Cyber Security Threats : An Overview

Dimple Arora

2-Mar-2012

Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
New Delhi

Cyber Security Threats : An Overview

- **Agenda**
  - **Current trends in cyber threats**
  - **Network Vulnerabilities**
  - **Types & methods of intrusions**

Network & Security

- **Computer Network** is an interconnected group of computing nodes, which use a well-defined, mutually agreed set of rules and conventions known as protocol, interact with each other meaningfully, and allow resource sharing preferably in a predictable and controlled manner.
- **Network Security** is the need to protect one or more aspects of network's operation and permitted use. Security requirements may be Local or Global in their scope, depending upon the network's or internetwork's purpose of design and deployment.

Threat

An event, the occurrence of which could have an undesirable impact on the well-being of an asset.

[ISC2]

International Information Systems Security Certification Consortium

Any circumstances or event that has the potential to cause harm to a system or network .That means, that even the existence of a(n unknown) vulnerability implies a threat by definition.

[CERT]

Vulnerability

- A feature or bug in a system or program which enables an attacker to bypass security measures
- An aspect of a system or network that leaves it open to attack
- Absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both

Vulnerability trends

- More than 90% of vulnerabilities disclosed are in Application software.
- Exploitation of zero-day vulnerabilities by focused cyber criminals even after release of patches .
- Fewer vulnerabilities are exploited for longer periods
- Exploitation of client side vulnerabilities is mostly automated.

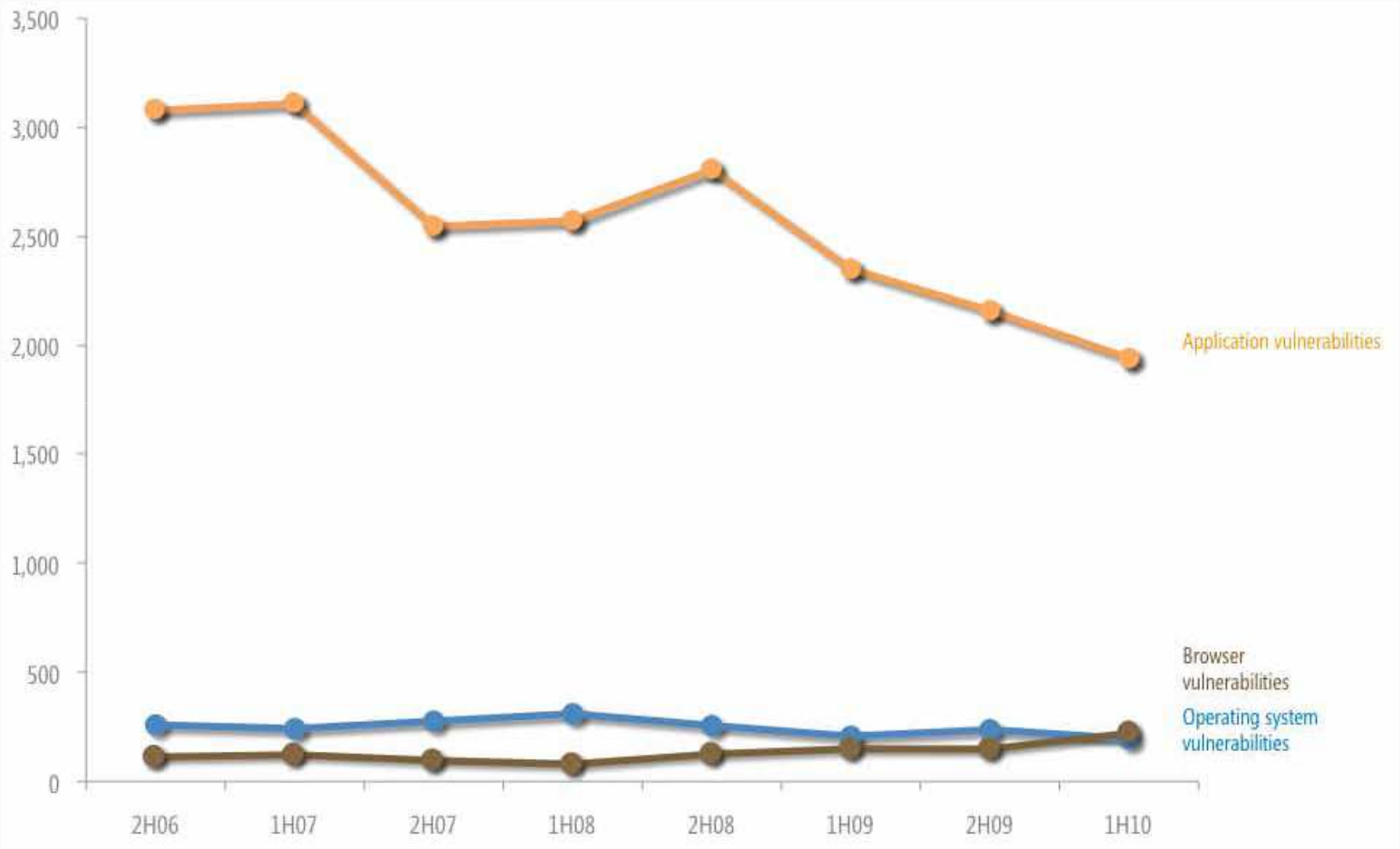
Intrusion Methods

1. ***Targeting hardware and security system***: This method assumes the would-be intruder knows some information about the hardware and security methods used in the facility he's attacking.
2. ***Exploitation of known weaknesses***: Software bugs are being brought attention quite frequently. Unfortunately sometimes, fixes for these bugs are not made available soon enough. This leads to exploits of these vulnerabilities.
3. ***Brute force attacks***: In this method, the attacker attempts to break a system by trying to guess its security codes, such as attempting to guess the root password by trying possible combinations of characters.

Intrusion Detection

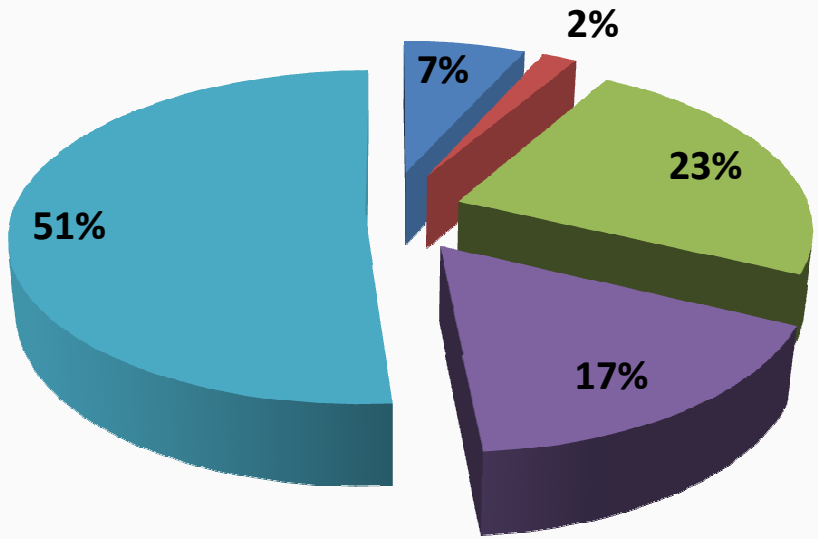
- Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network.
- An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system. Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system's resources.
- The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts.

Vulnerability Disclosure



Source: Microsoft SIR Vol.9

Incidents reported to CERT-In in 2011



- Phishing
- Network Scanning / Probing
- Virus/Malicious Code
- Others
- Website Compromise and Malware Propagation

Sources of Vulnerabilities

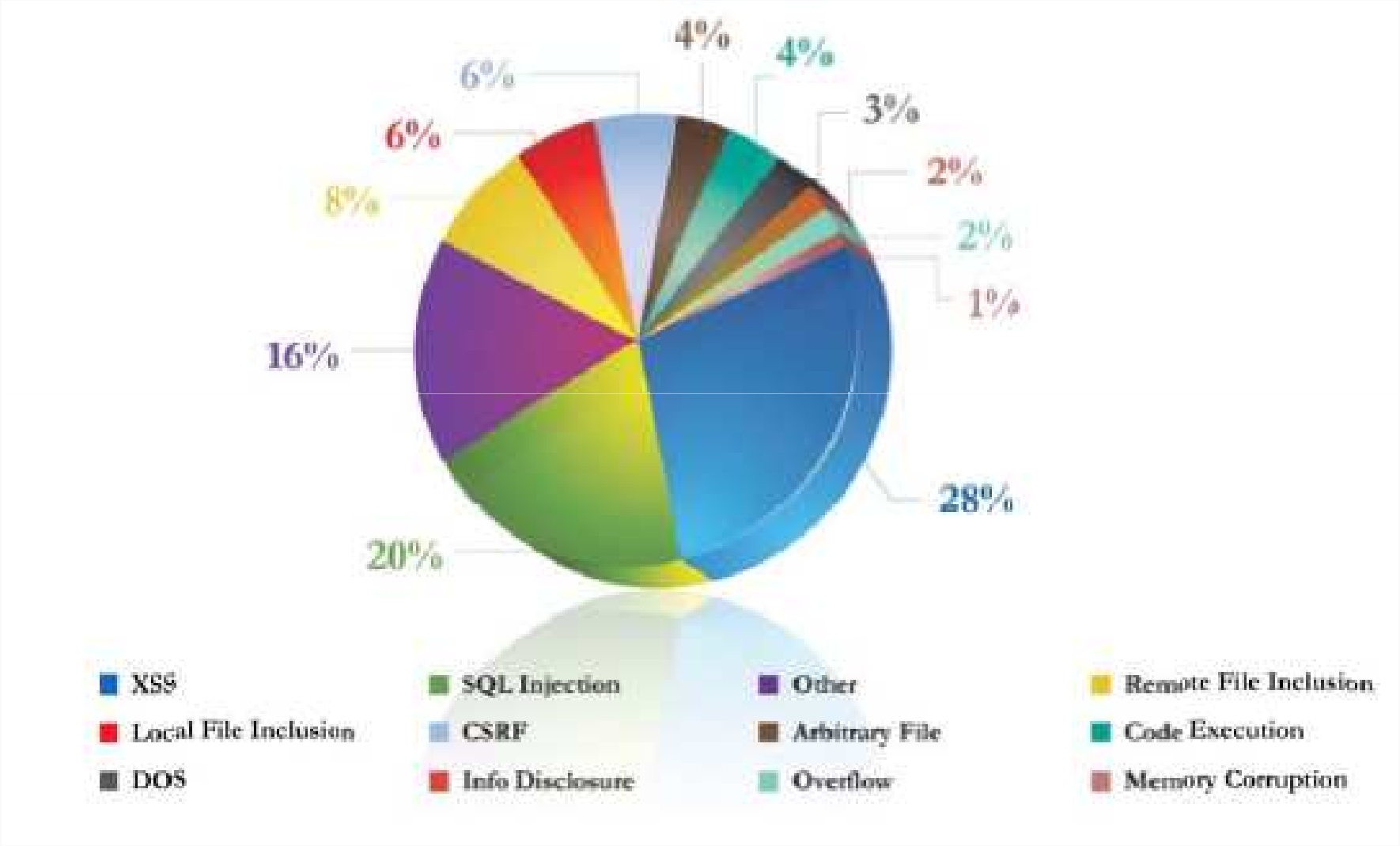
- There is no definitive list of all possible sources of these system vulnerabilities

- Among the most frequently mentioned sources of security vulnerability problems in computer networks are
  - design flaws,
  - poor security management,
  - incorrect implementation,
  - Internet technology vulnerability,
  - the nature of intruder activity,
  - the difficulty of fixing vulnerable systems,
  - the limits of effectiveness of reactive solutions,
  - social engineering

Cyber threats

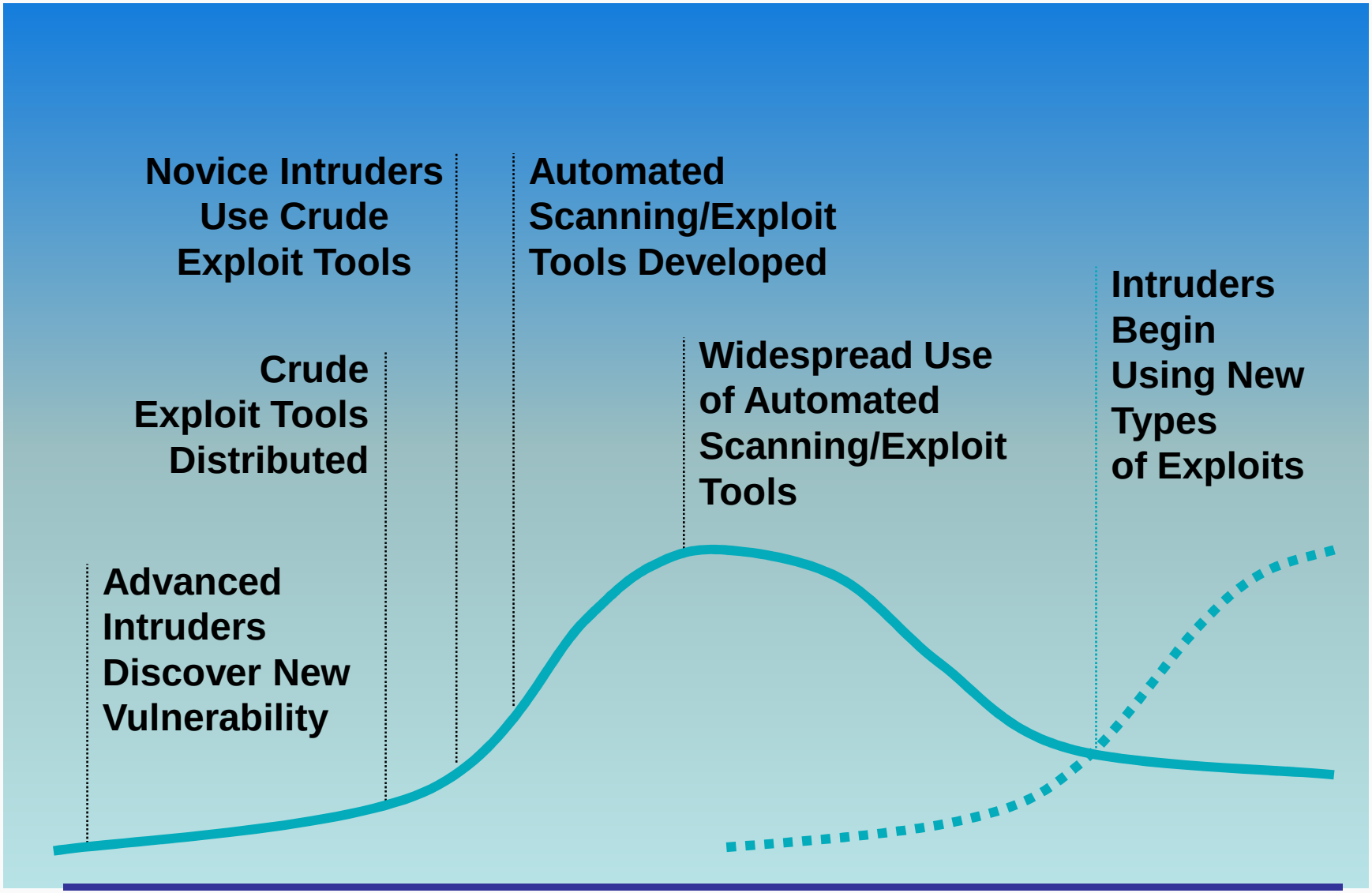
Threat Sources	Attacker Motives/Goals	Attack Methods
• Employees • Malicious • Ignorant • Non-Employees • Outside attackers • Natural Disaster	• Deny Services • Steal Information • Alter Information • Damage Information • Delete Information • Make a joke • Show off	• Social Engineering • Virus, Trojan Horses, worms • Packet replay • Packet modification • IP Spoofing • Mail bombing • Various hacking tools • Password cracking

Application Vulnerabilities

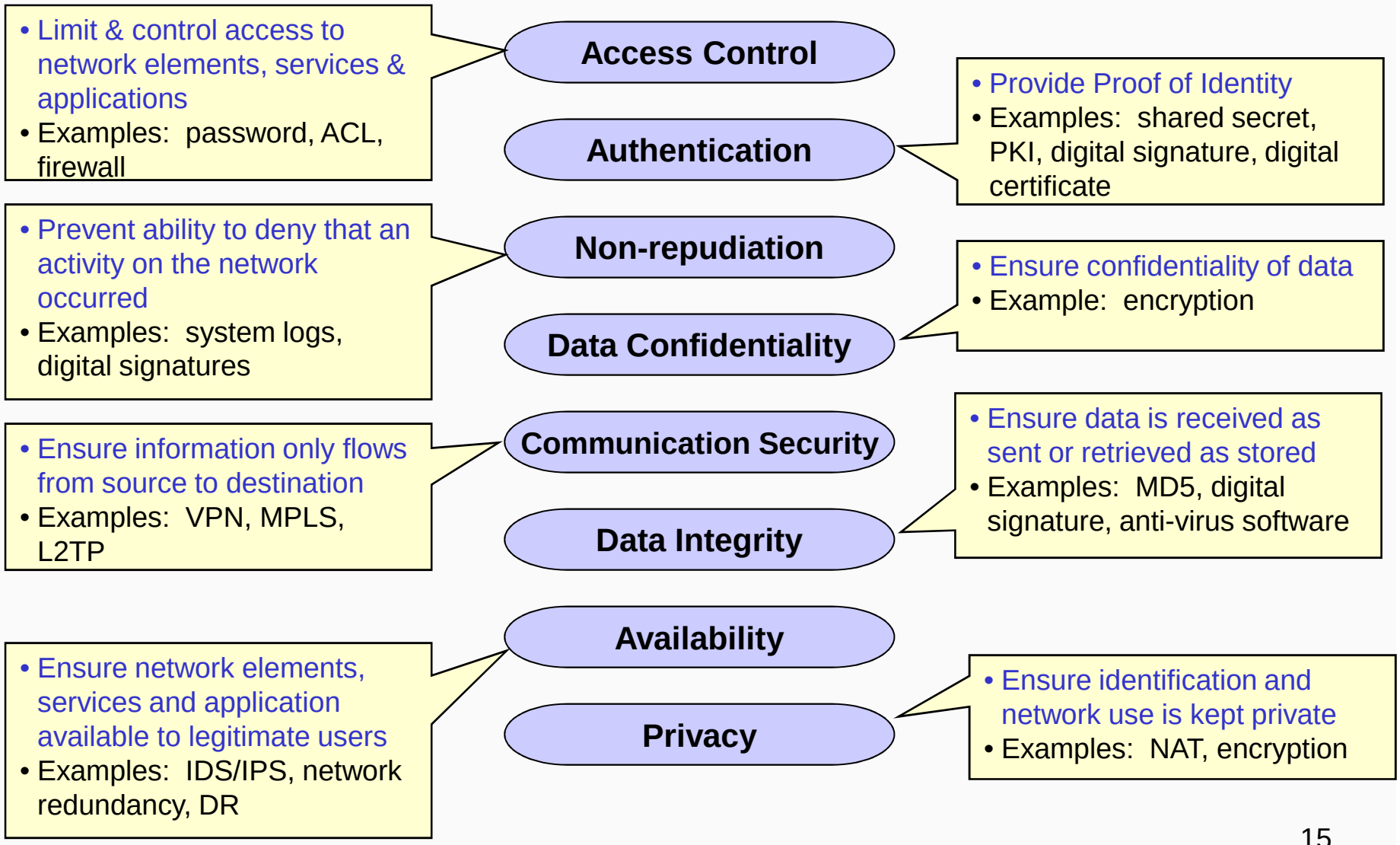


Source: Cenzic – Web app. Sec. Report 2010

Vulnerability Exploit Cycle

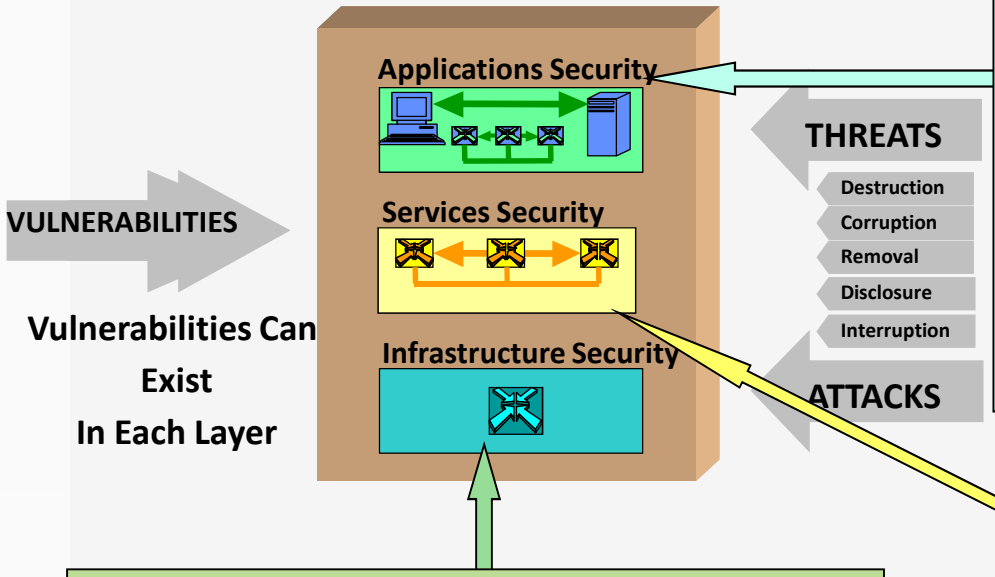


Eight Security Dimensions to Address the Network Vulnerabilities



Eight Security Dimensions applied to each Security Perspective (layer and plane)

Three Security Layers



3 - Applications Security Layer:

- Network-based applications accessed by end-users
- Examples:
  - Web browsing
  - Directory assistance
  - Email
  - E-commerce

2 - Services Security Layer:

- Services Provided to End-Users
- Examples:
  - Frame Relay, ATM, IP
  - Cellular, Wi-Fi,
  - VoIP, QoS, IM, Location services
  - Toll free call services

1 - Infrastructure Security Layer:

- Fundamental building blocks of networks services and applications
- Examples:
  - Individual routers, switches, servers
  - Point-to-point WAN links
  - Ethernet links

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

Cyber Security Incidents

National level

- Cyber Terrorism
- Attacks on Critical Infrastructure
- Web defacement
- Website intrusion and malware propagation
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service

Organisational level

- Website intrusion/ defacement
- Domain stalking
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Targeted attacks
- Phishing
- Data theft
- Insider threats
- Financial frauds

Individual level

- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Laptop theft

OWASP Top 10 Security Vulnerabilities

1. Cross Site Scripting (XSS)
2. Injection Flaws
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access

Organisational actions

- Security policies and procedures
- CSIRT/CISO/Administrator/Users
- Multi-layered defense mechanism
  - Network behavior analysis
  - Proxy logs
  - Perimeter Defense (IPS, DMZ, Firewalls)
  - Security Information and Event Management
  - Database Activity Monitoring
- Updated/Patched applications
- Host based Intrusion Prevention System
- Content inspection systems at perimeter
- Pre defined procedures for information sharing
- Authentication of emails (Digital signatures)
- User awareness

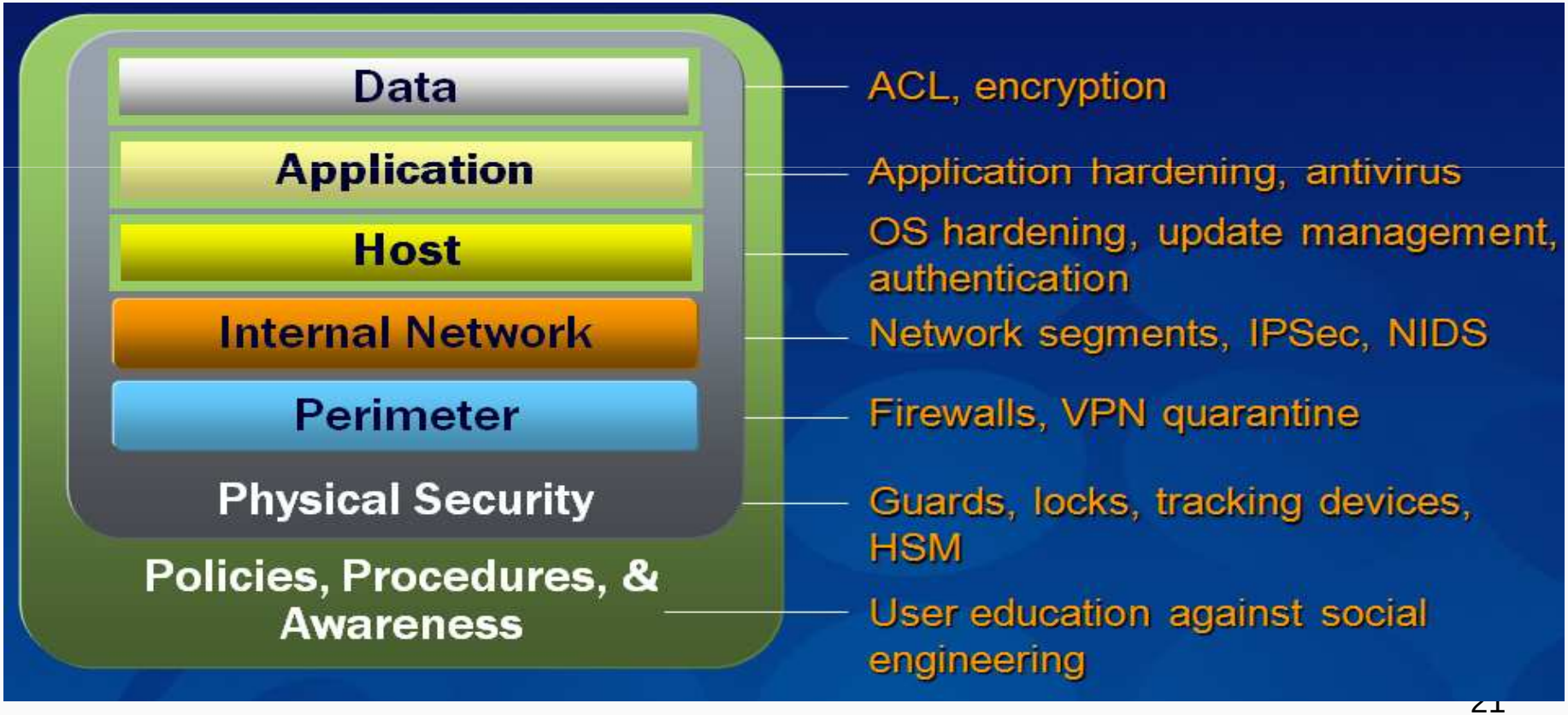
Actions for users

- Awareness! Awareness! Awareness!
- Install and enable :
  - Personal firewall
  - Anti-spyware
  - Anti-phishing controls
- Keep up-to-date patches and fixes on the operating system and application software
- Enable/Install anti phishing toolbars such as “Phishing Filter”, “Web Forgery” etc.
- Use latest Internet Browsers having capability to detect phishing/malicious sites.
- Exercise caution while opening unsolicited emails and do not click on a link embedded within
- Only open email attachments from trusted parties
- Practice limited account privilege.
- Report suspicious emails/system activities to Admin/CISO/CERT-In

Building secure environment

Defense in Depth:

- Using a layered Approach
  - Increases an attacker's risk of detection
  - Decreases an attacker's chances of success



Major Network Security Equipment

- Routers & Managed Switches
- Link Load Balancer
- Firewall (Universal Threat Management)
- VPN
- Intrusion Prevention System
- Antivirus and Antimalware Solution
- Antispam and email Security
- Web Security
- Filters
- Log Management & Analysis
- Network Access Control
- Management System
- Patch Management
- Backup Solutions
- Endpoint Security

darora@cert-in.org.in