

Report

Top Ten Web Vulnerabilities in Hong Kong and How to Avoid Them



HiTRUST.COM (HK) Inc. Ltd.

www.hitrust.com.hk

November 2006

CONTENT

Regulatory Compliance by Hong Kong Enterprises	2
Source of Data	3
Top 10 Network Vulnerabilities	4
Threats and Impacts	4
Common Unprofessional Practice in Hong Kong	5
Practical Tips: What You Can Do	6
What You Can Do #1: Enforce High Encryption Cipher	7
What You Can Do #2: Manage Security Patch Updates	7
What You Can Do #3: Harden New Servers	9
What You Can Do #4: Regularly Scan for Network & Application Vulnerabilities	10
What You Can Do #5: Well-plan Web Application Development	11
What You Can Do #6: Enforce Security Policy, Guideline & Procedure for Internal and Service Provider	12
Final words	12

The responsibility of IT Managers or CIOs in Hong Kong have been extended from upgrading corporate competence by harnessing IT power to electronic asset management and protection which is of crucial importance to both enterprises and its customers. In recent years, the demands of regulatory compliance, such as Basel II, SOX (Sarbanes-Oxley) and PCI (Payment Card Industry), from various governance authorities have produced mounting pressure on enterprises who are mandated to ensure their IT systems, network and database, especially customer data, are well protected under appropriate security measures. IT managers are thereby not just technical savvies mastering various servers and equipments, but guardians on network overlooking corporate and customer data security to safeguard corporate image as well as shareholder interest.

The purpose of maintaining network and data security is not any more referring to preventing loss of revenue, damage of reputation, breach of regulation, or anything that only matters to a corporate itself. It is now becoming a corporate social responsibility (CSR), in broadest sense, to guard against abuse of information technology that hurts the cornerstone of economy world – ‘trust’, thereby protect and enhance Hong Kong core competence.

Regulatory Compliance by Hong Kong Enterprises

Followings are local and international industrial regulations need to be complied with by certain enterprises in Hong Kong..

1. For Government Body (enforced by HKSAR Government internally)

Data, information and documents are classified into different categories: Top Secret, Secret, Confidential, Sensitive, or Public

- ◆ Confidential data must be encrypted when they are in transmission and storage
- ◆ Encryption strength - Encryption key must be at least 128 bits
- ◆ Enforce Separation of Duties
- ◆ Audit log must be performed for shared data access

2. The Personal Data (Privacy) Ordinance, Cap 486

3. Hong Kong Monetary Authority

- ◆ Technology & Risk Management Guideline specifies data security requirements, and all banks and financial institutes are expected to follow

4. PCI Security Standards Council

- ◆ All merchants accepting credit cards including American Express, Discover, JCB, MasterCard and VISA, shall enforce data protection to protect customer privacy information

5. Sarbanes-Oxley Act (SOX)

- ◆ US listed Companies and it Branches in Hong Kong (overseas) are mandated to follow the act

Source of Data

As an International Affiliate to the most prominent Internet security service provider, VeriSign, HiTRUST has been providing SSL certificate service to thousands of servers in Hong Kong for six years. While SSL is becoming prevalent on Internet, cyber attack and exploitation technologies are also evolving quickly. To help customers identify their network vulnerabilities and apply appropriate remediation, HiTRUST devised a network security assessment service conducted by its consultants as part of the standard SSL Certificate package, called Inspection and Acceptance Test. The service has been well accepted by customers since its launch in October 2005 as it gives enterprise IT managers an outsider's view of their servers which includes health check information and recommendation about their servers.

To get an overall picture of Hong Kong enterprise network security posture, especially web servers facing Internet, HiTRUST consulting service team compiled and scrutinized the data collected through the service. No major industry or sector was specially focused. More than 350 servers have been assessed through out the past year which are dispersed among various sectors, such as banks, government agencies, insurance companies, securities companies, trading companies, retailers, educational institutions, etc.

The research outcome reveals that more than half of the customers have not yet intensified their network security by implementing necessary enhancement specified in certain regulation. Some cases don't even meet the criteria that are generally accepted as basic network security practice. In general, medium severe vulnerabilities are not uncommon on the servers assessed. It is important to note that having a SSL certificated installed on a server does not necessarily mean SSL mechanism is properly exerted on the server.

Top 10 Network Vulnerabilities

This report lists top 10 common vulnerabilities found from the analysis of the data collected. Recommendations are also made to help enterprises apply proper remediation and common security practices to achieve regulatory compliance.

Top 10 Vulnerabilities	Percentage of Assessments with that vulnerabilities found
SSL Server Has SSL v2 Enabled	71.3%
Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerabilities	54.3%
Account Brute Force Possible Through ISS NTLM Authentication Scheme	52.3%
SSL Server Supports Weak Encryption Vulnerability	50.8%
Microsoft IIS Authentication Method Disclosure Vulnerabilities	39.9%
Microsoft IIS Internal IP Address/Internal Network Name Disclosure Vulnerability	31.0%
TCP Sequence Number Approximation Based Denial of Service	30.2%
WebDAV HTTP Method 'PROFIND' Enabled	25.2%
ICMP Timestamp Request	22.5%
Netscape/OpenSSL Cipher Forcing Bug	20.5%

From the results, argument would exist whether Microsoft products are more vulnerable than other vendors'. It may be true in part because hackers usually invest their resources on software that are commonly deployed. In our survey, the occurrence of certain Microsoft vulnerability is comparatively higher as Microsoft products has been quite extensively employed in Hong Kong. Therefore our results cannot be an indication that Microsoft is more vulnerable, instead, it reflects Microsoft popularity in Hong Kong.

Threats and Impacts

HiTRUST consultants have responded to numerous assessments and even incidents. Majority is related to the above vulnerabilities, which is caused mainly by the improper application of SSL protocol and the default server configurations set by vendors. Threats and impacts posed could be serious to companies' network security and reputation, as follow:

- **Disclosure of sensitive communication** - Messages encrypted with low encryption cipher are easy to decrypt. Flaws in the SSL v2 protocol allows man-in-the-middle attack to force the communication to a less secure level and then attempt to break the weak encryption. Even worse, some companies allow server authentication credentials to be transmitted in plaintext over the network without performing any encryption.
- **Brute Force Attacks** – Enabling NTLM authentication on the Microsoft IIS Web Server by default allows a remote user to perform account brute force by requesting a non-existing HTTP resource and an existing HTTP resource that does not actually require authentication.
- **Exposure of Internal IP address or Internal Network Name** –Vulnerability exists in default installation of IIS, which discloses companies' internal IP address or internal network name. Successful exploitation of this vulnerability could assist in further attacks against the target host.
- **Disclosure of Authentication Method** –When a valid authentication request is submitted with an invalid username and password, an error message is returned. Authentication methods supported by a given IIS server can be revealed to an attacker through the inspection of returned error messages. This information can then be used in further intelligent attacks against the server, or in a brute force password attack against a known user name.
- **Denial of Service on Web Server** – On TCP based services of target host, some implementation may allow attackers to make a successful approximation of an acceptable TCP sequence number. This will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. Other consequences may also results, such as man-in-the-middle attacks.
- **Cross-Site Tracing** – If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attackers. This may be the case even if the Web applications are not vulnerable to cross site scripting attacks due to input validation errors.
- **Compromise of Confidential Information** – HTTP and the WebDAV extension allow file information to be retrieved remotely from the Web Server. If there is no restricted access, anyone can retrieve information (like directory listings) from the Web Server. Besides, cipher forcing bug may also result in disclosure of sensitive information
- **Exposure of Internal System Clock for Attacks** – Unauthorized users can obtain information about your network by sending ICMP timestamps packet. For example, internal system clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

Common Unprofessional Practice in Hong Kong

It is important to note that the more than 90% of vulnerabilities have counter-measures. In conducting security assessment, besides vulnerabilities scanning, HiTRUST consultants encounter some "common unprofessional practice" which result in the vulnerabilities listed above when reviewing customer's network environment and security policy.

Top 10 Vulnerabilities	"Common Insecure Practice" causing the Vulnerabilities
SSL Server Supports Weak Encryption Vulnerabilities	SSL protocol is deployed for secure communication between a client and a server, but low encryption cipher is allowed.
SSL Server Has SSL v2 Enabled Vulnerabilities	Non-updated version of SSL (v2) is enabled by default
Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerabilities	Patches or guideline for these vulnerabilities are readily available from vendors' website, but they are not implemented on the servers. No hardening before the new server is connected to the Internet.
TCP Sequence Number Approximation Based Denial of Service	
WebDAV HTTP Method 'PROFIND' Enabled	
Netscape/OpenSSL Cipher Forcing Bug	
Microsoft IIS Internal IP Address/Internal Network Name Disclosure Vulnerability	
ICMP Timestamp Request	
Account Brute Force Possible Through ISS NTLM Authentication Scheme	
Microsoft IIS Authentication Method Disclosure Vulnerabilities	(No solution from vendor yet, but can be avoided by deploying IPS or application layer security measures)

Practical Tips: What You Can Do

From the assessment project, HiTRUST consultants have identified a number of tactics to address the causes of the vulnerabilities. These tactics help mitigate risk exposed on enterprise network effectively. It is also essential to apply these tactics regularly across the entire enterprise network.

1. Enforce High Encryption Cipher
2. Manage Security Patch updates
3. Harden New Server
4. Regularly Scan for Network & Application Vulnerabilities
5. Well-plan Web Application Development
6. Enforce Security Policy, Guideline & Procedure for Internal and Service Provider

What You Can Do #1: Enforce High Encryption Cipher

When an SSL handshake occurs between a client and server, a level of encryption is determined by the browser, the client computer operating system, and the SSL Certificate. Low-level encryption, 40 or 56 bits, is acceptable for sites with low-value information. However, a hacker with the time, tools, and motivation can crack the code in a matter of minutes.

Disable support for LOW encryption ciphers. High-level encryption, at 128 bits, can calculate 2^{88} times as many combinations as 40-bit encryption. That's over a trillion times a trillion times stronger. That same hacker with the same tools would require a trillion years to break into a session protected by an SGC-enabled certificate.

How to Improve:

It is highly recommended to install a unique certificate on each server to activate 128-bit or stronger encryption using an SGC-enabled SSL Certificate, such as VeriSign Global Secure ID (128-bit Compulsory). A unique certificate on each server helps reduce the risk of single point of private key compromise. An SGC-enabled certificate ensures that almost every site visitor, no matter what browser or operating system they use, will get connected at the highest encryption level.

Many millions of Internet users worldwide still use browsers that will not connect at 128-bit encryption unless there is an SGC-enabled certificate on the server. These browsers include certain Internet Explorer browser versions from 3.02 to 5.23, Netscape browser versions from 4.02 to 4.72. Browser versions prior to these are not capable of 128-bit encryption with any SSL Certificate. Even many Windows 2000 systems using Internet Explorer browser will fail to step up to 128 bits regardless of the version of Internet Explorer they're running

Subject to the browsers used, non-SGC SSL certificates in many cases encrypt at 40 or 56-bit strength while its CAs may claim to offer "128-bit certificates", but they do not offer 128-bit SSL encryption to the most possible site visitors.

Web sites accepting credit cards for on-line payment, handling personal privacy data or transmitting confidential information should offer 128-bit or stronger encryption protection to their site visitors.

What You Can Do #2: Manage Security Patch Updates

5 of the top 10 vulnerabilities are mainly the consequence of out-dated patching or users' negligence in following guideline. The following suggest how they can be addressed.

Vulnerability:

Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability - Solution for some of the common Web Servers are given below. For example:

Apache:	Recent Apache versions have a Rewrite module that allows HTTP requests to be rewritten or handled in a specific way.
---------	--

Microsoft IIS: Microsoft released URLScan, which can be used to screen all incoming requests based on customized rulesets. URLScan can be used to sanitize or disable the TRACE requests from the clients.

SunONE/iPlanet: SUN recommends to disable the trace method.

Vulnerability:

TCP Sequence Number Approximation Based Denial of Service – The Internet Engineering Task Force (IETF) has developed an Internet-Draft titled Transmission Control Protocol Security Consideration that addresses this issue. For example, BGP-specific workaround information has also been provided in the draft.

Vulnerability:

WebDAV HTTP Method 'PROPFIND' Enabled – To disable WebDAV, please refer to Microsoft article "How to Disable WebDAV for IIS 5.0" for complete information.

Vulnerability:

Netscape/OpenSSL Cipher Forcing Bug – The problem can be fixed by disabling one of the options (namely, SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG) from the options list of OpenSSL's libssl library

Vulnerability:

Microsoft IIS Internal IP Address/Internal Network Name Disclosure Vulnerability – Information about this vulnerability in Microsoft articles – Internet Information Server Returns IP Address in HTTP Header (Content-Location) and also Microsoft support hyperlinks.

No matter what platform is used, patch management policy should be developed in enterprise with a focus on reducing security vulnerabilities. It should not be a reactive procedure in response to incidents.

How to Improve:

Maintain a source of vulnerability information associated with each class of application and identify the staff primarily responsible for administering the application. A vulnerability alert list should be developed. Resources include:

1. Third-party vulnerability alert Web sites such as CERT Coordination Center (www.cert.org), and the SANS (System Administration, Networking, and Security) Institute (www.sans.org/sac)
2. Vendor Web sites such as Microsoft, HP and Sun
3. Vulnerabilities alert subscription service, charged or free.
4. Automated vulnerability scanning tools for regularly monitoring the risks of your systems.

How to Improve:

Additional support for managing vulnerabilities is available from vendors. For example, Microsoft has developed a variety of tools to scan, assess, and update their products. Sun Microsystems has developed the Patch Manager utility to scan Solaris 9 operating systems, identify vulnerabilities, and automatically download and install needed patches. However, care must be taken with all such tools, because side effects might result in other applications that interoperate with the newly patched application.

How to Improve:

Regular health check your server. Enterprises need to focus on vulnerability management because the problem exists before the patches are available.

- Vulnerabilities with Patch Available – Vendor are often under significant pressure to release patch as soon as possible. Before applying new patches to production environment, test should be conducted in a non-production environment to assess its effectiveness as well as side effects. As a low-cost alternative, some enterprises wait a few days to collect early adoptors' feedback and comments before installing patches.
- Vulnerabilities with NO Patch Available – Preventive measures include disabling certain services or functions, close monitoring to detect or thwart actual attacks via an intrusion detection and prevention system.

How to Improve:

Standardize client and server operating systems. Operating system standardization should be introduced as part of a timed refresh of the client installed base. This type of standardization also provides substantial benefits beyond the patch management process.

How to Improve:

Establish processes and benchmarks. Establish processes that will track patching effort and map results against company and industry benchmarks. Create straightforward, high level patching performance reports, distribute them widely, and show the patch management improvement through time.

How to Improve:

Consolidate hardware configurations. Reducing the number of hardware configurations from 50 to 25 can reduce the overall time to deploy patches and other minor updates by as much as 50 percent.

What You Can Do #3: Harden New Servers

One of the seriously unprofessional practices we found is that 90% of servers in Hong Kong are using default settings without hardening. Some of the vulnerabilities could be discovered and eliminated if server is hardened once it is setup. We would discuss it in a separate session.

What you can do better:

Establish administrative procedure or checklist for new server hardening. A server must not be connected to the Internet until it is secured by the following procedures:

1. Ensure that vendor supplied patches are acquired, systematically tested, and installed.
2. Remove unnecessary software, system service, and drivers.
3. Ensure security features are included in vendor-supplied system including, but not limited to, firewalls, virus scanning and malicious code protection, and other file protections.
4. Audit logging shall also be enabled. User privileges shall be set utilizing the least privileges concept of providing the minimum amount of access required to perform job functions. Privileges may be added according to the need demonstrated by the user. The use of passwords shall be enabled.
5. Disable or change the password of default accounts.
6. Scan for vulnerabilities
7. Implement best practices for securing their particular system platform(s).

What You Can Do #4: Regularly Scan for Network & Application Vulnerabilities

Vulnerability scanning gives enterprise a quick look of what is missing on their network and application. In this report, all the top 10 vulnerabilities are found by a single scan which costs almost nothing for enterprises. This is especially cost-effective to enterprises which have to upgrade or update their systems frequently in order to maintain their competence or service quality.

Most IT specialists are already familiar with network-layer vulnerability scanning while not so with application-layer scanning, it should be stressed that both types of vulnerability scanning are of equal importance to enterprises as effective security measures.

How to Improve:

To avoid web incidents, enterprise should first focus on **Web application level security**, and take regular web application health check because:

1. Web applications are usually **custom-made** and are not commercial application. Vulnerabilities in those applications may not be detected by "know vulnerabilities" checks by commodity security equipments or systems.
2. Web application are always **connected to important database**, like customer credit card number, transaction record, etc, which attracts most hacker interests and attentions.
3. Web applications are **publicly available** on the Internet, 24/7, not only for your enterprise customers, but also for hackers or unauthorized users.
4. According to a survey by the Garter Group, almost **three-fourths** of all Internet assaults are **targeted at Web applications**.
5. Such health check solidifies enterprise policies and procedures for **online compliance** and makes the online compliance process more efficient, sustainable. Well format report can be generated automatically.
6. As more and more web sites are adopting Web 2.0 technologies, XSS (Cross-Site Scripting) attacks which can't be detected by network-layer vulnerability scanning will proliferate.

How to Improve:

To eliminate configuration problems and identifies known vulnerabilities on the network level, taking regular health check on **network level** is essential because:

1. Most security breaches are targeting at known vulnerabilities for which there are existing countermeasures. Regular health check against known vulnerabilities **drastically lowers enterprise risk**.
2. Enterprises handling important data is required to take regular network security check in order to comply with a wide array of government and industry regulations, like SOX, PCI. Companies that do not fully **comply with security regulations** face serious consequences including heavy fines and legal action.
3. Ensuring the compatibility of configuration among enterprise security equipments maximizes their productivity on protecting the network, which help you gain **maximum ROI** from enterprise existing security infrastructure.

Enterprise should be fully aware of the importance of regular server scanning, patching, updating security features and signatures, and spyware checking.

What You Can Do #5: Well-plan Web Application Development

The concern of Web application security has been growing fast recently. Unlike network vulnerabilities where remediation is subject to the patch availability from vendors of those off-the-shelf products, fixing vulnerabilities found on home-grown or custom-built web application, however, is in large part enterprise's responsibility. As we can learn from some security incidents this year, Web application attacks like Google Hacking, Cross-Site Scripting are becoming more common in Hong Kong. By exploiting such vulnerabilities, hackers can access data on a Internet server without authorization or execute malicious codes planted in browsers on client side to intercept the victim's communication.

Many application and network vulnerabilities can be remedied by updating application or in some cases identifying poorly coded Web application, and scanning quarterly. The best approach, however, is to develop applications with security in mind.

How to Improve:

Updates your application. Ask the application vendors whether their current or older-version application store track data. Validate their statement yourself by testing the application or looking for third-party validation of the output and data stores.

How to Improve:

Identify poorly coded web application. Many data compromises occur because of improper coding, especially in Web applications. In fact in HiTRUST's experience, Web application vulnerabilities account for the largest percentage of compromise cases. Poor coding can result in weak password control or application that vulnerable to Cross-Site Scripting (XSS), SQL injection and other attack vectors. XSS attacks by taking advantage of a Web site vulnerability in which the site displays content that includes un-sanitized user-provided data. SQL injection attacks penetrate the network simply by using an Internet browser to execute code at the database layer of an application. This causes the database to hand over private information to hackers.

How to Improve:

To prevent cross-site scripting attacks from occurring, web developers should use static pages whenever possible and sanitize input/output. Have a third party conduct an application test and code review to ensure that your custom Web applications are securely coded. Improve internal software development lifecycle practices by integrating security into these cycles.

How to Improve:

Some companies may use automatic tools or managed service to scan their web application regularly. These convenient tools and service can, to some extent, provides an accurate picture over the network and application vulnerabilities with a small fraction of cost. The process may require assistance from an analyst, who can be prohibitively expensive when conducted in house. Some companies may choose to outsource this task to a qualified third party that can perform additional manual tests and analyze results for the company.

How to Improve:

A proper system development lifecycle process is part of a well-defined security program and involves well-defined phases: risk analysis; prototype design and building; testing; deployment; maintenance; and retirement. Ideally, security is applied at the analysis phase, and then built in and tested throughout the application's life. Avoid ad hoc development, implement replicable processes and document everything.

What You Can Do #6: Enforce Security Policy, Guideline & Procedure for Internal and Service Provider

A set of security policy, guideline and procedure are necessary for enterprises to follow as a standard to follow and should adequately reflect the risks and requirements aligned with enterprise business objective. If the policy is too strict it may hinder employee productivity and if it is too weak, it could open the enterprises to vulnerabilities and information loss or theft.

How to Improve: The security guideline (or as simple as a checklist) for application development, installation, configuration and testing should not be only followed by internal departments, but also the outsourced service provider who bare also take part in the above tasks.

Security policy, guideline, procedure should be well-communicated (or well-marketed) within your enterprise (especially for IT related departments) and outsourced service provider, with the following marketing 7 P approaches:

1. **(The Product Itself) Policy** – clearly developed your security policy. It is recommended to use a systematic approach by first considering the security interest of the organization or department as a whole. You can first identify the security requirements of your organization, and then establish your security policy followed by the ways to enforce. But periodic and continuous review and monitoring are definitely necessary in order to have an effective and efficient security policy.
2. **Price for Compliance with Policy** – the effort people need to pay. Certainly please emphasize value that people gain from following the policy would do them benefits, like reducing the risk and saving resources to recover in case of incidents
3. **Promotion** – communicate clear with relevant parties regarding the policy details. Make sure they understand the necessities of policy compliance and the value brought to their work and enterprise. Regular E-mail, File sharing on Intranet and training would be required
4. **Place or Distribution** – Security department figuring out the policy should communicate directly with different relevant parties, to make sure the communication is more effectively and information is correct.
5. **Physical Evidence** – Promote the security like an internal campaign. Visual reminder like, posters, internal email header, Intranet calendar, etc. can be a good way to “promote” the policy.
6. **People** – It is recommended to have top management from enterprise to endorse the policy, making the policy even more convincing
7. **Process and Control** – assist each relevant party to implement the policy. And define with outsourced vendors on the penalty for being not compliance with the policy. Policy will be review regularly to match the changing business environment and objective.

Final words

This report summarizes the study conducted by HiTRUST on the common web vulnerabilities found in Hong Kong. Recommendations to the vulnerabilities including best practices are given in the hope that could benefit readers.

The result shows that more than 70% of the servers surveyed still adopt low or insecure encryption, which coincides with the result of a study called "Hong Kong E-Commerce Security 2003", conducted by PISA (Professional Information Security Association) in 2003.

It said, "Although most of our sample web sites supported high grade encryption and secure SSL version, the study found that some still support low grade encryption and less secure SSL version. As SSL allows "no encryption but MAC only" mode, one of the questions is to find out if any web site supports this insecure mode. The study found that the answer of this question was YES". It is a strong indication of the inappropriate deployment of SSL. The study was primarily focused on network layer, not application layer. HiTRUST wishes to conduct another study regarding web application security in the near future.