

Tools for Cyber Security (A QIP Course)

शिवकुमार G. Sivakumar சிவகுமார்

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

May 22, 2017

- The **Good** (Web 1.0/2.0/3.0, 3rd Platform)
- The **Bad** (Threats, Vulnerabilities, Attacks)
- The **Ugly?** (Monitor, Analyze, React)



ज्ञानम् परमम् ध्येयम् (Knowledge is Ultimate Goal)

IIT Bombay's motto is the title of this slide.

न चोरहार्यं न च राजहार्यं न भ्रातृभाज्यम् न च भारकारी
व्यये कृते वर्धत एव नित्यं विद्याधनं सर्वधनप्रधानं

It cannot be stolen by **thieves**, cannot be taken away by the **king**, cannot be divided among brothers and does not cause a load. **If spent, it always multiplies**. The wealth of knowledge is the greatest among all wealths.

கற்றது கை மண் அளவு

கல்லாதது உலகு அளவு

What has been learned is like a fistful of sand,
What remains is like the whole earth!

If I have seen further [than others] it is by standing on the shoulders of giants... Issac Newton

विद्या ददाति विनयम् (Why this QIP course? *Consumer, Trader, Producer?*)



Web 1.0 may have *democratized access to information*, but it is like **drinking water from a fire hose!**

Search engines provide partial solutions, but cannot combine, categorize and infer!

Web 2.0 may have allowed *right to assembly/collaboartion*, but

- Proliferated unreliable, contradictory information.
- Facilitated malicious uses including loss of privacy, security.

What do you want from Web 3.0?

What you want to see/hear when you wakeup?

I have a dream ...

How to achieve? **AI** meets the web of **Open Enterprises!**



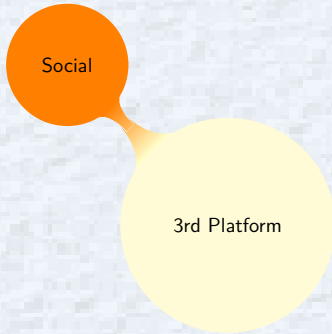
3rd platform: SMAC + IoT

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



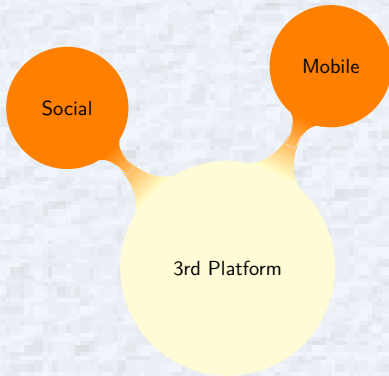
3rd Platform





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





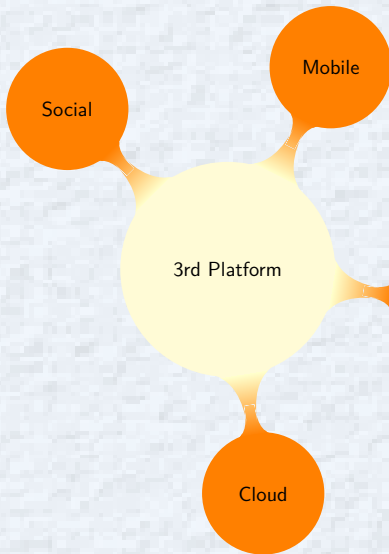
- Phone (Smart, Not-so-smart!)
- Wearables! (Google glass, Haptic)
- Internet of “Me” (highly personalized) Business (no *generic* products!)
- **BYOx**: Device security, App/content management nightmare.
- **Data Loss Prevention** (Fortress Approach - Firewall, IDS/IPS - won't work!)




3rd platform: SMAC + IoT

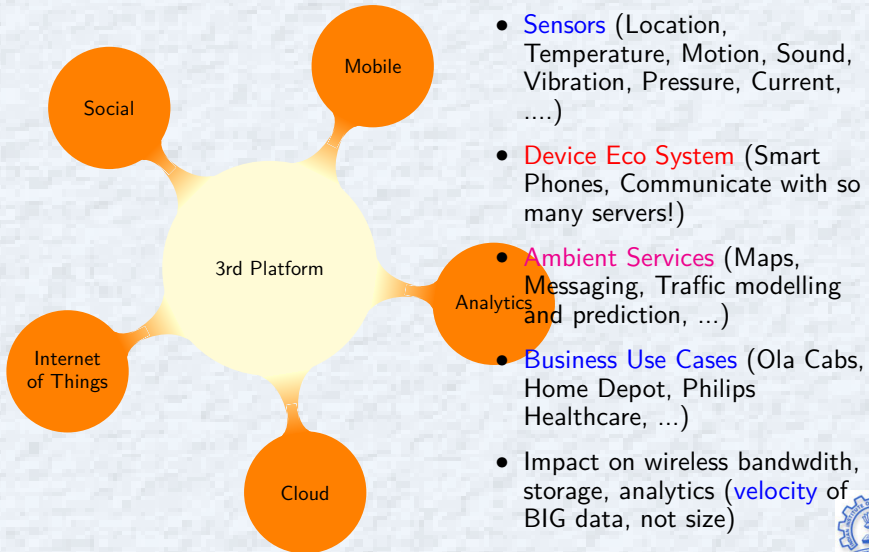


3rd platform: SMAC + IoT



- 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*?





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!



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.

Can you guess how we defend IIT Bombay?



Defending a Critical National Infrastructure



Our Solution

शिवकुमार

G. Sivakumar शिवकुमार

Computer Science and Engineering

भारतीय प्राच्योगिकी संस्थान मुंबई (IIT Bombay)

Tools for Cyber Security (A QIP Course)



Why this course?

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.**

Security cannot be an afterthought!

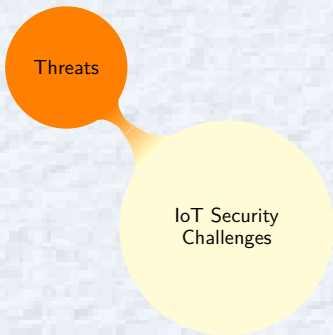
There is a tide in the affairs of men, Which taken at the flood, leads on to fortune. Omitted, all the voyage of their life is bound in shallows and in miseries. *Shakespeare*



IoT Security
Challenges

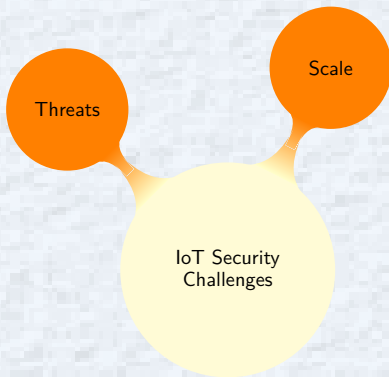
- Personal wearables
- Biomedical implants
(pacemaker, insulin control, ...)
- Smart Homes, Smart Grids ...
- Transportation industry





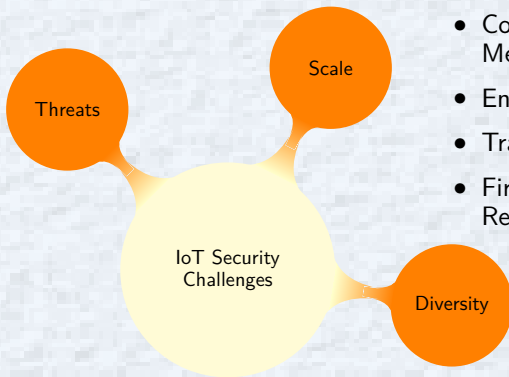
- Fridge ordering junk food.
- Fire in your kitchen!
- Malfunction of pacemaker, insulin injector.
- Driverless car taken over!
- Drone attack.





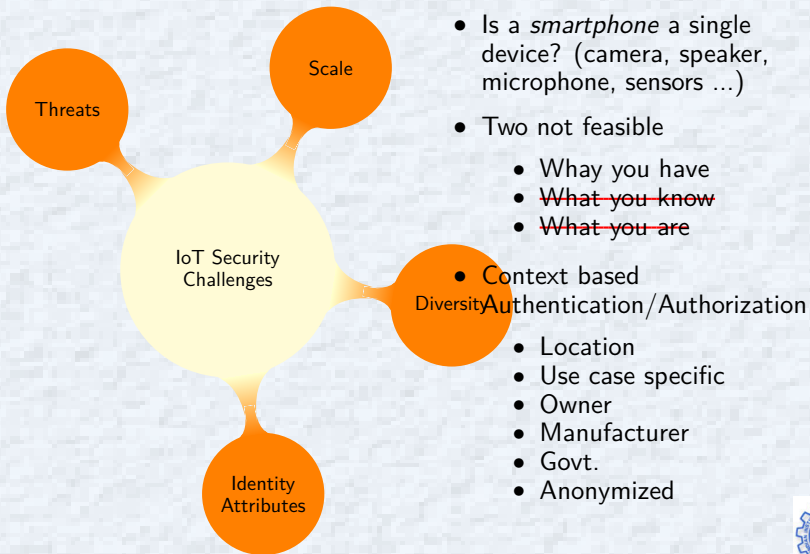
- Firefox has certificates for few hundred CAs.
- Top 3 CAs have over 80% market!
- Let's Encrypt (Free, Automated, Open)
 - Aims to encrypt 100% of web.
 - 1.7 million certificates for more than 3.8 million websites since Sept 2015!
- Gartner: From 4.8 billion connected devices in 2015 to 25 billion in 2020.
- Several orders of magnitude more.

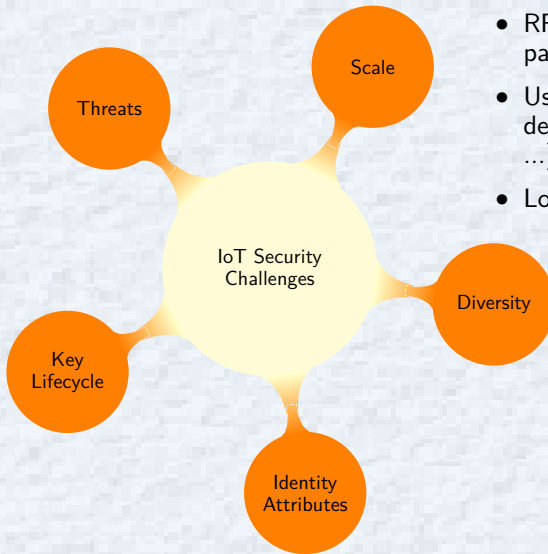




- Computational Power, Low Memory
- Energy constraints
- Transmission Range
- Firmware Upgrades, Reconfiguration





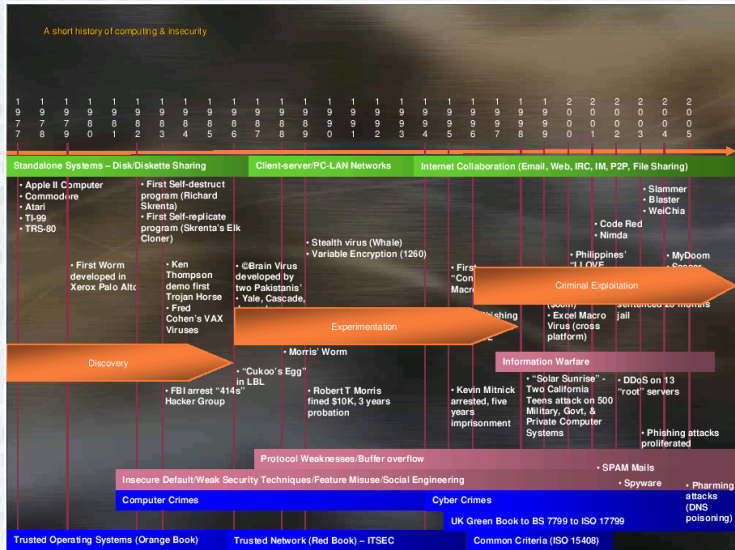


- RFID tag on International parcel
- User roles (manufacturer, dealer, owner, user, repairshop ...)
- Local versus Global namespace



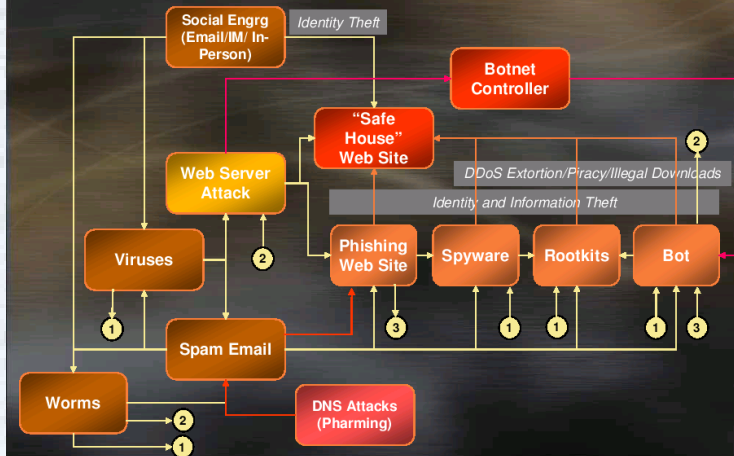
Internet Attacks Timeline

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



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

Attacks Orchestration



Cyber Crime Toolkits

Block



Rate: ★★★★★ 10 ratings

Views: 3,068

[Share](#)

[Favorite](#)

[Playlists](#)

[Flag](#)

[MySpace](#)

[Facebook](#)

[Digg](#)

[more share options](#)



From: **openflows**

Added: September 14, 2007

[\(more info\)](#)

[Subscribe](#)

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

URL: <http://www.youtube.com/watch?v=j9hApKU1ZoQ>

Embed: `<object width="425" height="344"><param name="`

▶ **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: EAStationTV

Views: 534



Cyber Crime Intro

00:58 From: Nate3169

Views: 1,645



A brief history of computer crime

03:09 From: sakiipooh



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)

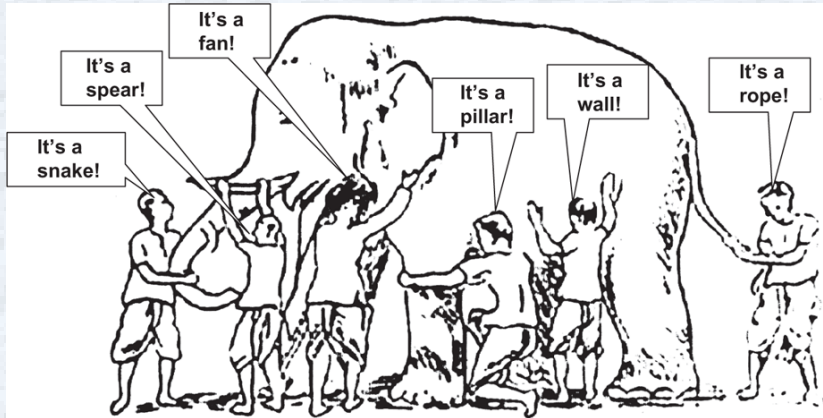
And all this with postcards (IP datagrams)!



Security Landscape



Blind men and the Elephant - अन्ध-गज न्यायः



Note: The risks of analytical thinking and fragmentation of knowledge



<http://fsf.org.in/> Richard M. Stallman
Linux, Apache, Android, Firefox, OpenOffice, Postgres,
Hadoop, OpenStack, ...

Free software

is a matter of freedom, not cost. ... The word *free* in free software has a similar meaning as in free speech, free people and free country ... Think of free software as software which is free of encumbrances ... Think of it as *swatantra* software.

Degrees of Freedom

- 1 Run the program, for any purpose
- 2 Study how the program works, and adapt it to your needs
- 3 Redistribute copies
- 4 Improve and release your improvements.



Tamil Proverb

What has been learned is like a fistful of sand, what remains is like the whole earth!

Solution?

Giving a scholar access only to *raw information* is like giving only seeds to a *hungry man*.

Way Forward?

Giving a student access only to *executable code* is like giving only *cooked rice* to a *farmer*.

How can *FOSS* close this gap?

Students move from being mere *users/consumers* to *producers*.

Great Empowerment!

Story about *Ramakrishna Paramahamsa*.

