poorly designed from a human factors point of view. For this reason, there is little or no use of SecurID within the building. Instead, all of the most sensitive servers, usernames, and applications are protected using reusable passwords.

In effect, where the highest security is needed, the lowest security is in use; where a security breach is less important, SecurID is required. There is no way to simply "turn off" a particular user if they leave the Bank or if their password list is lost or compromised.

This is a serious architectural issue and one which contributes to a massive vulnerability, especially to internal security threats.

Solution: Develop and implement a one-time password or challenge-response authentication system which does not encourage subversion by the system staff.

A hardware-based authentication system using a technology such as smart cards, in conjunction with a network-wide authentication server, would be simple enough to use that system staff would not be tempted to "work around" security by using reusable passwords.

All privileged usernames on all platforms, including NT, OpenVMS, Unix, and the routers and firewalls, should link back to this system so that:

4) the system is easy enough to use that it is not a burden to end users

5) the system is managed enough that all user access can be logged, enabled, and disabled, as necessary

6) the system is secure enough that it represents a significant improvement over reusable passwords

7. Issue: Modems continue to be deployed in an undisciplined way for unprotected external access

Risk: High

Affects: Network Infrastructure

In my November, 1998, visit, I made the following observation:

> Several terminal servers are maintained, separately from the normal dial-in router, which are directly attached to the Cash Bank network. Although some of these modems are set for "dial-back," not all are. In addition, the passwords for several of these terminal servers are the Digital defaults. This means that anyone who chances upon these servers can, if they can get to a "Local>" prompt, turn on TCP/IP and (because these are DECservers capable of doing PPP) have a direct TCP/IP connection to the Cash Bank network behind the firewall.

During this visit, I again found modems (in this case for outward paging services) which were connected to terminal servers, not protected by passwords, and accessible from remote locations.

More importantly, I was told (before finding these modems) that this was impossible, because the “telephone people” were responsible for providing lines for modems and these lines were restricted from in-dial. Because the IT staff assumed this to be true, no one had bothered to test these lines.

The dual failure of the telecommunications department (to properly manage and deliver modem lines) and of the IT staff (to verify that these lines and modems were properly installed and secured) is typical of large corporate security problems: an accumulation of small errors, none of which individually might matter, but all of which taken together open sufficient holes in the corporate network to cause concern.

While I hesitate to recommend additional bureaucracy in any environment (since people will simply ignore it and continue to do even more insecure things which are not logged or recorded at all), it is clear that the deployment of modems within Cash Bank is causing significant and long-term security problems.

Solution: Establish procedures for modem installations to eliminate or reduce the possibility of insecure dial-in connections

Procedures for installation, logging, and accounting for modems should be established with the following attributes:

7) a modem and a telephone line should be tracked **together** so that the telephone line attributes properly match the modem application

8) a manager must approve the combination of the telephone line order and the modem installation; the approval must include a statement of the security risk for both dial-in and dial-out applications and how these risks are being dealt with (an “approved modem installation document”)

9) all modems should bear a tag or sticker which tracks them to the approved installation document

10) these tags and installation documents should be audited quarterly or semi-annually to ensure that all modems in the building are properly tagged, and that all approved modem installation documents on file match current applications.

I am especially concerned because I did not visit the Ted facility, and it is very likely to me that security discipline for services such as modems is even more lax than it is in the CAC facility due to the lack of on-site trained personnel.

Solution: Regularly scan all telephone numbers within the CAC and Ted facilities for modems.

Several software packages are available which will do this, on a continuing or occasional basis. These will identify any modems which answer the phone and help identify potential problems at the earliest opportunity.

8. Issue: Pager modems are installed for out-dial which allow remote access

Risk: Moderate
Affects: Network Infrastructure

Several unprotected, unpassworded modems were found which were installed for outward access but would accept incoming calls.

Solution: Reconfigure modems to not answer the phone; reconfigure telephone switch to disallow incoming calls

9. Issue: Firewall web configuration contains anomalous web servers

Risk: Unknown
Affects: Network Infrastructure

The firewall web configuration has certain anomalous servers which no one was able to explain to me. In particular, access is allowed for any internal system to connect to web servers at 207.106.20.250. While all of the other exceptions in the firewall configuration have some symbolic name (such as “cantor” or “bloomberg”), this server has no symbolic name. It is also hidden inside of an inappropriately labeled group, “www-green.”

This configuration may be entirely innocuous, allowing someone (probably on the system staff) to connect to a particular web server without using authentication. Or, it could be a sign of some special “hole” which has been

punched through the firewall to allow a Trojan horse application to push data out of the Cash Bank network undetected. Such a hole would have to have been left by a staff person; no application could have made this change.

The security risk of this configuration itself is probably low or zero. What is more important is that this highlights the lack of a "concepts" or "architecture" document for the firewall. (This issue is brought up separately next)

Solution: Document or remove the listed exception

The exception address should be identified and a security decision as to whether unauthenticated access to that address is allowed should be made.

If this address is to be allowed, then it should be put in its own group and not hidden inside of the "www-green" group of WWW servers (since it is clearly not on the "green" network).

At the same time, all other "no authentication" access rules (market-news, cantor, bloomberg, www-green) should be reviewed and each IP address should be evaluated to determine whether (a) they are correct and (b) whether unauthenticated outgoing access to those servers is appropriate.

10. Issue: No Network Security Policy Document; No Security Architecture Document

Risk: High

Affects: Network Infrastructure and Servers

It is traditional for security auditors to go into an organization and complain about the lack of a network security policy. Organizations rarely get around to writing them, and they are almost always out of date. This has become so commonplace that it is almost not worth wasting the time.

However, in the case of Cash Bank, the lack of a policy has seriously hampered my ability to do an audit. Normally, although there is no written policy or architecture document, enough of the staff understand what is going on to explain what is really meant by the organization.

Thus, when Mr. Funds said "our network is switched, so …" he was, in effect, describing the security policy. (It turns out that the network is **not** switched, which is then an auditable event, but that's a different issue) However, for large parts of the network security, particularly those involving the firewall, the

individual who knew what the informal security policy is has left the organization.

Therefore, when I look at the firewall, I can see a particular configuration. But I cannot tell whether this configuration is what Cash Bank intended, because there is neither a network security policy to explain what the firewall **should** do, nor is there a staff member to explain what they **think** the firewall does.

For this reason, I am particularly dissatisfied with the results of my firewall audit. I have twelve pages of notes which document what the firewall actually does, but without a description from someone at the Bank of what the firewall should do, I find it difficult to identify issues and risks.

Solution: Write a Security Policy

Even if the scope of the task seems hopelessly large, I strongly urge the organization to take the time to write a policy of what the firewall **should** do. Preferably, this should occur without having any knowledge of what the firewall actually does (or, more importantly, what the firewall is capable of doing).

Then, the firewall configuration should be adjusted to match the intentions of the organization.

11. Issue: ScreenD configuration does not make use of stateful options

Risk: Moderate
Affects: Firewall

The ScreenD configuration on the Cash Bank firewall is fairly restrictive. However, there are many places where it does not make use of the best practices available for the technology available. In particular, most rules are of the form:

```
From _A__ to _B__ port x accept

From __B__ to __A__ port any accept
```

While this is not in-and-of-itself incorrect, it opens up a hole in the firewall for an intelligent attacker to source a low-port attack through the firewall.

Instead, all cases of this style of rule should be replaced with the appropriate semi-stateful rule using the “flags” keyword:

```
From ___A___ to ___B___ port x accept
```

```
From ___B___ to ___A___ port any accept flags ack
```

Solution: Modify the firewall screenD configuration to use the best technology available

Although the AltaVista firewall does not include stateful inspection for screend.conf, it does allow semi-stateful restriction of connects by requiring TCP flags. Where not implemented, this should be.

12. Issue: Firewall has unused services running

Risk: Moderate
Affects: Network Infrastructure

The firewalls are running several services which are not currently used. For example, I found 38 UDP and TCP-based services, in addition to the "strafe" services which are used to detect port scans.

Solution: Disable all unused services

Unused services, such as the OTP servers for S/Key and Cryptocard, should be disabled. Servers which provide no useful information, such as the "finger" and “time” server, should also be disabled or deleted.

13. Issue: Green to Blue attacks are not prevented

Risk: Moderate
Affects: Firewall

The firewall configuration has a rule for access from blue nets (the DMZ) to green nets (the internal network) for port 80. The effect of this rule is that any intruder with access to a system on the DMZ has full ability to connect in through the firewall, so long as the attack originates on source port 80.

Although someone would have to have intimate knowledge of the firewall to make this attack immediately, such a hole is typical and would not be that difficult to infer. Several “hacker” tools are available which test for exactly this kind of problem.

This is only a threat for an attacker (or insider) who has full privileged access to a system (although any system will do) on the DMZ.

Solution: Review and modify this rule in screenD

At the very least, a semi-stateful flag (as noted above) should be added to this rule. Preferably, the entire purpose of this rule should be reviewed and the rule changed.

14. Issue: Test services still present

Risk: Low
Affects: Firewall

A "test" gxd (generic proxy) is present in the firewall. This is not being used and should be removed. It presents the opportunity for an insider to hide a configuration hole inside of the firewall, or for a staff member to accidentally mis-configure a proxy.

Solution: Remove test generic proxy.

15. Issue: Telnet service enabled on the firewall

Risk: Moderate
Affects: Firewall

A telnet server is running on the firewall on non-standard port 6789. This is probably in place for remote management of the server. Although this service is now protected by TCP wrappers (using hosts.allow and hosts.deny files), it apparently was not until a few minutes before I arrived to examine the firewall.

I am willing to concede that remote management of a firewall is a useful thing. However, the firewall also has a built-in tunnel server (which provides both authentication and encryption). It is also running a standard Unix operating system (as evidenced by the easy installation of TCP wrappers) so there is no reason that other security tools, such as SSH (the encrypted, secure-shell), could not be used instead of normal telnet.

Solution: Replace the unencrypted re-usable password telnet server.

The telnet server on the firewall should be disabled and replaced with one which has stronger authentication and encryption. This could be done with SSH.

Preferably, the telnet server would also be linked to the existing OTP SecurID system so that reusable passwords are not used for internal logins. (See also my notes on a "better" OTP or token-based system above)

16. Issue: Firewall configuration management is insecure

Risk: Low
Affects: Firewall

I hesitate to note this issue, because **any** kind of configuration management is obviously such an improvement from last year. However, the mechanism by which the CAC ("master") configuration is moved to the Ted ("slave") firewall is very insecure. It depends on an NFS server which is used to push the CAC configuration to Ted.

This is all controlled by the cron job `xfers.sh`.

The issue is that NFS is totally insecure---it is a stateless file system which has little or no authentication. Thus, an internal user could simply override the NFS service security, write a "new" configuration to the NFS server, and the Ted firewall would happily pick it up.

Solution: Cryptographically sign the configuration

Solving this hole is very simple: the CAC firewall should cryptographically sign the configuration (perhaps using an application such as PGP) before moving it to the NFS server.

The Ted firewall can verify the authenticity of the configuration as it downloads it and only install a configuration which is known to be authentic.

In the most secure environment, a person would have to enter the pass-code to unlock the private key of the CAC firewall, but it would be a great step forward to simply have a built-in private key which is known to the configuration generator. This would not protect against an unauthorized user making changes to the CAC firewall (which would automatically propagate to the Ted firewall),

but this is a much lower risk than having **any** random internal user push a whole new configuration to Ted without detection.

Any configuration change, whether authenticated or not, should also be logged by the Ted firewall. It does not appear that these changes are logged or audited anywhere.

I note also that failure of the `xfers.sh` job does not appear to trigger an audit or log event of any kind.

17. Issue: AltaVista Firewall is a dead product

Risk: Low
Affects: Firewall

Since the Compaq / Digital merger, the AltaVista product line was spun out of Compaq. Although AltaVista as a brand was acquired by CMGI, the AltaVista firewall was sold (or given) to Axent, which also sells the Raptor firewall (originally owned by Raptor and sold as "Eagle").

Unfortunately, although AltaVista Firewall is a good product, it is a dead product and has not been significantly updated since 1997. It does not make use of stateful inspection for packet filters, and its proxies are particularly CPU-intensive and cannot handle high loads with many users.

While the Cash Bank does not see security risks at this point, the continued dependence on a product which has been orphaned in the way that AltaVista Firewall has been orphaned is dangerous for future use. This will become a particular problem as Cash Bank is forced to use the screend.conf packet filters rather than proxies for performance reasons as Internet use and services increase.

I am also concerned because the Bank has purchased a large number of Cisco PIX systems, which have a firewall function (in addition to their main use, Network Address Translation). While these boxes do provide some security protection, they are not fully featured firewalls in the sense that the AltaVista Firewall is (or could be).

Solution: Cash Bank needs to re-evaluate their firewall product line

The Cash Bank IT staff currently has little expertise in the management and configuration of the existing firewall. While Mr. Funds has significant experience, this is not his primary responsibility. It is appropriate that the Bank

review their firewall strategy, preferably in concert with Axent, the new "owner" of the AltaVista Firewall, to determine whether they should continue with AltaVista products or move to a different product line.

It would be wise to do this before investing additional resources in training on the AltaVista product.

18. Issue: Network Security Architecture is more complex than it needs to be

Risk: Moderate to High

Affects: Network Infrastructure

I am concerned about the security architecture, or lack of it, inside of the Cash Bank. In particular, I made the following observations:

1) The console terminal server has an amazingly baroque configuration which is quite confusing, even to the system manager, yet which does not add security. The mis-apprehension that a complicated configuration increases security may cause configuration errors later on.

2) The new internal network configuration, which relies heavily on stacks of PIX firewalls, appears to exist largely as a series of viewgraphs and does not have any sustaining documentation or pre-made configuration.

3) The firewall is essentially undocumented, yet is a complex system. (It required 12 pages to document the security aspects of the configuration, without including subtleties such as logging and any Unix system management)

It appears to me, as an outsider, that the Cash Bank is throwing large piles of expensive equipment at the security problem in the hope that by buying name brand equipment and configuring each piece will build a secure network.

The problem with this strategy is that there is no over-all architecture and the amount of equipment and paths through the network is getting larger and larger and more and more complex. In the security business, complexity is **always** a danger sign. Complex configurations are easily broken, usually as a simple human error, and the more pieces involved, the easier it is to break the configuration.

It is not obvious to me that there is a problem, but this is largely because most of the equipment is still being configured and installed. However, it is clear that

there is the potential for a problem. While the Cash Bank staff dealing with all of this equipment is competent and hard-working, I am not sure that an overall architecture is clear in anyone's minds (beyond the buzzwords on a viewgraph).

Solution: Cash Bank should establish a security architecture

By writing and documenting a security architecture, each "piece" of the network security puzzle can be evaluated against some external criteria for form, function, and---most importantly---security configuration.

In the absence of a clear security architecture (and it may be that such an architecture exists in someone's mind, but I was not given an opportunity to discover it), the configuration at Cash Bank is rapidly becoming more complex than any one person can understand. This leads to potential errors, omissions, and misconfigurations.

I commented about the complex nature of the mail routing in my last visit to Cash Bank, and I think that this is a sign that things are getting more complex, and not less complex. It is a danger sign for the future.

19. Issue: Firewall Generic Proxies misconfigured for Authentication

Risk: Low
Affects: Firewall

The firewall has ten generic proxies which are used for outgoing access to certain services, such as LDAP (called "Entrust," which is a bit deceptive), PC DUO, and Real Audio.

Some of these are configured to have special rules for authenticated users. However, the AltaVista Firewall generic proxy does not support authentication, so these rules are meaningless.

It is also unclear why generic proxies are used, rather than the http proxy, for web traffic to the Green network. If no web proxy service is required, it would be more efficient to use ScreenD than bother with a generic proxy, which will affect performance much more.

Solution: Review all Generic Proxy rules for appropriateness and remove "dead" rules or replace useless proxies with ScreenD configuration.

The proxies include:

AV Tunnel 98 (port TCP 3265)
Blue-Green-443 (port TCP 443)
Blue-Green-80 (port TCP 80)
Entrust (really LDAP)
GARBAN (port TCP 6235)
MarketNews (6 proxies, ports TCP 2220 through 2225)
PC DUO (port TCP 5000)
Real Audio (port TCP 554)
Site Server (port TCP 507)
Test (port TCP 1234)

20. Issue: Time service on network not well configured

Risk: Low
Affects: Network Infrastructure and servers

Accurate time service is critical for security logs, because log times often need to be coordinated to the second or millisecond for security events. A single network-wide time service should be created and all servers (Unix, OpenVMS, and Windows NT) should synchronize to that service using the NTP protocols.

The firewall is configured to support NTP, but in a naïve way: the firewall connects to many NTP servers, when a correct configuration would be done with two or at most three stratum 2 servers. Polling that many servers is bad network behavior and abuses a public resource for no reason.

More importantly, the NTP service used is an unauthenticated one, which means that if this time is used for synchronization (such as with the ACE server), it is subject to spoofing or modification by outside parties. Note that the external router does not filter NTP down to the specified servers.

As another example, CBNEW01 uses NTP, but does not hit the firewall for the time; instead it gets it from CBNEW02---even though the firewall has the most accurate time.

Solution: Install internal, trusted, NTP server and configure all servers to use it for time source.

With the easy availability of GPS-based NTP servers at costs of less than $1000, there is no reason to depend on unreliable external sources for very, very accurate time. Cash Bank should install a GPS-based NTP server such as the Lantronix GPS server.

Once a stable NTP time source is available, all servers and routers should synchronize to that time source so that all times are correct and consistent within the network. Freeware NTP clients are available for Windows NT in the Microsoft-provided Resource Kit (both Intel and Alpha platforms); Cisco routers and servers have been able to use NTP for time synchronization for at least 5 years; Unix and OpenVMS TCP/IP NTP packages are commonly available.

The firewall should also get time from an internal source, rather than an external source. Once this is set up, systems in the DMZ can get time from the firewall, and NTP passage through the external router can be blocked.

21. Issue: CBNEW01 has an extraordinarily large number of services running

Risk: High

Affects: Unix servers

N.B.: I looked primarily at the CBNEW01 Unix system, although I also looked briefly at CBNEW03. Therefore, most of these comments are directed at CBNEW01. However, the issues brought up should be reviewed on all Unix servers, not just CBNEW01.

CBNEW01 is running 26 TCP-based services, and 21 UDP-based services. Many of these are completely un-used in the Cash Bank environment (such as the BIFF service or the KDEBUG service); many others might be used only occasionally (such as the NTALK and TALK services or the FINGER service).

In the Unix community, there are constantly bug reports related to poorly-written network services. Many of these bug reports boil down to one of a small set of problems: services which do not properly check buffer lengths ("buffer overflow bugs") and services which do not properly parse their arguments.

Because of the potential for undiscovered bugs, the most basic Unix network security rule is: disable unused services. This provides insurance against undiscovered bugs, particularly in services which are not used or which are not essential.

Although the Unix servers are not considered "production" at this time, they will be shortly and security should have been tightened down by now.

Solution: Disable unused services immediately.

At a minimum, the system manager should review the TCP and UDP services running on these systems and disable any which are not critical to production applications.

I use the term "critical" very specifically, because there are services which may be of use but which are not required for correct operation. These include the Berkeley r-services (which are much less secure than the traditional TCP-based connection services such as Telnet).

The system manager should prepare a list of running services and identify, for each service, the function of the service and why it should be running. As always in security, anything not understood should be disabled.

For CBNEW01, the list would include:

TCP ports 1526, dns, telnet, 2894, 2049, 1018, SMTP, 1004, 7937, 7938, 1575, 6000, 1025, PRINTER, 1024, DTSPC, CFGMGR, KDEBUG, finger, exec, login, shell, ftp, altv-tu, AdvFS, and 111

UDP ports dns, 666, 3095, 3096, 3097, 2049, 7938, 177, 1030, 1029, time, ntalk, biff, 1028, advfs, 1026, pmgkr-snm, snmp, ntp, and syslog.

22. Issue: Many systems allow connects from insecure sites

Risk: Low
Affects: Network Infrastructure; Unix; Windows NT

Although the Cash Bank firewall is supposed to shield the network from connects from insecure sites, systems themselves should not be completely unprotected.

This is an issue which I brought up at the last audit, and it continues to be a problem. As far as I can tell from my analysis of Windows NT and Unix servers (I did not look at OpenVMS servers this time), no action has been taken.

Solution: Use IP-based screening

All systems which are capable of IP-based screening should be configured to only accept connections from legal Cash Bank networks. This will ensure that any rogue connection or failure of the firewall will not leave the Cash Bank network wide open.

Cash Bank IS staff should produce guidelines for each of the major operating systems (Unix, probably via TCP wrappers, OpenVMS, and NT) to list legal networks which should be allowed, denying all others.

23. Issue: Unix systems run NFS

Risk: Low

Affects: Network Infrastructure; Unix; Firewall

The Unix systems use NFS for some functions. I am not sure, but it appears that this is largely as a convenience for firewall data transfers.

Unfortunately, NFS is a fairly insecure application and is designed to be used in an environment where there is total trust. NFS also requires the entire RPC infrastructure, which has other potential denial-of-service and resource advertisement issues.

It would be desirable for the Unix systems running production applications to not run NFS unless there is a strong overriding reason for it. I realize that it is difficult to do "cluster-like" operations without NFS, so it is possible that there are applications which require it. However, I would suggest that these be reviewed and that use of NFS be reduced wherever possible.

In the case of the firewall NFS communication for configuration control, a small server or VMS partition should be set up as an NFS server, rather than sharing this function with the Unix servers. This will be more important when the Unix servers such as CBNEW01 go production and cannot tolerate downtime or delay.

Solution: Review use of NFS.

Review any cases where NFS is enabled and disable if possible. If NFS is required for non-resident applications (such as the firewall), consider moving it to a separate dedicated server.

24. Issue: Unix systems run X

Risk: Moderate
Affects: Unix servers

The default configuration for Digital Unix (and for most Unix operating systems) is to enable the X window system on the console.

X itself is not insecure, but is designed to operate in an environment of trust. The current implementation of X allows any user on the local host to effectively "take over" an X session running on the console. This would allow an unprivileged user to upgrade their privileges when the console is used to log in.

Solution: Disable X.

If the **only** reason that X is enabled on the Unix servers is for console login access, then it should be disabled and console access should be via simple command-line shell. Once the operating system is installed, there is little need for X on the console.

25. Issue: DNS on CBNEW01 is out of date

Risk: Low
Affects: Network Infrastructure

I was unable to fully understand the DNS setup at Cash Bank, largely due to time limitations during my visit. DNS itself is not a security issue (unless Berkeley R-Services are used), but proper DNS configuration can do a great deal to assist the network and security manager by ensuring that system names are properly mapped to IP addresses. This reduces the chance of error, and helps in the diagnosis of general network and security problems.

CBNEW01 is listed as the primary DNS server for 8 domains, including 2 "Cash Bank.com" domains and 6 IP address domains (in-addr.arpa). However, these names are not being updated, which means that the DNS information is either stored elsewhere (in which case CBNEW01 should not be a primary for those domains) or the DNS information is not being updated (in which case it needs to be).

CBNEW01 also has an out-of-date cache file, which doesn't matter, because CBNEW01 should be a "slave forwarder" DNS server (although it isn't).

Solution: Provide a coherent DNS strategy and implement on all servers

The AltaVista Firewall supports a split DNS with both internal and external entries. A strategy which makes use of the AltaVista firewall for external DNS and internal servers (such as the OpenVMS or Unix systems) for internal DNS should be established.

DNS servers should be established in two locations (CAC and Ted) and be automatically updated with BIND's primary/secondary mechanism. If possible, two different platforms (i.e., one Unix and one OpenVMS) should be used to minimize the risk of a monoculture problem.

All servers should have their DNS configuration modified to use the two DNS servers in the two locations and no others.

26. Issue: Unix servers generally not secure

Risk: High
Affects: Unix

I found several other problems with Unix servers that are leftover from my last visit and which have apparently not been addressed. I am repeating them here because I think that the checklist of issues is very important and should be dealt with before any system moves into production. I found one or more of the problems listed below on the servers I looked at. These problems range from low to high risk:

1) Unix servers are listening on **many** TCP and UDP ports, including a wide variety of services which are both potential security problems and management headaches.

2) RHOSTS files were used for root r-services access, allowing anyone with privileges on certain systems to log on without a password (in certain circumstances).

3) SUID/GID applications such as ppp, slip, uucp, sendmail, uucp, and spop were available.

4) Non executable images were SUID/GID.

5) The following issue was present at the last visit, but my notes do not show whether I checked for this at the November, 1999 visit. I repeat it here as a

matter of record, although I have no evidence that the problem exists on the systems I examined: NFS export of filesystems may be allowed to "world;" other unrestricted NFS exports may be available.

Solution: Complete security audit and cleanup of Unix systems

Before these systems can be put into production, they need to have a thorough analysis of network security configuration options. It is also likely that the systems themselves have internal security issues which have not been resolved. At least the following should be done:

1) Remove unnecessary services, including NFS and r-services, unless absolutely necessary.

2) Remove all rhosts files (should not be used with r-services disabled anyway)

3) Evaluate all SUID/GID applications and remove any not in active use.

4) Remove or restrict NFS export.

5) Install TCP wrappers to control and log TCP/IP network access.

Add OTP (SecureID) where possible.

27. Issue: CBNEW01 is logging DNS queries inappropriately

Risk: Low
Affects: CBNEW01

CBNEW01 is logging all DNS queries. This generates over 20 Mb of log file each day. All of this information is useless for either security or system management purposes. More importantly, having useless information in log files can hide real problems.

This logging also consumes a great deal of system resources.

In my last audit, I noted that servers should enable access filters to protect themselves in the case of firewall failure. One of the IT staff comments was that this might introduce extra load on the servers and this was why the filters were not implemented.

If spurious logging such as DNS queries was eliminated, this would "free up" scarce resources which would be more than adequate to compensate for the additional load which a kernel mode screening filter would cause.

Solution: Eliminate useless logging

28. Issue: CBNEW01 log files are not being reviewed

Risk: Moderate
Affects: Network Infrastructure; Unix; Windows NT; OpenVMS

Each of the operating environments chosen by Cash Bank is capable of generating substantial logs. Some of these will include security events (such as login failures or password changes) and some will include general auditing information (such as file modifications or process creation / deletion).

Since my last visit, I see that log files from the firewalls are being gathered onto the Unix servers nightly, which is a good improvement.

I also see that some, but not all, of the Cisco routers and PIX firewalls are using SYSLOG to send log information to the Unix servers or to the firewall.

These logs are one key to early detection of security problems. They will help to identify attempted security abuses. They will serve as early-warning systems for break-in attempts. And if a break-in does occur, good logs will be one of the few tools available to understand the extent of the penetration and damage.

In my previous visit, I saw examples where security events (in the NT domain) where being created yet there was no in-house expertise able to find the logs of these events. Furthermore, these events were impacting system operations. I see that there is additional system staff concern on this issue, but I do not see that much action has occurred in this area.

Solution: Logs from all sources must be examined on a daily basis, typically by an automated procedure, to identify violations of security policy and possible break-in attempts.

Because these logs are so comprehensive, and because there are many operating environments (including Unix, the firewall, NT, OpenVMS, and the Cisco routers), they are also large.

These logs are also in diverse locations both on each operating system and within an operating system: auditing logs, accounting logs, security logs, and event logs may all be in different files.

Systems which are not currently logging (such as the PSI router and some of the PIX firewalls) should all log to a common SYSLOG server. In some cases, this may need to be the firewall; in all other cases, this should be a single system inside of the firewall.

I think that CBNEW01 should not be that system, because it has other applications to maintain. It is possible that another SYSLOG server should be established, with mirroring or clustering to Ted, specifically to act as a drop-box for log files.

A critical balance must be maintained between too much reporting and too little reporting. If the log analyzer generates reams of information every day which is generally irrelevant or not understood by those reading it, then the report will be ignored. Conversely, if the log analyzer is too strict, it may fail to identify events which are important to notice.

Unfortunately, building a proper log analysis tool is a complicated and frustrating process. The security analyst must balance the amount of information collected along with the daily analysis report. Nevertheless, this is a critical requirement. If the logs are not analyzed, then they are doing the organization little good.

Another reason to evaluate the logs before a problem is to identify "normal" behavior. A normal operating system environment may routinely kick out some unusual security logs as part of every-day operation. These should be identified, understood, documented, and filtered so that if a problem is suspected, the log can be evaluated with understanding.

29. Issue: Internal network devices are being deployed with default passwords

Risk: High

Affects: Network Infrastructure

The age of the “dumb hub” is over; almost all network devices, whether hubs, switches, or routers, now have system management capability. As an example, the IT staff recently deployed a new HP switch inside the network without configuring it. The HP switch picked up an IP address via DHCP, and I was able to manage it from my workstation.

Since the HP switch has port mirroring capabilities, I was able to select ports and redirect traffic from one port to another. If I had been plugged into that particular switch (or if I was plugged into another switch which had VLAN trunking with 802.1q), then I would have been able to monitor traffic on any port of the "switched" network. (I set the password on the system account to "system" to discourage others from following in my footsteps.)

This is only a single example; many other devices (such as Cisco routers) are coming out-of-the-box with web servers which allow certain monitoring functions.

Solution: Ensure that all network devices have passwords and static IP addresses defined before deployment; disable monitoring functions where appropriate

30. Issue: Internal systems are being deployed with insecure web servers

Risk: High
Affects: Personal workstations

I ran a port scan on large chunks of the internal network and found a variety of web servers which probably should be disabled. The following were found and should be examined to see if they should be disabled:

190.15.9.7, .8 – PIX servers

190.15.9.24, .25 – Console servers

190.15.9.40 – cisco 3600

190.15.9.51, .52 – Brocade NFS servers

190. 15.10.231 – Windows PC running Personal Web Server

190.15.11.23 – Windows PC running Personal Web Server

CBNEW07 – Cisco resouce manager software

190.15.20.10 – Windows NT server running IIS with "Out Of The Box" (insecure) configuration

The complete results of the Port 80 scan are as follows:

```
Service Scan Wed, Nov 17, 1999 12:37:26 PM
```

Service Scan for port 80 (www-http - World Wide Web HTTP) on 190.15.1.1 to 190.15.20.255

Address	Name	Type (TCP/UDP/Both)
190.15.2.1	ops01.ny.Cash Bank.com	TCP
190.15.2.2	190.15.2.2	TCP
190.15.2.8	ops08.ny.Cash Bank.com	TCP
190.15.2.4	190.15.2.4	UDP
190.15.2.10	190.15.2.10	TCP
190.15.2.11	190.15.2.11	TCP
190.15.2.12	190.15.2.12	TCP
190.15.2.15	190.15.2.15	TCP
190.15.2.18	190.15.2.18	TCP
190.15.2.13	190.15.2.13	UDP
190.15.2.16	190.15.2.16	UDP
190.15.2.17	190.15.2.17	UDP
190.15.2.23	190.15.2.23	UDP
190.15.2.25	190.15.2.25	UDP
190.15.2.29	190.15.2.29	UDP
190.15.2.35	190.15.2.35	TCP
190.15.2.30	190.15.2.30	UDP
190.15.2.32	190.15.2.32	UDP
190.15.2.39	190.15.2.39	TCP
190.15.2.34	190.15.2.34	UDP
190.15.2.40	190.15.2.40	TCP
190.15.2.36	190.15.2.36	UDP
190.15.2.37	190.15.2.37	UDP
190.15.2.38	190.15.2.38	UDP
190.15.2.47	190.15.2.47	TCP
190.15.2.42	190.15.2.42	UDP
190.15.2.48	190.15.2.48	TCP
190.15.2.49	190.15.2.49	TCP
190.15.2.45	190.15.2.45	UDP
190.15.2.51	190.15.2.51	TCP
190.15.2.46	190.15.2.46	UDP
190.15.2.52	190.15.2.52	TCP
190.15.2.53	190.15.2.53	TCP
190.15.2.54	190.15.2.54	TCP
190.15.2.55	190.15.2.55	TCP
190.15.2.59	190.15.2.59	UDP
190.15.2.71	190.15.2.71	UDP
190.15.2.72	190.15.2.72	UDP
190.15.2.73	190.15.2.73	UDP
190.15.2.76	190.15.2.76	UDP
190.15.2.81	190.15.2.81	UDP
190.15.2.87	190.15.2.87	TCP
190.15.2.82	190.15.2.82	UDP
190.15.2.83	190.15.2.83	UDP
190.15.2.84	190.15.2.84	UDP
190.15.2.86	190.15.2.86	UDP
190.15.2.88	190.15.2.88	UDP
190.15.2.91	190.15.2.91	UDP
190.15.2.93	190.15.2.93	UDP
190.15.2.94	190.15.2.94	UDP
190.15.2.95	190.15.2.95	UDP

190.15.2.96	190.15.2.96	UDP
190.15.2.101	190.15.2.101	UDP
190.15.2.112	190.15.2.112	TCP
190.15.2.114	190.15.2.114	TCP
190.15.2.111	190.15.2.111	UDP
190.15.2.122	190.15.2.122	TCP
190.15.2.125	190.15.2.125	TCP
190.15.2.121	190.15.2.121	UDP
190.15.2.123	190.15.2.123	UDP
190.15.2.124	190.15.2.124	UDP
190.15.2.133	190.15.2.133	TCP
190.15.2.130	190.15.2.130	UDP
190.15.2.141	190.15.2.141	TCP
190.15.2.143	190.15.2.143	TCP
190.15.2.146	190.15.2.146	TCP
190.15.2.150	190.15.2.150	TCP
190.15.2.151	190.15.2.151	UDP
190.15.2.162	190.15.2.162	UDP
190.15.2.175	190.15.2.175	TCP
190.15.2.173	190.15.2.173	UDP
190.15.2.181	190.15.2.181	TCP & UDP
190.15.2.182	190.15.2.182	UDP
190.15.2.191	190.15.2.191	UDP
190.15.3.1	190.15.3.1	TCP
190.15.3.2	190.15.3.2	TCP
190.15.3.3	190.15.3.3	TCP
190.15.3.4	190.15.3.4	TCP
190.15.3.5	190.15.3.5	TCP
190.15.3.9	190.15.3.9	TCP
190.15.3.10	190.15.3.10	TCP
190.15.3.11	190.15.3.11	TCP
190.15.3.31	190.15.3.31	UDP
190.15.3.51	190.15.3.51	UDP
190.15.6.2	ntnew02.ny.Cash Bank.com	TCP
190.15.6.6	ntnew06.ny.Cash Bank.com	TCP
190.15.6.9	ntnew09.ny.Cash Bank.com	TCP
190.15.6.15	ntnew15.ny.Cash Bank.com	TCP
190.15.6.20	nttest01.ny.Cash Bank.com	TCP
190.15.6.23	nttest03.ny.Cash Bank.com	TCP
190.15.6.30	ntnew30.ny.Cash Bank.com	TCP
190.15.7.5	190.15.7.5	TCP & UDP
190.15.7.15	ntTed15.ny.Cash Bank.com	TCP
190.15.7.16	ntTed16.ny.Cash Bank.com	TCP
190.15.9.1	gateway.ny.Cash Bank.com	UDP
190.15.9.6	190.15.9.6	UDP
190.15.9.7	Cash Bank-wfc-pix1-int.ny.Cash Bank.com	UDP
190.15.9.8	Cash Bank-wfc-pix2-int.ny.Cash Bank.com	UDP
190.15.9.24	main-console-ny.ny.Cash Bank.com	TCP
190.15.9.25	main-console-Ted.ny.Cash Bank.com	TCP
190.15.9.40	comm_ny_3600.ny.Cash Bank.com	TCP
190.15.9.51	190.15.9.51	TCP
190.15.9.52	190.15.9.52	TCP
190.15.10.35	190.15.10.35	UDP
190.15.10.231	190.15.10.231	TCP
190.15.11.23	190.15.11.23	TCP

190.15.11.37	190.15.11.37	UDP
190.15.11.171	190.15.11.171	TCP
190.15.15.23	190.15.15.23	TCP
190.15.16.4	CBNEW02.ny.Cash Bank.com	TCP
190.15.16.7	CBNEW07.ny.Cash Bank.com	TCP
190.15.17.4	190.15.17.4	TCP
190.15.20.1	190.15.20.1	TCP
190.15.20.2	190.15.20.2	TCP
190.15.20.3	190.15.20.3	TCP
190.15.20.4	cb-intranet2-new.ny.Cash Bank.com	TCP
190.15.20.6	190.15.20.6	TCP
190.15.20.7	190.15.20.7	TCP
190.15.20.8	190.15.20.8	TCP
190.15.20.9	cb-system-new.ny.Cash Bank.com	TCP
190.15.20.10	190.15.20.10	TCP

Solution: Run port scans, review results, and disable where appropriate

31. Issue: Some internal routers missing internal protection

Risk: Low

Affects: Network Infrastructure

Routers inside of the network should have protection in case of a firewall or routing failure. This would take the form of (at least) the following:

1) Restricting remote logins from authorized sources, such as the "management" network

2) Disabling connects to AUX port

3) Possibly disabling the console port entirely. (This has other repercussions for network management)

4) Setting routes inside of the router to only allow traffic to authorized Cash Bank networks

5) Disabling remote management such as the http server

Solution: Review configuration of remote site routers (including router to Frankfurt) and correct as appropriate

Note also that the long-term load on the Atlanta router is 0%. This router is severely over-configured for the task it has to perform. A 3640 router installed where a 2501 would do the job wastes $8K or more in resources.

32. Issue: SNMP configuration inconsistent

Risk: Low
Affects: Network Infrastructure

Cash Bank does not seem able to decide whether they think SNMP is a security risk or not. In some systems, SNMP has been disabled. In others, SNMP has been locked down with a non-obvious password for the Read-Only community. In others, SNMP is open with the default "public" community string for Read-Only access.

Obviously, no external access to SNMP should be allowed and this should be blocked both at the external router and at the firewalls. The firewalls should not have SNMP enabled (it currently does not).

Solution: Revisit SNMP configuration on all routers, servers, hubs, switches, and other manageable entities to build a consistent configuration.

My opinion is that SNMP inside of a network is so helpful that access to it should be generally enabled, even if an SNMP management system is not currently operating. However, using the default "public" community is too great of a threat---anyone sitting inside of the network would be able to map the entire network very quickly using this string.

My recommendation is to leave SNMP turned on, but to change the default "public" read-only community string to something else.

Attempts to read SNMP from the outside should be logged by the external routers to SYSLOG and investigated.

33. Issue: Externally controlled routers should not participate in dynamic routing algorithms

Risk: Moderate
Affects: PSI router, possibly others (ECash Bank?)

Routers which are not controlled entirely by Cash Bank and which are not entirely within the bounds of the firewall should not have any dynamic routing algorithm enabled. This is especially true of EIGRP, which is the same algorithm used inside of the Cash Bank network.

Routers such as the PSI router are specifically set up for a small and very constrained topology. They should not run dynamic routing protocols because there is no useful information gathered by such a protocol and, more importantly, there is the risk of leaking Cash Bank routes out.

The EIGRP session on the PSI router, for example, will be blocked by the Service PIX firewall---if the PIX is operating correctly. In the case that it is operating correctly, static routes are appropriate for the PSI connection. In the case that it is **not** operating correctly, you would not want the EIGRP sessions to extend across that PIX.

As the number of PIX firewalls begins to multiply within Cash Bank, the routing architecture should be examined carefully to ensure that extraneous routing information can neither be injected nor gleaned from the network.

Solution: Disable all dynamic routing protocols on external and multiply-controlled routers.

Note, of course, that in the case of a multi-home Internet configuration, it may be necessary to run a dynamic routing protocol such as BGP4 to properly handle the multiple Internet connections. In this case, it is particularly important that the BGP information not be "leaked" into any other dynamic routing protocols, such as RIP or EIGRP.

34. Issue: Remote-CA/Ted router needs access lists

Risk: Moderate
Affects: Network Infrastructure

The Remote-CA router is used for dial-in purposes---it connects both to the core network (for authentication) and to a Citrix network (for user access). This is a particularly baroque configuration which depends on a clever use of routes and IP addresses to keep remote users off of the internal network yet able to access the Citrix network.

I commented previously on a configuration error I saw in this router, which has since been repaired. This is an example, however, of a particularly fragile configuration. If someone inadvertently turned on dynamic routing, for example, the whole "security" of this link would be compromised.

I would suggest that because Cash Bank is fairly insistent that external users must only have access to Citrix systems that additional access lists be added to

this router to make sure that only authentication and management traffic can travel out the Ethernet0/1 interface and that all user traffic is enabled (possibly only with Citrix protocols, although this may be too severe) through the Ethernet 0/0 interface.

Solution: Add access lists to Remote-CA router.

The same thing will also be necessary in Ted since there is a parallel router for Ted with the same function.

I also note that there is some unused access list in the Ted router which may be the vestige of an attempt at this recommendation. It is slightly disturbing that the two configurations are not more closely matched.

35. Issue: RIP is a poor routing protocol

Risk: Moderate
Affects: Network Infrastructure; Unix; Windows NT; OpenVMS

At my last visit, I noted that RIP was in use in several routers. Although this has largely been eliminated, there are still several routers (such as the RSM router in Comm2 (192.85.9.1)) which are running RIP.

RIP is a poor routing protocol for several reasons:

1) It is chatty, sending all routes out on broadcast addresses every 30 seconds.

2) It is insecure, because there are no limits on who can broadcast routes or what they can broadcast.

3) It is unauthenticated; there are no assurances that a given RIP advertisement comes from the system it purports to come from.

4) RIP v1 is classless

All these make RIP a dangerous choice. Not only will malicious users be able to inject spurious RIP routes into the Cash Bank network, but any misconfigured Unix workstation inside of the Cash Bank network could cause a denial of service by advertising a default route through itself.

Solution: Disable RIP everywhere

RIP as a routing protocol should be replaced with an authenticated, peer-to-peer routing protocol. The EIGRP protocol, although not based on open standards (it is proprietary to Cisco) is already in use at Cash Bank and would be a good choice.

For systems which have no need of routing information, such as hosts, and for systems for which routing information is spurious (such as the firewalls and external routers), static routes should be used to "hard-code" routes into place which will take the place of any static routing information.

Under no circumstances should the firewalls listen to a dynamic routing protocol of any kind.

36. Issue: External router needs to be closed down more tightly

Risk: Moderate
Affects: Network Infrastructure

The routers between the Red firewall network and the Internet have an access list which is supposed to restrict traffic from the Internet. While it does have some good points, there are still a small number of specific errors in this configuration:

1) At the end of the access list, any traffic which was not specifically denied is permitted, both in TCP and IP.

2) While TCP access to services such as “telnet” is blocked explicitly, access to services such as “rlogin” is not. This would not be an issue if the problem in (1) were rectified, and the access list would be much shorter.

3) Access to the router itself is not blocked, permitting any IP-based attack.

In addition, this router is still running the tcp-small-services and (more importantly) udp-small-services. Since there is no way to use most of those services from the inside, they are not likely to be useful and should be disabled.

Solution: Reconfigure external router to eliminate “default accept” rules.

37. Issue: External router should have access lists on output to internal network

Risk: Low
Affects: External router

In the case that a user was able to get an unprivileged connection to the external router (such as via the unprotected RLOGIN service or RSHELL service), there is no protection in place to keep the user from making a second connection into the Cash Bank network---there is no access list in place.

Solution: Add output access lists to ensure that connections from the router cannot occur.

38. Issue: External router has additional Ethernet connection (not in production)

Risk: High

Affects: External router

The external router has two internal Ethernet connections, one to the RED firewall network and one to another network. This connection has no comment in the router configuration, and I was unable to find this connection on the network diagrams I was given.

However, I was shown two proposed configurations which had a second connection internally. One was to a LAPD proxy, and the other was to a PIX. Neither of these connections was in production at the time of my visit. Therefore, it was premature to have these configurations established on the external router.

I did not discover this until I had left the Cash Bank network and was reviewing the configurations, so it is possible that there was only a software configuration and no hardware connection, which would reduce the risk considerably.

Still, additional unprotected connections into the Cash Bank network should not be configured on external routers until the internal systems have been configured, tested, reviewed, and are in full production.

Solution: Remove connections to non-production networks from software and hardware configuration.

39. Issue: External router configurations do not match

Risk: High

Affects: External routers

The Ted external router does not match the configuration of the CAC external router, particularly in the area of security access lists. The CAC router is much more restrictive, although both have problems with access lists as noted above.

Solution: Review Ted configuration and synchronize with CAC configuration.

40. Issue: Systems not running current security-oriented patches

Risk: Low

Affects: NT Systems

The system I looked at, NTNEW02, is running Windows NT v4 with Service Pack 3 applied.

The current NT service pack level is 6 (5 at the time of my visit). More importantly, though, is that there have been many security-oriented hot-fixes for Windows NT since Service Pack 3. Most of those have not been applied to NTNEW02.

The vast majority of these security hot-fixes from Microsoft are to prevent denial-of-service attacks, which are not a major concern inside of the Cash Bank firewall. However, there have been some security fixes which affect IIS (Internet Information Server, Microsoft's web server which is in use at Cash Bank) operation as well as NT operation which are important inside of the firewall.

Since the Cash Bank WWW server is also a Windows NT system, the security service packs and hot fixes should be installed on that system with greater urgency. In this case, the risk could be HIGH, since IIS (and by extension, Site Server) security problems are well known in the hacker community. Cash Bank offers an easy target to vandalism of its web pages without these fixes.

Solution: Keep up to date with service packs and security hot-fixes

This is, of course, more difficult to do than to say. Cash Bank should have a small production Windows NT server used by IT staff only (with IIS and Exchange) which is used as a first testing and staging point for Microsoft patches. Once they have been proven in that environment, they can be migrated to the rest of the production NT servers.

While a certain amount of caution is desirable, being 2 years behind in patches and bug fixes is asking for trouble.

N.B.: The following issues are all identified for Windows NT systems. However, not all of the Cash Bank systems are configured with these security vulnerabilities. These are listed here to assist the Cash Bank staff in their own NT auditing activities.

41. Issue: Look for Legal Notice on logon

Risk: Low
Affects: Windows NT

A 1988 incident in the United States involving unauthorized use of computer systems was unsuccessfully prosecuted when the defendants claimed that the "Welcome to …" message before and after login was an open invitation to use the systems. In an unrelated incident, an employee successfully recovered damages from an employer because she was not informed that her activities were being monitored.

As a reaction to both of these incidents, many system managers believe that an inexpensive yet critical part of system security is to properly warn potential intruders or unauthorized users that they are unwelcome and that all users are being monitored. The language of this warning varies from organization to organization. I observe that Cash Bank is already doing this on their OpenVMS and some Unix systems.

Windows NT can do this as well.

Solution: Add a legal notice before logon screen is shown.

To display a legal notice, use the Registry Editor to create or assign the following registry key values on the system to be protected:

```
Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: \Microsoft\Windows NT\Current Version\Winlogon
Name: LegalNoticeCaption
Type: REG_SZ
Value: Whatever you want for the title of the message box
Hive: HKEY_LOCAL_MACHINE\SOFTWARE
Key: Microsoft\Windows NT\Current Version\Winlogon
Name: LegalNoticeText
Type: REG_SZ
```

```
Value: Whatever you want for the text of the message box
```

42. Issue: Administrator account should be renamed, and a new Adminisrator account should be created

Risk: Low
Affects: Windows NT

The built-in Administrator account should be to something less obvious. The Administrator account (because of its heavy requirement in system operations) is the one account that can never be locked out due to repeated failed log on attempts, and consequently is attractive to hackers who try to break in by repeatedly guessing passwords. By renaming the account, you force hackers to guess the account name as well as the password.

Renaming the account also helps in social engineering, because all staff would know that anyone asking for the "Administrator" account password is unauthorized and should not be given any access to any system at all.

However, once the account is renamed, a second account should be created, which has no privileges or access, called "Administrator." This can serve as a decoy for potential attacks and should have auditing set up so that any successful login or unsuccessful login attempt is immediately alerted for investigation.

Solution: Rename Administrator account; create a decoy. Do not forget to do this for systems which have local SAMs!

43. Issue: Remove Guest account; other un-needed accounts.

Risk: Moderate
Affects: Windows NT

The Guest account is not useful in a secure environment such as at Cash Bank. It should be removed, not only from the Domain SAM (Security Accounts manager daabase) , but also from any other SAM on a workstation or non-PDC/BDC Windows server.

Other accounts and groups present by default in non-PDC/BDC Windows servers (which have internal SAMs in addition to access to the group SAM) need to be carefully investigated. These will have a group "Power Users" which

should be removed, and all accounts except those needed for direct use of the system (typically the local Administrator account) should be removed or disabled. If an IUSR_xxxx or IWAM_xxxx account was created, it should be disabled or removed unless the system actually does run IIS or Web-based SQL services.

The local Administrator account should be renamed & a decoy set up on systems with local SAMs as well.

Remember: you can always disable an account and re-enable it if a problem occurs. There is no point in disabling an account after a security problem has occurred.

Solution: Remove guest accounts or other unused/un-needed accounts. Monitor local SAMs for un-needed accounts and adjust as necessary.

44. Issue: FAT file systems cannot be secured properly

Risk: Moderate
Affects: Windows NT

The FAT file system cannot be properly secured in a Windows NT environment. FAT is in use as the MYLEX_BT2 partition (NETNEW02) and the C$ partition on NETNEW01.

The NTFS file system provides more security features than the FAT system and should be used for all partitions at the Cash Bank. The only reason to use FAT is for the boot partition of an ARC-compliant RISC system (such as a Digital/Compaq Alpha NT server). A system partition using FAT can be secured in its entirety using the Secure System Partition command on the Partition menu of the *Disk Administrator* utility.

Solution: Convert all workstation and server partitions to NTFS except where required for Alpha booting.

45. Issue: Windows NT Workstation Registries not protected

Risk: High
Affects: Windows NT Workstations only

Depending on the version of Windows NT installed, NT Workstation registries may not be protected from remote modification. Since all operational and

security (indirectly) information is stored in the registry, this is a very high risk problem.

The Registry Editor supports remote access to the Windows NT registry. To restrict network access to the registry, use the Registry Editor to create the following registry key:

```
Hive: HKEY_LOCAL_MACHINE
Key: \CurrentcontrolSet\Control\SecurePipeServers
Name: \winreg
```

Then, the Registry Editor can be used to set security permissions on this key. These permissions define which users or groups can connect to the system for remote registry access. Generally, this should be set so that only the Administrator account can modify the registry.

Note that SMS, if in use at Cash Bank in the future, may have specific requirements and these should be investigated before widespread registry editing takes place.

Solution: Edit Registry as appropriate after considering risk.

46. Issue: Boot Access needs to be controlled

Risk: Moderate

Affects: Windows NT

Physical security of a personal computer is very difficult to achieve. In general, most operating systems assume that someone with direct physical access to the hardware has greater "privileges" than a remote user. Windows NT is generally well protected against this fallacy, but there are still vulnerabilities.

Physical access to the computer hardware and to the boot process should be limited if possible.

1) Disable floppy-based boot in the CMOS if possible.

2) Place a locking device in the floppy drive which keeps it from being used. It is unlikely that floppy drives are used in Cash Bank for any production use. N.B. If, in fact, floppies are being used instead of the network, this should be investigated as a separate security issue. Floppy disk security is notoriously bad in all environments due to people's propensity to re-use floppy disks.

3) Ensure that all local hard drives are NTFS.

4) Lock the computer case, if possible. These locks are not very strong, but they will discourage unauthorized casual access to hardware.

5) Use a power-on password before booting if the CMOS supports it.

Solution: Follow recommendations as listed above for all workstations.

47. Issue: User Rights need to be carefully controlled

Risk: High
Affects: Windows NT

User rights should be evaluated. For example, the Exchange service account should not have "Log On Locally." Why does the CAKPTBA account have "Add Workstation to Domain?" (this may be OK) Why are there deleted accounts which have the right "Restore files and directories?" Why does "ZDV Manuals" have "Take ownership of files or other objects?" Why is anyone in the "Debug Programs" group on a production Windows NT server?

The main rights to review include:

Access this computer from network

Log on locally – for Windows NT servers, this should be granted to the system administrator only.

Shut down the system

Log on over network – for Windows NT, the system administrator typically does not have this right.

Solution: Review user rights and revoke where not needed.

Microsoft Corporation provides the following tables which may be of interest or helpful in this task. I reproduce them here without editing.

There are several user rights that administrators of high-security installations should be aware of and possibly audit. Of these, you might want to change the default permissions on three rights, as follows:

	Groups assigned this	Recommended	Groups assigned	Recommended

User Right	right by default on workstation & stand-alone server	change for workstation & stand-alone server	this right by default on domain controller	change for domain controller
Log on locally. Allows a user to log on at the computer, from the computer's keyboard.	Administrators, Everyone, Guests, Power Users, and Users	Deny Remove Everyone and Guests this from having this right.	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	No Change
Shut down the system. (SeShutdownPrivilege) Allows a user to shut down Windows NT.	Administrators, Everyone, Guests, Power Users, and Users	Deny Remove Everyone, Guests and Users from having this right.	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	No Change
Access this computer from the network Allows a user to connect over the network to the computer	Administrators, Everyone and Power Users	Administrators, Power Users and Users	Administrators, Everyone	Administrators, Backup Operators Server Operators, Print Operators, Users and Guests it is enabled

The rights in the following table generally require no changes to the default settings, even in the most highly secure installations. However, it is advisable to walk through the list and make any changes as per the needs of a particular installation.

User Right	Groups assigned this right by default on workstation	Groups assigned this right by default on server
Act as part of the operating system (SeTcbPrivilege) Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	(None)	(None)
Add workstations to the domain (SeMachineAccountPrivilege) Allows users to added workstations to a particular domain. This right is meaningful only on domain	(None)	(None)

controllers.		
Back up files and directories (SeBackupPrivilege) Allows a user to back up files and directories. This right supersedes file and directory permissions.	Administrators, Backup Operators, Server Operators	Administrators, Backup Operators, Server Operators
Bypass traverse checking (SeChangeNotifyPrivilege) Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	Everyone	Everyone
Change the system time (SeSystemTimePrivilege) Allows a user to set the time for the internal clock of the computer.	Administrators, Power Users	Administrators, Server Operators
Create a pagefile (SeCreatePagefilePrivilege) Allows the user to create new pagefiles for virtual memory swapping.	Administrators	Administrators
Create a token object (SeCreateTokenPrivilege) Allows a process to create access tokens. Only the Local Security Authority can do this.	(None)	(None)
Create permanent shared objects (SeCreatePermanentPrivilege) Allows user to create special permanent objects, such as \\Device, that are used within Windows NT.	(None)	(None)
Debug programs (SeDebugPrivilege) Allows a user to debug various low-level objects such as threads.	Administrators	Administrators
Force shutdown from a remote system (SeRemoteShutdownPrivilege) Allows the user to shutdown a Windows NT system remotely over a network.	Administrators, Power Users	Administrators, Server Operators
Generate security audits	(None)	(None)

(SeAuditPrivilege) Allows a process to generate security audit log entries.		
Increase quotas (SeIncreaseQuotaPrivilege) Nothing. This right has no effect in current versions of Windows NT.	Administrators	Administrators
Increase scheduling priority (SeIncreaseBasePriorityPrivilege) Allows a user to boost the execution priority of a process.	Administrators	Administrators
Load and unload device drivers (SeLoadDriverPrivilege) Allows a user to install and remove device drivers.	Administrators	Administrators
Lock pages in memory (SeLockMemoryPrivilege) Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.	(None)	(None)
Log on as a batch job Nothing. This right has no effect in current versions of Windows NT.	(None)	(None)
Log on as a service Allows a process to register with the system as a service.	(None)	(None)
Manage auditing and security log (SeSecurityPrivilege) Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. Note that this right does not allow a user to set system auditing policy using the Audit command in the Policy menu of User Manager. Also, members of the administrators group always have the ability to view and clear the security log.	Administrators	Administrators
Modify firmware environment variables (SeSystemEnvironmentPrivilege) Allows a user to modify system environment variables	Administrators	Administrators

stored in nonvolatile RAM on systems that support this type of configuration.		
Profile single process (SeProfSingleProcess) Allows a user to perform profiling (performance sampling) on a process.	Administrators	Administators
Profile system performance (SeSystemProfilePrivilege) Allows a user to perform profiling (performance sampling) on the system.	Administrators	Administrators
Replace a process-level token (SeAssignPrimaryTokenPrivilege) Allows a user to modify a process's security access token. This is a powerful right used only by the system.	(None)	(None)
Restore files and directories (SeRestorePrivilege) Allows a user to restore backed-up files and directories. This right supersedes file and directory permissions.	Administrators, Backup Operators	Administrators, Server Operators, Backup Operators
Take ownership of files or other objects (SeTakeOwnershipPrivilege) Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators	Administrators

48. Issue: Groups and their usage should be investigated

Risk: High

Affects: Windows NT

The groups "Guests" and "Everyone" have no real use in the Cash Bank environment. They should be replaced, where the concept is appropriate, by "Authenticated Users." Windows NT is notoriously lax about allowing "Everyone" Full Control access to files throughout the operating system.

For example, on NTNEW02 the AUTOEXEC.BAT and CONFIG.SYS give everyone Full Control; the /WINNT partition is similarly unprotected. In general, only the Administrator account should have the ability to write to these files and directories; Everyone generally needs only read access.

Review access privileges to the boot and startup files on the root of the partition: AUTOEXEC.BAT, BOOT.INI, CONFIG.SYS, NTDETECT.COM and NTLDR to ensure that Everyone does not have access to write to these directories and files.

The /WINNT directory and all subdirectories should have access available to Administrators, Creator/Owner, and System (Full Control). Everyone or Authenticated Users should have only Read access.

The following exceptions then will provide a recommended level of security:

/WINNT/REPAIR: only Administrator access
/WINNT/SYSTEM32/CONFIG: change Everyone access to "List"
"Everyone" then needs privileges to Read, Write, and Execute files in the following directories in /WINNT: /COOKIES, /FORMS, /HISTORY, /OCCACHE, /PROFILES, /SENDTO, and /Temporary Internet Files. Most of these directories are part of the desktop. On a server which is only logged into by a system administrator, these additions are not needed.

Solution: Review file ACLs which offer Full Control to Everyone for appropriateness and tighten down where necessary.

Remember, it is easier to tighten down protections and loosen them if operational problems are caused then to clean up a security breach later.

49. Issue: Registry ACLs could be tightened – NOT RECOMMENDED

Risk: Low
Affects: Windows NT

Microsoft recommends a variety of changes to the ACLs on many registry keys in very high security environments. However, these changes are fairly dangerous because they can cause software to break (if it cannot modify its own registry entries). In an environment which is otherwise well-protected, I do not believe that these changes are appropriate. However, for the sake of the record, I will include the Microsoft advice here. I advise against these precautions

because of the marginal increase to network and operating system security and because of the danger to disruption of applications and software.

In addition to the considerations for standard security, the administrator of a high-security installation might want to set protections on certain keys in the registry.

By default, protections are set on the various components of the registry that allow work to be done while providing standard-level security. For high-level security, you might want to assign access rights to specific registry keys. This should be done with caution, because programs that the users require to do their jobs often need to access certain keys on the users' behalf.

For each of the keys listed below, make the following change:

	Access allowed
Everyone Group	QueryValue, Enumerate Subkeys, Notify and Read Control

In the HKEY_LOCAL_MACHINE on Local Machine dialog:

\Software

This change is recommended. It locks the system in terms of who can install software. Note that it is **not** recommended that the entire subtree be locked using this setting because that can render certain software unusable.

\Software\Microsoft\RPC (and its subkeys)

This locks the RPC services.

\Software\Microsoft\Windows NT\ CurrentVersion

\Software\Microsoft\Windows NT\ CurrentVersion\Profile List

\Software\Microsoft\Windows NT\ CurrentVersion\AeDebug

\Software\Microsoft\Windows NT\ CurrentVersion\Compatibility

\Software\Microsoft\Windows NT\ CurrentVersion\Drivers

\Software\Microsoft\Windows NT\ CurrentVersion\Embedding

\Software\Microsoft\Windows NT\ CurrentVersion\Fonts

\Software\Microsoft\Windows NT\ CurrentVersion\FontSubstitutes

\Software\Microsoft\Windows NT\ CurrentVersion\Font Drivers

\Software\Microsoft\Windows NT\ CurrentVersion\Font Mapper

\Software\Microsoft\Windows NT\ CurrentVersion\Font Cache

\Software\Microsoft\Windows NT\ CurrentVersion\GRE_Initialize

\Software\Microsoft\Windows NT\ CurrentVersion\MCI

\Software\Microsoft\Windows NT\ CurrentVersion\MCI Extensions

\Software\Microsoft\Windows NT\ CurrentVersion\PerfLib

Consider removing Everyone:Read access on this key. This allows remote users to see performance data on the machine. Instead you could give INTERACTIVE:Read Access which will allow only interactively logged on user access to this key, besides administrators and system.

\Software\Microsoft\Windows NT\ CurrentVersion\Port (and all subkeys)

\Software\Microsoft\Windows NT\ CurrentVersion\Type1 Installer

\Software\Microsoft\Windows NT\ CurrentVersion\WOW (and all subkeys)

\Software\Microsoft\Windows NT\ CurrentVersion\Windows3.1MigrationStatus (and all subkeys)

\System\CurrentControlSet\Services\LanmanServer\Shares

\System\CurrentControlSet\Services\UPS

Note that besides setting security on this key, it is also required that the command file (if any) associated with the UPS service is appropriately secured, allowing Administrators: Full Control, System: Full Control only.

****Software\Microsoft\Windows\CurrentVersion\Run

\Software\Microsoft\Windows\CurrentVersion\RunOnce

\Software\Microsoft\Windows\CurrentVersion\Uninstall

In the HKEY_CLASSES_ROOT on Local Machine dialog:

\HKEY_CLASSES_ROOT (and all subkeys)

In the HKEY_USERS on Local Machine dialog:

\.DEFAULT

50. Issue: Encrypt SAM-derived registry keys to prevent privileged users from cracking passwords

Risk: Low

Affects: Windows NT

The SAM (Security Accounts Manager) database contains all usernames and passwords, using strong encryption. Some information derived from the SAM is stored in the registry where it is not protected by the same encryption, but only by ACLs (access control lists) and a hash function.

Since Administrators have access to the registry, a program which was able to get Administrator privileges or an unethical Administrator could use this information to backwards-engineer valid username/password pairs, including that of the Administrator user.

Windows NT has an option to encrypt this information when stored in the registry. The problem with doing this is that this affects the ability of Windows NT to recover from certain disasters without additional manual intervention.

The SYSKEY program (part of NT4 SP3) can be used to encrypt this information. Complete details on the operation of SYSKEY and the implications of using SYSKEY are in Microsoft Knowledge Base article Q143475.

Solution: Read Q143475 and decide whether the benefits exceed the risks.

Relevant information from Q143475 is included here for reference.

The strong encryption capability with the Windows NT 4.0 System Key hotfix is an optional feature. Administrators may choose to implement strong encryption by defining a System Key for Windows NT. Strong encryption protects private account information by encrypting the password data using a 128-bit cryptographically random key, known as a password encryption key.

Only the private password information is strongly encrypted in the database, not the entire account database. Every system using the strong encryption option will have a unique password encryption key. The password encryption key is itself encrypted with a System Key. Strong password encryption may be used on both Windows NT Server and Workstation where account information is stored. Using strong encryption of account passwords adds additional protection for the contents of the SAM portion of the registry and subsequent backup copies of the registry information in the %systemroot%\repair directory created using the RDISK command and on system backup tapes.

The System Key is defined using the command Syskey.exe. Only members of the Administrators group can run the Syskey.exe command. The utility is used to initialize or change the System Key. The System Key is the “master key” used to protect the password encryption key and therefore protection of the System Key is a critical system security operation.

There are three options for managing the System Key designed to meet the needs of different Windows NT environments. The System Key options are the following:

• Use a machine-generated random key as the System Key and store the key on the local system using a complex obfuscation algorithm. This option provides strong encryption of password information in the registry and allows for unattended system restart.

• Use a machine-generated random key and store the key on a floppy disk. The floppy disk with the System Key is required for the system to start and must be inserted when prompted after Windows NT begins the startup sequence, but before the system is available for users to logon. The System Key is not stored anywhere on the local system.

• Use a password chosen by the Administrator to derive the System Key. Windows NT will prompt for the System Key password when the system is in the initial startup sequence, but before the system is available for users to logon. The System Key password is not stored anywhere on the system. An MD5 digest of the password is used as the master key to protect the password encryption key.

The System Key options using either a password or requiring a floppy disk introduce a new prompt during the initialization of the Windows NT operating system. They offer the strongest protection option available because master key material is not stored on the system and control of the key can be restricted to a few individuals. On the other hand, knowledge of the System Key password, or possession of the System Key disk is required to boot the system. (If the System Key is saved to a floppy disk, backup copies of the System Key disk are recommended.) Unattended system restart may require that System Key material be available to the system without Administrator response. Storing the System Key on the local system using a complex obfuscation algorithm makes the key available only to core operating system security components. In the future, it will be possible to configure the System Key to obtain the key material from tamper proof hardware components for maximum security.

WARNING: If the System Key password is forgotten or the System Key floppy disk is lost, it may not be possible to start the system. Protect and store the System Key information safely with backup copies in the event of emergency. The only way to recover the system if the System Key is lost is using a repair disk to restore the registry to a state prior to enabling strong encryption. See the Repair Issues section below.

Strong encryption may be configured independently on the Primary and each Backup Domain Controllers (DCs). Each domain controller will have a unique password encryption key and a unique System Key. For example, the Primary DC may be configured to use a machine generated System Key stored on a disk, and Backup DCs may each use a different machine generated System Key stored on the local system. A machine generated System Key stored locally on a Primary domain controller is not replicated.

Before enabling strong encryption for Primary domain controllers, you may want to ensure a complete updated Backup domain controller is available to use as a backup system until changes to the Primary domain are complete and verified. Before enabling strong encryption on any system, Microsoft recommends making a fresh copy of the Emergency Repair Disk, including the security information in the registry, using the command, RDISK /S.

The SYSKEY command is used to select the System Key option and generate the initial key value. The key value may be either a machine generated key or a password derived key. The SYSKEY command first displays a dialog showing whether strong encryption is enabled or disabled. After the strong encryption capability is enabled, it cannot be disabled. To enable strong authentication of the account database, select the option “Encryption Enabled”, and click OK. A confirm dialog appears reminding the administrator to make an updated emergency repair disk. A new dialog appears presenting options for the Account Database Key. Use the options available on Account Database Key dialog to select the System Key.

After selecting the System Key option, Windows NT must be restarted for the System Key option to take effect. When the system restarts, the administrator may be prompted to enter the System Key, depending on the key option chosen. Windows NT detects the first use of the System Key and generates a new random password encryption key. The password encryption key is protected with the System Key, and then all account password information is strongly encrypted.

The SYSKEY command needs to be run on each system where strong encryption of the account password information is required. SYSKEY supports a “-l”

command option to generate the master key and store the key locally on the system. This option enables strong password encryption in the registry and allows the command to run without an interactive dialog. The SYSKEY command can be used at a later time to change the System Key options from one method to another, or to change the System Key to a new key. Changing the System Key requires knowledge of, or possession of, the current System Key. If the password derived System Key option is used, SYSKEY does not enforce a minimum password length, however long passwords (greater than 12 characters) are recommended. The maximum System Key password length is 128 characters.

SYSKEY should be applied to all domain controllers. If this is not done, the SAM on the backup domain controllers (BDCs) will not be as secure as that on the primary domain controller (PDC). Thus, the point of installing SYSKEY would be defeated.

REPAIR ISSUES

Introduction of strong encryption of account password information changes the SYSTEM and SAM portions of the registry in ways that affect the repair options available for recovery of a Windows NT system. Always use the RDISK command with the /S option to create a new Emergency Repair Disk including a backup copy of the SYSTEM and SAM portion of the registry in the \Repair folder.

For complete recovery options, the following Emergency Repair Disks should be available:

• Prior to installing the System Key hotfix, create a fresh repair disk. This disk is a "pre-hotfix" repair disk that contains a copy of the system configuration and account information prior to installation of the hotfix. The "pre-hotfix" repair disk may be used to recover the registry and system files using the Windows NT distribution CDROM.

• After installation of the System Key hotfix, but before enabling strong encryption using the SYSKEY command, create a repair disk. This repair disk is "hotfix Before Encryption". This repair disk can be used to repair the Registry to the state before strong encryption is enabled, for example it may be used to recover a system if the Windows NT System Key is lost or forgotten.

• After running SYSKEY to enable strong encryption, create a repair disk. This repair disk is "hotfix After Encryption". This repair disk, and subsequent updates to this repair disk, can be used to recover the registry with strong encryption intact using the System Key in effect at the time the repair disk was last updated.

The System Key hotfix support for strong encryption affects the following system components:

SYSTEM and SAM registry hives
Three system security component files: Winlogon.exe, Samsrv.dll, Samlib.dll

In general, the repair process needs to use matching versions of these components. Whatever repair option you choose, the repair process will coordinate repair of the registry hives with the matching system files.

More information on repair issues is available on Microsoft Knowledge Base article Q143475.

51. Issue: Default SMB protections allow for Everyone full control access

Risk: Low
Affects: Windows NT

By default, when Windows NT creates a “share,” it offers Everyone full control access to the share. However, the NTFS security system then provides additional security to restrict access. This is normally adequate, but may not be for default shares created for FAT drives, floppies, or CD-ROMs.

All default administrative shares (ADMIN$, A$, C$, E$, etc.) should be examined to ensure that the access controls built-in to them are correct for FAT-installed volumes. For Windows NT Workstations, if the C$ share is not being used, it should be removed along with any other default administrative shares for ADMIN$, the floppy, and CD-ROMs.

Do not rely, however, on the SMB server access controls to protect NTFS volumes. The NTFS file ACLs should be the first line of defense against unauthorized modification of data.

Consider disabling creation of default administrative shares entirely by setting AutoShareServer and AutoShareWks to 0 in \System\CurrentControlSet\Services\LanmanServer\Parameters in HKEY_LOCAL_MACHINE. Of course, this will not delete existing administrative shares.

Solution: Review and adjust as appropriate

52. Issue: SMB File Access Security Poorly Designed

Risk: Moderate
Affects: Windows NT

In its efforts to ensure backwards compatibility, Microsoft has done a poor job of security in building network access to files. The SMB (Server Message Block) protocol has a variety of vulnerabilities which can be exploited by unauthorized users who have LAN access.

In addition, what security does exist in SMB operates fairly laxly without modifications to the base operating system.

Microsoft has continued to attempt to repair these problems in recent Windows NT service packs. However, to make use of these patches, changes to the registry must be made. In addition, full SMB security may preclude access by Windows 95 clients, which are completely insecure.

To enable SMB message signing, which helps prevent Man-in-the-Middle attacks and which provides SMB message authentication, the registry must be edited by setting RequireSecuritySignature in System\CurrentControlSet\Services\LanManServer\Parameters for HKEY_LOCAL_MACHINE to 1.

This will require the server to only communicate with clients which have the new security features for Windows NT added in Service Pack 3 to NT V4. The symmetric change to clients, which will ensure that they only communicate with servers which support the new security features is to set RequireSecuritySignature in System\CurrentControlSet\Services\Rdr\Parameters for HKEY_LOCAL_MACHINE to 1.

This will disable connection to non-secure servers. Thus, the server must be edited first; clients second.

Windows NT also supports LanManager password security, which is known to have vulnerabilities. More importantly, the default behavior of Windows NT is to send LanManager password challenges with **all** challenges, even ti Windows NT servers which do not need it, thus exposing passwords to easy analysis. LanManager password authentication should be disabled on all Windows NT clients by setting LMCompatibilityLevel to 2 (disable LM challenge/response) in System\CurrentControlSet\Control\LSA in all clients and servers. Note that this will restrict access to/from Windows 95.

Microsoft Knowledge Base articles Q147706, Q166730 and Q161372 provide more information on this change.

Solution: Edit the registry on servers, then clients, as noted.

53. Issue: OS/2 and POSIX subsystems represent unknown security quantities

Risk: Low

Affects: Windows NT

As part of the basic architecture of Windows NT, Microsoft designed the core operating system to be able to emulate other operating systems. One of those systems is Windows (thus, WOW, Windows on Windows, shows up frequently in system operations). Microsoft also included OS/2 and POSIX, two operating systems which they thought might be critical to the success of Windows NT.

As a result of this architecture, all Windows NT systems come built in with POSIX and OS/2 routines. Unfortunately, these have not been exercised thoroughly with respect to security and represent unknown quantities.

Since it is highly unlikely that Cash Bank is making use of either OS/2 or POSIX compatibility mode, these should be removed from production servers and workstations.

Solution: Remove OS/2 and POSIX where not required.

54. Issue: FTP Servers allow writing by anonymous users

Risk: High

Affects: Network Infrastructure, Windows NT

The FTP server on NTNEW02 is exporting 6 directories, all of which are writeable by anonymous users.

No writeable anonymous FTP services should be allowed. If an application needs to move data with FTP to another application, it is preferable to embed passwords in the applications than to allow anyone on the entire network to push data to the NT server without restriction.

Note that the FTP server exports entire disk partitions---exporting a particular directory of a partition does not limit access "above" that directory. (exporting directories such as \tram, \transfer, \gps, and \cars is simply a user interface convenience and does not add to security or constrain access beyond what NTFS constrains.) If practical, then, FTP should only be enabled on specific disk partitions which are set up for FTP and which do not share data with other applications.

When configuring FTP servers, Cash Bank should not use the default anonymous user account of GUEST. A special FTP guest account should be set up with a secure password. (The FTP server will use this automatically). This account should not be member of any privileged groups so that the only default group that shows up in the security token during log on is Everyone. The account should not be allowed "Logon on Locally" user rights.

Solution: Remove write privileges from anonymous user on all FTP-exported directories. Modify username and partition assignments if possible.

55. Issue: Removeable Media not protected --- NOT RECOMMENDED

Risk: Low
Affects: Windows NT

Microsoft offers the following advice regarding floppy disks and CD-ROMS which I do not agree with. However, I reproduce it here in case there are special circumstances at Cash Bank which make this relevant. I believe that it is a greater impediment to operation and that floppies should be secured with physical access controls instead.

> By default, Windows NT allows any program to access files on floppy disks and CDs. In a highly secure, multi-user environment, you might want to allow only the person interactively logged on to access those devices. This allows the interactive user to write sensitive information to these drives, confident that no other user or program can see or modify that data.

When operating in this mode, the floppy disks and/or CDs on your system are allocated to a user as part of the interactive log on process. These devices are automatically freed for general use or for reallocation when that user logs off. Because of this, it is important to remove sensitive data from the floppy or CD-ROM drives before logging off.

Note: Windows NT allows all users access to the tape drive, and therefore any user can read and write the contents of any tape in the drive. In general this is not a concern, because only one user is interactively logged on at a time. However, in some rare instances, a program started by a user can continue running after the user logs off. When another user logs on and puts a tape in the tape drive, this program can secretly transfer sensitive data from the tape. If this is a concern, restart the computer before using the tape drive.

To Allocate Floppy Drives During Log On

Use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateFloppies
Type:	REG_SZ
Value:	1

If the value does not exist, or is set to any other value, then floppy devices will be available for shared use by all processes on the system.

This value will take effect at the next log on. If a user is already logged on when this value is set, it will have no effect for that log on session. The user must log off and log on again to cause the device(s) to be allocated.

To Allocate CD-ROMs During Log On

Use the Registry Editor to create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateCDRoms
Type:	REG_SZ
Value:	1

If the value does not exist, or is set to any other value, then CD-ROM devices will be available for shared use by all processes on the system.

This value will take effect at the next log on. If a user is already logged on when this value is set, it will have no effect for that log on session. The user must log off and log on again to cause the device(s) to be allocated.

56. Issue: Password choice should be restricted

Risk: Low to Moderate
Affects: Windows NT

It is common knowledge that reusable passwords are the greatest problem in network and system security. Most operating systems provide some mechanism to encourage users to select stronger passwords. These mechanisms typically include:

1) Restricting the length of time a password must be used (expiration)

2) Maintaining history to prevent re-use of passwords (this is done in Windows NT with a minimum change time, since NT does not maintain password history information)

3) Enforcing requirements on the content and form of passwords, including length, types of characters, inclusion of dictionary words and username variants.

In Windows NT, items (1) and (2) were built into the operating system. However, item (3) is not and must be specifically enabled by using the PASSFILT.DLL provided in Windows NT Service Pack 2 (and higher). Cash Bank could write their own PASSFILT.DLL to filter passwords, but for the short term, this Microsoft-provided utility will be a good start.

To enable PASSFILT.DLL, edit the Notification Packages registry key in System\CurrentControlSet\Control\LSA in HKEY_LOCAL_MACHINE to add the string "PASSFILT" to the entry. Ensure that the PASSFILT.DLL (in \WINNT\SYSTEM32\) is protected so that Everyone has read/execute access only.

At the same time, the Novell password filter FPNWCLNT should be removed. This is because this password filter is, by default, writeable by Everyone and could be replaced with a password filter which trivially captures all users passwords when they try to change them. If Novell file sharing is not in use, then this password filter is not needed and should be removed.

Windows NT's PASSFILT.DLL requires passwords to meet the following tests:

- Passwords must be at least six (6) characters long. (The minimum password length can be increased further by setting a higher value in the Password Policy for the domain).
- Passwords must contain characters from at least three (3) of the following four (4) classes:

Description	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters") such as punctuation symbols	

- Passwords may not contain your user name or any part of your full name.

57. Issue: Disable Anonymous LAN Manager Services

Risk: Low
Affects: Windows NT

Windows NT networking through LAN Manager allows for certain unauthenticated users to read a variety of network parameters, SAM (Security Accounts Manager) database information, and the Windows NT registry (where allowed by the ACLs on the registry itself). This is normally not a significant issue, especially if the registry is properly protected with ACLs. However, it is a simple matter to restrict unauthenticated user access by editing a few registry keys.

Since users will normally always authenticate themselves to a domain before examining registry, SAM, or network parameters, these changes will have no effect on normal operation.

Disable unauthenticated (NULL session) access by removing NULL from the list of NullSessionPipes in System\CurrentControlSet\Services\LanManServer\Parameters in HKEY_LOCAL_MACHINE and setting RestrictAnonymous to 1 in System\CurrentControlSet\Control\LSA in the same registry hive.

More information on these edits is available in Microsoft Knowledge Base articles Q143474 and Q143138.

Solution: Edit registry as recommended

58. Issue: Simple TCP/IP Services are enabled

Risk: Low
Affects: Windows NT

The Simple TCP/IP services on Windows NT are small TCP and UDP services which can be used for test of connectivity to Windows NT. However, few network managers use these services, relying instead on the PING and TRACEROUTE tools.

The problem with Simple TCP/IP services, particularly in the UDP mode, is that they can be used for denial of service attacks on the Windows NT server. This is not likely to be an issue inside of the Cash Bank firewall. However, under the general principle of not running services which are not used, these should be removed.

Solution: Using Network Control Panel, remove Simple TCP/IP Services.

59. Issue: Users are able to disable the password-protected screen saver

Risk: Moderate
Affects: Windows NT

The current desktop configuration at Cash Bank allows the end user, once logged on, to disable the password-protected screen saver. If computing security policy requires the use of this kind of protection---which I agree with, despite the obvious inconvenience---then the desktop load should be modified so that user and system policy (using the system policy editor provided with Windows NT) disallows modification of the screen saver characteristics.

Solution: Review Cash Bank Security Policy and, if appropriate, edit Windows NT system policy to enforce password-protected screen saver.

If Cash Bank is not using Windows NT policies already, this can also be effected by using a login script which sets the appropriate registry keys. A call to

REGEDIT (REGEDIT/S) in the login script with an argument of a file which has the following contents:

```
[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaveTimeOut"="xxxx"
"ScreenSaveActive"="1"
"SCRNSAVE.EXE"="C:\WINNT\SYSTEM32\LOGON.SCR"
"ScreenSaverIsSecure"="1"
```

where "xxxx" is the number of seconds before the screen saver should activate. Obviously, this file should be stored in a protected area on the NT server for Everyone "Read" access only.

60. Issue: NT Domain Trusts Extend Beyond Reasonable Bounds

Risk: Moderate
Affects: Windows NT

The Cash Bank NT production servers have a two-way trust relationship with the TEST domain. Even though the TEST domain is not currently in use, the presence of this trust implies that a TEST domain machine---which may not be configured as securely or with as much care as a production machine---would have full privileges in the production domain.

In any secure environment, the chain of trust from secure systems outward is only as secure as the weakest link. By breaking the relationship between TEST and PROD domains (or by making the relationship one where TEST trusts PROD (actually CB_CA_PROD), but the reverse is not true), the chain which Cash Bank IT staff have to concern themselves gets much shorter and much more manageable.

GartnetGroup, in the first part of 1998, concluded in a conference titled "Windows NT: Strategies for Success" that the complex and confusing nature of Windows NT domains makes it undesirable to use the domain structure at all. This is one way to one the security pitfalls of domains, but I disagree that they should be dismissed altogether. I would lessen the severity of the GartnerGroup solution by simply not using multiple domains, or not creating trust relationships between them when they are necessary.

Establishing multiple domains is almost impossible without receiving user requests for information or resources on other domains. These requests are inevitably fulfilled by establishing trust relationships between separate domains.

In addition, simply administering the multiple domains is made much simpler by creating trust relationships (replicating logon scripts, files, and directories). The problem with maintaining disparate domains is that the act of creating trust relationships is not intuitive, and the act of maintaining the rapidly increasing permissions and trusts between them becomes confusing (and an annoying chore). Therefore, it is not the simple presence of multiple domains and trust relationships that creates a security problem, it is their use in practice and the dificulty of keeping track of all the information necessary to keep things secure. Don't use them.

Solution: Remove trust from PROD to TEST domains.
At the same time, the trust relationship between INTRANET and CB_CA_PROD should be reviewed to see if it is appropriate. Since this is a one-way trust, it is likely that there is no security issue there.

61. Issue: Full set of Emergency Repair Disks is not available

Risk: Moderate (not Security, but Operations)
Affects: Windows NT

Cash Bank IT staff does not have a full set of Emergency Repair Disks available for each Windows NT server in production operation. Although these would only be absolutely necessary when both the NT disks or system was corrupted and the backup system was corrupted, this is not inconceivable. In certain kinds of data corruption, it could be days or weeks before the problem is actually discovered, and the backup tapes could all be contaminated.

It would be desirable to have a full set of Emergency Repair Disks sent off with the off-site backups on a regular basis.

Note that this is not a security issue directly, but an operations issue.

Solution: Review possible need to have Emergency Repair Disks for Windows NT servers and adjust operations procedures as appropriate.

62. Issue: Running WWW and FTP on main NT server undesirable

Risk: Low
Affects: Windows NT

In a normal Internet environment, the most likely avenue for a security attack is the IIS (Internet Information Server) server provided by Microsoft. IIS offers both WWW and FTP services.

The range of security holes in these applications have only begun to be plumbed and new problems (and associated patches) have come out with regularity since the release of IIS. The use of Site Server at Cash Bank adds complexity---and hence insecurity---to the total system as well.

Because of the poor track record of the IIS and Site Server servers with regard to security, it is desirable that they be segregated away from the main production NT servers at Cash Bank. At the very least they should be taken off main servers, such as NTNEW02, and moved to standalone systems. In an ideal environment, they would be in separate domains, disconnected from the production NT domain entirely.

It goes without saying that this is doubly true of servers which are outside of the firewall, although I did not see any NT connectivity through the firewall. Still, should any proposal come forward to provide NT networking services through the firewall, this may become an issue.

I strongly recommend that the WWW and FTP services be taken off NTNEW02 and moved to a standalone NT server.

Solution: Reconfigure WWW and FTP services as recommended.