Guidelines for Website Security and Security Counter Measures for e-Governance Project

Mr. Lalthlamuana
PIO, DoICT

Background (1/8)

Nature of Cyber Space

- Proliferation of Information Technology
- Rapid Growth in Internet
- Increasing Online Transactions
- Information Systems are essential part of critical infrastructure

Background (2/8)

Security of Cyber Space - Risks

- Internet Systems vulnerable target for attack
  - Systems not securely configured
- In recent years the attack techniques have become sophisticated
- Rapid proliferation of viruses and worms

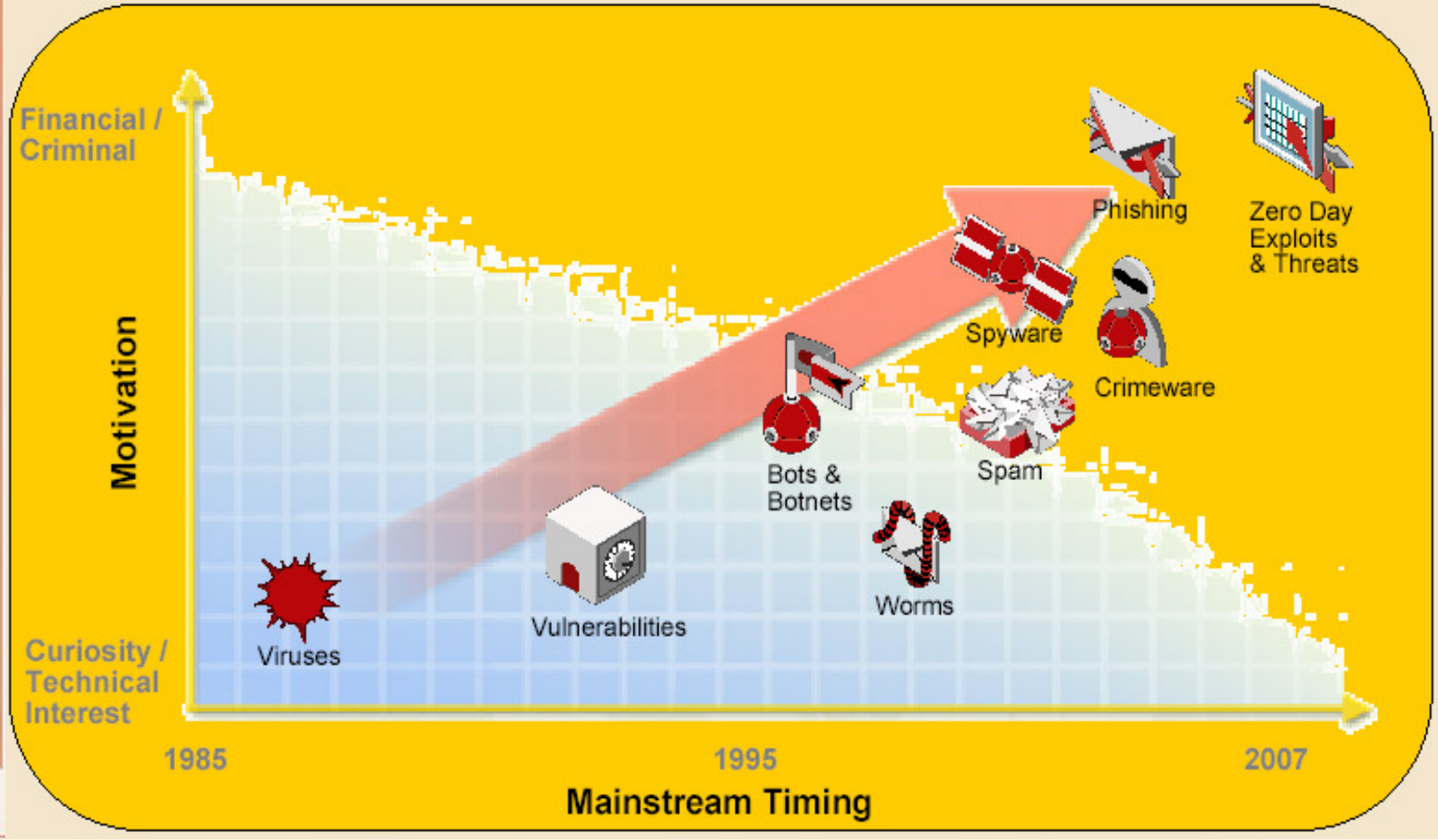
Background (3/8)

Security of Cyber Space - Risks

- Critical infrastructures such as telecommunications, transportation, energy and finance can get affected by attacks on Information infrastructures
- Attackers not confined to geographical boundaries

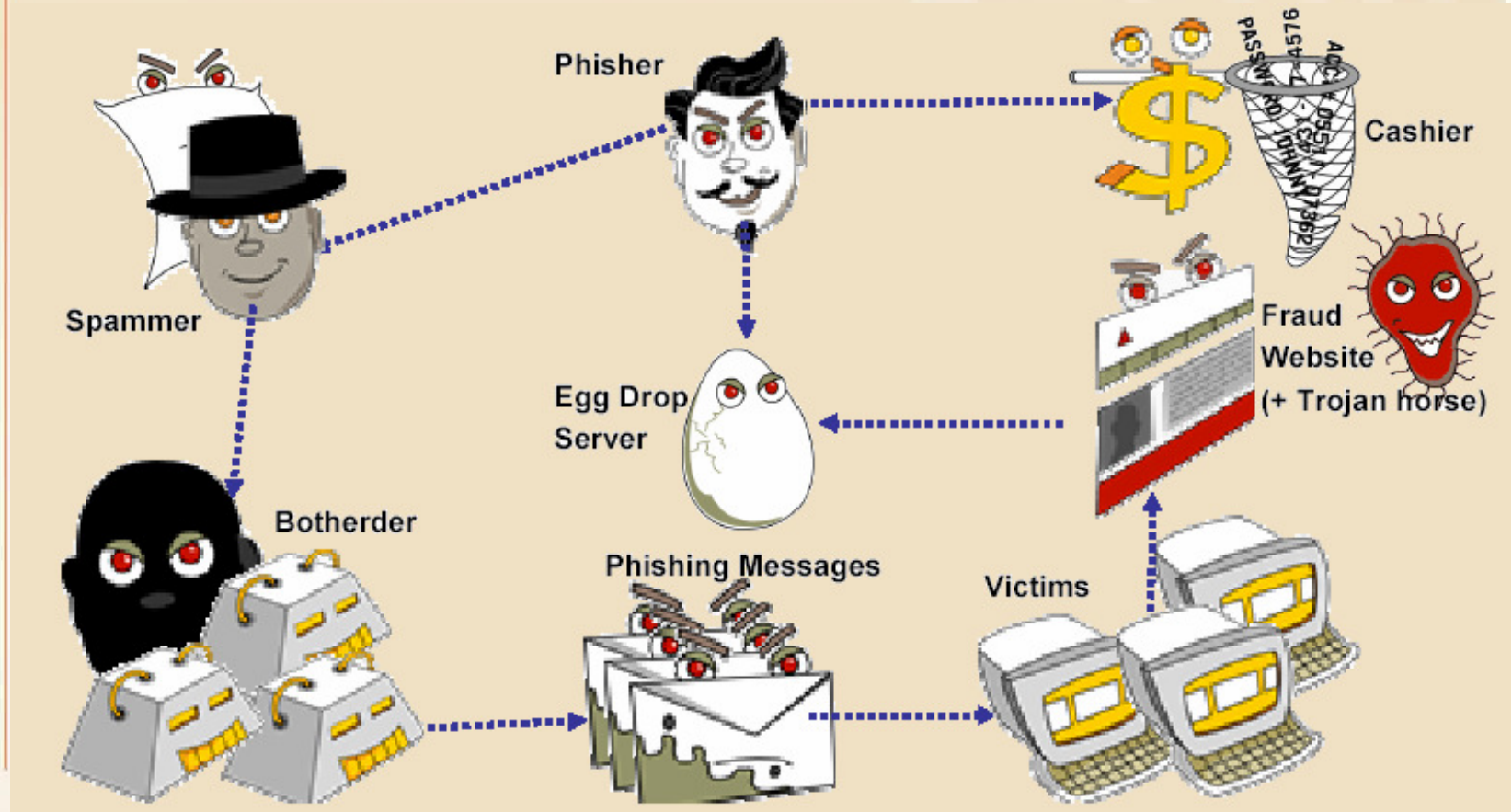
Background (4/8)

Threats are Evolving



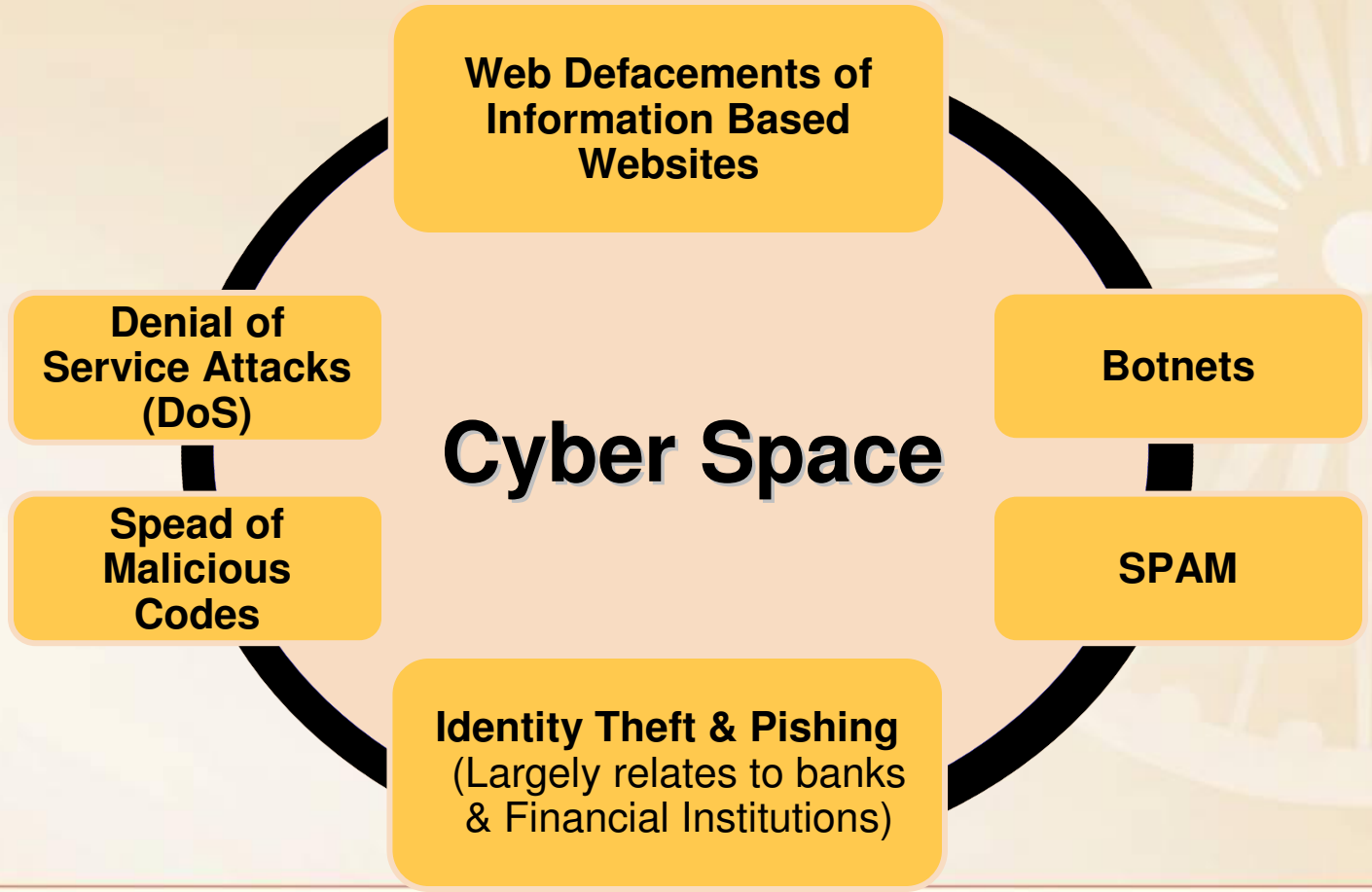
Background (5/8)

The Fraud Food Chains



Background (6/8)

Nature of Cyber Security Breaches



Background (7/8)

Effects of an Attack

- Unauthorized use/misuse of computing systems, defacement of websites
- Loss/alteration/compromise of data or software
- Monetary/financial loss
- Loss or endangerment of human life
- Loss of trust in computer/network system
- Loss of public confidence

Background (8/8)

Security Incidents	2004	2005	2006	2007	2008
Phishing	3	101	339	392	604
Network Scanning / Probing	11	40	177	223	265
Virus / Malicious Code	5	95	19	358	408
Spam	-	-	-	-	305
Website Compromise & Malware Propagation	-	-	-	-	835
Denial of Service	-	-	-	-	54
Others	4	18	17	264	94
Total	**23**	**254**	**552**	**1237**	**2565**

Table 2. Year-wise summary of Security Incidents handled

Source: CERT-IN

Guidelines for Website Security

A Web Server is a Computer host configured and connected to Internet, for serving web pages on request. Information on Public web servers can be accessed by people anywhere on the Internet.

Introduction (1/4)

Common Security Threats

- Unauthorized access
  - Defacement
  - Content Theft
  - Data Manipulation
- Improper usage
  - Launch pad for external attacks
  - Hosting improper/ malicious contents (e.g. Pishing)
- Denial of Service (DoS)
- Physical Threats

Introduction (2/4)

Common Security Flaws

- Insufficient network boundary security controls
- Flaws or bugs in web hosting software (OS, Application, etc.)
- Insecure design and coding of hosted application
- Weak password
- Social engineering
- Lack of operational control

Introduction (3/4)

Common Hacking/ Attack Methods

- CERT-In: Hacking – How they do it?
  http://www.cert-in.org.in/advisory/CIAD200303.pdf

Introduction (4/4)

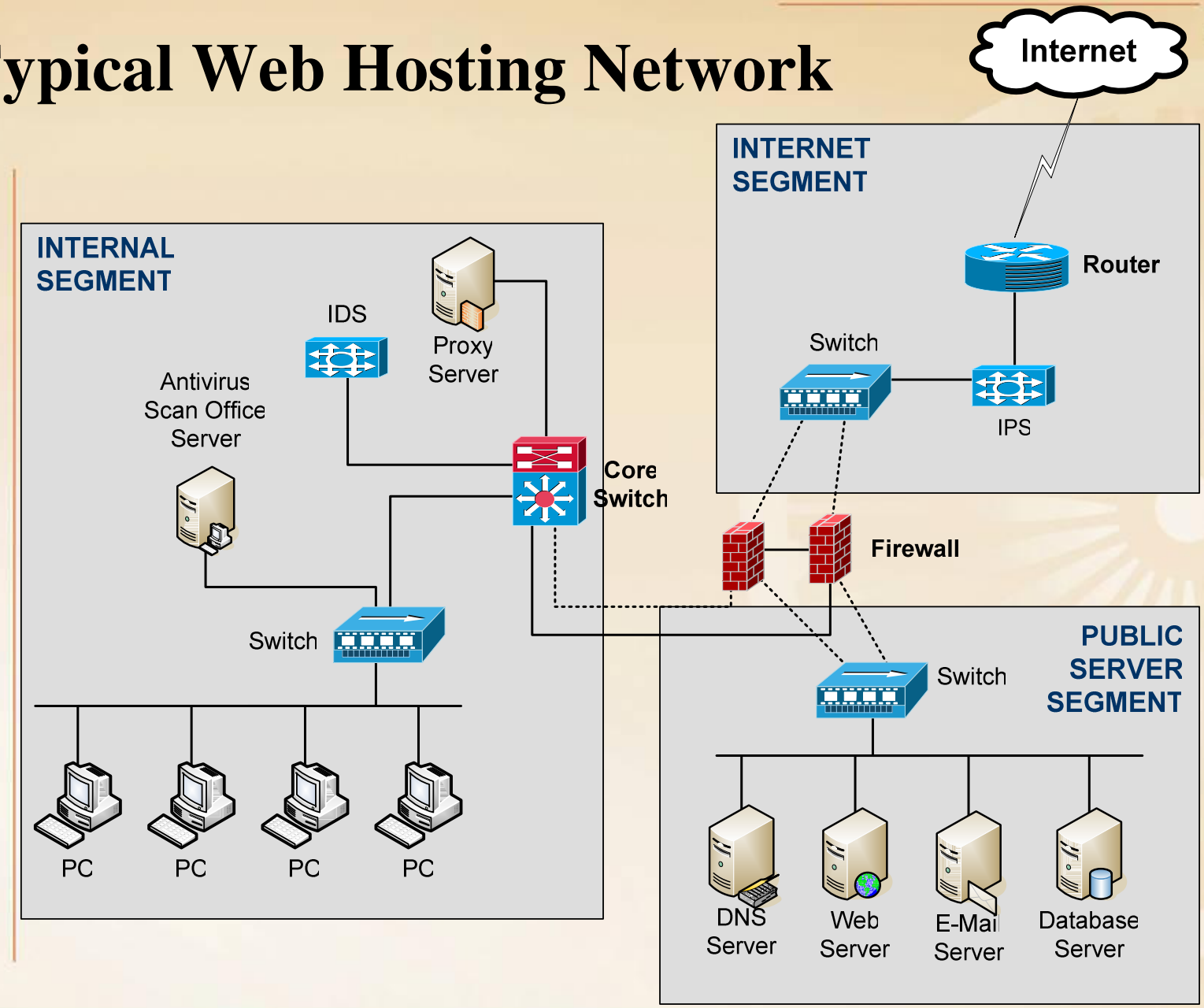
Defense in Depth

- Perimeter/Network Defense
  - Packet filtering, State-full inspection, IDS
- Host Defense:
  - Server Hardening, host IDS
- Application/Database Defense:
  - IIS/Apache security, antivirus, secure coding practice

Network Security

- Web Hosting Network
  - Internet Segment (External Zone)
  - Public Server Segment (DMZ Zone)
  - Internal Segment (Internal Network)
- Guidelines
  - CERT-In: Network Perimeter Security
    http://cert-in.org.in/presentation/perimeterSecurity.pdf
  - NIST: A guide for selecting Network Security Products
    http://nist.gov.in/publications/nistpubs/800-36/NIST-SP800-36.pdf

Typical Web Hosting Network



Host Security

- Considered the following
  - Selection of OS of Web Server (Windows or Linux)
  - Remove all services which is not required
  - Update OS & Application Software regularly with latest service pack and patches
  - A strong Password policy should be enforced
  - Enable detailed logging including failed logging
- Guidelines
  - Microsoft: Windows Server 2003 Security Center http://microsoft.com/technet/security/prodtech/win2003/default.mspx
  - CERT-In: Securing Red Hat Linux 9.0 as a Web Server http://cert-in.org.in/guidelines/CISG-2004-01.pdf

Web Server Security

- Considered the following
  - Remove all files that are not part of the Web site
  - Third-party free modules available should not be used without proper checking and verification of their functionality and security.
  - Configure the web server to use authentication & encryption technologies (SSL)
  - etc.
- Guidelines
  - Apache: Apache Security Guideline http://httpd.apache.org/docs/misc/security_tips.html
  - CERT-In: Web server security guideline http://cert-in.org.in/guidelines/CISG200304.pdf

Secure Coding Practices

- Considered the following:
  - Consider security implications before selecting the scripting language viz Java applets, javascripts, vbscript, PHP, etc.
  - Common security to be considered are SQL Injection, Cross Site Scripting and Information Leakage
- Guidelines
  - Open Web Application Security Project: A guide to building secure web applications http://www.owasp.org/documentation/guide
  - MSDN: Design Guideline for secure web applications http://msdn.microsoft.com/library/default.asp

Database Security

- Consider the following
  - Stay updated with latest Service Packs and Patches
  - Remove unnecessary services and protocols
  - Secure the Database server behind a firewall and use IDS/IPS to detect any intrusion attempts.
- Guidelines
  - Microsoft: SQL Server Security Centre http://microsoft.com/technet/security/prodtech/dbsql/default.mspx
  - CISecurity: Oracle Security Testing tools and guide http://www.cisecurity.com

Content Management

- Use of remote authoring tools for editing content directly on public Web site is not recommended
- If remote administration is required, configure computers for remote admin through a secure channel
- Configure web content uploading through secure communications channel e.g. SSH
- Content uploaded on the web server should be verified to ensure that it is free of any malicious content.

Logging and Backup

- Logging
  - Use a centralized Syslog server
  - Establish different log file names for different virtual Web sites
  - Ensure log files are regularly archived, secured and analyzed
- Backup
  - Ensure regular backup of files
  - Maintain latest copy of Web site content on a secure host or on media
- Guidelines:
  - CERT-In: Implementing Central Logging Server using syslog http://www.cert-in.org.in/syslog.htm

Physical Security

- Considered the following
  - Natural Calamity Threats
  - Physical Access Controls
  - Electromagnetic Shielding
  - Disaster Recovery Centre

Security Audit/Penetration Testing

- Available tools
  - CISecurity: www.cisecurity.com
  - Microsoft Windows best practice analyser
  - Web applications stress testing http://wpoison.soundforge.net/
  - Vulnerability scanners i.e Retine and shadow security scanner. In Open Source, Nessus and nikto
- Reference:
  - CERT-In: http://www.cert-in.org.in/securitytools.htm

Security Policy

- The Web Server Security Policy should incorporate -
  - Network and Host Security Policy
  - Web Server Backup and Logging Policy
  - Web Server Administration and updation Policy
  - Classification of documents to be published on Web Server
  - Password management policy
  - Encryption policy
  - Physical security
- Guidelines
  - NIST: Guide for Developing security plans for IT http://csrc.nist/gov/publications/nistpubs/800-18/planguide.pdf

Incident Handling and Recovery

- A Computer Security Incident Response Team (CSIRT) should be created within the organization to handle incidents through the following six stages of incident handling.
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Follow-up

Third Party Hosting

- In selecting a thrid party hosting, a user should keep the following:
  - Hosting Servers should be located in India
  - Hosting organization should have its infrastructure and Web server audited by auditors empanelled by CERT-In.
  - Hosting organization should also have their Web server tested by A&P testing experts periodically.

Web Server Security Thumb Rules

- Web Administrators should be adequately skilled
- Use software only from trusted source
- Keep all software updated
- IS security audit and A&P test should be carried out regularly
- A dedicated machine should be used as a web server
- Changes to configuration should be documented (Revision control program)
- Central Syslog server should be used
- Encryption should be used

THANK YOU…