Large Enterprise Application Security

Dave Aitel
Immunity, Inc.
www.immunitysec.com
April 2, 2004

Illustration 1Small Skipper (Thymelicus sylvestris)

Abstract

Large enterprises use a different class of software than small companies. This software and the environment it is purchased in is subject to particular constraints that often require a different strategy. This paper presents the problems with concrete and current examples and suggests some solutions.

Table of Contents

Background on Immunity, Inc.

Immunity is a consulting and information security firm based in New York, Palo Alto, Buenos Aires, Argentina, and the Netherlands. Our customers include many of the Fortune 100 and our vulnerability disclosures include weaknesses in many of the major products on the market. This paper combines the knowledge we've gained from our engagements in an attempt to provide a working synthesis for discussion. More information on Immunity can be found at http://www.immunitysec.com/

Introduction

Large enterprises of a thousand people or more often have distinctly different information security architectures than smaller companies. However, typically they treat their information security as if they were still small companies. This paper attempts to demonstrate that not only do large companies have an entire ecology of specialized software, specific to large companies and their needs, but that this software has different security implications than consumer or small business software. Recognizing these differences, and examining the way this can be taken advantage of by an attacker, is the key to both attacking and defending a large enterprise.

Differences in applications for large enterprises

This section lists and categorizes the implementation details that separate a large company from a smaller one, in terms of information security technology. It then examines some case studies as to how vulnerabilities have affected different products of this nature.

Enterprise commercial off the shelf software

Large enterprises use a number of specialized off the shelf software products. A sample of these are listed below, along with their corresponding risks and security attributes.

Virtual Private Networks

Whereas small companies and individual consumers have the luxury of having their information technology space be in a single geographic area, a large enterprise has a sales force, multiple remote offices, and connections with customers and parters that send sensitive data over the larger Internet, or even over a less-secure company intranet. For this reason, large enterprises are almost certain to have one or more VPN technologies widely deployed, in addition to having leased lines directly connecting them to larger customers or partners, and sometimes vendors. This makes a large network difficult to properly segment, and in may cases, no network security layer exists on the internal network at all, or that security is negated by hosts that travel often between different security domains.

Management Software

Virus signatures, patches, and software deployment are almost always distributed to a standard workstation build in large enterprises. This requires management software to deploy the patches, and often management software to manage the management software. It's not uncommon to have five or more TCP/UDP ports open on a workstation that all have different management responsibilities. SNMP, while often publicly castigated for its poor security, is almost always enabled. Management software almost always includes a

OS-independent layer for communications, encryption, and transport. Because enterprises rely on any number of rare platforms, each management software vendor has chosen to recreate or wrap the API's that are not present in all of them. This often allows for bugs in one version and not the other – a command parser may be different from one version of Unix to the next, or from Unix to Windows, and in some cases, a bug that affects all of the platforms a piece of management software runs on, may only be high risk on one of them.

It should be noted that vulnerability assessment products are themselves enterprise-grade software, and are no-doubt under-assessed.[1]

Directory Services

Large environments need to quickly locate services and people, and for this reason ActiveDirectory and Novell Directory Services are both in common use. In some academic environments, you will also see large deployments of Kerberos and AFS. While single-sign on is a nice feature for a large enterprise with many thousands of users, it is also a huge advantage to an attacker. Without copious auditing, it's difficult to tell an attacker with stolen credentials from a normal user. Users are not aware that when they have a single-sign-on system, they are granting access to all system resources when they log into one system resource from, to, or sometimes just near a compromised host.

This is one of the cornerstones of enterprise application security problems: some security vulnerabilities are emergent behaviors of the scale of the application. Not all of them can be examined as the sum of their parts.

SAP, Oracle Financial software

Truly large and complex software, incorporating a proprietary database and proprietary middle-ware and presentation layer tools, SAP was recently audited by FX of Phenoelit (http://www.blackhat.com/presentations/win-usa-04/bh-win-04-fx.pdf), a German security research organization. As expected, many vulnerabilities were found in every layer. Tools such as SAP and Oracle Financial software typically hold a company's most valuable data, but for a variety of reasons have no public security record.

Databases

Large enterprises often have two or more databases widely deployed in their networks. In many cases, important data will be stored in Microsoft Access databases on individual workstations. It is important to note that out of the large databases, only Microsoft SQL Server has had a reasonable recent security review. Immunity has never during a network security review seen a database server with patches and service packs recently applied. It's also exceedingly rare that all the default users for a database have been removed or

1 This was pointed out to me during peer-review by someone who had found several vulnerabilities in exactly these kinds of products. Another good example are the recent vulnerabilities in RealSecure.

had their passwords changed. For the most part, databases are kept on the back-end, but for companies with flat networks, this can mean that any employee's workstation can log into the company's main databases.

There are many reasons for this weak stance in security. For the most part, the database administration team (if its more than one person) has total purview over all changes made to the database server. Because downtime often costs significant money, and any patches may cause unforeseen and impossible to debug errors, databases are rarely, if ever, modified. In addition, because memory and speed are at a premium on these heavily loaded machines, they often cannot deploy host-based defenses such as a host intrusion prevention system.

A database is an extremely complex piece of software, built for performance. Almost all of them are written in C and where performance shortcuts are made, buffer overflows result.

Hence, the market for database security scanners faces a crisis: on the one hand, companies need their product for things even as simple as basic password auditing. On the other hand, companies don't want to be charged per-database scanned, and they are rarely likely to make changes based on a database scanner's recommendations. Database scanners run from fairly expensive (1-5K per host) to horribly expensive. To further confound the fledgling database scanner market, companies are loath to run any kind of scanner on a live database server.

With a product as insecure as most database servers, when new low-hanging-fruit vulnerabilities are still easy to find, it is questionable whether patching a production database ensures any level of protection from a moderately skilled attacker at all.

Because of these factors, a CISO should expect both that there will be more vulnerabilities released this year against DB2 and other less explored databases (Oracle and MSSQL have already gotten a pounding) and should also expect that there were vulnerabilities patched by database vendors that were not made public (both Oracle and Microsoft have been making severe efforts to become more secure).

Rare or unique software

While products such as SAP can also be thought of as “rare” software, it's often that a large company due to legacy installments, is the sole, or one of very few, customers of an almost-dead technology. This rarely seen software was often written before buffer overflows were widely used, and is almost never maintained beyond what is necessary to satisfy operational constraints. Even finding and installing this software for an audit can sometimes be near-impossible, but for a determined attacker, it can also be a bonanza of security vulnerabilities.

Proprietary

Of course, any large enterprise will have large parts of itself dedicated to producing proprietary software, or building modules for other software. This software is never download-able by the public, and hence, is never audited by a third party (such as a security consulting company) for security weaknesses. When this software is sold to a customer as part of a service (such as your bank's web application which you would use to do balance look-ups, or Quickbooks Online, for example), it becomes exposed to the hostile intentions of the Internet at large. In many cases, proprietary software is used to hook a company up with its commercial parters or customers, and is not sold to the public. In these cases that software is even less likely to have received a security review of any kind, despite the fact that any vulnerabilities in that software reflect directly back on the companies reputation.

Collaboration

Collaboration and work-flow software, such as Lotus notes, or Microsoft Office 2003, provide little or no benefit to smaller companies, and have significant overhead. For a large company, however, the ability to merge and track documents automatically is an essential feature. It's fair to say that there will be few public announcements of vulnerabilities in Microsoft Office 2003's DRM server, since it is rare that an independent research firm will go through the effort to even set it up.

Hardware Platforms

Large enterprises by definition have a history. That history may include legacy systems such as Compaq Tru64 (installed at the Vatican, for example). Other proprietary Unixes, such as AIX, HP-UX, Irix, while still available, are not seen in smaller firms, but may have a wide acceptance at a larger enterprise which has relied on these technologies for decades, or has an extensive relationship with a particular hardware vendor. Obviously, large mainframes and clusters provide application security environments unfamiliar to many security professionals.

Software "Suites"

It is often the case that a software vendor will offer a package deal – license your enterprise for everything we sell for one low price. Of course, in many cases, this means they then go buy substandard software companies to flesh out their offerings. This can result in the suite having many products which are poorly secured, even if they are functional.

Large Enterprise Specific Weaknesses

Heterogeneous risk profiles

With most consumer software, the level of risk posed by any given vulnerability is obvious and widely discussed. Most installations of consumer-grade software are relatively similar, and independent research firms will quickly verify publicly the exploit-ability of any given bug.

However, when a vulnerability is disclosed enterprise-grade software, a CISO is faced with a difficult set of decisions:

1. Does this vulnerability affect any part of my infrastructure?
2. Is this vulnerability worth fixing?

With a smaller firm, or for a consumer, the question of whether to patch your system or not patch your system is an easy one: you patch your system. With a larger firm, each round of patching can cost millions of dollars. Automated patching systems help, but doing QA when your payroll system goes down due to some bug in the patch can mean the difference between keeping your job and hitting the street. With the time for an worm epidemic to be loosed on the Internet shortening to days after a vulnerability is announced, QA can become out of the question. A large enterprise's CISO has to decide immediately whether a vulnerability is worth patching at all.

By heterogeneous risk profiles, Immunity is trying to encapsulate that between any two large companies, the risk posed by a single software vulnerability varies widely.

Let's take recent vulnerabilities to illustrate the difficulties faced:

NAI ePolicy Orchestrator Content-Length Vulnerability

Unlike many other enterprise applications, McAffee ePolicy Orchestrator has had a security history, previously being reviewed by Andreas Junestam. Further information on these earlier vulnerabilities is here:

- http://www.atstake.com/research/advisories/2003/a073103-1.txt
- https://knowledgemap.nai.com/phpclient/viewKDoc.aspx?externalID=KB_NAI33260&sliceID=&docID=KC.KB_NAI33260&url=kb/kb_nai33260.xml&dialogID=4868733&docType=DOC_KnowledgeBase&iterationID=1

Because it is a virus management platform, it's likely that ePolicy Orchestrator runs on every host in your environment. And when three different vulnerabilities come out that could enable remote code execution, you're likely to bite the bullet and immediately begin patching. However, it is not safe to assume that just because several vulnerabilities come out in an enterprise product, that the researcher has done a thorough review. In

many cases with enterprise software, there are just too many vulnerabilities for one reviewer to cover.

Let's look at another, more recent, vulnerability in the same product.

From http://www.networkassociates.com/us/downloads/updates/hotfixes.asp:

```
Release Notes for McAfee® ePolicy Orchestrator(TM)
                    Version 3.0.1
                       Patch 3

...

-   This release addresses the McAfee ePolicy
    Orchestrator Agent HTTP POST Buffer
    Mismanagement Vulnerability; vulnerability
    identifier:  CVE-2004-0095.
```

And of course from cve.mitre.org:

Name CAN-2004-0095 (under review)
Description McAfee ePolicy Orchestrator agent allows remote attackers to cause a denial of service (memory consumption and crash) and possibly execute arbitrary code via an HTTP POST request with an invalid Content-Length value, possibly triggering a buffer overflow.

Now without public confirmation of an exploit (unlikely because the product is not widely distributed to the public), what CISO could make a decision to spend a million dollars patching their systems based on that information?

Immunity's notice on that same vulnerability is here:
http://lists.immunitysec.com/pipermail/dailydave/2004-March/000347.html
Having a clear warning that a vulnerability is easily exploitable – something the vendor almost always knows, but somehow fails to share with their customers – can make all the difference between a murky decision, and a clear one.

The problems faced with this vulnerability were:
- Misleading or absent information about the scope of the vulnerability
- Widespread deployment of ePO made the actual risk extremely high

It's important to look at your vendors with a critical eye when it comes to the information they release. On one hand, you don't want them to release working exploits before you have an opportunity to patch your systems, but you also don't want them to issue misleadingly vague advisories. This is one case where the risk of the exploit was extremely high, but the wording of the advisories led people to believe that the problem was not that severe.

HP HTTPD Certificate Upload Vulnerability

In March, 2004, HP issued an advisory based on a vulnerability Immunity discovered in their Compaq Web Management product. To quote from the Immunity advisory on the subject:

"Remote, unauthenticated certificate upload in Compaq Web Management (HP HTTP)

Compaq Web Management includes a number of daemons, which listen on a number of TCP ports, and also to SNMP requests. On port 2381, an SSL HTTP server runs. If the system is configured to let anonymous users browse it, a common configuration, then a bug in the validation system allows users to upload their own certificates to be trusted by the client system. This would then allow that machine to be administered remotely via such mechanisms as Secure Task Execution.

This is considered a critical problem, as Compaq Web Management is often installed on every machine in an enterprise.

This bug is exploitable, and can be done over and over. No knowledge of the Windows version is needed to be effective. This would probably work on all the other systems supported by Compaq Web Management."

The HP advisory is located here:
http://archives.neohapsis.com/archives/compaq/2004-q1/0006.html
"SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP HTTP Server (Version 5.0 through Version 5.92) for Microsoft NT/Windows 2000, HP-UX, Netware, Linux Survey, Compaq Array Configuration, System Insight Manager XE (SNMP & DMI Agents). Compaq Foundation Agents for Servers. "

The problems faced with this vulnerability were:

- Wide range of versions affected
- Wide range of platforms affected
- Must examine policy or software settings to determine if vulnerability affects your hosts (anonymous access turned on). Not all hosts in an enterprise will be vulnerable, and some enterprises will not have any vulnerable hosts at all, depending on their configuration policies.

Computer Associates Unicenter TNG Awservices Vulnerability

The Immunity Awservices advisory is here:
http://www.immunitysec.com/downloads/awservices.sxw.pdf
"
Remote, unauthenticated stack overflow Computer Associates Unicenter TNG Utilities awservices.exe

Computer Associates has developed a suite of tools that help enterprises manage the software on their machines. In doing so, they developed several proprietary protocols,

which are implemented in various daemons, listening on TCP and UDP ports, and running as SYSTEM. These daemons are vulnerable to classic stack overflows. In particular, Immunity reviewed cam.exe and awservices.exe, and found many examples of exploitable problems in both. These are considered critical problems, as they are often installed on every machine in an enterprise.

These bugs are exploitable, but are one-shots, and require knowledge of the Windows version to be effective in some cases. If these processes exit, they will leave an event log.

It should be noted that strcpy() and strcat() are used heavily. Other, similar problems are no doubt evident in many other services in Unicenter. If you use Unicenter, it is recommended you receive a source code audit of it from a security vendor you trust, using your infrastructure and configuration as a guide. What one company uses from Unicenter may be completely different from what your company uses.

Affected

All known versions of Unicenter TNG 2.4 are affected. According to Computer Associates, this problem was previously fixed in TNG 2.5
“

According to Computer Associates, Unicenter supports fifty different platforms.

The problems faced with this vulnerability were:

- Although Windows is clearly vulnerable, it is unknown if hosts running on Unix (or Siemens or other more rare platforms) are easily exploitable, so the risk to an enterprise can vary depending on which systems Unicenter is deployed on.
- Patching this vulnerability requires a deployment across almost any kind of server or workstation in the enterprise. Each patch may cause downtime, so it may be wise to delay patching certain servers, while still rolling patches out to all the Windows workstations.

Summary of difficulties

As seen, these are the main difficulties a CISO faces with each new vulnerability:

- Multiple and rare architectures. Because the risk profile of a single software vulnerability may be completely different across the platforms it runs on – on HP-UX, which is widely deployed, it may not be exploitable, but on Windows, which is only deployed on non-critical systems, it may be easily exploitable. Multi-platform means two different things to small and large organizations. To a small organization, it often means “Windows and Unix”, to a large organization, it can mean anything from Windows and Unix, to various types of mainframes, Cray supercomputers, and specialized networking equipment. It's not uncommon for an enterprise software

vendor to support twenty different platforms, each with their own risk rating for each vulnerability. This makes is difficult for a CISO to know if a given vulnerability is truly high-risk on their company's deployment.

- Enterprise-specific software products almost never get a solid review. A proper security review of a piece of software, such as SAP, can cost a hundred thousand dollars. Without significant pressure from customers, SAP has no incentive to do so, or to make the results of such a review public so that customers can determine the risk of running SAP in their environment. When a number of vulnerabilities came out in ePolicy orchestrator, CISOs had no verification that this was the result of a solid review with a resulting disclosure of risk, or if the reviewer simply stopped when the program crashed and didn't truly assess the vulnerabilities found.
- Vendor reports on vulnerabilities are rarely complete.
- Enterprise vulnerabilities are difficult to assess. Many tools exist to scan a network for known vulnerabilities. Nessus, ISS Scanner, NGS Typhon, Foundstone, Qualys, and other tools can be used to scan for standard Unix and Microsoft vulnerabilities. But it is unlikely that enterprise-specific products have entries in vulnerability databases, and hence, these types of tools are useless for a large enterprise's most vulnerable software. In addition, these tools are generally different than the tools an enterprise uses to distribute patches. A smart CISO is looking for an integrated enterprise security platform, that is cross platform in the way a large enterprise is cross platform, and combines network scanning, patch management, and software auditing. The generation after that will, no doubt, include host and network intrusion detection.

Information Security Strengths of Larger Enterprises

Large enterprises have significant new weaknesses, but they also have corresponding information security strengths:

- While one of the major sources for vulnerabilities in a large enterprise is their management software, this very same software allows a CISO to maintain a stable level of patches and configurations across entire ranges of their enterprise.
- A large enterprise's CISO can apply a dedicated security team, a luxury out of reach of smaller ventures
- The sheer size of a global organization can give a CISO time to react to new threats before they affect the entire enterprise, if they have proper network monitoring and network segmentation choke-points. A good example is Checkpoint's Application Intelligence, which allows you to disable SMB file access. When a new worm comes out, every network in the enterprise can have updated firewalls within minutes, which will prevent that worm from accessing files across their boundary.
- Some of the same management tools that are needed by a large enterprise can be turned into specialized intrusion detection tools. For example, automated logging on the single-sign-on system can determine if a user is behaving abnormally, and potentially lock them out if improper access requests are made.

Management issues for large enterprises

- Mergers and acquisitions present a special challenge, especially as these acquisitions proceed overseas to Asian countries, with their corresponding history of poor information security.
- It's hard for a CISO to take advantage of a business's special partnerships and business position without a CSO above them who truly understands the technology. Many CSO's have a law enforcement, not a technical, background, so they may not realize that they can ask for source code from some of their larger vendors (or that they may be asked for source code themselves!)

Conclusions

Immunity makes the following predictions based on our experience and analysis of the enterprise security situation today.

Linux

Linux's advantages are slim for a home user, more interested in getting their camcorder to work than being secure. But for an enterprise who can deploy Grsecurity (www.grsecurity.org) Linux's traditionally low TCO can be augmented by a near-zero patching cost. Expect to see Linux's phenomenal security features and trustworthyness propel it into large enterprises as much as its inexpensiveness. Many extremely large organizations are doing this already.

Database Security

Database security is just the tip of the iceberg. Large applications that require databases have emergent properties which adversely affect their security. Web applications are a specific example of this, but SAP-like and “rich client” applications will continue to pose unique vulnerability classes to a sophisticated attacker.

Targeted Epidemics (“The Fortune 500 Worm”)

Targeted epidemics – worms which affect only enterprise applications ("The Fortune 500 Worm"[2]) and which are released within an enterprise's network boundaries solve many of the problems with worms as an attack tool. A worm affecting only awservices.exe would most likely not spread outside a single enterprise, and would be able to reach almost every machine within that enterprise. Because enterprise software is poorly reviewed, many low-hanging fruit (worm-able vulnerabilities) still exist, allowing a worm creator to know that his creation will be reliable and resilient to defenses. Imagine a worm targeted at some piece of software your enterprise uses extensively, such as McAffee e-Policy Orchestrator, which sent every spreadsheet file it found out to a random email on the Internet. Because it is targeted, there are few preexisting defenses, and the worm would easily infect the entire organization, causing catastrophic damage.

Injecting the worm may be something as simple as a targeted spam message, or an unreleased exploit in one Microsoft's products. It may be impossible to trace the attacker back to this injection point.

Because most CISO's think of the problem of vulnerabilities as something to be solved with patches, having several Fortune 500 worms targeted at a single company could allow an attacker to repeatedly take a company down at moments that are critical to that company's success, such as the Christmas season.

Independent Verification

One defense, of course, is for large enterprises to become more proactive about their commercial off the shelf applications. Develop a relationship with a security consulting company, or more than one security consulting company, that you can trust to be honest, and have that company assess (perhaps at the vendor's expense) any large vendor's software that you place on more than 20 machines in your enterprise.

Vendor Relationships

It is the job of the CISO to ensure that the vendors you rely on for your enterprise's software are giving you the truth, the whole truth, and nothing but the truth about the risks posed by new vulnerabilities in their software. When a vendor misleads you, or does not give you the information you need to do your job, hold them accountable, or look for another vendor. Be aware of the past of vendors you're looking into relationships with.

2 "The Fortune 500 Worm" term was coined by rocky during a peer review of the concepts in this paper.