

Introduction to Cyber Security

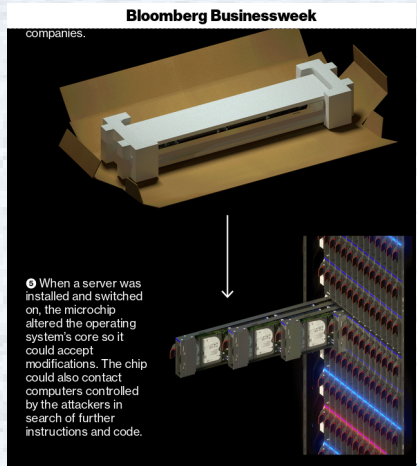
शिवकुमार G. Sivakumar சிவகுமார்

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

- Setting the Stage (Some recent incidents)
- The **Good** (The Dream: AI meets Web 3.0 & SMAC + IoT)
- The **Bad** (The Nightmare: Computer & Network Security)
- The **Ugly?** (Deception Technologies and Behaviour Analysis)



Compromising the Supply Chain



Are some countries *more trustworthy* than others?



Can this happen to you?

KeyGrabber USB

Small, fast, and smart

This keystroke recorder has up to **8 gigabytes** memory capacity, organized into an advanced flash FAT file system. Super-fast data retrieve is achieved by switching into **Flash Drive mode** for download.

Completely transparent for computer operation, no software or drivers required. Supports **national keyboard layouts**.



Features

- **Huge memory capacity** (up to 8 gigabytes), organized as an advanced flash FAT file system
- Memory protected with strong **128-bit encryption**
- Works with **any USB keyboard**, including those with built-in hubs
- **Super fast** memory contents download (up to 125 kB/s)
- No software or drivers required, **Windows, Linux, and Mac** compatible
- **Transparent** to computer operation, **undetectable** for security scanners
- Quick and easy **national layout** support



blackMail

Dear All,

There is a very **ingenious blackmailing email** circulating around asking for money in bitcoins. ... they all have a few similar features:

- They include a password that you probably have used
- Claim to have installed malware, and record video of you through your webcam.
- Threaten to reveal your adult website habits and send videos ...
- Demand bitcoins...

Subject: 15xxxxxxx@iitb.ac.in is hacked

From: 15xxxxxxx@iitb.ac.in

Date: Thu, October 18, 2018 4:35 pm

Hello!

My nickname in DARKNET is derrik82. I hacked this mailbox more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

So, your password from 15xxxxxxx@iitb.ac.in is xxxxxxxx. Even if you changed the password after that - it does not matter, my virus

...

I was most struck by the intimate content sites that you occasionally visit. You have a very wild imagination, I tell you!

...

Send the above amount on my BTC wallet (bitcoin):
1EZS92K4xJbymDLwG4F7PNF5idPE62e9XY
Since reading this letter you have 48 hours!



Insider Attacks

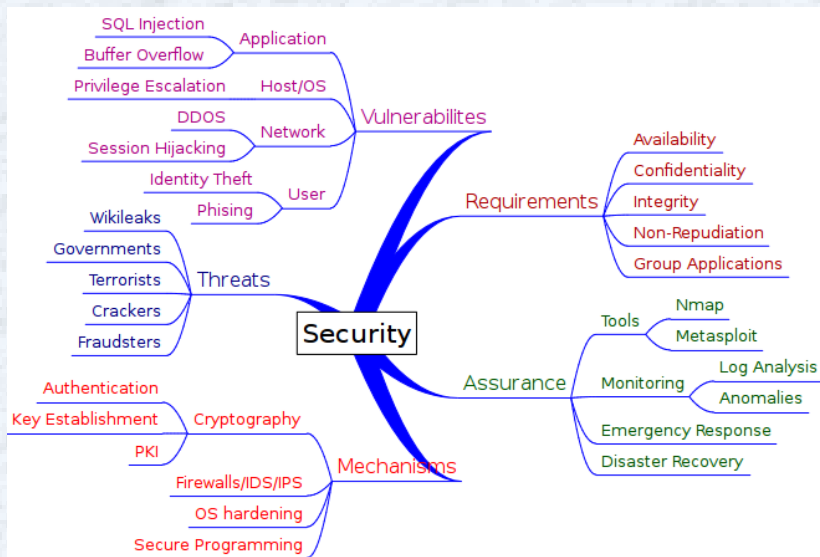
- CBI
- Paytm
- ...

[From https://en.wikipedia.org/wiki/Insider_threat] A report published on the insider threat in the U.S. financial sector[6] gives some statistics on insider threat incidents: 80% of the malicious acts were committed at work during working hours; 81% of the perpetrators planned their actions beforehand; 33% of the perpetrators were described as "difficult" and 17% as being "disgruntled".

The insider was identified in 74% of cases. Financial gain was a motive in 81% of cases, revenge in 23% of cases, and 27% of the people carrying out malicious acts were in financial difficulties at the time.



Partial Landscape (from CISO/CTO perspective)



Cyber Security Framework, NIST (April 2018) (CEO perspective)

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Common taxonomy and mechanism for

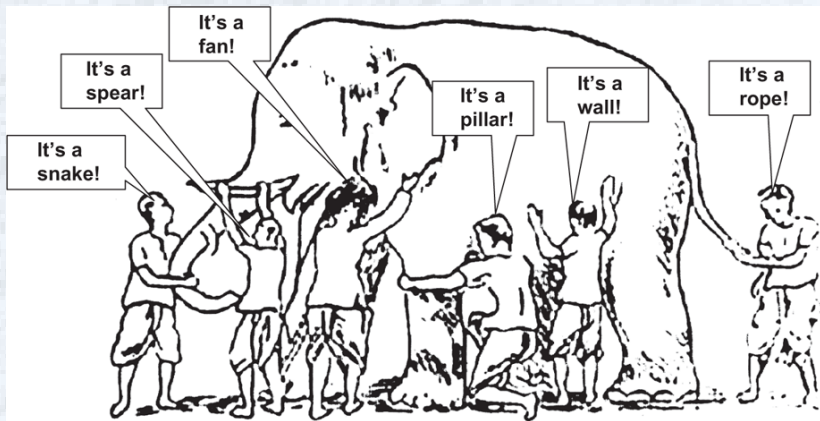
- Describing current cybersecurity posture
- Target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress
- Communicate with stakeholders about cybersecurity risk

Not one size fits all!

We will return to this framework at the end.



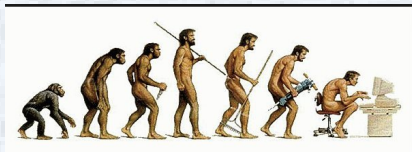
One Single Truth? अन्ध-गज न्यायः



Note: The risks of analytical thinking and fragmentation of knowledge



Stone Age to Information Age



Homo **Erectus**, Homo **Sapiens**, Homo **Deus** [Yuval Noah Harari], 21 Lessons

Technology (Wikipedia Definition)

Technology is the usage and knowledge of tools, techniques, crafts, systems or methods of organization in order to **solve a problem** or **serve some purpose**.

Zero, Wheel, Printing Press, Radio, Lasers, ...

Any sufficiently advanced technology is indistinguishable from magic. [Arthur C. Clarke]

- Why **Information Technology** is different?
Transistor, VLSI, Microprocessor, ...
- **Danger**: Computers are coming! Taking away our jobs!
Construction, Farming, Banking, Surgery, **Composing music, Teaching!**
Be very scared!



Web 1.0, Web 2.0, Web 3.0

Web 1.0 [1990-2005] (Right to Information)

- Internet: Info anytime, anywhere, any form
- Like *drinking water from a fire hose*
- Search Engines to the rescue

Web 2.0 [2005-2015] (Right to Assembly)

- Social Networking (Twitter, Facebook, Kolaveri, Flash crowds)
- Producers, not only consumers (Wikipedia, blogs, ...)
- *Proliferated unreliable, contradictory information?*
- *Facilitated malicious uses including loss of privacy, security.*

Web 3.0 [current] (AI & ML meet Semantic Web)

- Intelligent Agents that "understand"
- What do you want when you get up and put on computer?
- *I have a dream!*(MLK)



Open Enterprises of the Future

What the Future Holds?

Modify a Google Calendar to allow a colleague to add a Faaso's roll order to a meeting invite that can be picked up by Ola and delivered by a drone to a client's office five minutes before the scheduled meeting starts.

What this needs?

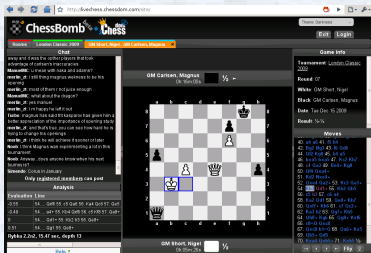
- Multi-Party Services Orchestration
- Transparent Information Flow
- Transparent Event Flow
- Semantic Consistency
- Network and Protocol Adaptability
- End-to-End Security
- Business Management

In the Security context, this is securing **M2M** communications!



Artificial Intelligence & Machine Learning

- Can AI of computers match NS of humans?
- Old Joke: *Out of sight, out of mind*
- Consider chess, once the *holy grail* of AI.

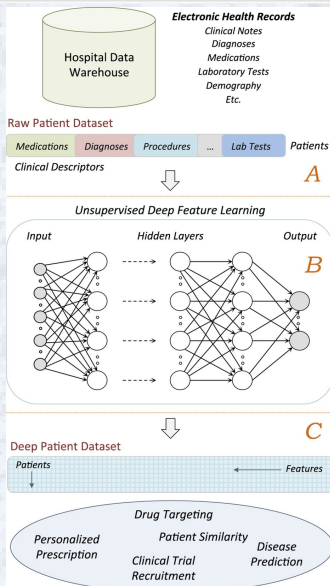


Does not play the human way at all! Mostly parallelized search in hardware (200 million positions/second!)

- December 2017: **AlphaGo Zero** used *reinforcement learning* to teach itself chess in 4 hours! Beat world's best program *Stockfish* comprehensively!



Deep Patient



Are doctors practicing **medical science?**


<https://www.nature.com/articles/srep>

The machine was given no information about how the human body works or how diseases affect us. It found correlations that let it predict the onset of some diseases more accurately than ever, and some diseases, such as schizophrenia, for the first time at all. It does this by creating a vast network of weighted connections that is just too complex for us to understand.



3rd platform: SMAC + IoT

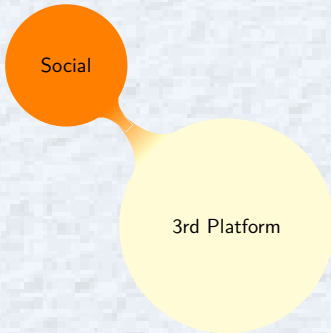
- Main Frame (1960s ...)
- Client Server (1990s ...)
- Today (Handheld, Pervasive Computing)



3rd Platform



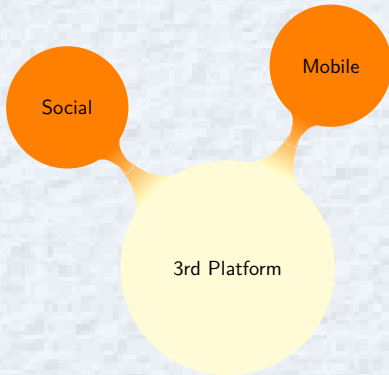
3rd platform: SMAC + IoT



- What's App (how many engineers?)
- Facebook, Twitter, GooglePlus ...
- Web 2.0 (**Right to Assembly**)
- Crowdsourcing (Wikipedia)
- Crowdfunding (no banks!)



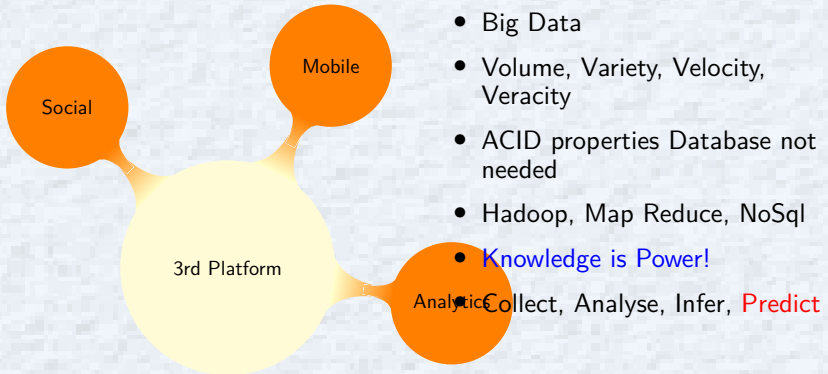
3rd platform: SMAC + IoT



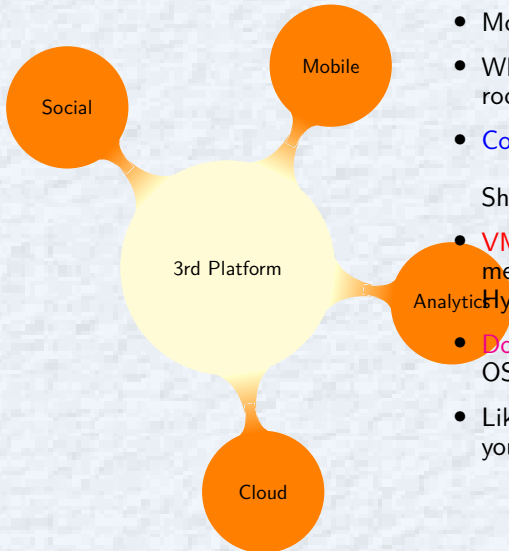
- Phone (Smart, Not-so-smart!)
- Wearables! (Google glass, Haptic)
- Internet of "Me" (highly personalized) Business (no *generic* products!)
- **BYOx**: Device security, App/content management nightmare.
- **Data Loss Prevention** (Fortress Approach - Firewall, IDS/IPS - won't work!)




3rd platform: SMAC + IoT



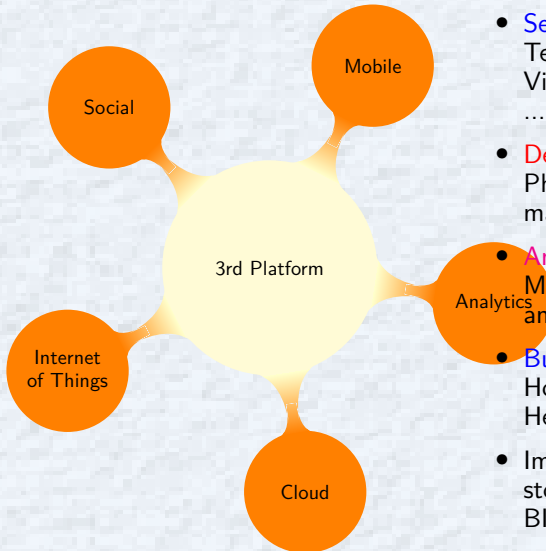
3rd platform: SMAC + IoT



- Moore's law
- What could fit in a building .. room ... pocket ... blood cell!
- **Containers** Analogy from Shipping 
- **VMs** separate OS from bare metal (at great cost- Hypervisor, OS image)
- **Docker**- separates apps from OS/infra using containers.
- Like *IaaS*, *PaaS*, *SaaS* Have you heard of **CaaS**?



3rd platform: SMAC + IoT



- **Sensors** (Location, Temperature, Motion, Sound, Vibration, Pressure, Current,)
- **Device Eco System** (Smart Phones, Communicate with so many servers!)
- **Ambient Services** (Maps, Messaging, Traffic modelling and prediction, ...)
- **Business Use Cases** (Ola Cabs, Home Depot, Philips Healthcare, ...)
- Impact on wireless bandwidth, storage, analytics (**velocity** of BIG data, not size)



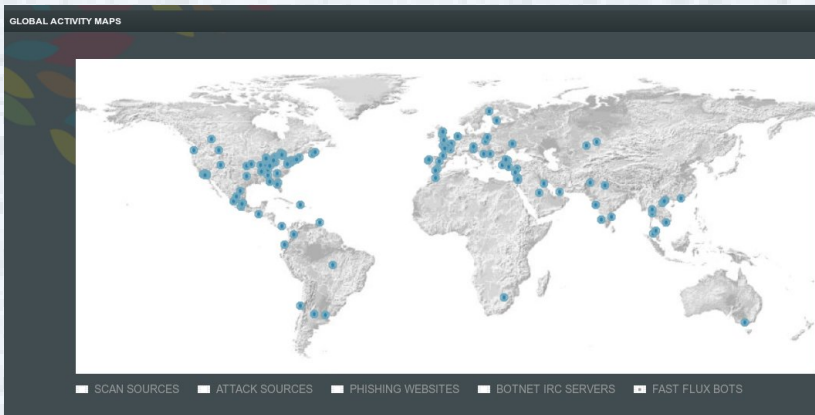
Internet's Nightmare

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 challenge
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.





TOP THREAT SOURCES (PAST 24 HOURS)						HOST	ASN	COUNTRY
COUNTRY	RANK	ATTACKS PER SUBNET	SCANS PER SUBNET	BOTNETS	PHISHING	DOS		
 US (United States)	1	0	0 B	422	86889	713		
 CA (Canada)	2	0	0 B	58	30624	40		
 FR (France)	3	0	0 B	50	11352	10		
 GB (Great Britain)	4	0	0 B	59	8613	148		
 NL (Netherlands)	5	0	0 B	41	8504	152		
 EU (European Union)	6	0	0 B	5	8497	1		
 SG (Singapore)	7	0	0 B	2	8460	0		
 CN (China)	8	0	0 B	9	5978	948		
 TR (Turkey)	9	0	0 B	8	7692	3		
 RU (Russian Federation)	10	0	0 B	48	5658	5		
 BR (Brazil)	11	0	0 B	0	5260	10		
 DE (Germany)	12	0	0 B	103	4455	17		



ATLAS

Threat Portal
LIVE UPDATING

RES

ATLAS DATA FEED

2539

DDoS Attacks Per Day Worldwide

253.29

Peak Attack in Gbps Past 24 Hours

1083

Active Botnets Detected

ACTIVE THREAT LEVEL ANALYSIS SYSTEM

ATLAS®

The Internet's first globally scoped threat network

The ATLAS portal today is a public resource that delivers a sub-set of the intelligence derived from the ATLAS sensor network on host/port scanning activity, zero-day exploits and worm propagation, security events, vulnerability disclosures and dynamic botnet and phishing infrastructures. It includes:

BOTNETS	GLOBAL ACTIVITY MAP
DOS ATTACKS	PHISHING
FAST FLUX BOTS	SCANS

SCANS SOURCES | **ATTACK SOURCES**

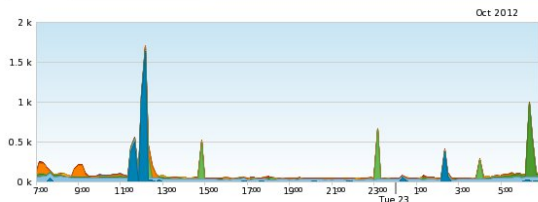
**DDOS ATTACK PROTECTION:
ARBOR NETWORKS' ATLAS**

What if you could see the traffic flowing through the Internet?

Real-time Intelligence- atlas.arbor.net

COUNTRY REPORT
GLOBAL INDIAView: [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?

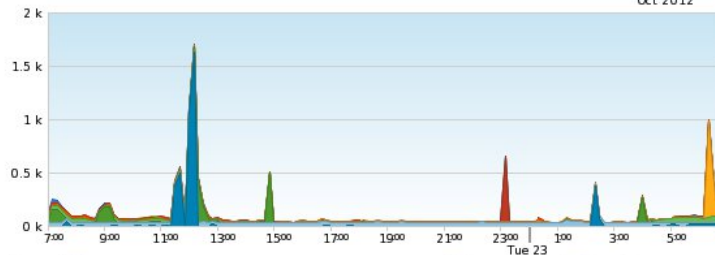
SOURCES (past 24 hours) ^ v -

SCANS

ATTACKS

BY ASN

Oct 2012



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 phishing 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

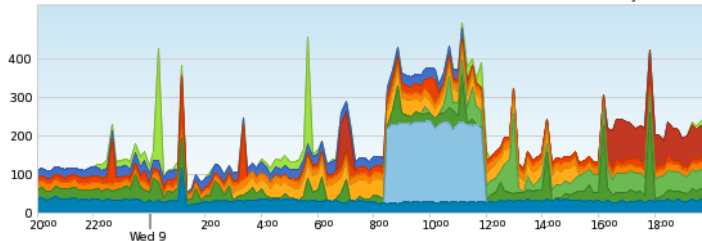
ASN	Phishing URLs hosted	Percentage
AS45815 (HOSTCOIN-AS-IN-AP)	25	27.2%
AS18229 (CTRLS-AS-IN)	19	20.7%
AS4755 (TATACOMM-AS)	13	14.1%
AS32613 (IWEB-AS)	13	14.1%
AS10929 (NETELLIGENT)	8	8.7%
AS9583 (SIFY-AS-IN)	4	4.3%
AS37986 (TULIP)	4	4.3%



Malicious Servers

BY HOST

Jun 2010



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%



Internet Attacks Toolkits (Youtube)

Cyber Crime Toolkits



Rate: ★★★★★ 10 ratings

Views: 3,068



Share



Favorite



Playlists



Flag



MySpace



Facebook



Digg

[more share options](#)

Block



From: **openflows**

Added: September 14, 2007

[\(more info\)](#)

Subscribe

CBC News Today host Nancy Wilson speaks with Jesse H...

URL

Embed

► More From: **openflows**

▼ Related Videos



Trailer: The New Face of Cybercrime

03:27 From: FortifySoftware

Views: 14,223



Worlds No. 1 Computer Hacker on the History Channel

08:19 From: no1hacker

Views: 67,506



Cyber Crime

10:27 From: EASationTV

Views: 534



Cyber Crime Intro

00:58 From: Nate3169

Views: 1,645



A brief history of computer crime

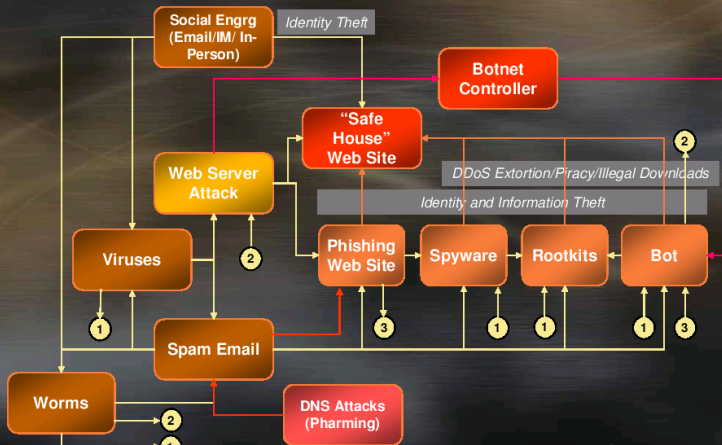
03:09 From: sakiipooh



Internet Attack Trends

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

Attacks Orchestration



What is a Computer Network?

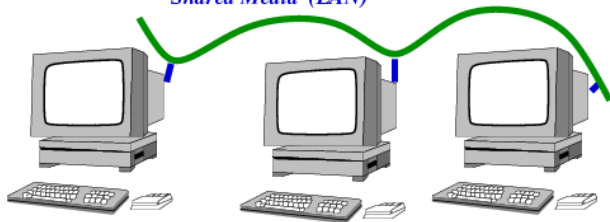
TWO

Point-to-Point



or MORE

Shared Media (LAN)

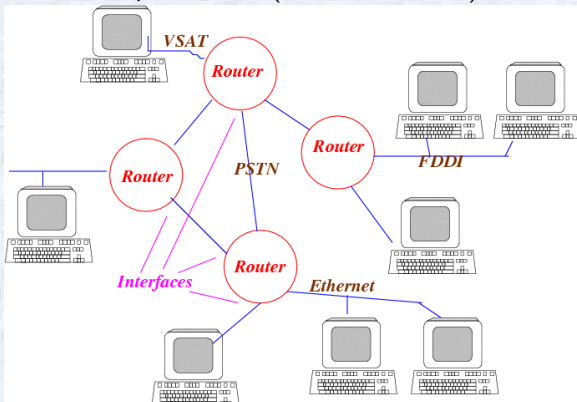


COMPUTERS sharing a LINK!



So, what's Internet?

- A bottom-up collection (**interconnection**) of networks

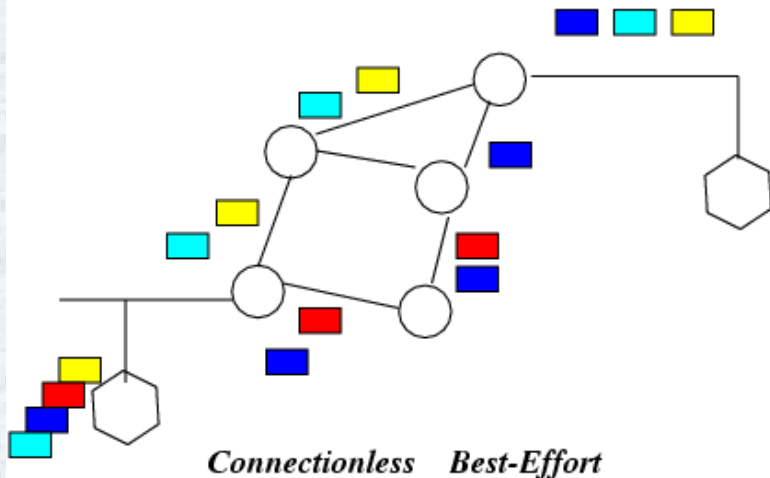


- TCP/IP is the **only** common factor
- Bureaucracy-free, reliable, cheap
- Decentralized, democratic, chaotic

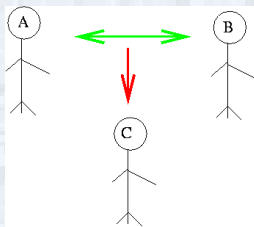


Packet Switching in Internet

Datagram Routing through Internet



Exchanging Secrets



Goal

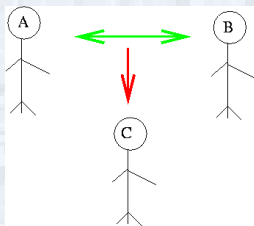
A and B to agree on a secret number. But, C can listen to all their conversation.

Solution?

A tells B: *I'll send you 3 numbers. Let's use their LCM as the key*



Exchanging Secrets



Goal

A and B to agree on a secret number. But, C can listen to all their conversation.

Solution?

A tells B: *I'll send you 3 numbers. Let's use their LCM as the key.*



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...*



Zero-Knowledge Proofs



Goal

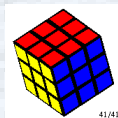
A to prove to B that she knows how to solve the cube. Without *actually revealing* the solution!

Solution?

A tells B: *Close your eyes, let me solve it...*



Zero-Knowledge Proofs



Goal

A to prove to B that she knows how to solve the cube. Without *actually revealing* the solution!

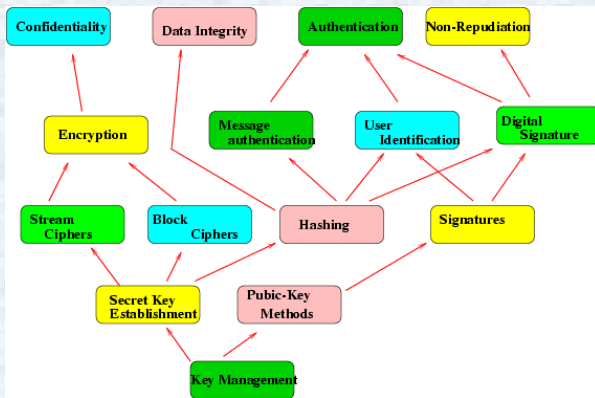
Solution?

A tells B: *Close your eyes, let me solve it...*



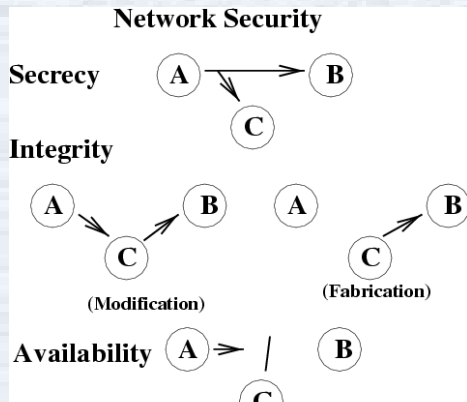
Cryptography and Data Security

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



Vulnerabilities

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



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/Pseudonymity** 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)

And all this with postcards (IP datagrams)!

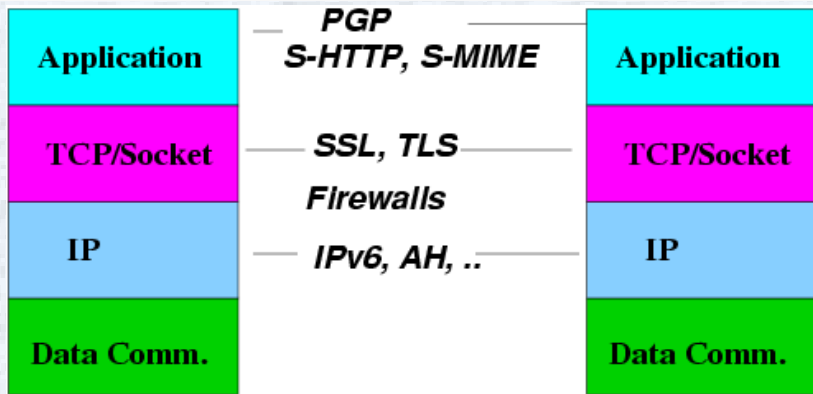


Security Mechanisms

- **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 applica

but better control

Threat-Defence Matrix

2 types of organizations- those who have been compromised and those who do not know that they have been compromised!

Threat	Defence	Example
Known	Known	Malware, DoS, SQL Injection .. This is Hygiene, but what's your score? VA-PT, IS-Audit
Known	Unknown	Zero-Day, APT, Risk Analysis and Mitigation Sandbox (Evasion e.g. Macro on File-Close) Threat Hunting (Has it happened to us?)
Unknown	Unknown	???? (Kill chain) Recon Lateral Shift Exfiltration



Tackling the Known-Known

← → ↻ 🏠 https://www.cvedetails.com/vulnerability-list/vendor_id-26/Microsoft.html

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Switch to Infos://](#)

Home
[Browse](#)
[Vendors](#)
[Products](#)
[Vulnerabilities By Date](#)
[Vulnerabilities By Type](#)

Reports :
[CVE Score Report](#)
[CVE Score Distribution](#)

Search :
[Vendor Search](#)
[Product Search](#)
[Version Search](#)
[Vulnerability Search](#)
[By Microsoft References](#)

Top 50 :
[Vendors](#)
[Vendor CVE Scores](#)
[Products](#)
[Product CVE Scores](#)
[Versions](#)

Other :
[Microsoft Subsites](#)
[Business Emails](#)
[CVE Definitions](#)
[About & Contact](#)
[Feedback](#)
[CVE Help](#)
[FAQ](#)
[Privacy](#)

Microsoft : Security Vulnerabilities

CVE Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
 Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVE Score Descending](#) [Number Of Exploits Descending](#)
[Copy Results](#) [Download Results](#)

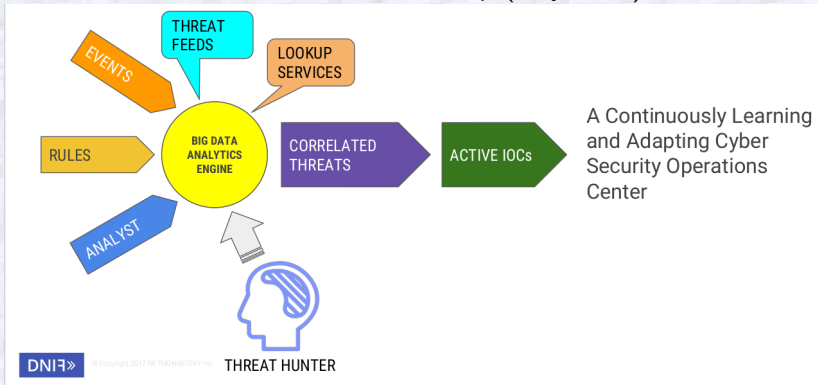
#	CVE ID	CWE ID	# of Exploits	Vulnerability Types	Publish Date	Update Date	Score	Acc
1	CVE-2017-11940	119		Exec Code Overflow	2017-12-08	2017-12-21	7.8	
The Microsoft Hardware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Win Server 2016, Windows Server, version 1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specific Remote Code Execution Vulnerability". This is different than CVE-2017-11937.								
2	CVE-2017-11939	200		Info	2017-12-12	2017-12-27	4.0	
Microsoft Office 2016 Click-to-Run (CTR) allows an information disclosure vulnerability due to the way Microsoft Office Vulnerability".								
3	CVE-2017-11937	119		Exec Code Overflow	2017-12-07	2017-12-21	7.8	
The Microsoft Hardware Protection Engine running on Microsoft Forefront and Microsoft Defender on Windows 7 SP1, Win Server 2016, Windows Server, version 1709, Microsoft Exchange Server 2013 and 2016, does not properly scan a specific Remote Code Execution Vulnerability".								
4	CVE-2017-11936	284			2017-12-12	2017-12-27	9.0	
Microsoft SharePoint Enterprise Server 2016 allows an elevation of privilege vulnerability due to the way web requests are handled.								
5	CVE-2017-11935	119		Exec Code Overflow	2017-12-12	2017-12-27	9.0	
Microsoft Office 2016 Click-to-Run (CTR) allows a remote code execution vulnerability due to the way files are handled.								
6	CVE-2017-11934	200		Info	2017-12-12	2017-12-29	4.3	
Microsoft Office 2013 RT SP1, Microsoft Office 2013 SP1, and Microsoft Office 2016 allow an information disclosure vulnerability due to the way they handle information disclosure vulnerability".								
7	CVE-2017-11930	119		Exec Code Overflow	2017-12-12	2017-12-21	7.8	
Man. Con. ChakraCore, and Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Wind								

- Anti-Virus
- Firewall
- Patch Management
- IDS/IPS
- WAF
- ..



Tackling the Known-UnKnown (Threat Hunting)

Slide borrowed from CERT-IN workshop (July 2018)



Tackling the UnKnown-UnKnown

Deception Technologies

- Decoys
 - Fake servers/services (ATM, Swift, ...)
 - Must *blend* and *adapt* (not stale)
 - ...
- Lures
 - Vulnerable Ports/Services
 - Mis-configuration
- Breadcrumbs
 - Mis-direction
 - File with credentials/mis-direction



Tackling the UnKnown-UnKnown

User and Endpoint Behaviour Analysis

- Try saying *I love you* 10 times everyday to your spouse!
- All antennas will go up!
- All defence mechanisms will be strengthened.

AI/Machine Learning to the rescue.

- Behaviour profiling (Baseline)
- Watch for anomalies
- Correlate with threats
- Reduce false positives



What next?

चिन्तनीया हि विपदां आदावेव प्रतिक्रिया
न कूपखननं युक्तं प्रदीप्ते वह्निना गृहे

The effect of disasters should be thought of beforehand. It is not appropriate to **start digging a well when the house is ablaze with fire.**

आचार्यात् पादमादत्ते पादं शिष्यः स्वमेधया ।

सब्रह्मचारिभ्यः पादं पादं कालक्रमेण च ॥

one fourth from the **teacher**,
one fourth from **own intelligence**,
one fourth from **classmates**,
and one fourth **only with time**.

