Cyber Crime and Internet Security

शिवकुमार G. Sivakumar சிவகுமார்

Computer Science and Engineering
भारतीय प्रौद्योगिकी संस्थान मुंबई (IIT Bombay)
siva@iitb.ac.in

October 26, 2012

- The Good (Web 1.0, 2.0, 3.0)
- The Bad (Vulnerabilities, Attacks)
- The Ugly? (Defence, Offence, Forensics)

Theme/Scope of Talk

- ``Can't live with them, can't live without them!''
- Know Your Enemy (threats/Vulnerabilities)
  Can cyber/internet crimes cause events like the following?
  - July 2006 Mumbai rains
  - 26/11 attack on Mumbai
  - Gulf of Mexico oil spill
  - Mangalore air crash
  - Stop all Mumbai local trains
  - Damage BARC nuclear reactor
  - Disrupt all Mumbai mobile phones? (Prof. Jhunjhunwala's example)
- How to protect Critical National Infrastructure?
  - Passive Defence
  - Counter Intelligence (Technical side)
- Demo from atlas.arbor.net and cert-in.org.in

Your questions/suggestions *now* will be invaluable!

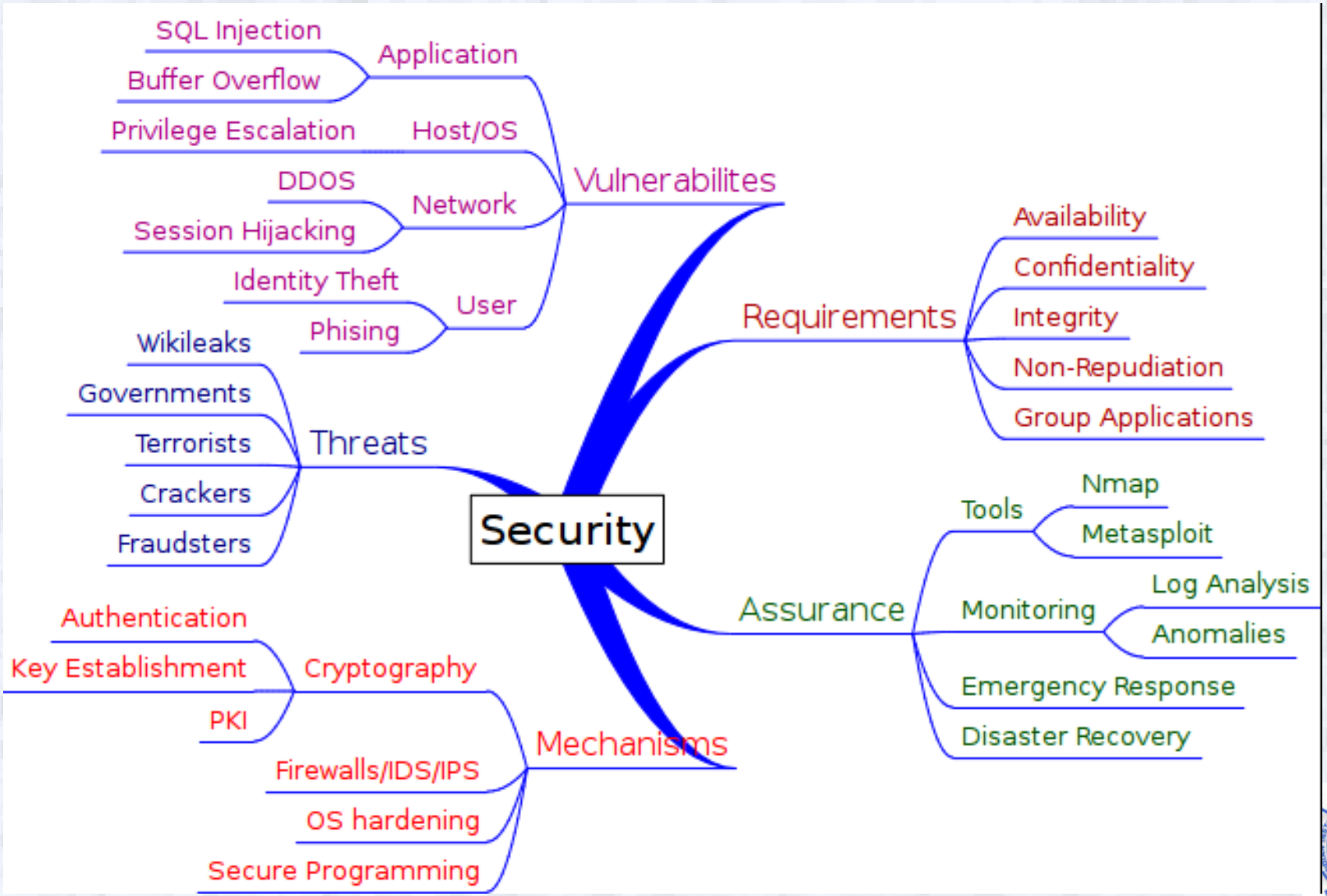
Security Concerns

Match the following!

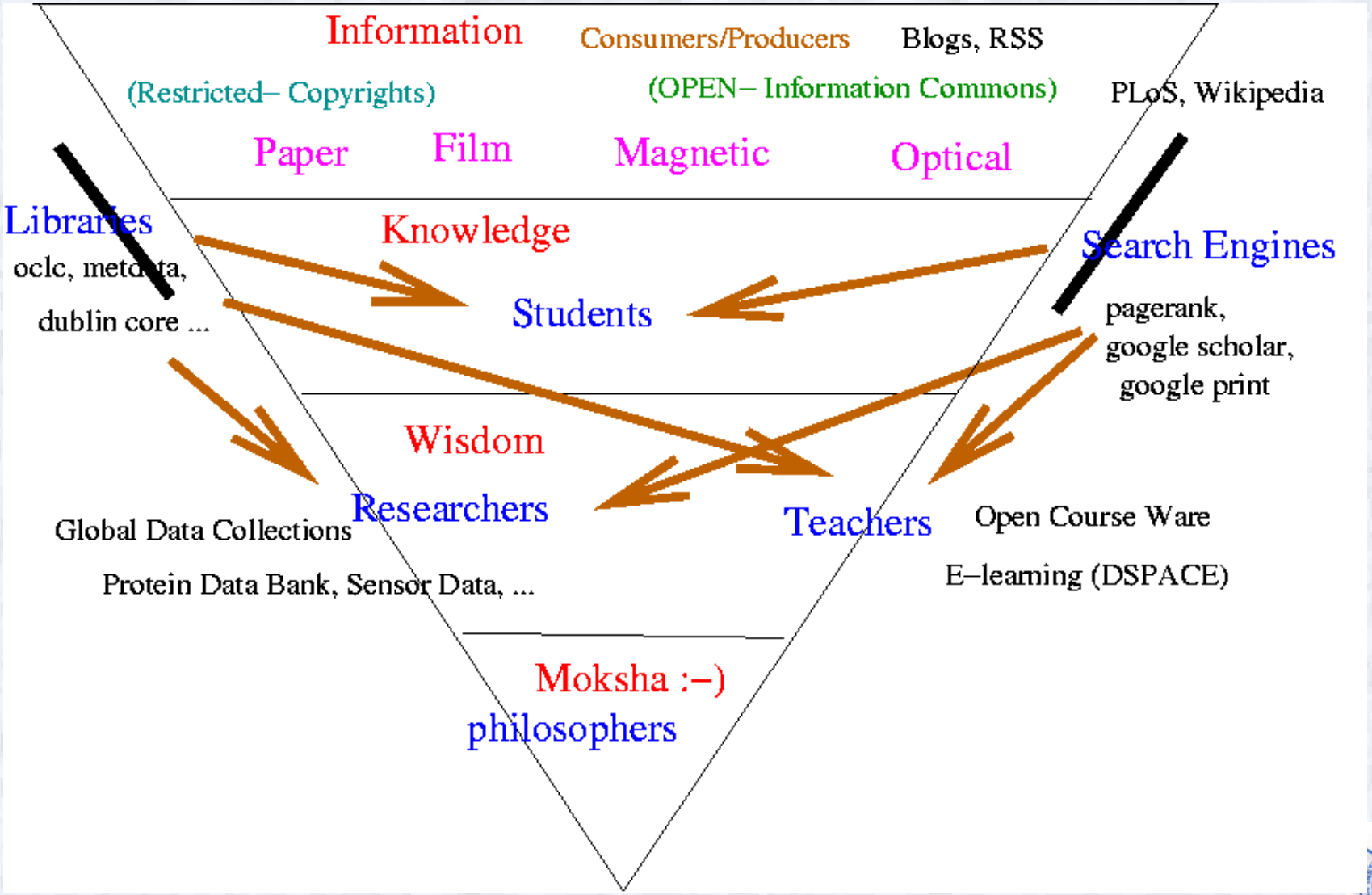
Problems	Attackers
Highly contagious viruses	Unintended blunders
Defacing web pages	Disgruntled employees or customers
Credit card number theft	Organized crime
On-line scams	Foreign espionage agents
Intellectual property theft	Hackers driven by technical challeng
Wiping out data	Petty criminals
Denial of service	Organized terror groups
Spam E-mails	Information warfare
Reading private files	...
Surveillance	...

- Crackers vs. Hackers
- Note how much resources available to attackers.

Partial Landscape

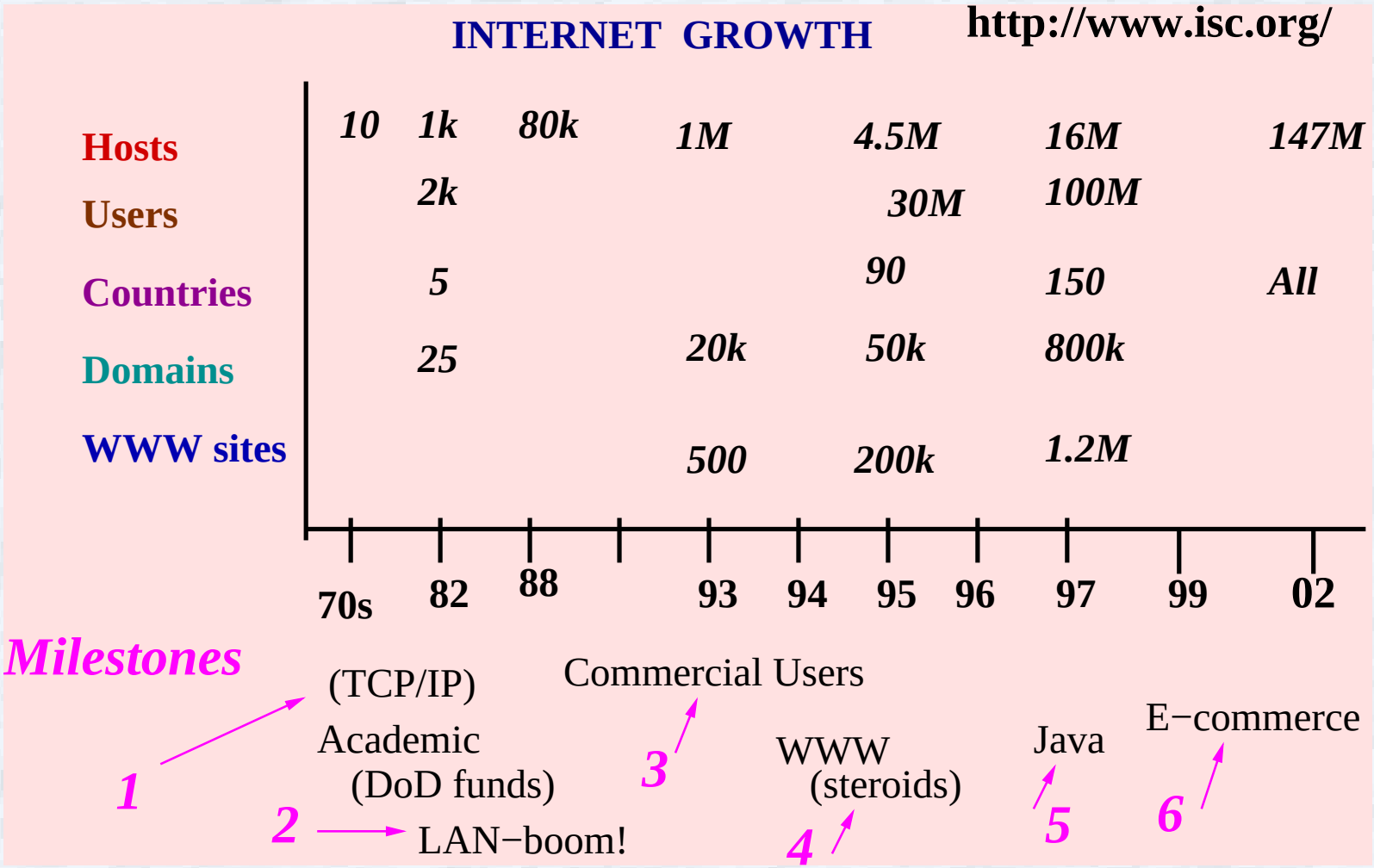


The Good side first!



How is learning affected?

Internet's Growth and Charter



Information **AnyTime, AnyWhere, AnyForm, AnyDevice, ... WebTone** like DialTone

Search Engines and Page Rank

- How to drink water from a firehose?
- Search Engines (google) *crawl* the web for us.
- Recall (all available?) and Precision (all relevant?)
- How to rank the pages? (syntactic?)
- Reliability/Trust/Security issues

What do profs do?

Visit *www.phdcomics.com* to find out!

Web 2.0 Definition (O'Reilly)

Web 2.0

Web 2.0 is the network as platform, spanning all connected devices; delivering software as a *continually-updated service* that *gets better the more people use it*, consuming and remixing *data from multiple sources,* including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an *architecture of participation,* and going beyond the page metaphor of Web 1.0 to deliver rich user experiences.

Examples

RSS/Blogs/FeedReaders, Slashdot/Digg, Wikipedia (printing press: people can read, Web2.0: people can write!)
Mashups- ingeniously combining web services e.g. Google Maps in other applications e.g. Mumbai Navigator

Semantics and Intelligence (Web 3.0)

Collaboration is necessary, but is it sufficient?
Want to know

- When cheap Mumbai-Chennai round trips are available
  - with package tours to Mahabalipuram, if possible
  - but not on weekdays
  - ...
- Whenever new articles on chess appear
  - only in English, Tamil or German
  - but other langauges ok if it is about V. Anand!
  - but not written by ...
  - ...

Two *margas* for moksha

- Monkey way is Web 1.0/2.0 (syntactic web)
- Cat way is Web 3.0 (sematic web)

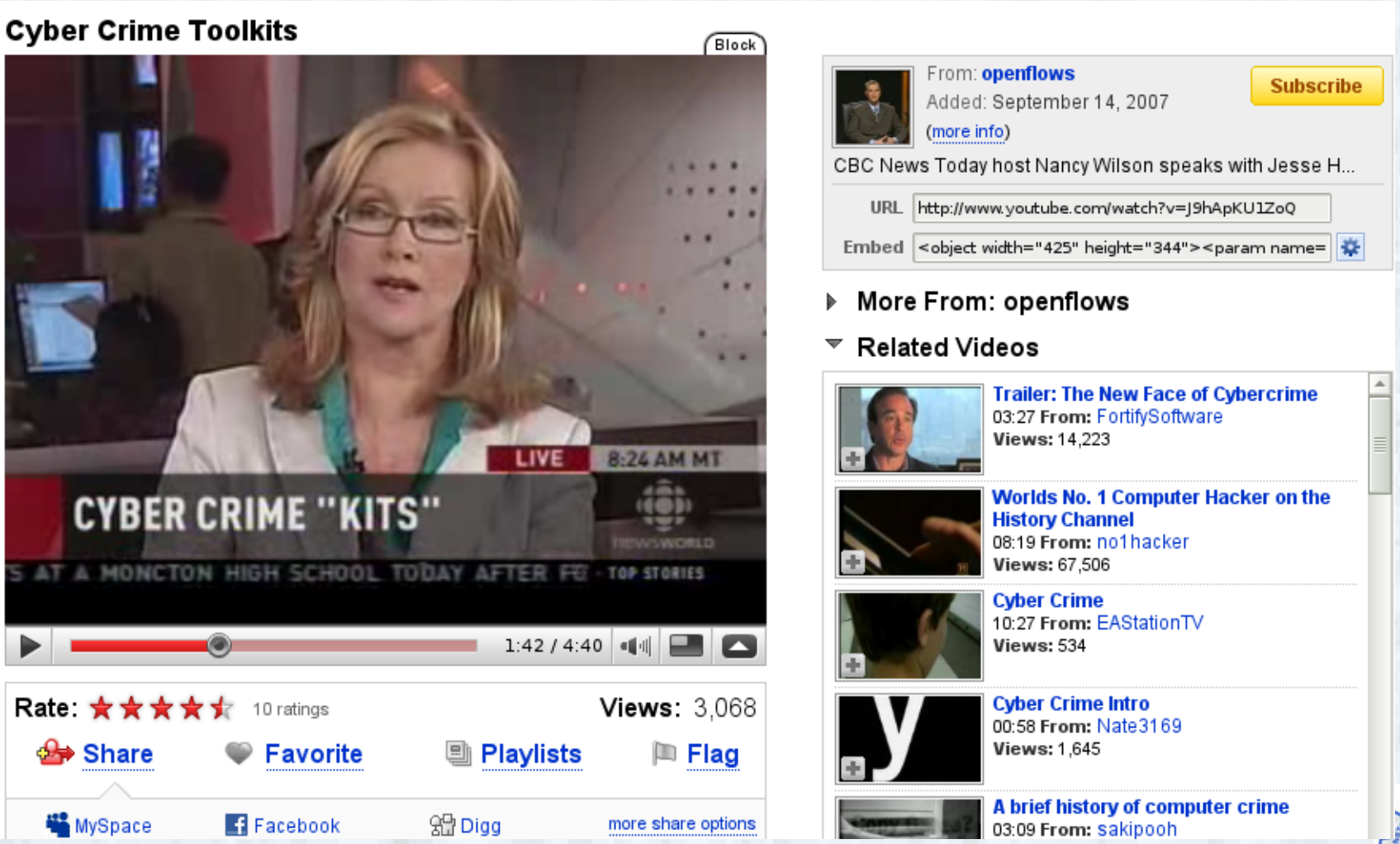
What are Cyber crimes?

Cybercrime

Activity in which computers or networks are a tool, a target, or a place of criminal activity. (Categories not exclusive).

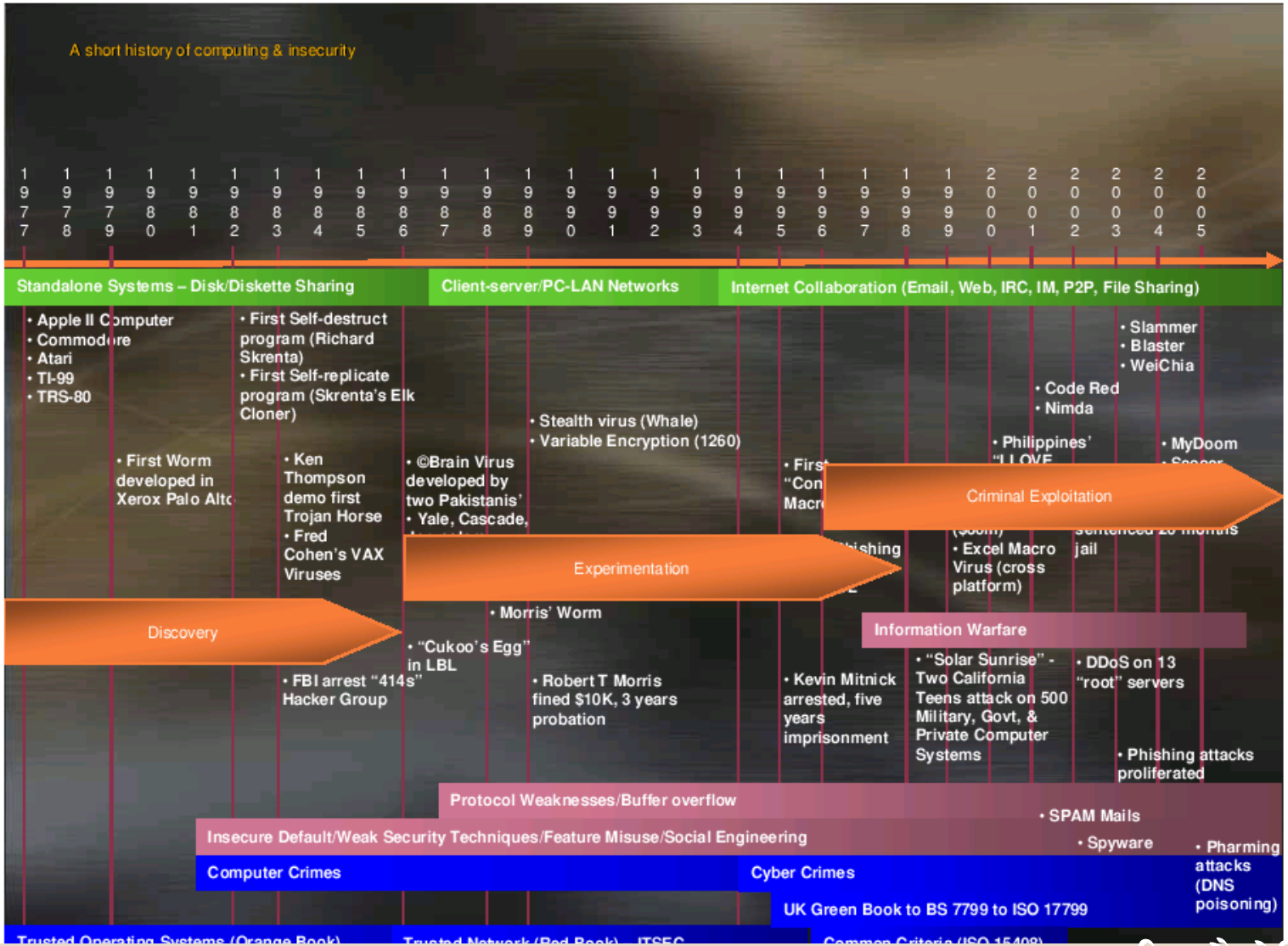
- Against People
  - Cyber Stalking and Harrassment
  - (Child) Pornography
  - Phishing, Identity Theft, Nigerian 419
- Against Property
  - Cracking
  - Virus and Spam
  - Software/Entertainment Piracy
  - Trade secrets, espionage
- Cyber Terrorism!
  - Hactivism! (in some countries!)
  - Information Warfare

Internet Attacks Toolkits (Youtube)



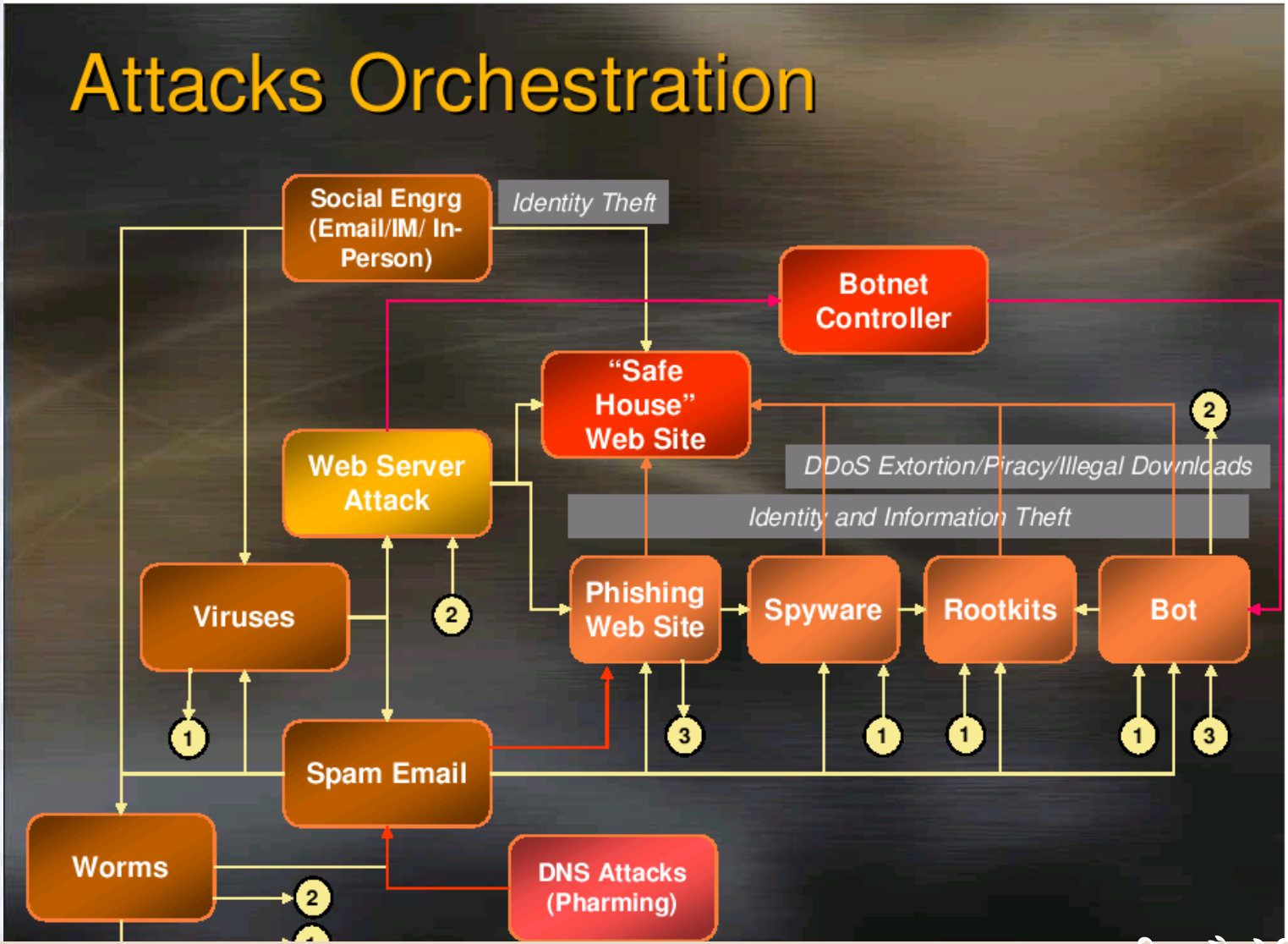
Internet Attacks Timeline

From training material at http://www.cert-in.org.in/



Internet Attack Trends

From training material at http://www.cert-in.org.in/



Indian IT Act 2000

- Basic Legal Framework
- Electronic documents, signatures as evidence
- Cyber Crimes & Punishments
  - Secn 43: Damage to Computers/Network
  - Secn 65: Tampering source code
  - Secn 66: ``Hacking'' (cracking)
  - Secn 67: Obscenity (bazee.com!)
  - Secn 69: Interception
- Several Initiatives (PKI, CERT-IN, Cyber cells, ...)

cert-in.org.in

2011 Annual Report

Security Incidents	2004	2005	2006	2007	2008	2009	2010	2011
Phishing	3	101	339	392	604	374	508	674
Network Scanning / Probing	11	40	177	223	265	303	277	1748
Virus / Malicious Code	5	95	19	358	408	596	2817	2765
Spam	-	-	-	-	305	285	181	2480
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344	4394
Others	4	18	17	264	148	160	188	1240
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**

Table 2. Year-wise summary of Security Incidents handled

Excellent Training Programs

Workshop on "Data Centre Security" on October 21, 2011

A workshop on "Data Centre Security" was conducted on October 21, 2011. The workshop was targeted for State Data Centres. Aim of this workshop is to explore State Data Centre environment and related security issues. The workshop addresses Data Centre Security Parameters, Devices in Data Centre Design, Security Devices, Security Policy Implementation and Audit and ISMS. Data Centre managers, System/Network administrators, IT/ Information Security Managers from these organizations attended the workshop.

[Presentation Material]

Workshop on "Log Management, Compliance & Auditing" on October 17, 2011

A workshop on "Log Management, Compliance & Auditing" was conducted on October 17, 2011. The workshop was targeted for Govt. Depts./Ministries, PSUs and critical sector organizations. Aim of this workshop is to explore Log Management and related security issues. The workshop addresses Log management architecture, Log Monitoring, review, compliance & auditing , Log Management latest tools & techniques and necessity of ISO 27001 standard in context of Log Management. System/Network administrators, IT/ Information Security Managers and senior IT officials from these organizations attended the workshop.

[Presentation Material]

Workshop on "Phishing Attacks and Mitigation" on September 29, 2011

A 1-day workshop on "Phishing Attacks and Mitigation" was conducted on September 29, 2011. The workshop was targeted for Banking organizations/financial institutions and critical sector organizations. Aim of this workshop is to explore current trends in phishing threats & mitigation strategies. The workshop addresses current phishing attacks scenario and countering techniques & solutions. Senior IT/ Information Security professionals from these organizations attended the workshop.

[Presentation Material]

Workshop on "Web Application Security : Current threats & mitigation" on September 09, 2011

A 1-day workshop on "Web Application Security : Current threats & mitigation was conducted on September 09, 2011. The workshop was targeted for Govt. Depts./Ministries, PSUs, ISPs and critical sector organizations. Aim of this workshop is to explore current trends in threats to web applications & its mitigation strategies. The workshop addresses technologies critical to protect the enterprise data and applications, emerging security trends in cyberspace and exploring of protection tools. Information Security professionals, application developers and senior officials from these organizations attended the workshop.

[Presentation Material]

Defending a Critical National Infrastructure

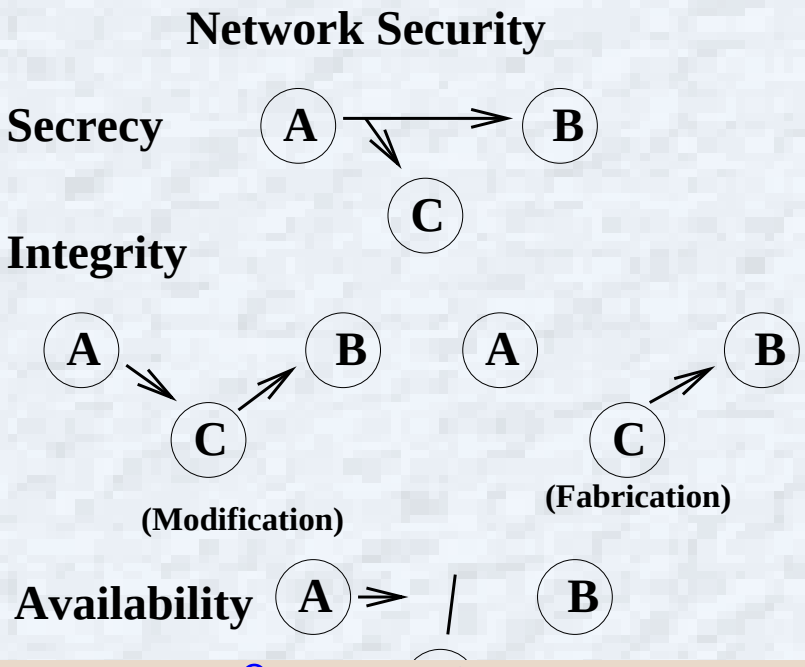
Recent fibre cut.

Defending a Critical National Infrastructure

Our Solution

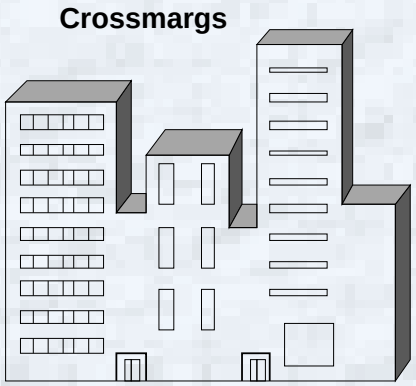
Vulnerabilities

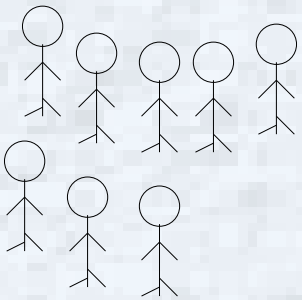
- **Application Security**
  - Buggy code
  - Buffer Overflows
- **Host Security**
  - Server side (multi-user/application)
  - Client side (virus)
- **Transmission Security**

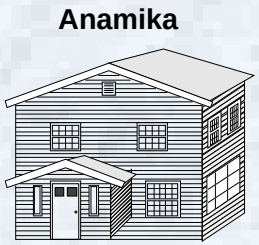


Denial of Service

Small shop-owner versus Supermarket







- What can the attacker do?
- What has he gained or compromised?
- What defence mechanisms are possible?
  - Screening visitors using guards (who looks respectable?)
  - VVIP security, but do you want to be isolated?
- what is the Internet equivalent?

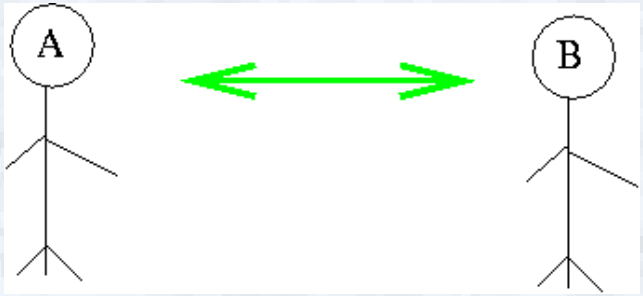
DDOS increasingly the biggest worry on Internet. (Pearl Harbour comparison)

Security Requirements

Informal statements (formal is much harder)

- Confidentiality Protection from disclosure to unauthorized persons
- Integrity Assurance that information has not been modified unauthorizedly.
- Authentication Assurance of identity of originator of information.
- Non-Repudiation Originator cannot deny sending the message.
- Availability Not able to use system or communicate when desired.
- Anonymity/Pseudonomity For applications like voting, instructor evaluation.
- Traffic Analysis Should not even know who is communicating with whom. Why?
- Emerging Applications Online Voting, Auctions (more later)

Mutual Authentication



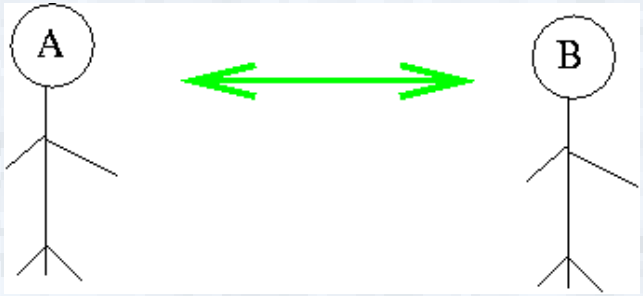
Goal

A and B to verify that both know the same secret number. No *third party* (intruder or umpire!)

Solution?

A tells B: *I'll tell you first 2 digits, you tell me the last two...*

Mutual Authentication



Goal

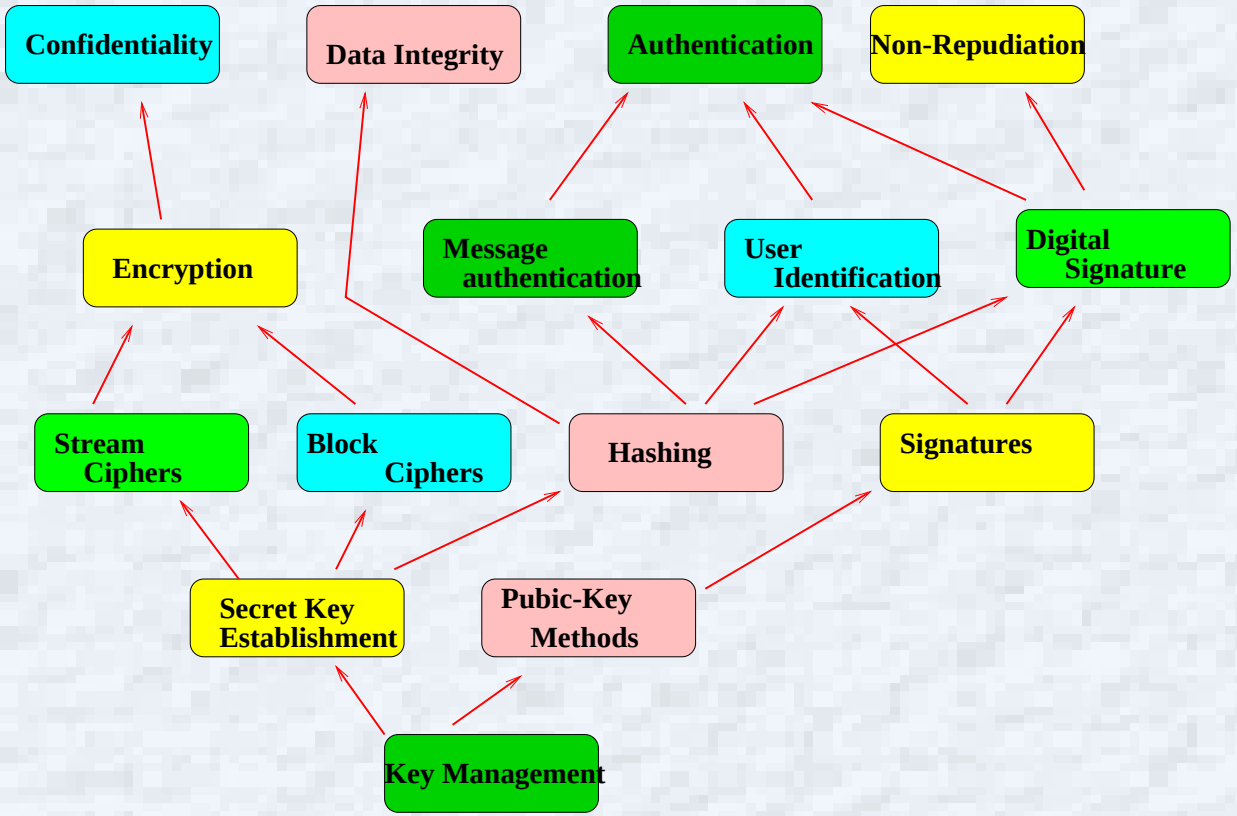
A and B to verify that both know the same secret number. No *third party* (intruder or umpire!)

Solution?

A tells B: *I'll tell you first 2 digits, you tell me the last two...*

Cryptography and Data Security

- *sine qua non* [without this nothing :-]
- Historically who used first? (L & M)
- Code Language in joint families!



Security Mechanisms

- **System Security:** ``Nothing bad happens to my computers and equipment''
  virus, trojan-horse, logic/time-bombs, ...

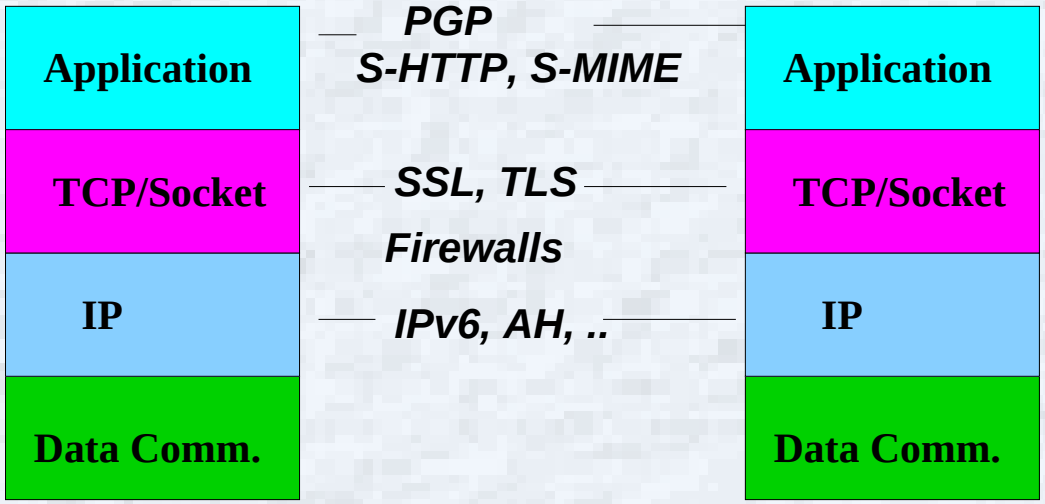
Security Mechanisms

- **System Security:** ``Nothing bad happens to my computers and equipment''
  virus, trojan-horse, logic/time-bombs, ...
- **Network Security:**
  - **Authentication Mechanisms** ``you are who you say you are''
  - **Access Control** Firewalls, Proxies ``who can do what''

Security Mechanisms

- **System Security:** ``Nothing bad happens to my computers and equipment''
  virus, trojan-horse, logic/time-bombs, ...
- **Network Security:**
  - **Authentication Mechanisms** ``you are who you say you are''
  - **Access Control** Firewalls, Proxies ``who can do what''
- **Data Security:** ``for your eyes only''
  - Encryption, Digests, Signatures, ...

Network Security Mechanism Layers



Encryption can be done at any level!

Higher-up: more overhead (for each application)

but better control

Cryptograhphic Protocols underly all security mechanisms. Real Challenge to design good ones for *key establishment*, *mutual authentication* etc.

Forensics

From www.forensicswiki.org

Topics

- **File Analysis**:
  - **File Formats**: PDF, DOC, DOCX, JPEG, GIF, BMP, LNK, MP3, AAC, Thumbs.db, ...
  - **Forensic file formats**: AFF, gfzip, sgzip, ...
- **File Systems**: FAT, NTFS, ext2/ext3, ufs, ffs, reiserfs, ...
  - **Cryptographic File Systems**: File Vault, EFS, CFS, NCryptfs, TCFS, SFS, ...
- **Hardware**:
  - **Busses**: IDE, SCSI, Firewire, USB, ...
  - **Media**: RAM, Hard Drives, Memory Cards, SmartCards, RFID Tags...
  - **Personal Digital Devices**: PDAs, Cellphones, SmartPhones, Audio Devices, ...
  - **Other Devices**: Printers, Scanners, ...
  - **Write Blockers**: ...
- **Recovering data**: bad data, deleted data, overwritten data, Sanitization Standards
- Encryption
- GPS
- Forensic Corpora
- Network forensics: OS fingerprinting, Hidden channels, Proxy servers
- Steganography, Steganalysis
- **Metadata:** MAC times, ACLs, Email Headers, Exif, ID3, OLE-2, ...
- **Legal issues:** Case law
- **Further information:** Books, Papers, Reports, Journals, Websites, Blogs, Mailing lists, Organizations, Vendors, Conferences

Tools

- **Disk Imaging**: dd, dc3dd, dcfldd, dd_rescue, sdd, aimage, Blackbag, ...
- **Data Recovery**: ...
- **Disk Analysis**: EnCase, SMART, Sleuthkit, foremost, Scalpel, frag_find...
- **Live CDs**: DEFT Linux, Helix (Pro), FCCU Gnu/Linux Boot CD, Knoppix STD, ...
- **Metadata Extraction**: wvWare, jhead, hachoir-metadata, ...
- **File Analysis**: file, ldd, ltrace, strace, strings, ...
- **Network Forensics**: Snort, Wireshark, Kismet, NetworkMiner...
- **Anti-Forensics**: Slacker, Timestomp, wipe, shred, ...
- **Other Tools**: biew, hexdump, ...

Network Forensics

From en.wikipedia.org/wiki/Networkforensics
Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

Surveillance- atlas.arbor.net

COUNTRY REPORT

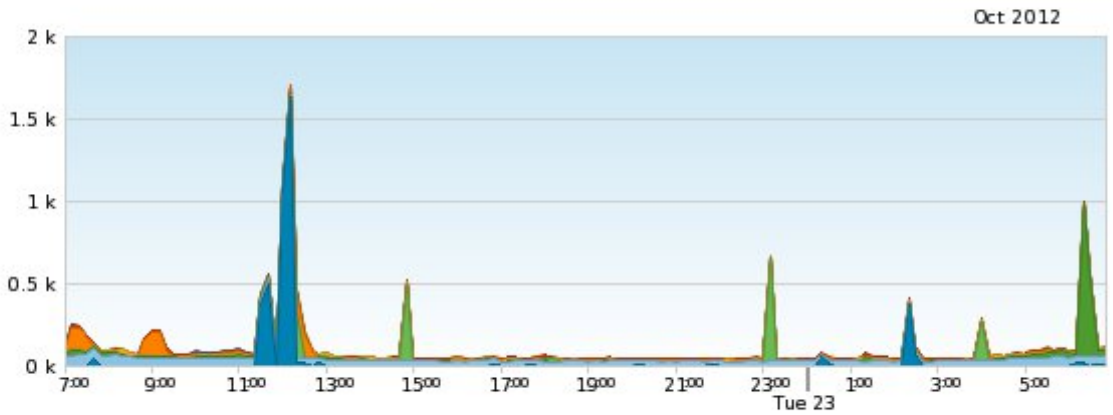
GLOBAL INDIA

View: Activity | Sources | Malicious Servers

Output: Print | XML | CSV

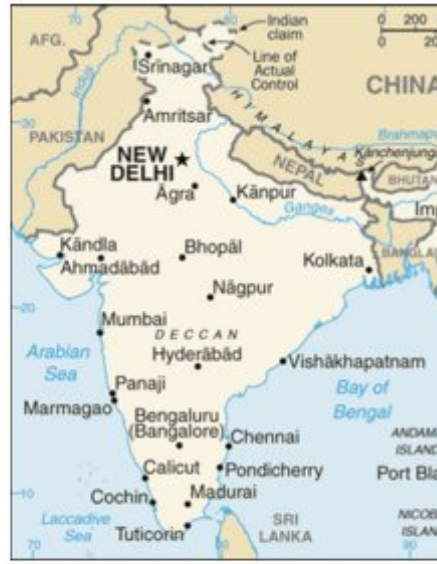
ACTIVITY (past 24 hours)

SCANS | ATTACKS | DOS



Key	Service	Bytes per subnet	Percentage
	TCP/23 (telnet)	4.05 kB	26.9%
	TCP/445 (microsoft-ds)	3.03 kB	20.1%
	TCP/80 (http)	2.37 kB	15.8%
	TCP/22 (ssh)	1.74 kB	11.6%
	TCP/139 (netbios-ssn)	1.36 kB	9.0%

BACKGROUND



Internet Statistics

Internet Hosts (est.)	2,707,000
Internet Users (est.)	80,000,000

Current Threat Rank

1 CA (Canada)

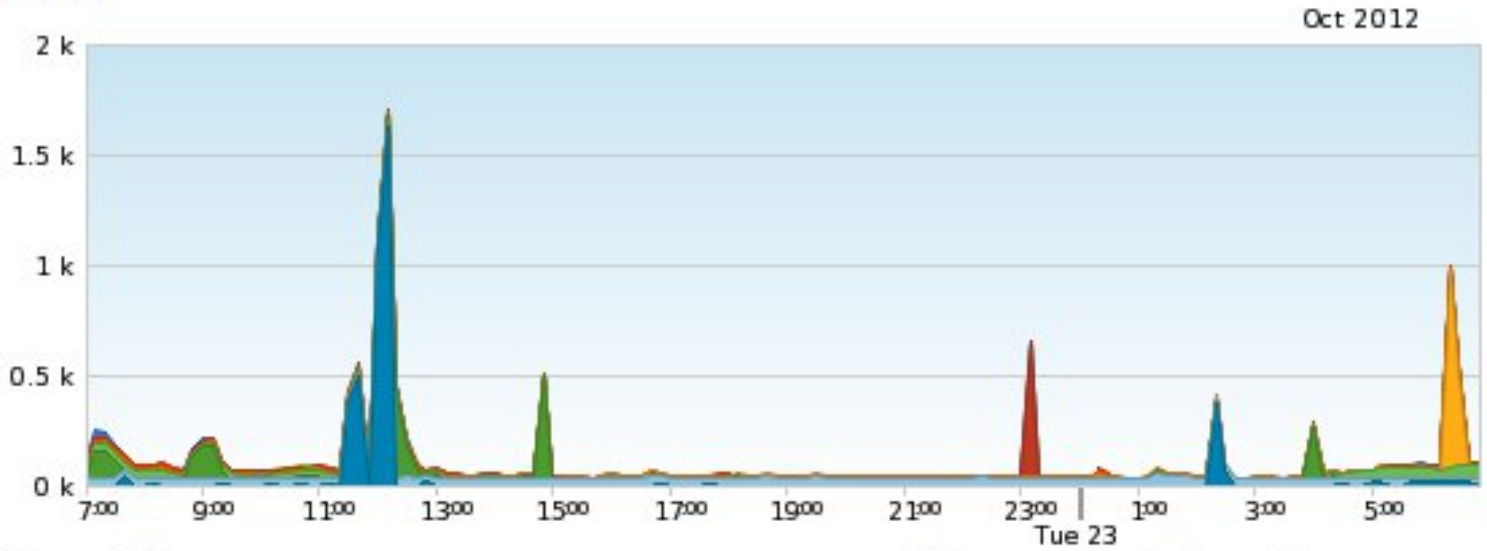
2 US (United States)

Who is scanning?

SOURCES (past 24 hours)

SCANS | ATTACKS

BY ASN



Key	ASN	Bytes per subnet	Percentage
	AS17908 (TCISL)	4.00 kB	26.6%
	AS4755 (TATACOMM-AS)	2.70 kB	17.9%
	AS18101 (RELIANCE-COMMUNICATIONS-IN)	2.26 kB	15.0%
	AS9829 (BSNL-NIB)	1.55 kB	10.3%
	AS37986 (TULIP)	1.35 kB	8.9%
	AS33480 (WEBWERKSAS1)	1.10 kB	7.3%
	AS24560 (AIRTELBROADBAND-AS-AP)	818.47 B	5.4%

Who is hosting phising sites?

MALICIOUS SERVERS (past 24 hours)

BOTNETS | PHISHING

BY TARGETED BRAND

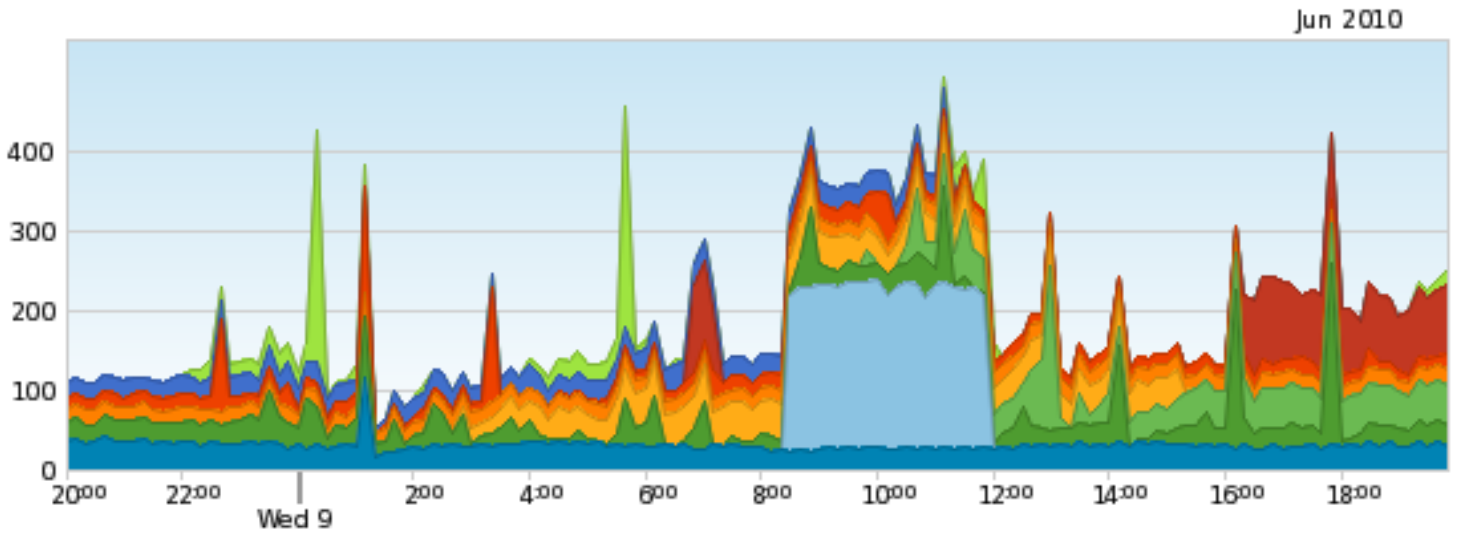
Brand Name	Phished URLs	Percentage
PayPal	32	34.8%
Other	60	65.2%

BY ASN

ASN	Phishing URLs hosted	Percentage
AS45815 (HOSTCOIN-AS-IN-AP)	25	27.2%
AS18229 (CTRLS-AS-IN)	19	20.7%
AS4755 (TATACOMM-AS)	13	14.1%
AS32613 (IWEB-AS)	13	14.1%
AS10929 (NETELLIGENT)	8	8.7%
AS9583 (SIFY-AS-IN)	4	4.3%
AS37986 (TULIP)	4	4.3%

Malicious Servers

BY HOST



Key	Host	Bytes per subnet	Percentage
	61.246.241.44 (ABTS-MP-Static-044.241.246.61.airtelbroadband.in)	4.39 kB	13.1%
	59.162.59.217	4.31 kB	12.8%
	58.68.41.6	3.90 kB	11.6%
	115.113.79.98 (115.113.79.98.static-hyderabad.vsnl.net.in)	2.63 kB	7.8%
	210.212.14.180	2.61 kB	7.8%
	203.76.129.99	2.52 kB	7.5%
	115.113.41.196 (115.113.41.196.static-kolkata.vsnl.net.in)	2.31 kB	6.9%
	119.252.145.173 (host-119.252.145.173.rediffdns.com)	2.17 kB	6.5%

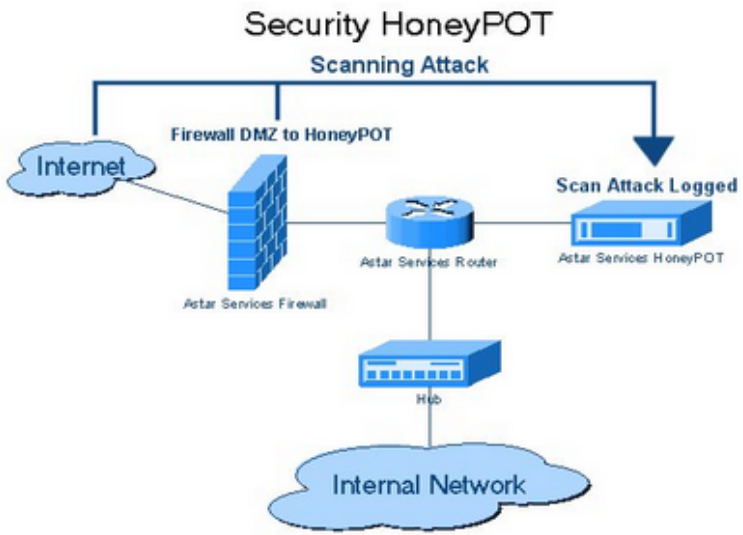
Offence is Best Defence?

Honeypots - to attract bees. http://www.honeynet.org/

Security HoneyPots

Security Honeypots are closely monitored network decoys serving several purposes: they can distract adversaries from more valuable machines on a network, they can act as an early warning system for new attack and exploitation trends, and they allow in-depth examination of adversaries during and after the exploitation of a honeypot.

Honeypots are a highly flexible security tool with different applications for security. They are not a one-time solution to a single problem. Instead, they have multiple uses, such as prevention, detection, or information gathering. Honeypots all share the same concept: a security resource that should not have any production or authorized activity. In other words, the deployment of honeypots in a network should not affect critical network services and applications. A honeypot is a security resource who's value lies in being probed, attacked, or compromised without allowing the crucial systems on your network to be harmed.

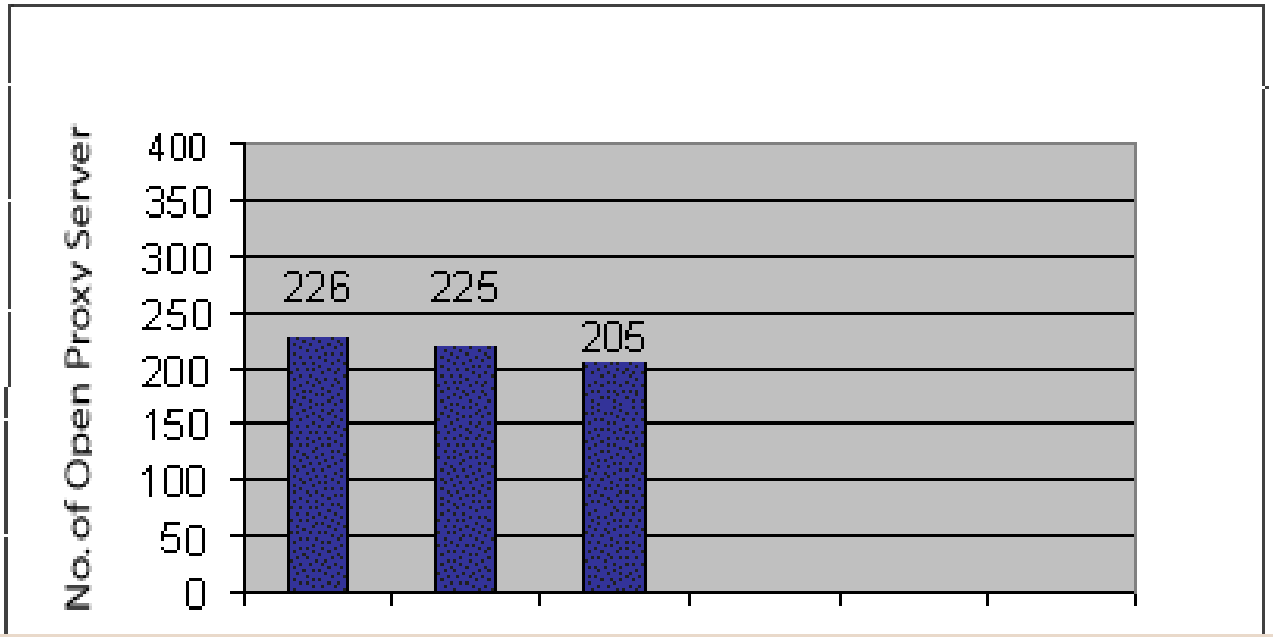


Open Proxy (CERT-IN Stats)

Open Proxy Server Statistics

Open Proxy Servers are widely prevalent on the Internet and are being misused by malicious users to route traffic bypassing network controls. Open Proxy Servers are major sources of Spam on the Internet and are also used to launch attacks on other systems. CERT-In is regularly tracking open proxy servers hosted in India. CERT-In also contacts the open proxy owners and helps them to reconfigure their servers properly. For further details on Open proxy servers refer to white paper (Open Proxy Servers), published by CERT-In. The following statistics represents the number of open proxy servers being identified by CERT-In monthly.

Open Proxy Server Statistics of 2010



War Driving: Mumbai Police

Mumbai police to look out for unsecured Wi-Fi connections

PTI, Jan 9, 2009, 04.16pm IST

Article | Comments

MUMBAI: City policemen will be soon seen roaming in the streets with laptops in their hands in search of unsecured Wi-Fi connections.

In an initiative taken by the Mumbai police, in the backdrop of terror mails sent before blasts and terror attacks, policemen will be sent to various locations in the city in search of unsecured Wi-Fi connections.

"If a particular place's Wi-Fi is not password protected or secured then the policemen at the spot has the authority to issue notice to the owner of the Wi-Fi connection directing him to secure the connection," DCP Sanjay Mohite said.

The notice will be issued by the police under section 149 of the Criminal Procedure Code which is to prevent the commission of a cognizable offence.

The step was taken at a conference today where around 80 police personnel were present to learn about Wi-Fi connections and cyber crime.

Terror mails were sent through unsecured Wi-Fi connections prior to the Delhi and Ahmedabad blasts. While the mail sent before the Ahmedabad blasts was traced to the residence of US national Kenneth Heywood in Navi Mumbai, the mail sent prior to the Delhi blast was traced to a residence in suburban

War Driving: Google way

Google: Oops, we spied on your Wi-Fi

by Marguerite Reardon and Tom Krazit

Google admitted in a blog post Friday that it has been snooping on Wi-Fi users as its Street View **cars** have been riding around neighborhoods throughout the world collecting data for its mapping service.

In a blog post, the company said it has parked its Street View cars and stopped collecting data after it realized that it has been inadvertently collecting data about people's online activities from unsecured Wi-Fi networks over the past four years. The disclosure could not come at a worse time for Google, following **strident criticism over its Google Buzz launch from privacy experts** and a growing unease among consumers regarding the amount of data it collects.

A Google Street View car makes its rounds in Singapore in 2008.
(Credit: CNET Asia)

Google had apparently told **German authorities last month** that it had been collecting "publicly broadcast SSID information (the Wi-Fi network name) and MAC addresses (the unique number given to a device like a Wi-Fi router) using Street View cars." **But it said that it did not collect payload data** or information sent over the network.

Google now says that information was incorrect.