Securing WebSphere V6 Technology

This month's newsletter covers some of the key fundamentals of security, some interesting security stories and trends, followed by an in-depth look at WebSphere Application Server (WAS) V6 security.

Year 2005 began with one of the largest bank frauds in US history - the fraud was 100% internal. IBM completed a study that indicated that about 70% of threats came from inside corporations. Trends in security indicate that companies are finally absorbing these statistics and moving to a more comprehensive security model away from the previous perimeter security mentality - an information "fortress" with "walls" of network equipment. Improved internal security practices such as enhanced hiring practices and higher levels of security awareness amongst employees should reduce vulnerabilities.

WAS V6 has several new security benefits that include conformance to the latest Web Services standards, a High Availability Manager and improved means to restrict unwanted user requests. Included is a checklist to lock down WAS and several ways to improve WAS security related performance. Last, if you are interested in deeper security information, look in the section "Want to know more about Security?"

We ain't a Bank!

For the last 5 years, the comment I heard most from organizations when I mentioned security was either "We ain't a Bank" or we are a bank but we do not need that much security. When I say "not much security", I mean environments with almost no security. All "pipes" in cleartext where installing the most basic of network sniffer software could collect user/passwords to databases, SQL queries with bank card numbers, expiry dates, balances and social security numbers could all be "picked off". Many companies have tight security, but many did not. However, that has largely changed since Sarbanes-Oxley has arrived along with other government regulation that helps financial institutions stay tough security wise. Another reason corporations have to increase the level of security is the growing number of threats from both inside and outside the organizations.

Security 101 - Fundamentals You Better Know When Talking About Security

Whether your concern is corporate or personal security, knowing some of the fundamentals of security can help you make the right decisions and look smarter. Below are the top five strategic concepts you need to know and if interested in more information, look at the "Want to know more about Security?" section.

1. **A security system must have the first three to be effective :**
    a. **Vaults** to protect the booty,
    b. **Alarms** to detect the pirates, and a
    c. **Response** to the alarms. Optionally,
    d. **Deterrents** by making the pirates walk the plank.

2. **The strategic principles of information security require a balance amongst three attributes:**
    a. **Confidentiality** – information is accessible only to those authorized to have access.
    b. **Integrity** – safeguarding the accuracy and completeness of information.
    c. **Availability** – ensuring that authorized users have access to information.

3. **Business requirements need to be understood for security purposes through the following:**
    a. **Risk Assessment**
        i. Threats to assets are identified.
        ii. Vulnerabilities and likelihood of occurrence are evaluated.
        iii. Potential impact determined.
    b. **Legal, statutory, regulatory and contractual requirements related to security**.
    c. **Objectives and requirements for information processing.**

4. **The tactical categories of controlling information security threats are:**
    a. **Administrative –** policies, standards, procedures, guidelines, etc.
    b. **Technical -** authentication, logical access control, encryption, etc.
    c. **Physical –** locks, guards, environmental controls (temperature, humidity), fire, etc.

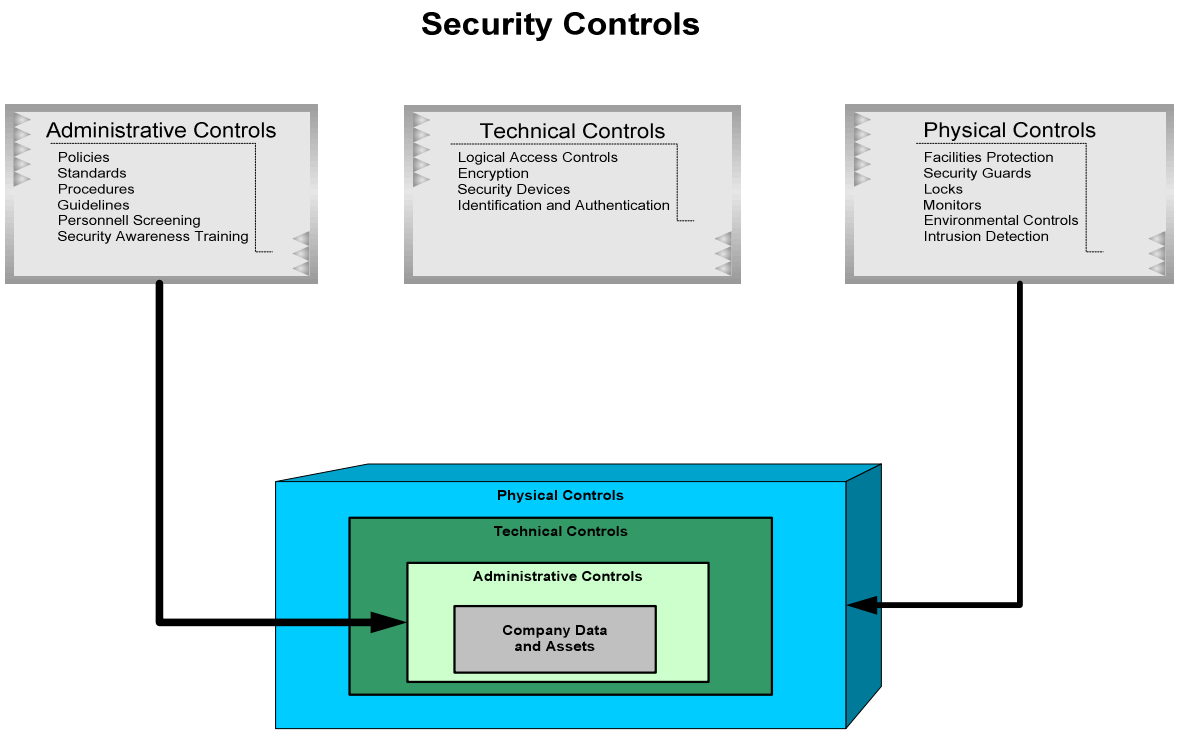
5. **Corporate officers that do not incorporate due care and due diligence into operations are liable legally for negligence.** Due care is creating the administrative controls and due diligence is enforcing those controls.

When protecting assets, companies must decide on the right combination of **vault** strength, sophistication of **alarms** and speed and fidelity of **response**. For example, if vaults are rated to stop thieves for 30 minutes, then alarms must be triggered and a response must be made in that timeframe. The cost decision is typically based on value of the assets being protected. If there is a loss, both tangible and intangible value is at risk. Typically, insurance protects the tangible loss of the assets, but what most companies miss and insurance companies will not cover, is the intangible value of the loss. Companies such as financial institutions whose primary asset is information have market capitalization based largely on intangibles. For example, Coca-Cola has billions of dollars of market capitalization locked up in the value of their brand. So, a significant loss that impacts credibility will likely have a minor impact on the balance sheet while potentially having a devastating effect on market capitalization and resultantly on their stock price.

Vaults, alarms and response while required for physical assets are also required for information assets. When information has to be protected, owners must balance budgets across three major concerns for **confidentiality, integrity and availability of information.** Typically, the **military**

is deeply concerned about confidentiality. So much so, that they would rather have data destroyed than fall into the wrong hands. Destroyed data would still be confidential but both integrity and availability would be lost. On the other hand, **commercial businesses** typically need a balance of all three. The mixture of the three is based on the cost/benefit to the business customers and even the criticality and profitability of a particular business unit.

The balance of confidentiality, integrity and availability is determined by understanding the requirements through **risk assessment**, **regulatory requirements** and **company objectives**. Three major types of security controls can be used to satisfy these requirements - **administrative**, **technical** and **physical** controls as shown in the figure below. The most critical area of technical controls that is often overlooked but cause businesses great losses or even bankruptcy is business continuity planning and disaster recovery (see Want to know more about Security section). While executives and senior management are substantially involved in administrative controls, IT implements policies and standards with technical controls and to some degree physical security that relates to IT.



Security 201 - Internal Threats, What Internal Threats?

I hear this from many IT personnel throughout North America so don't feel bad if you have the same response. It's true that there are far more remote attacks on organizations systems than a few years ago. Many are from remote areas of the world where there are no reciprocating laws so enforcement is difficult. But all the data indicates that most organizations have overcompensated for these external threats by building out huge network and security "fortresses" at the

expense of vetting internal risks. Below are some examples of threats to people, organizations and property. As you will see, many are of an internal origin.

1. **Bankruptcies** – it's estimated that one-third (33%) of bankruptcies is the result of theft[1].
2. **High growth start-up businesses have highest internal fraud** – smaller business that want to grow quickly typically have many new hires. Compounding the risk is limited HR screening practices. This makes them far more susceptible to internal fraud, business losses and bankruptcies.
3. **Fraud** - An Ernst and Young report found that 82% of the worst frauds in 1999-2000 were committed by employees[2].
4. **Banking** –Mid-level managers are responsible for the largest portion of internal fraud. Interestingly, IT personnel account less than 15% of banking theft and fraud.[2]
5. **Fast Food Restaurants** – Approximately 66% of hold-ups/robberies are performed by past or current employees.
6. **Organized Crime** – Could this be an industry? They would much rather attack a company by planting their people in organizations and "social engineer" fraud than do it the hard way, through networks, software diddling and systems corruption.

Some of the causes for costly internal threats going unchallenged are:

1. **People across many job functions have been fed popular press security.** The problem is the media gets word of viruses but not of internal threats such as fraud and theft.

2. **It is bad business for a company to admit they have been defrauded.** With a high profile physical bank robbery, financial institutions have no choice in receiving media attention. It is another matter when the threat is less visible. Companies want to keep problems to themselves so that their customers, partners and financial markets do not lose confidence in their abilities.

3. **Television series and movies that feed this misinformation.** Current Hollywood products are a little more accurate in identifying the top threats. A recent movie called "Firewall", with Harrison Ford is more on the money when the hackers are too lazy to hack the networks and taking Ford's family hostage. Why go to computer science school for 4 years when you can just act tough and learn to fire a gun in a few days. This tactic is known as social engineering and is the real biggest threat to an organization's security.

"As any experienced hacker – ethical or criminal – will attest, it is more effective to focus on people errors and poor security practices than it is to try to crack today's sophisticated technology solutions."[3]

4. **Most companies have insufficient security training at both the business unit and IT level.**

Recent Events

1. **Largest bank fraud in US history committed in 2005. No hacking, all internal mid-level Managers, no IT workers involved!**

http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101903,00.html

2. **Recent 2005 survey of business executives by IBM found that almost 70% of threats to corporate security came from inside the organization[4].**

Security 301 - Trends in 2006 You Better Know When Talking About Security

From the results of a Deloitte 2005[3] worldwide survey of financial industry executives and security officers found:

1. **The top threat concerns are financial fraud and viruses. "**The majority of respondents who experienced some form of breach experienced it from within the walls of their organization. In many instances, employees have unlimited access to customers' vital data, including government issued numbers (e.g. Social Insurance and Social Security Numbers) and account number information."[3]
2. **Top business challenges are increasing threat sophistication and lack of employee awareness and training.**
3. **Primary reasons for security projects failures are:**
   a. Lack of business buy-in (34%).
   b. Integration problems due to poor up-front design and architecture (48%).
   c. Unrealistic timelines and budgets (56%).
4. **There will be less focus on perimeter security and more emphasis on a holistic security strategy.**
   With lack of security training, staff focuses on the popular press security, building a perimeter fortress out of network and hardware components.

Four high level actions that can be taken to quickly increase security levels

1. **Review the ISO 17799 security framework** - Assure broad coverage is instituted, not just at the "walls of the fortress".
2. **Set in place HR policies that do the proper background checks on personnel.** Criminal and reference checks could substantially lower an organization's threat level. According to ISO 17799 security framework, background checks should include and can be automated into the hiring process:
   a. Availability of appropriate character references.
   b. Check for completeness and accuracy of the applicants curriculum vitae.
   c. Confirmation of claimed academic and professional qualifications.
   d. Independent identity checks.
3. **Have appropriate backups**.
4. **Restrict employee access control to "need to know".** Strength in procedures and well-trained staff to design and implement security is critical. This will set employees and the company up for success, rather than failure.

Security 401 – Reducing Risks in Software

It's generally accepted in the security industry that the more complex the software, the more vulnerabilities that will exist. Complexity increases for several reasons but a major problem is that software takes engineering and design talent. Unfortunately, enterprise software has low levels of design maturity, mostly IT is "coding it" not engineering/designing it. The problem can be summed up by Schneier:

"Anyone can build a traffic light, but it takes a different mindset to conceive of a citywide traffic control system"

Bruce Schneier "*Secrets & Lies, Digital Security in a Networked World"*

1. **Low modularity increases complexity inducing more security vulnerabilities.** Because there is less design/engineering of software, modules are designed with tighter coupling resulting in increased complexity and hence lower security.
2. **The more complex the system the more you need expertise to figure it out.** Then the people managing the experts and the complex system have difficulty coping with the accountability for those systems.
3. **The more complex the system the harder it is to complete the software application.** When the analysis and design are complex, so is the coding, implementation, verification and testing. Security flaws go up.
4. **The more complex the system the more difficult it is to test.** With complexity comes an increased number of paths through the software. This means more test cases and greater potential for security flaws.

WAS V6 Security 101 – What's new!

There is at least 2000 pages on WAS security that you need to really understand to fully lock down WAS. In release V3.5, simply turning on security had a dramatic negative impact on performance. Lab tests by IBM indicated anywhere from 30-40% performance impact in that version. Therefore, many companies that have high volume applications left WAS security off and depended on operating system level security and the good faith of its employees. But, V6 has stepped up the level of sophistication in terms of:

1. **Web Services that meet the latest industry standards** – WS-1 and OASIS. You can make the case that the inclusion of WS-TX increases availability.
2. **High Availability Manager** – Software level fault tolerance that increases availability. This feature allows grouping of similar managed processes so that if one process in the group fails, the failed processes workload can be moved to another process in the group. For example, deployment managers (DM) can be grouped. If one DM fails, another DM in the group can take over its in-flight tasks. WLM management allows failover of in-flight transactions.
3. **Improved network and protocol management** - Network transport chains that help protect WAS from such things as Denial of Service attacks.

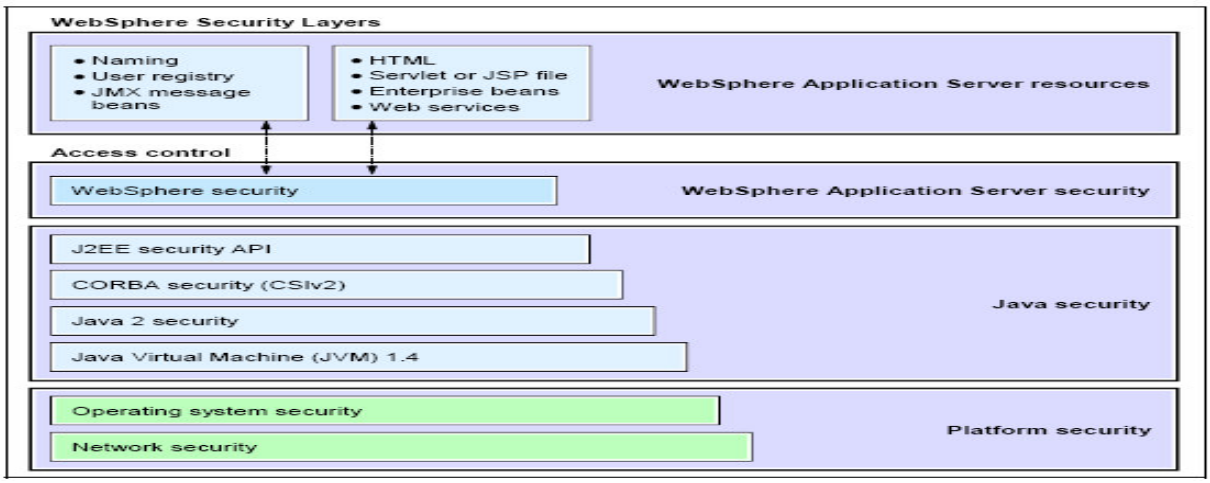
4. **"Profiles" that increase WAS instance isolation**. This affects all of CIA because separate configurations on each WAS instance has an improved degree of isolation.

What's WAS Security look like in V6?

WAS V6 has two levels of granularity: the global level and the application level. The idea is that you can turn on global security and actively limit or enhance security at a particular application server level.

Global Security refers to the security placed on an entire security domain. A security domain consists of all the servers that are configured with the same user registry realm name. Practically, this is all the servers in the cell that are configured with (typically) a LDAP server. Configuring the global security includes:

1. **WebSphere Security**
    a. **LDAP** – Light Weight Directory Authentication Protocol - attaching to a user registry typically via LTPA.
    b. **JAAS** - Java Authentication and Authorization Services – Role based access control.
    c. **JSEE** – IBM Java Secure Socket Extension – IBM SSL implementation for WAS.
    d. **DRS** – Data Replication Services has option to use secure (encrypted) transfers to enables replication of Sessions, DynaCache and Stateful Session Bean objects amongst application servers in a cell.
    e. **JMX** – Java Management Extensions – Ship commands amongst managed processes. Uses SOAP/HTTPS for secure transfer of commands.
2. **J2EE Security** – Role based protections on Servlets/JSP's, EJB methods
    a. **JACC – Java Authorization Contract for Containers -** interact with third-party authorization providers – Tivoli Access Manager.
    b. **J2C** -Java 2 Connector Authentication - connecting to enterprise resources such as CICS, SAP, PeopleSoft, IMS.
3. **Corba Security** - CSIv2 - Common Secure Interoperability for distributed communications – connecting between EJB containers.
4. **Java 2 Security** – securing underlying access to OS system resources.



Application Level Security

Application level security is either declarative or programmatic security. Declarative security considerations are set at the WAS server level while programmatic security exists in the application code. **Best practices would dictate to define as much security as possible through the declarative approach.**

Declarative Security

The easy way to think of **declarative** security is it is DECLARED in the deployment descriptors that WAS reads, NOT the application. The application neither knows anything about nor takes any action on the security declared. Declarations are made a deployment time versus programmatic security which works at runtime. WAS reads declarations at start-up of the application from a descriptor file. So the advantages of declarative security are:

1. **Lowers code complexity:** It does not add to the complexity of the application software. This reduces security flaws, at least in the application code.
2. **Easier maintainability:** It allows security to be modified without changing the application code. This reduces the amount of regression testing of the application although the combined solution of application and WAS needs to be retested. Typically, this would involve infrastructure only.

The three things that have to be set to make declarative security work for **Web Resources such as servlets, JSP and HTML**:

1. **Roles** – logical security names so that the application does not have to know runtime roles that typically are located in the company's operating system or LDAP directories. These details are implementation dependent. Tellers may be a logical name defined in WAS and it will be mapped to a LDAP defined group BankTellers as all the bank tellers in the company.
2. **Constraints –** combination of asset to be protected (URL or HTTP method), role(s) allowed access to the asset. Servlets, JSPs and HTML can all be secured.

3. **Authorized Roles –** What **roles** can access which **constraints**?

Declarative Security for EJB's depend on roles as defined for web resources. However, EJB roles are assigned to the EJB interfaces and methods. EJB may call other EJB and there needs to be authentication during this communication. EJB calls can use the Users identity (default), the server or specific security role. For most applications, components should be run with the default, User identity.

Programmatic Security

Typically, programmatic security is only needed when a finer level of security is required down and into the methods. This type of security is only recommended in the most stringent of security requirements.

WAS V6 Security 201 – What you need to lock down?

There are principally two places data can be found, in-transit or stored. In WAS V6 the in-transit, stored and access control points in the application that need to be reviewed and locked down are:

In-Transit Data Privacy and Integrity Checklist

1. Web Browser to Web Server.
2. Web Server to WAS Web Containers.
3. WAS to Authentication servers such as LDAP.
4. WAS to Access Control servers such as Tivoli Policy Manager.
5. WAS to Enterprise Systems such as Mainframes, SAP, ERP, etc.
6. WAS to Relation Databases Management Systems (RDMS).
7. WAS to Messaging (JMS, WMQ, Message Beans, ESB).
8. WAS to Web Services.
9. WAS to other WAS or other application servers (i.e., BEA Weblogic) via Corba distributed communications.
10. Administrative internal communications between managed processes – SOAP/JMX.
11. Session Information replicated across servers.
12. Session, DynaCache, Stateful Session Bean data redundancy – DRS communications across servers encryption.

When securing the channels one of the critical tasks is to change the default key files on all nodes and deployment managers.

In Storage Data Checklist:

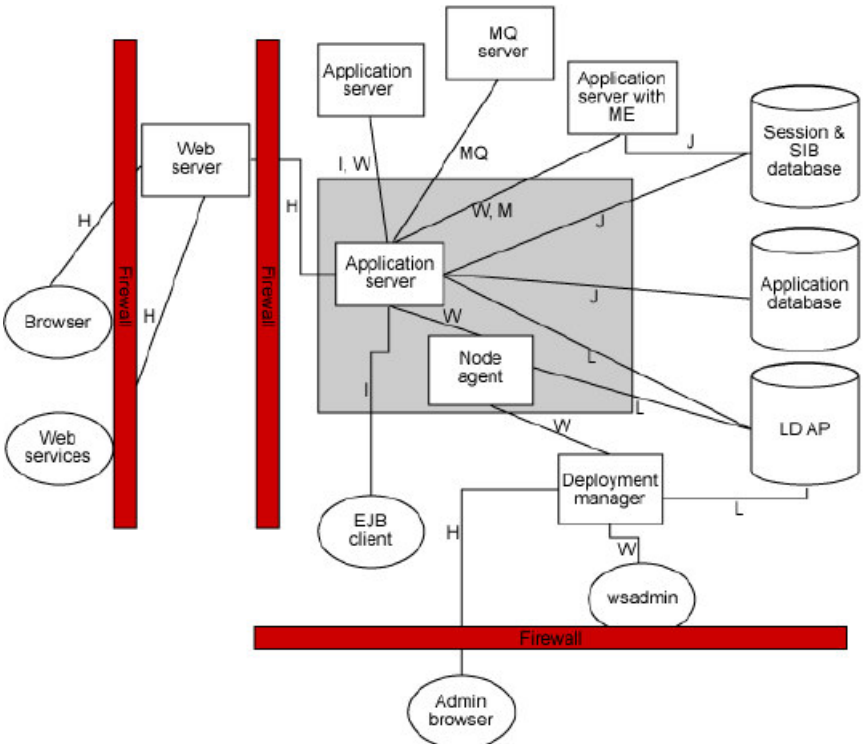
1. WebSphere product configuration data – operating system and Java 2 protection.
2. WebSphere product files access – directory and file ownership and permissions.
3. Application resource data stored at the EAR level – property files and other security information is not adversely exposed.

Access Control/Authorization Checklist

1. Admin Console – Four levels of access control for administrative purposes.
2. Block serving of servlet classes – serveServletsByClassnameEnabled.
3. Restrict to trusted servers – Communication between Web Servers and WAS only are allowed, all other sources fail to connect.
4. Restrict JNDI to read only.
5. Assign Groups to Roles – assembling the application.
6. Assign RunAs roles – assembling the application.
7. Assign EJB method permissions for security roles – assembling the application.

Authentication Checklist

1. Enable Global Security – Single Sign On with horizontal and downstream propagation of tokens.
2. Enable Session Authentication – user can access only their session – session integration.
3. Restrict applications to their J2EE resources only - Container versus application authentication.
4. Restrict Servlets – Method level Gets, Posts, Deletes can be restricted by role.



H – Http Transport
W – WebSphere Internal Transport
J – JDBC database communication
L – LDAP communications
MQ – WebSphere MQ communications
M – SIB message protocol – WebSphere Enterprise Service Bus

WAS to DB2, Oracle and Microsoft SQL Server – New means to secure the pipes

In DB2 V8.2 there are new means to secure the JDBC Connection. Oracles JDBC security mechanism has been around much longer since 8.1.7.4. Oracles encryption up to 10.1 has only been 40 bit. However, 40 bit might be enough to satisfy you security requirements. Last, Microsoft came out with a new JDBC driver in December, 2005 that is much more secure.

WAS V6 Security 301 - Minimizing the impact of increased security on performance.

When you get married, your level of security goes up because marriage helps mitigate risks related to one partner earning if another is not able to. However, to get the spouse you might have to sell the Corvette and get a van – trading performance for security. Likewise, in WAS there is always a trade-off between performance, features and security. Security typically adds more processing time to your requests, but for a good reason. Remember though, not all security features are required in your environment. When you decide to tune security, you should create a benchmark before making any changes to ensure the changes are improving performance. Here are a few key points that might help increase the performance of WAS V6 security.

1. **Hardware accelerators increase performance when there are several SSL handshakes, not bulk encryption**. Hardware accelerators currently supported by WAS only increase the SSL handshake performance, not the bulk encryption and decryption. An accelerator typically only benefits the Web server because Web server connections are short-lived. All other SSL connections to WAS are, or should be, long-lived.

2. **The SSL_RSA_WITH_RC4_128_MD5 cipher suite is the best performing.** The digest algorithms MD5 is 25% faster than SHA, however, SHA is more secure than MD5. Triple DES is the most secure, but the performance cost is high when using only software.

3. **Consider reducing or disabling security for applications that don't need it while keeping global security on.**

4. **For less sensitive data, reduce cipher strength.** If you send a large amount of data that is not very security sensitive, reduce the strength of your ciphers. The more data you have to bulk encrypt and the stronger the cipher, the longer this action takes. If the data is not sensitive, do not waste your processing power with 128-bit ciphers.

5. **Client certificates add little overhead:** Consider using SSL client certificates instead of a user ID and password to authenticate Java clients. Since you are already making the SSL connection, using mutual authentication adds little overhead while removing the service context containing the user ID and password completely.

6. **SSO web inbound security attribute propagation performance depends on the application's characteristics-Test drive it**. Consider disabling or enabling the "Web

Inbound Security Attribute Propagation" option on the SSO panel if the function is not required. In some cases, having the function enabled improves performance. This improvement is most likely for higher volume cases where a considerable number of user registry calls reduces performance. In other cases, having the feature disabled improves performance. Improvement typically occurs when the user registry calls do not take considerable resources.

7. **Improve Web Services performance with the unlimited JCE.** Improve the performance of web services security by downloading a Java Cryptography Extension (JCE) unlimited jurisdiction policy file that does not have restrictions on cryptography strength.

Which one are you? A Jimmy Carter who struggled as President or a Ronald Reagan who got a lot done.

There are two types of thinking patterns according to Leonard[5] – **divergent** and **convergent** thinking. High capacity for convergent thinking aids in finding solution to analytical problems. Like IQ tests or accounting problems. Divergent thinking best suites situation where there is no clear answer. Like, do we help Africa, invade Iraq or do we enter a new market. Obviously, there is no equation to solve these questions. The less data the more divergent thinking helps.

Convergent thinkers in meetings want to keep things to a schedule. The upside to convergent thinking is in time-pressured situations it works well. Where it doesn't work well is when you need to generate innovative ideas. Innovative ideas come from free flowing and often extended thinking sessions. In these situations, convergent thinkers often want to be kept to schedules and often generate fewer ideas and likely not the best.

On the other hand, **divergent** thinkers value ideas and don't like to keep to schedules – it hinders their thinking. Since less analytical problems don't have clear answers, they get shoved up the organization to the top. This is where divergent thinking pattern helps the most, when there is no clear solution. So, while Jimmy Carter was great at analytical issues, it was not ideal for the role of a President. Conversely, Reagan's divergent pattern of thinking likely horned through days in showbiz and Hollywood, served him well.

Want to know more about Security?

I am amazed with the high quality of material that the US government puts out on its Internet site. You can get a lot of free advice at the expense of the US taxpayer. I believe the US government overall see's a big threat to many businesses in the US that would not otherwise put in place adequate security. So, they have gone to great length to educate and outline security for the US public. Because of the Internet, there is a spill over to everyone in the world.

1. Broad Overview **- CISSP Certification Guide,** Shon Harris, 3rd Edition, 2005. This is a great reference and covers a lot of ground about security fundamentals in 1000 pages.

2. Broad Overview **– Secrets & Lies –** Bruce Schneier. Schneier is less formal preferring to impart deeper insights into security rather than just information. The book is a well-written account of the entire security landscape from operating systems, cryptography to social engineering. The downside is it is written like a novel and has no figures or graph to explain concepts.

3. Broad Overview **- "Security Engineering" -** by Anderson – The best compendium on more technical issues in security**.** The book covers everything under information security. He worked in the banking industry, so he has a lot of examples about how unsophisticated individuals "worked" their banking employers systems to commit fraud. It also covers banking and accounting, credit card security, biometrics, telecom, copyright, etc.

4. Broad Overview **– An Introduction to Computer Security**: The NIST Handbook, NIST, US Department of Commerce, National Institute of Standards and Technology.

5. Enterprise Security Framework **- ISO-17799:2005 – This is a necessary document if you are planning a businesses security.** It contains a high-level description of everything you need to have for a complete security solution for the company.

6. Business Continuity - **Contingency Planning Guide for Information Technology Systems** – US Department of Commerce, NIST – National Institute of Standards and Technology, 800-34

7. Physical Security **– FM 3-19.30 Physical Security – US Department of the Army –** Depending on how paranoid you are, this document could also be used as a guide on locking down your personal property, house, etc. Recommendations on such things as setting up bearers to truck and car bomb attacks, what kind of dogs are best for personal protection, building material and lighting to minimize penetration by thieves, how much concrete or steel you need to stop a particular type of bullet and means to minimize theft of product stock within stores and distribution centers.

References

1. US Army, FM 3-19.30, Physical Security, 2001, Headquarters, Department of the Army
2. Anderson, Security Engineering, Wily, 2001
3. http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf
4. Braun Research, Jan. 2006 for IBM Canada.
5. Leonard, "Putting Your Company's Whole Brain to Work", Harvard Business Review, July, 1997