IET Sectors The Institution of Engineering and Technology

IET The Institution of Engineering and Technology | IoT Panel

Fresh Thinking to SAFENET for IoT

A Position Paper

IoT Security

October 2018

www.theiet.in/IoTPanel

Contents

Table of Figures

List of Contributors

A. Primary Authors / Drafting Committee

Name	Designation	Organisation	E-mail address
Mr. Arvind Tiwary	Chair, IoT Forum	TiE	arvind_t@sangennovate.com
Mr. Arnab Chattopadhayay	Senior Director	CapGemni	arnab.chattopadhyay@capgemini.com
Mr. Kishore Kar	Chief Business Officer	Cyber Security Integrators India Pvt Ltd	kishore.kar@cybersiindia.com
Mr. Madhukar Khare	Founder	Wispero	madhukar.khare@wispero.com
Mr. Sumanth Naropanth	Chief Executive Officer	Deep Armor	sumanth.naropanth@deeparmor.com
Mr. Suniel Kumar	Founder - Director,	Nexiot	suniel.kumar@nexiot.com
Mr. Syam Madanapalli	Director - IoT	NTT DATA Services	syam.madanapalli@nttdata.com

B. Contributors (Working Group Cyber Security – IET IoT Panel)

Name	Designation	Organisation	E-mail address
Mr. Balaji Rajendran	Principal Technical Officer	CDAC	balaji@cdac.in
Mr. Manas Ingle	Legal Associate	NovoJuris Legal	Manas@novojuris.com
Mr. Madhav Chablani	Consulting	CIO	madhav.chablani@tippingedge.in
Mr. Santosh Kumar Jinugu	Director	Deloitte India	sjinugu@deloitte.com
Mr. Vinay Bhagavatula	Senior Manager , Risk Advisory	Deloitte India	vinayb@deloitte.com

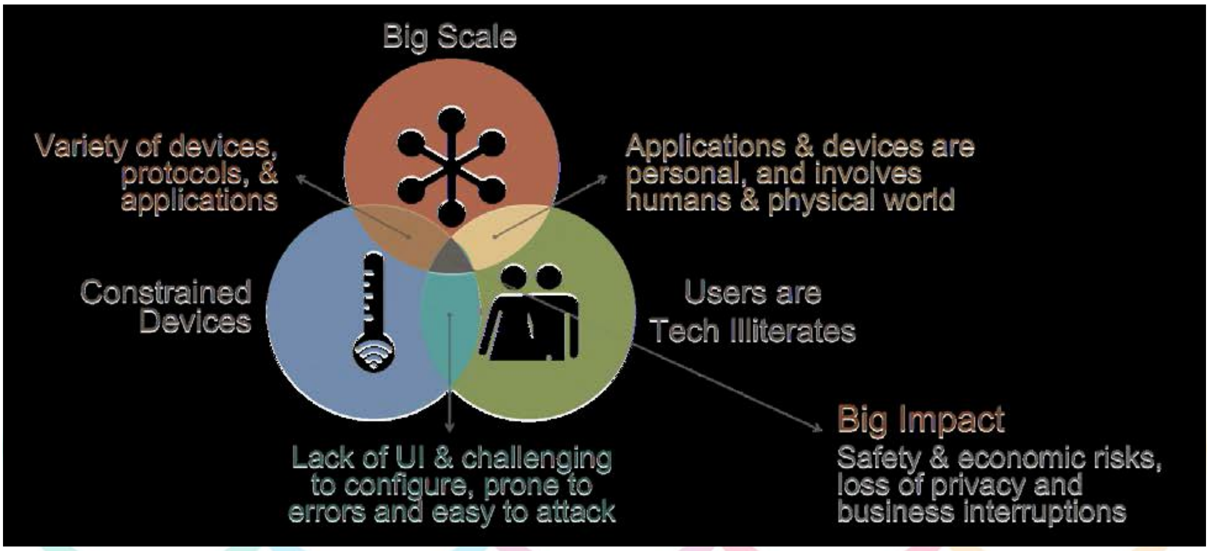
C. IET Review Committee

Name	Designation	Organisation
Shri T. V. Ramachandran	Founder & CEO	Advisory@TVR
Mr. Shekhar Sanyal	Country Head	IET
Ms. Anitha Kaveri	Manager – Sector and Special Projects	IET
Ms. Neha Abhyankar	Sector Support Executive	IET

IoT Security context

The Internet of things is soon making way for Internet of threats unless we radically change the model of securing and provide safety. As Figure 1 IOT Security complexityFigure 1 IOT Security complexity shows IoT has new complexity. It has devices outside controlled environments and constrained in terms of power (mostly being battery operated), computing resources (e.g. processing power, memory) and in its support of protocols

Figure 1 IOT Security complexity



Big Scale

Variety of devices, protocols, & applications

Applications & devices are personal, and involves humans & physical world

Constrained Devices

Users are Tech Illiterates

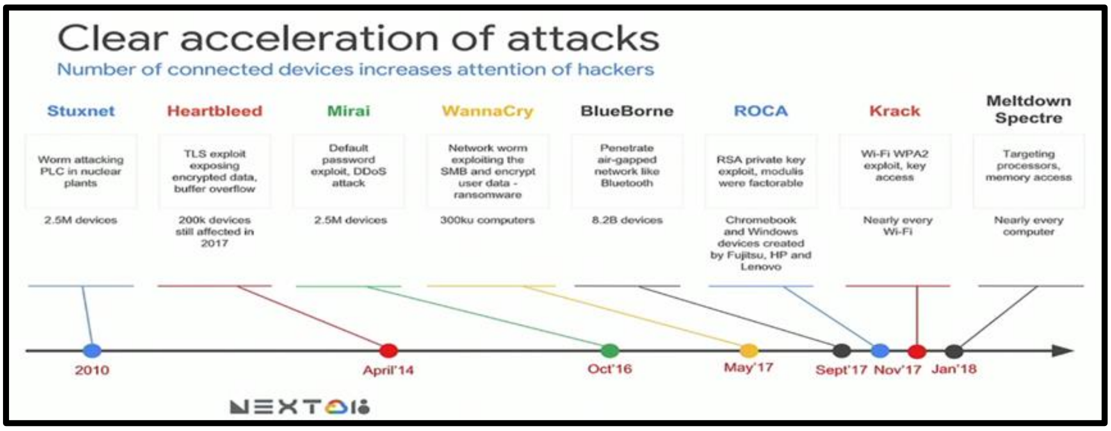
Big Impact

Safety & economic risks, loss of privacy and business interruptions

Lack of UI & challenging to configure, prone to errors and easy to attack

The sophistication and frequency of attacks is vast and exceeds the capacity of most organizations or governments to manage. Ransomware attackers have even got law enforcement to pay in some US cities. The Figure 2 Acceleration of IoT Security Attacks conveys the Internet of Threats scenario…

Figure 2 Acceleration of IoT Security Attacks



Clear acceleration of attacks

Number of connected devices increases attention of hackers

Stuxnet: Worm attacking PLC in nuclear plants. 2.5M devices. 2010

Heartbleed: TLS exploit exposing encrypted data, buffer overflow. 200k devices still affected in 2017. April'14

Mirai: Default password exploit, DDoS attack. 2.5M devices. Oct'16

WannaCry: Network worm exploiting the SMB and encrypt user data - ransomware. 300ku computers. May'17

BlueBorne: Penetrate air-gapped network like Bluetooth. 8.2B devices. Sept'17

ROCA: RSA private key exploit, modulis were factorable. Chromebook and Windows devices created by Fujitsu, HP and Lenovo

Krack: Wi-Fi WPA2 exploit, key access. Nearly every Wi-Fi. Nov'17

Meltdown Spectre: Targeting processors, memory access. Nearly every computer. Jan'18

1. Simplifying the task by changes in technical and legal approaches (Techno-Legal) . Our approach aims to increase cost and probability of legal penalty by quantum order for the adversaries so that they will have to consider crossing a higher barrier in pursuing mass scale cyberattack. This is similar to the reduction of spam as ISP shut of frequent emailers unless registered and regulated and users would provide real time feedback on spam messages. **Spam Victims fought back with institutional support. This is also the broken window theory** [1]

2. Making it more economical so more organizations can subscribe. Mass adoption will lead to less success for criminals and reduce frequency of low skill attacks

3. Make it scalable by enabling a pool of technical skilled providers with innovative tools to manage millions of users and billions of devices

4. We are breaking new ground in many “established” methods of Cybersecurity. *We limit ourselves to IoT as risk here is of lives and not just reputation or financial cost.*

5. A major departure from conventional cybersecurity practise is an offensive defence. We advocate imposing costs and apprehending criminal as primary purpose of this experiment. **Unless attackers fear penalty it is a losing battle**. We outline the current approach in these areas

Our approach2 is based on a 3-year experiment within a regulatory sandbox we expect will be created by Government of India under ***Section IV Strategy*** of the NATIONAL CYBER SECURITY POLICY[1]. The key highlights of our approach are:

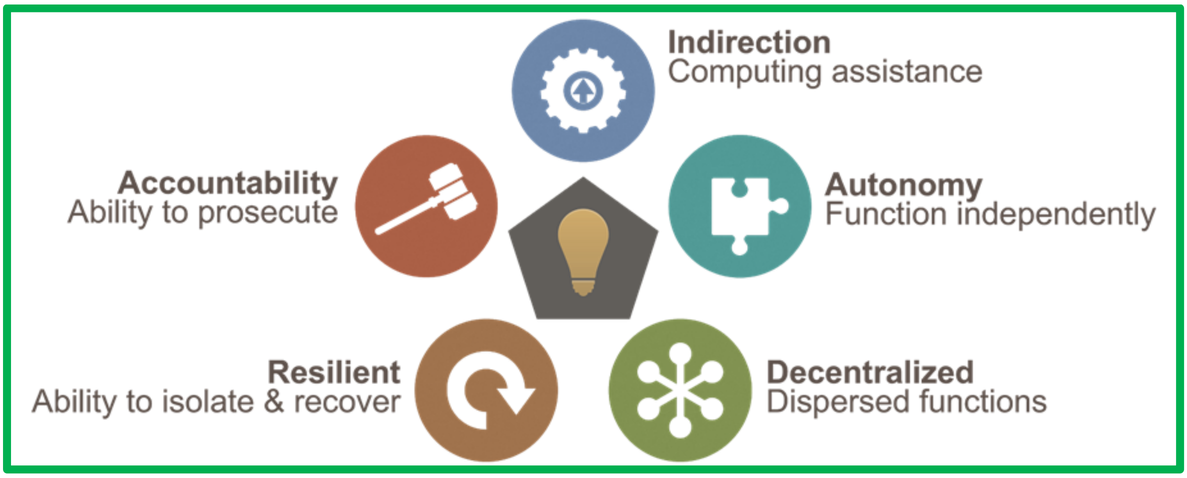
FreshThinking

We are proposing a 3-year regulatory sandbox to experiment and prove this approach. We suggest a Self-Help Groups (SHG) and neighbourhood watch approach based on FreshThinking[2] . FreshThinking advocates a multi-dimensional collaboration and offensive defence as illustrated in Figure 3 Elements of FreshThinking.

[1] http://meity.gov.in/content/national-cyber-security-policy-2013-1

[2] http://www.iotforindia.org/wiki/FreshThinking by IoTForum

Figure 3 Elements of FreshThinking



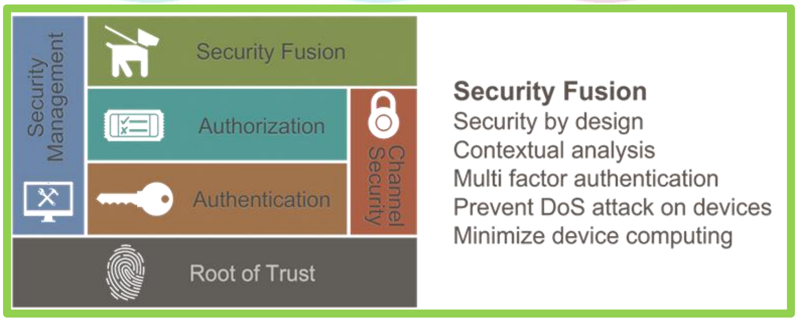
SAFENET

We use the word SAFENET as an indicator of an IoT Network that conforms and allows the ideas suggested. This document is a policy position paper and will not go into implementation details but an Annexure I: A brief outline of Technical implementation of SAFENET (page 22) indicating some ideas on implementing SAFENET and the areas where new technical tools are needed is enclosed.

Major ideas

Cybersecurity is based on four fundamentals Identity, Authentication and Authorization as visualized in Figure 4 Security Fusionand prevention of misuse of functionality

Figure 4 Security Fusion



In our approach the state declares areas of Cyberspace as “Protected System”[3] at different levels (Like a Township, An airport or a hospital complex as in physical space). Some are secured by government organizations like NCIIPC 4 and some use ‘empanelled’ providers. An empanelled provider is a Managed Service Provider (MSP) and can use crowd sourcing, AI and dynamic probability-based techniques to implement protection schemes. We assume a Fog architecture5 and the evolving IEEE Roof standard6 to be followed by the edge network implementations. For offensive defence we expect the regulators to allow some degree of self-defence and action-in-advance before

[3] Sec 2.ze and Sec 70 of IT Act Information Technology Act ITAA amended 2008

an attack progress further. That is ability to prevent is more preferred then forensic ability to establish nature and perpetrator of crime and initiate criminal suit.

1 Use an Identity based Network

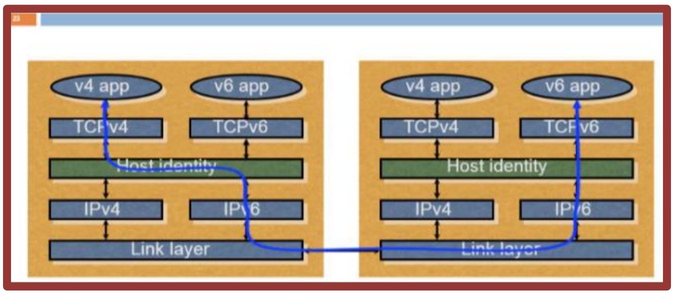
IP address or MAC are insufficient as identity both because they can be spoofed[4] and IoT uses non-Internet protocols also (BLE, LPWAN etc). A Hardware root of trust (HRoT) is needed.

a) Use TEC TSA Model [5]

b) We need a e-KYC of devices as well as users. IP or MAC of the device is insufficient. There are different methods like eUICC and Hardware root of trust (HRoT) like ARM PSA. The industry is evolving and some methods can be provided as options especially for Smart City and Transport and Logistics (Ports, Railways, Grid). Currently setting up device KYC and crypto certificates needs a fair amount of time, is difficult and mis configuration is quite frequent and expensive compared to low cost footprint needed in mass IoT deployment. Recommendations on changed tool set for mass usage of low-cost PKI and Hardware root of trust (HRoT) using ARM PSA[6] , eSIM[7] or UICC etc need to be developed.

c) We assume a Host Identity Protocol (HIP)[8] type will be used across the entire IoT network so that each component i.e. endpoint device, Gateway, Network infrastructure like routers etc are identified by a cryptographic signature and not by IP or MAC or geolocation assumptions. HIP replaces IP address with a Token Host Identity Tag (HIT). HIT is the public key of a crypto based identifier. So HIP [9]overlays a crypto based identity as shown in Figure 5 HIP a waist " Identity layer " over TCP/IP

Figure 5 HIP a waist " Identity layer " over TCP/IP



[4] Spoofing implies change in identity : https://en.wikipedia.org/wiki/MAC_spoofing

[5] http://tec.gov.in/pdf/Studypaper/identity%20management%20approved.pdf

[6] https://developer.arm.com/products/architecture/platform-security-architecture

[7] UICC, eSIM , Secure elements https://www.gemalto.com/mobile/secure-elements

[8] https://tools.ietf.org/html/rfc5201 . See also https://www.temperednetworks.com/blog/what-is-the-host-identity-protocol-and-why-is-it-so-important/

[9] https://datatracker.ietf.org/wg/hip/about/

2 Identity is not sufficient for Authorization

Hackers are migrating to identity theft[10] or impersonation as devices and OS are hardened. Social engineering attacks have led to compromise of the email of CIA director John Brennan[11]. The wide spread use of voice assistants like Alex or spoken commands over IVR call centres interaction introduces Voice-Hacking and spells death of secure physical zones as described by Menny Barzilay[12].

Even Apple has moments of epiphany on cyber theft as described in the "*Apple Is Struggling to Stop A 'Skeleton Key' Hack on Home Wi-Fi*" Forbes Article [13]. Third part accessories use a secure HW key thru Mfi chip.[14] This allows a Mac laptop or desktop to "trust" an IoT Device that is identified thru Mfi technology. Thus, IoT devices can issue commands to other parts of the apple eco system.

> "If you hack a device with MFi, you can use that board to impersonate any host device you want that's enabled with Apple MFi," Bailey explained. "There's no way for an Apple iOS device to guarantee the MFi chip isn't being instrumented for malicious purposes... iOS will automatically provision security keys to the hacked MFi device.

For IoT Devices in semi-public place a new class of attacks is physical tampering, side channel attacks to derive security credentials or replacement. Similarly, with more automated operations where machines issue commands to other machines (M2M), API needs to be identified and secured as well.

In traditional cybersecurity the identity of a "actor" is established thru authentication and leads to access controls like read, write, issue commands. Clearly that fails. We need more as described in Risk based Authorization (Page: 9).

3 Risk based Authorization: A Rose is not a Rose anymore…

Risk based authorization or attribute-based context aware authorization[15] is the most important innovation required in SAFENET. An enterprise example [16] may help. It does not use conventional cyber security perimeter defence approach. Each node is identified and a context-based trust is derived to allow access to another node. Some describe this a Zero-Trust approach.

A node is a combination of

Figure 6 Attribute-Based Access Control (ABAC)

[10] https://simility.com/blog/types-of-identity-theft/

[11] https://www.defenseone.com/threats/2015/10/dont-be-shocked-cia-

[12] https://techcrunch.com/2017/05/23/alexa-dont-talk-to-strangers/

[13] https://www.forbes.com/sites/thomasbrewster/2018/04/26/skeleton-key-exploits-apple-mfi-trust/#1298d8ae503c

[14] https://mfi.apple.com/MFiWeb/getFAQ.action

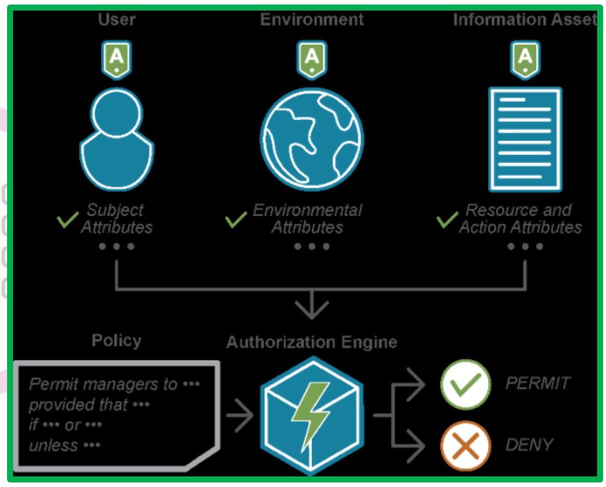
[15] https://www.axiomatics.com/attribute-based-access-control/

[16] Google Beyond Corp is a good case study but our example is not limited by Beyond Corp. https://storage.googleapis.com/pub-tools-public-publication-data/pdf/44860.pdf

- User (All of the system admin , App installer and business user logged in to device)
- Hardware
- Firmware
- OS
- Middleware
- Application (Browser, App, API invoker)

The context is derived from eKYC of the device, the user and state of the device (Is the browser updated?) and past history of usage (Administrators laptops was not used for 2 weeks: Put on low trust) as well as neighbours of the user and state of activity and attacks on the sub net or the SAFENET. See a visualization from Axiomatics in Figure 6 Attribute-Based Access Control (ABAC). The system may assign different trust level to same device

1. Full access
2. No high security functions
3. Only read
4. No access



Unlike traditional passive cybersecurity, SAFENET proposes active defence. If we suspect a device or user, we may initiate a surveillance. All actions of that device Inward and outward) are logged (*A Cyber CCTV spotlight*) and we may take steps to change trust level

If this is suspected anomalous traffic then:

1. Create a deception, place device in a tarpit or send to a simulated honeypot and check malignant behaviour
2. Random disruption of traffic and checks on malignant behaviour
3. Request other devices or gateway in neighbourhood to watch and vote on suspected device
    a. In many context super user functions like changing configuration of a “key” device may need voting by multiple “administrators”
4. Request a physical inspection, replacement
5. Isolate the subnet of devices which may be compromised

This is the ideal authorization capability. Past implementations of Attribute based Access Control (ABAC)[17] in Identity and Access management (IAM) components have not been promising. We assume that in new age of Big Data, machine learning (ML) and more active usage of offensive technology this may be possible and is well worth a pilot. We advocate offensive intelligent gathering (See 5 Anton Piller for obtaining evidence page: 11) and crowd sourced or neighbourhood watch

[17] http://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained

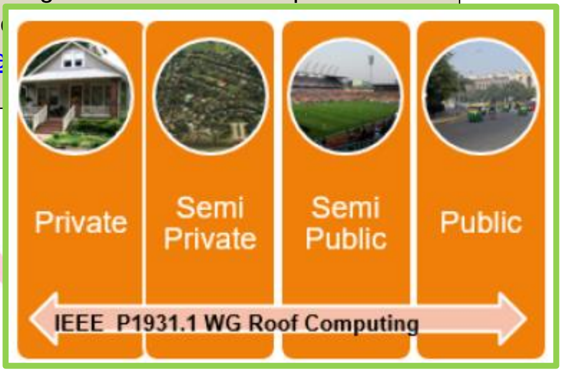
(See 7 Neighbourhood watch and intelligence page: 13) and other methods which would provide data across the entire SAFENET not just one enterprise. ML based dynamic risk driven authorization is a very well-funded new start-up activity

- ✓ 6 AI Cybersecurity Startups to Watch in 2018[18]
- ✓ AI Companies Race To Get Upper Hand In Cybersecurity — Before Hackers Do[19]
- ✓ Exploiting machine learning in cybersecurity[20]

5 Anton Piller for obtaining evidence

In cyber security the effort, expertise and resources required to establish crime is large and probabilistic. One way to reduce this is to allow more frequent use of preventive inspection of a suspect. The law should allow a civilian actor to enter and gather the data and activity trace (investigate) of a “suspected” attacker. An Anton pillar approach needs to become standard method in cybercrime prevention as establishing source and proof is very difficult afterwards

> an Anton Piller order (frequently misspelled Anton Pillar order) is a court order that provides the right to search premises and seize evidence without prior warning. This is intended to prevent the destruction of relevant evidence, particularly in cases of alleg
> infringements. https://en.wikipedia.org/wiki/Anton_Piller_orde



We expect a protocol where the “Victim” submits an electronic request to a designated point under CERT-in with supporting evidence of frequent pings, telnet access, DNS attacks etc and obtains permission (within 15-20 minutes) to ask ISP to cooperate in walling off the alleged attacker and taking snapshot of the device used by attacker within an hour at worst. This capability will require remote access trojan (RAT) and malware to be infected into attacker site under guidelines of cyber-Anton-Piller. The essence of speed and complete blocking of the suspected attacker will severely limit rampant sleeper bots. This offensive capability is necessary. A Traffic police does not wait for an accident but pulls over and tickets suspected bad drivers. There is a chance of false investigation and civil penalties for the victim may be possible and allowed but the right to defend by advance preventive action is a MUST.

6 Self-defence rights in Cyberspace

Cyber Space is more like the Wild West. Self-defence and Community self-help are necessary to manage cyber-attacks and catch cyber criminals. One way to control cyber exploitation is to allow companies to exercise their right to self-defence in cyberspace. As a general legal principle, an entity can defend its property using reasonable force. The exercise of this right generally involves the use of

[18] https://www.nanalyze.com/2017/12/6-ai-cybersecurity-startups-watch-2018/

[19] https://www.investors.com/news/technology/ai-companies-artificial-intelligence-cybersecurity/

[20] https://techcrunch.com/2016/07/01/exploiting-machine-learning-in-cybersecurity/

non-lethal force to neutralize an immediate threat to property. Here, a company could exercise its right to defend property (its computer networks and intellectual property). We propose that Nation states should consider designated parts of cyberspace as Semi-Private or Semi-Public territory. IEEE Roof computing serves as a technical basis of federated management. See ROOF COMPUTING FOR Grouping of IoT devices Page: 18

In the physical world we can see a continuum from private to public places. A retail mall is a semi-public space and a multi tenanted office complex or gated community is a semi private space. A Wimbledon event or a concert may not allow free unrestricted access. Frisking, identification and tactics to keep cars and suitcases far away are deployed.

We propose limited delegation of rights to semi-public and semi-private cyber spaces. So, a multi tenanted cloud provider like Microsoft Azure or Amazon AWS can impose specific restrictions and deny access to suspected attackers even while the facility may be for public use like a diagnostic lab providing remote medical checks. Semi-public places use a low trust approach and take preventive actions on any suspicious behaviour. Deep packet inspection may be a norm

If a set of designated endpoints in the Internet are classified as “secure” and intrusions subject to Indian laws then a range of techniques to find the attacker and impose costs are much higher. Rights of self-defence and ability to inspect visitors and even take punishing action are well established in physical space.

Reducing rampant crime in high seas (piracy) needed a different set of laws and actions to catch criminals before the crime was committed and the pirates disappeared. Cybercrime is similar and a similar legal framework is needed.

An example below shows a US court tested case.

Criminal law has long recognized that citizens are sometimes justified in taking limited measures against criminals. Concepts such as citizen's arrest, self-defence and abatement of a nuisance can serve as defences to allegations that a citizen committed a crime when reacting to criminal activity. These concepts support reasonable actions by citizens, which are in proportion to the threat. A related idea in criminal law is that of *consent*. If someone consents to you coming onto their property, then you are not committing the crime of trespass when you do enter the property. Consent was a relevant factor when a University of Wisconsin system administrator hacked into the personal computer of a student. According to a federal appeals court, the student consented to the hack.

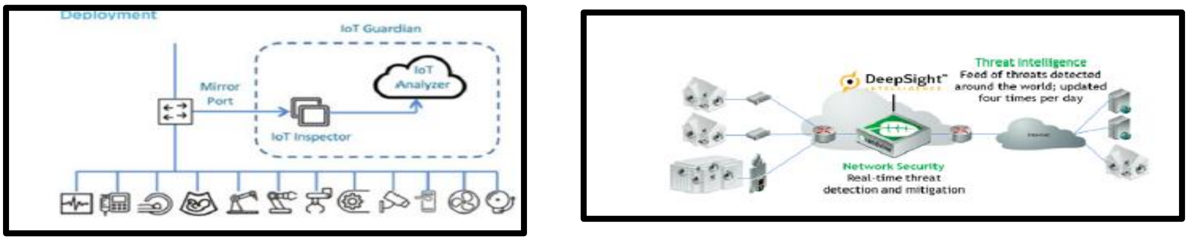
"If you access our site in connection with an effort to engage in phishing, then you consent to us surveilling, harassing and retaliating against your phishing activities." With terms like these, the bank is compiling evidence that it is within its rights to spy on phishers targeting it and to stuff their phishing sites with junk data. The bank is building the case that its justified security measures do not violate laws

http://www.sans.edu/research/leadership-laboratory/article/cyber-consent

7 Neighbourhood watch and intelligence

A large number of new cybersecurity start-ups especially from Israel are proposing a local network-based AI or machine learning approach as illustrated in Figure 7 Subnet Intelligence the new theme to detect compromised devices. Key is sharing data among neighbours.

Figure 7 Subnet Intelligence the new theme


Deployment
IoT Guardian
Mirror Port
IoT Analyzer
IoT Inspector
DeepSight
Threat Intelligence
Feed of threats detected around the world; updated four times per day
Network Security
Real-time threat detection and mitigation

We suggest a semi-public or semi-private cyberspace like IoT network should do this actively and in well-advertised fashion. We are encouraging decentralized resident-based policing as a way to reduce cyber-crime. Neighbourhood watch and Town watch[21] were popular in older times when modern cities with a new governance and police authority did not take over.

An example of local data and collaboration is the case of **Wirex** botnet. This suggest ability to share data, intelligence and act jointly in smaller groups (Neighbourhood)

> Researchers from Akamai, Cloudflare, Flashpoint, Google, Oracle Dyn, RiskIQ, Team Cymru, and other organizations cooperated to combat this botnet. Evidence indicates that the botnet may have been active as early as August 2nd, but it was the attacks on August 17th that drew the attention of these organizations. This post represents the combined knowledge and efforts of the researchers working to share information about a botnet in the best interest of the internet community as a whole. This blog post was written together by researchers from numerous organizations and released concurrently by Akamai, Cloudflare, Flashpoint, and RiskIQ.
>
> https://blog.cloudflare.com/the-wirex-botnet/

[21] https://en.wikipedia.org/wiki/Neighborhood_watch

8 Reducing profitability of hackers

The New York Times carried an interesting piece: Banks Adopt Military-Style Tactics to Fight Cybercrime[22]. Extracts are very important to get to the essence of the cybercrime

> Banks Adopt Military-Style Tactics to Fight Cybercrime
>
> Cybercrime is one of the world’s fastest-growing and most lucrative industries. At least $445 billion was lost last year, up around 30 percent from just three years earlier, a global economic study found, and the Treasury Department recently designated cyberattacks as one of the greatest risks to the American financial sector. For banks and payment companies, the fight feels like a war — and they’re responding with an increasingly militarized approach.
>
> …..
>
> “This is not that different from terrorists and drug cartels,” Matt Nyman, the command center’s creator, said as he surveyed his squadron of Mastercard employees. “Fundamentally, threat networks operate in similar ways.”
>
> ……
>
> Former government cyberspies, soldiers and counterintelligence officials now dominate the top ranks of banks’ security teams. They’ve brought to their new jobs the tools and techniques used for national defense: combat exercises, intelligence hubs modeled on those used in counterterrorism work and threat analysts who monitor the internet’s shadowy corners.
>
> ……
>
> Cybersecurity has, for many financial company chiefs, become their biggest fear, eclipsing issues like regulation and the economy.

HBR covers this in How a Cyber Attack Could Cause the Next Financial Crisis[23]

Unless the profitability of cybercrime is drastically reduced we are only storing up bigger more rampant mass criminal attacks all over. Current cybersecurity is passive defence and with rapid success by hackers (a 1 in 100 chance is very lucrative) the threat level and number of vulnerabilities has exploded.

[22] https://www.nytimes.com/2018/05/20/business/banks-cyber-security-military.html

[23] https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis

The Ever-Growing Threat of Unknowns

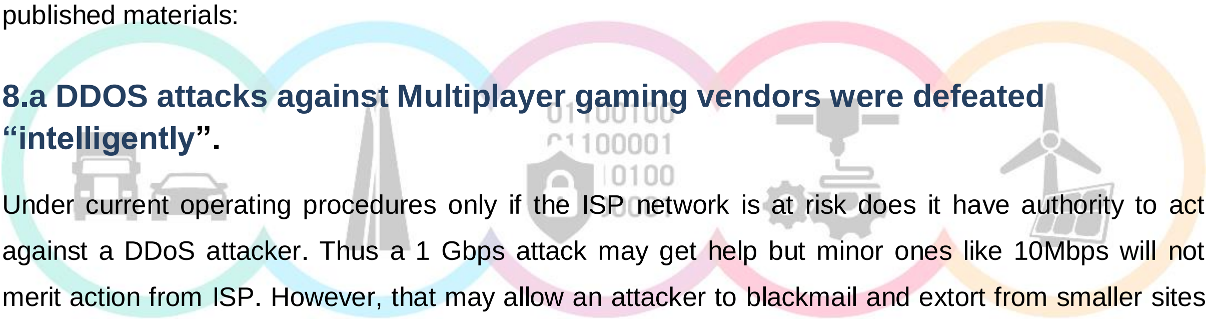
Yet, the demand for beating the threat of unknowns is only getting bigger as the threat continues to grow at a dizzying pace. Consider these staggering stats, for example:

- There are over 100 unknown malware attacks hitting an organization every hour; and
- Over 360,000 new malicious files appearing daily.

It's no surprise, then, that in a recent report, it was found that of the 300 global IT and InfoSec professionals surveyed, 49% believe that unknown malware is the greatest risk to their organization.

http://bit.ly/2D5Rmgf

There are many initiatives to manage this Cambrian explosion of cybercriminal behaviour. *The traditional (which is not working) is asking for more quality and Security be Design, placing legal requirements and creating a liability driven legal regime where responsibility is placed at only a few actors in the supply chain.* However new ways are emerging and here are some extracts from published materials:



8.a DDOS attacks against Multiplayer gaming vendors were defeated "intelligently".

Under current operating procedures only if the ISP network is at risk does it have authority to act against a DDoS attacker. Thus a 1 Gbps attack may get help but minor ones like 10Mbps will not merit action from ISP. However, that may allow an attacker to blackmail and extort from smaller sites that may suffer business. An example is multiplayer games who used to lose customers when games became slow or erratic under DDoS

"A more elegant and faster approach exists using software-based multi-dimensional analytics, making detection more precise. They combine real-time network telemetry with advanced network analytics and other data such as DNS and BGP (among others) to see down to the source of attack traffic in real time. Armed with this kind of analysis, it becomes possible to create simple, effective filters at the peering edge of the network for the zombie PCs, IoT devices and/or cloud servers that are carrying out the attack. The offending traffic doesn't have to be sent to the scrubbers; it is simply blocked at the edge."

See https://venturebeat.com/2017/12/10/gaming-companies-outsmart-ddos-attack-with-new-software-security-solutions/

This is a key idea of FreshThinking that the peer edge of the community exercises lot of intelligent control. IoT networks should not allow connection from any place that is not white-listed. The sending ISP should be white listed and sender needs to be white listed. This type of advanced edge surveillance will greatly reduce sleeper bots' action and discourage small time hackers.

8.b Deception based offensive defence

As noted by Dan Woods in a Forbes[24] article

> Deception technology gives defenders a rare advantage against attackers by doing something that other forms of cybersecurity don't: Provide early and accurate detection by laying a minefield of attractive decoy systems and content to trip up attackers. This is all done within the organization's networks and serves as a high-fidelity warning system of attacks that have bypassed perimeter security controls.

8.c Hack back Posture:

Google and JP Morgan have quietly adopted policies to attack back at foreign state hackers. Hannah Kuchler of the Financial Times in July 27 2015 article *Cyber insecurity: Hacking back*[25] reports that many organizations are fed up with the deteriorating cyber security environment and moving to legal or illegal offensive methods. Google has been at the forefront of this approach and fairly open and public.

"it's pretty awesome: If you hack Google, they will hack your ass right back." Matt Buchanan,GIZMODO[26]

8.d Presidential Policy Directive 20

Now the Trump lead US Government joins the fray with a new "gloves-off" policy by reducing Presidential Policy Directive 20, or as its often referred to PPD 20.

> President Donald Trump has eliminated rules governing the process for launching cyberattacks, giving the military freer rein to deploy its advanced hacking tools without pushback from the State Department and the intelligence community. Trump's decision, the latest example of his desire to push decision-making authority down the chain of command, could empower military officials to launch more frequent and more aggressive cyberattacks against adversaries like Russia and Iran.
>
> https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095

9 Faster administrative action for frequent crimes

On the internet it takes a few days before hackers start probing an IP address and tools like Shodan [27]etc help in a directory of devices (webcam, CISCO routers, Acid pumps in swimming pools, Traffic signals, SCAD machines, Power plants…). See Figure 8 Shodan the IoT devices directory

[24] http://bit.ly/2NnSEIj

[25] https://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d#axzz3iKYhVbjq

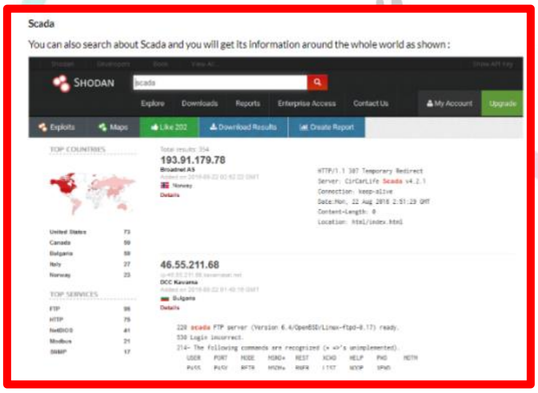
[26] https://gizmodo.com/5449037/google-hacked-the-chinese-hackers-right-back

Figure 8 Shodan the IoT devices directory

If a device of host suffers several pings, telnet or ssh attempts it may be acceptable to not just deny but to act against the intimidator. A simpler method to document such attempts and a "automatic" approval for the IoT Network manager to shut access to the network by the intimidator is a stronger broken-windows theory action. This will impose costs and require more effort by attackers reducing volume of attacks.

Similarly, a DoS attack is difficult for an endpoint or a host. Again, using laws of rioting and public order a Sec 144 type of ban or mass action is possible. In IoT Network the operator or SAFENET provider should have authority to shut down attackers even if the network as a whole is not affected but only a specific device is targeted. For example, a 100Mbps attack on a hospital MRA equipment would be a small pin prick for the large network but requires too much skill and effort by the hospital. If the SAFENET manager can be allowed to declare a Sec 144 for a local neighbourhood a sub- sub-net and terminate the attackers access to the IoT network it is more effective. *Again, a security stance which is well communicated and acted upon reduces incentives for criminals*.

It may be argued that many compromised devices may be denied access as the owner may not be aware that the device they have has been taken over by a criminal. This is possible and technical ways to determine the command centre and acting on the command centre may be better but preventive action reducing success of DDoS will reduce incentives for rampant DoS attacks.



Scada

You can also search about Scada and you will get its information around the whole world as shown :

```
HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.2.1
Connection: keep-alive
Date:Mon, 22 Aug 2018 2:51:29 GMT
Content-Length: 0
Location: html/index.html
```

```
220 scada FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
530 Login incorrect.
214- The following commands are recognized (* =>'s unimplemented).
   USER    PORT    MODE    MSND*   REST    XCWD    HELP    PWD     MDTM
   PASS    PASV    RETR    MSOM*   RNFR    LIST    NOOP    SPWD
```

As an analogy Traffic Police does not wait for an accident but can pull over and ticket a rash driver or impound a car. Sometimes the owner is not involved. It may be driver or unauthorized driver. The law is clear. The parties may be joint and severely liable. The traffic officer does not need prior court approval or act as a judicial officer. A simple, fast administrative procedure for SAFENET to act like a traffic police and shut down and impound "offensive" devices and bot is proposed. The ultimate authority will flow from CERT-in under section 70 of ITAA (2008). A device /owner wrongly impounded may follow a simple administrative process to get relief. But there is no liability or pushback on SAFENET to act prematurely. This is a basic posture that SAFETY AND SECURITY precede other rights in IoT where life and death are consequences of hack.

10 SAFENET and IEEE ROOF: A simple sketch

At high level, SAFENET is a federated technology / administrative / legal framework for managing IoT security in India. At the core of SAFENET is a proposal that uses self-help groups (SHG) to help achieve security / privacy for the overall IoT network in India. It is a distributed, hierarchical framework for IoT security evolved from the Open Fog Consortium approach. The concept of SAFENET is based

[27] http://www.hackingarticles.in/shodan-search-engine-hackers-beginner-tutorial/

on a principle of neighbourhood ***watch*** and the principle of ***Anton Piller.*** At a conceptual level, SAFENET achieves IoT security monitoring and prevention using three core steps at a high level

1. Hierarchal grouping of IoT devices and neighbourhood watch principles using Fog Architecture. This is further elaborated in technical project 3 Segmenting network later

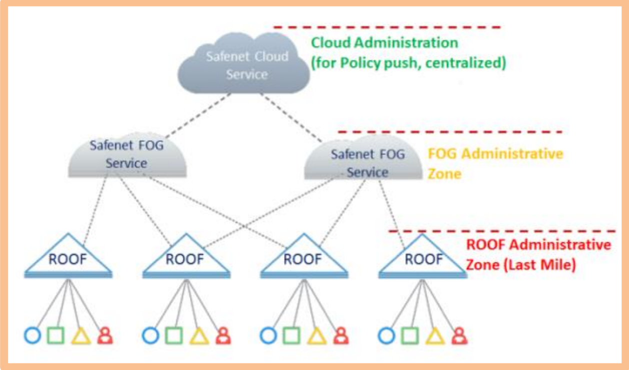


Figure 9 Creating Administrative Zones using Roof Computing

2. Analysing and reporting malicious behaviour by SAFENET managed service providers using a proposed IEEE ROOF standard under development

3. Self Help Groups that help achieve the federated structure of SAFENET

ROOF COMPUTING FOR Grouping of IoT devices

Real Time Onsite Operational Facilitation (ROOF COMPUTING) is an upcoming IEEE Standard 1931.1 that defines protocols, framework and standards for technical and functional interoperability for IoT systems that operate and co-operate in a secure and independent manner within the context of a local environment such as home, factory, office or airport, etc. In the context of SAFENET, multiple IoT devices are grouped together to form a ROOF. Each roof defines an administrative zone as shown in Figure 9 Creating Administrative Zones using Roof Computing . SAFENET aims to define the Fog architecture that is (a) secure (b) federated (c) privacy aware (d) provides role-based access (e) provide Intrusion detection & prevention methods (f) AAA functionality (g) alert services to name a few. In addition, the architecture is hierarchical, with each hierarchy will have SLAs in terms of response times. In principle the SAFENET will be Fog service that will be a combination and intelligent integration of self-developed / open source / and commercially available tool chains. One of the responsibilities of the Self-Help Group is to keep a watch on respective analytics from different administrative zones defined by the Roof computing architecture (and the devices within it), and report any abnormal behaviour to appropriate users / organizations or legal entities. SAFENET working group aims to develop this administrative / legal framework of reporting / logging incidents on the Fog layers

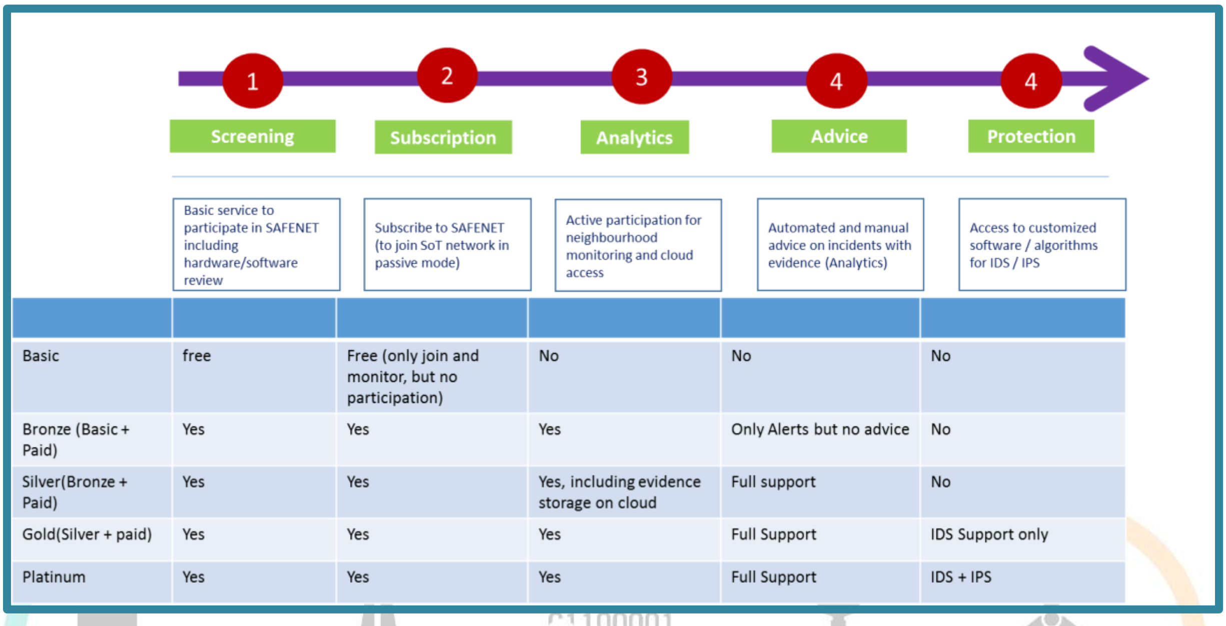
SAFENET aims to propose policies for grouping. The grouping can be at a level of functionality like “camera devices” or locality like “all devices within 100 meters of the Airport” or domains like “environment monitoring devices”.

Each Roof is a semi-public / semi-private IoT network. Anyone who has signed up for SAFENET can join a group / roof. Joining the Roof is a voting protocol, where majority of the devices within the Roof have to agree of a device joining or leaving the network.

SAFENET FREEMIUM

SAFENET proposes the use of ***Freemium business*** model to access the services offered by SAFENET. A conceptual view of the freemium business model in Figure 10 Conceptual Freemium Business Model for SAFENET.

Figure 10 Conceptual Freemium Business Model for SAFENET



Basic service to participate in SAFENET including hardware/software review

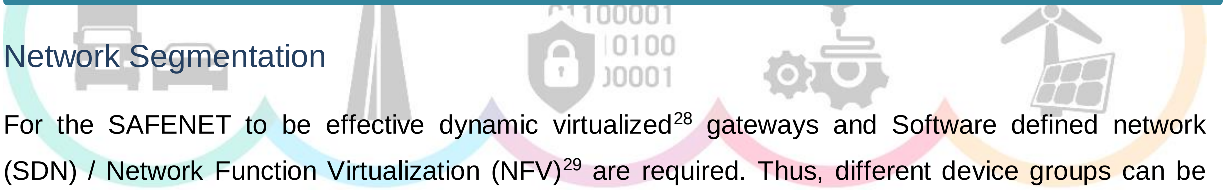
Subscribe to SAFENET (to join SoT network in passive mode)

Active participation for neighbourhood monitoring and cloud access

Automated and manual advice on incidents with evidence (Analytics)

Access to customized software / algorithms for IDS / IPS

Basic	free	Free (only join and monitor, but no participation)	No	No	No
Bronze (Basic + Paid)	Yes	Yes	Yes	Only Alerts but no advice	No
Silver(Bronze + Paid)	Yes	Yes	Yes, including evidence storage on cloud	Full support	No
Gold(Silver + paid)	Yes	Yes	Yes	Full Support	IDS Support only
Platinum	Yes	Yes	Yes	Full Support	IDS + IPS



Network Segmentation

For the SAFENET to be effective dynamic virtualized[28] gateways and Software defined network (SDN) / Network Function Virtualization (NFV)[29] are required. Thus, different device groups can be apportioned in virtual segments. Suspected compromised devices can be walled off and subjected to surveillance of all outgoing and incoming traffic with deep packet inspection. The network should provide the following facilities:

a) Ease of device configuration QR code, BARCODE

b) Ability to isolate IoT devices from public internet; avoid compromised device from building intranet weakness esp. shared symmetric key case

c) Ability to dynamically re configure the IoT Network to respond to threats from targeted DDoS just for this subnet etc

d) Assist in deploying deception (Honeypots) to gather intelligence

e) Log "sensitive" traffic, changes in device configuration. Failed logins etc

[28] https://www.lifewire.com/virtual-machine-4147598

[29] https://www.webopedia.com/TERM/N/nfv-network-functions-virtualization.html

Issues

The basic ideas elaborated in this paper have been discussed earlier and have had some “standard” objection.

The first public presentation of FreshThinking was at IoTNext[30] on Nov 9th 2017, Bangalore and covered in IoTWiki[31] . Subsequently these ideas have been discussed in various forums and the three main concerns or questions are follows:

A. Feasible

A common question is more technical feasibility. Many of the requirements stated here will need new tools and some innovation. *Cyber Anton Piller* is an example. That is the research agenda in the sandboxed 3 year project.

B. Offensive

Most lawyers and cyber security professionals are had wired to object to offensive methods in Cyber security. The dogmatic response is to beef up security, train and retrain staff and deploy even more expensive and difficult to manage cybersecurity tools and consultancy. Our position is we are living in a *#Brexit, #Trumpit* world and what is not working cannot be the only effort in protecting in a war we are losing with cybercriminals. In all such situation proportionate offense is well established and used. Why should cybersecurity be a holy cow where attackers are “protected” and victims are “handicapped”

C. Vulnerability a Security issue?

One of the confusions in cyber security is to assume any vulnerability is a cybersecurity issues and “expensive” methods and tools must be used and someone should be liable. The liability is always the victim side rarely the oppressor. In the physical world a pick pocketer can steal your wallet at many places. An attacker can catch you in a hotel lobby or in a shopping mall. We do not expect the Mall operator or the Hotel to be the solely liable. There is an expectation that the community will help and the attacker may be caught, identified and punished with high probability. So vulnerability in physical world does not normally mean a expensive fortification of the Hotel or the Mall or the recommendation to the consumer to wear latest 6 inch bullet proof armour [3 inch armour was no longer safe].

D. Gold plated IoT

A underlying issue is that IoT devices and solutions need a much lower price point for mass adoption in India. We need to reduce cost of safety by reducing profits of attackers not by making IoT too expensive. An example would be the consequences of gold plating is defined benefit pensions schemes. Thru much of USA and UK over years more and more stringent legislative costs were

[30] Presentation at IoTnext 2017 https://www.youtube.com/watch?v=ndLvhuaRVyE

[31] http://www.iotforindia.org/wiki/FreshThinking

added to defined benefit pension scheme. Many large companies including GM[32] went thru a near death experience and re-structuring

E. Privacy

A vast share of Cybersecurity and lawyers are hardwired to mix privacy with Security. Deep packet inspection raises objections. Our response is Safety and Security are related. Privacy is not a security issue. Safety is. We need not apply a liability regime of Anglo-Saxon economy to India. Privacy needs are different in different context. In a war or a disaster where thousands are at risk of death personal privacy will take a lower importance. In many commercial contracts the buyer has not been willing to pay "unreasonable expenses" for adding privacy. Gold plated requirements need to be questioned.

For medical devices there is a limited need for "privacy" and it should be possible to meet them.

F. Hackers are wining: We must change

Thursday 20th September 2018 CNBC India TV interview[33] reported this

> Jamie Dimon says cyber warfare is the biggest risk to the financial system.
>
> "We have to make sure because cyber — terrorist and cyber countries — they could cause real damage. We're already spending a lot of money and J.P. Morgan is secure but we should really worry about that," Dimon told CNBC-TV18's Shereen Bhan in New Delhi.
>
> Dimon put inflation running too hot as his second biggest concern, warning the reactionary raising of interest rates from the U.S. Federal Reserve could be the cause of a "traditional" recession.
>
> https://www.cnbc.com/2018/09/20/jp-morgan-jamie-dimon-says-cyber-is-biggest-risk-to-the-financial-system.html

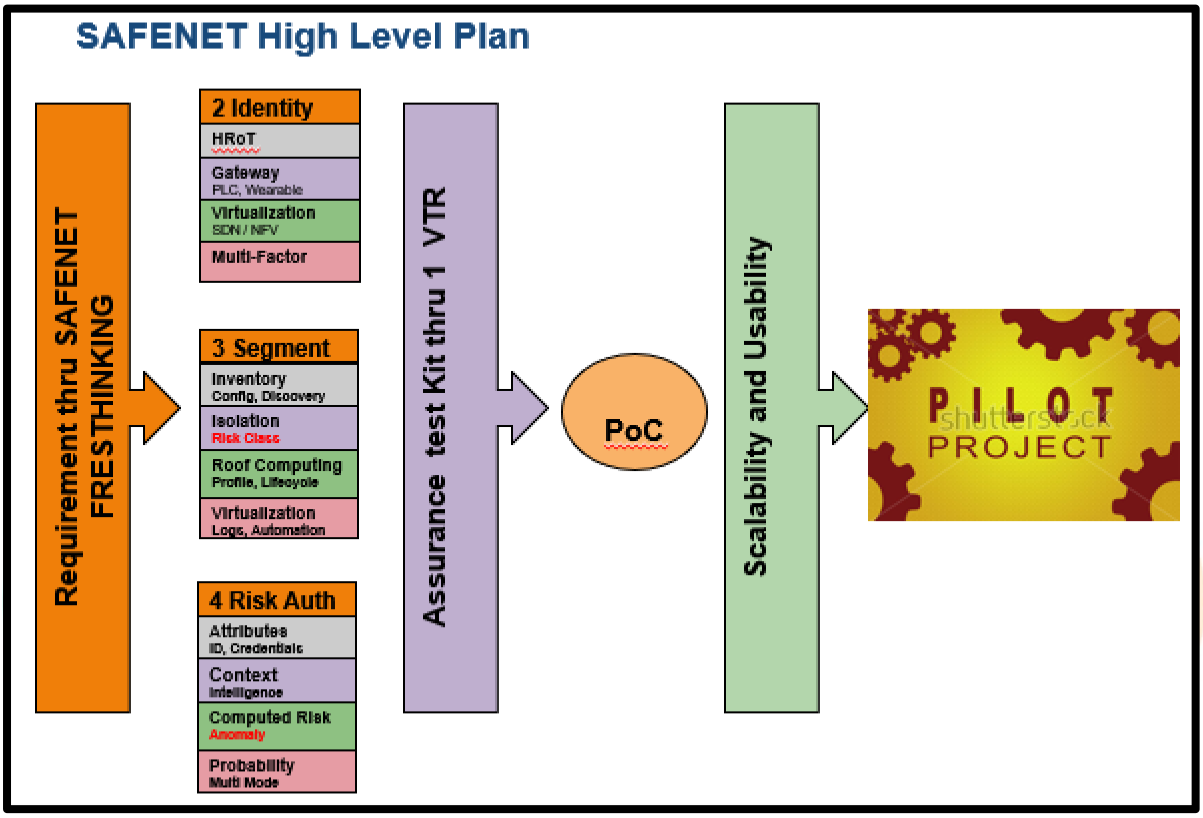
Hackers are winning the cyberwar and urgent major change in our approach to security is needed. This approach paper elaborates some of them. Much will be learnt by experimenting under a sandbox provided.

[32] GM's Pension: A Ticking Time Bomb for Taxpayers? http://content.time.com/time/business/article/0,8599,1981958,00.html
[33] https://www.cnbc.com/video/2018/09/20/biggest-vulnerability-today-is-cyber-jpmorgan-ceo-says.html

Annexure I: A brief outline of Technical implementation of SAFENET

We assume following (technical) projects once the SAFENET gets approval. These will be designed and developed in subsequent year 2 and deployed in a Proof of Concept (PoC) in Year 3. After PoC a Pilot in a semi-public and semi-private facility before industrialization in year 4 and rollout subsequently. A high-level view is shown in Figure 11 Project Roadmap.

Figure 11 Project Roadmap



I.A Projects

1 Vulnerability/Threat/Risk (VRT) Model

a. Builds on NCIIPC PC6 Vulnerability/Threat/Risk (VTR) Assessment and industry standard methods to create IoT and India specific vulnerability and threat model.

b. This will also be used for assurance of the other projects and blocks.

c. We use 3 layers to group VTR.

   i. Physical layer is important and somewhat new in IoT from cybersecurity as devices are in semi-public or public places outside Data centre and "employees" and subject to tampering, replacement or side channel attacks

   ii. IoT Network use Bluetooth and protocols apart from TCP/IP and UDP. These like Zwave, Zigbee, LoRa have their own needs. Also, we have brownfield industrial machines like SCADA and PLC as endpoints

iii. API. In M2M there is a significant automation with devices issuing commands. These are done thru API calls and in the past, they have not been well secured.

2 Identity and Authentication

a) Use TEC TSA Model [34]

b) Currently setting up device KYC and crypto certificates needs a fair amount of time, is difficult and mis configuration is quite frequent and expensive compared to low cost footprint needed in mass IoT deployment. Recommendations on mass usage of low-cost PKI and Hardware root of trust (HRoT) using ARM PSA, eSIM or UICC etc

c) Techniques for multi factor authentication using in band and out of band (OOB) on same device, multi device voting (Like using 3 controllers in a space flight to decide shifts).

d) Recommendation of N:N authentication where a IoT Sensor may participate in multiple domains with multiple stakeholders

3 Segmented Network

a) Inventory of devices, applications and network components identification and management at decentralized level

b) Ease of device configuration QR code, BARCODE

c) Ability to isolate IoT devices from public internet; avoid compromised device from building intranet weakness esp shared symmetric key case

d) Ability to dynamically re configure the IoT Network to respond to threats from targeted DDoS just for this subnet etc

e) Assist in deploying deception (Honeypots) to gather intelligence

f) Logging of Device operations, configuration and failed actions

g) For IoT Devices in semi-public place more capability for “Forensic Memory analysis” IoC (Indicator of Compromise)

4 Risk Based Authorization

a) Use of Digital Trace across the entire spectrum and forensic as well as anticipatory like in

b) Dynamic Assessment of threat and risk to sub net or Network

c) Identity Authentication should have a confidence level based on context or attributes of users, application, network and devices with history

d) Adapt STIX 'Structured Threat Information Expression’ and TAXII ‘Trusted Automated Exchange of Indicator Information'

e) MUD Manufacturers Usage Description standard for managing remote asset servicing

f) Multi device Authorization

[34] 1 Use an Identity based Network Page 5

g) Anomaly detection at subnet level using machine learning with user and entity behaviour analytics ("UEBA") as a probabilistic identifier

I.B SAFENET

a) A walled garden for specific class of devices and users based on new techno-legal approach

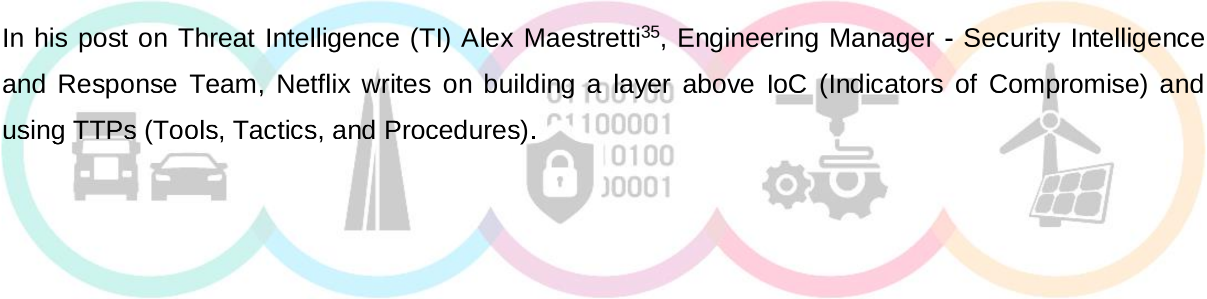
b) Due to high frequency of cyberattacks we are assuming a new legal frame where prevention takes precedence of after the crime investigation and proceedings. This assumes that probability-based risk assessment can be used to investigate activity and impose isolation or deny access and usage much like actions taken by police to curb bad driving or deny crowd and riots formation

c) A decentralized self-help groups (SHG) acting as neighbourhood watch. This reduces “event noise” at a National central command centre and allows different experiments as different places for different types of threats.

I.C AI/ML in Risk based Authorization

Patterns detection versus Indicators of Compromise detection

In his post on Threat Intelligence (TI) Alex Maestretti[35], Engineering Manager - Security Intelligence and Response Team, Netflix writes on building a layer above IoC (Indicators of Compromise) and using TTPs (Tools, Tactics, and Procedures).



[35] uses the monicker “Architect of devious but principled security solutions”

TTPs versus IOCs

It has been said that every problem in computer science can be solved with another level of abstraction. In a way you can consider TTPs (Tools, Tactics, and Procedures) an abstraction layer over IOCs. With TTPs we can find enough applicable commonalities regardless of attack(er) type to make the case that TTPs and *not* IOCs should be the primary goal of TI. TTPs encapsulate the general modus operandi of a given actor or even more generally of a class of actor. These will always be useful to understand, both for red teams to model and for defenders to build controls against (detective and preventative).

Whereas an IOC might be a hash of a specific RAT, the *tool* model would be the concept of the RAT itself regardless of how it is packed. The *techniques* would be the type of operations the RAT enabled, the way it established command and control communications, how it establishes persistence, and the like. The *procedures* would be the use of this RAT as part of the attacker’s post exploitation runbook. Taken together this intelligence provides a strong direction regarding where to look, but is not limited by a specific value for which to look for.

TTPs have been *de rigueur* for some time now, but sharing still occurs largely through storytelling. TTPs do not lend themselves to machine readable formats in the way IOCs do. There has been recent progress adopting taxonomies like MITRE ATT&CK to talk about TTPs more efficiently, but work remains to be done towards automated sharing. Ultimately I would love to see something like Palantir's ADS as a medium for *sharing TTPs by sharing detection strategies* for them, perhaps all the way to detection code (yara?) if we could agree on a generalized rules engine and solve some stubborn data schema issues - or perhaps abstract to a common Event Query Language as Endgame suggests. I would propose that the future of TI sharing is at the nexus of intelligence and detection engineering.

https://www.linkedin.com/pulse/evolution-iocs-alex-maestretti/

Ben Dickson notes lucrative sale in the dark web of stolen identities and says

“*Behavioural analytics*

One of the benefits of AI algorithms in user account security is that they can find potentially compromised accounts in real time without breaking the user experience. Deep learning algorithms can create a model of a user’s behavior by analyzing the way the user interacts with a platform, such as login times, IP addresses, devices, or even more detailed actions such as typing, clicking and scrolling habits or the use of keyboard shortcuts.

Afterward, AI algorithms will transparently monitor future interactions through the same account and flag or block behavior that deviates from the established baseline. The process is called adaptive authentication or risk-based authentication, and requires users to perform extra authentication and identity verification steps only if the application's AI algorithms deem their behavior as suspicious.

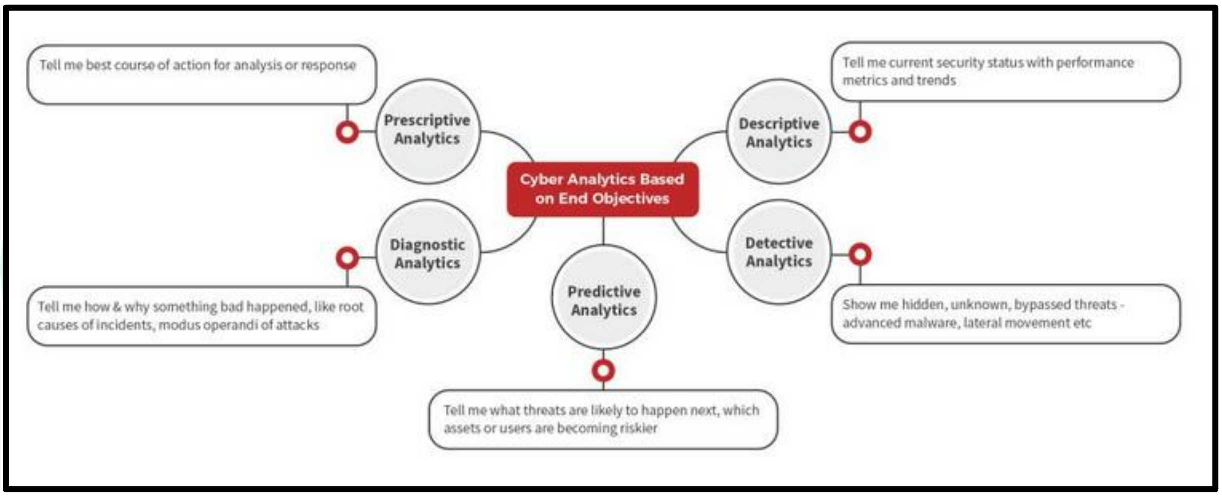
https://thenextweb.com/artificial-intelligence/2018/07/13/authentication-cybersecurity/

Machine Learning in Risk Based Authorization

We outline the project research agenda. One common issue is getting enough data. Anomaly detection is a poor use case for ML as its in rare occurrence. We assume we can create more data thru deception-based intervention and more emphasis on Reinforcement learning rather than classification. As pilots scale we expect to develop methods for pooling data from private and public parties under CERT-in.

There are many expectations from Analytics/(AI/ML) in cybersecurity as visualized in Figure 12 Objectives of AI/ML in Cybersecurity

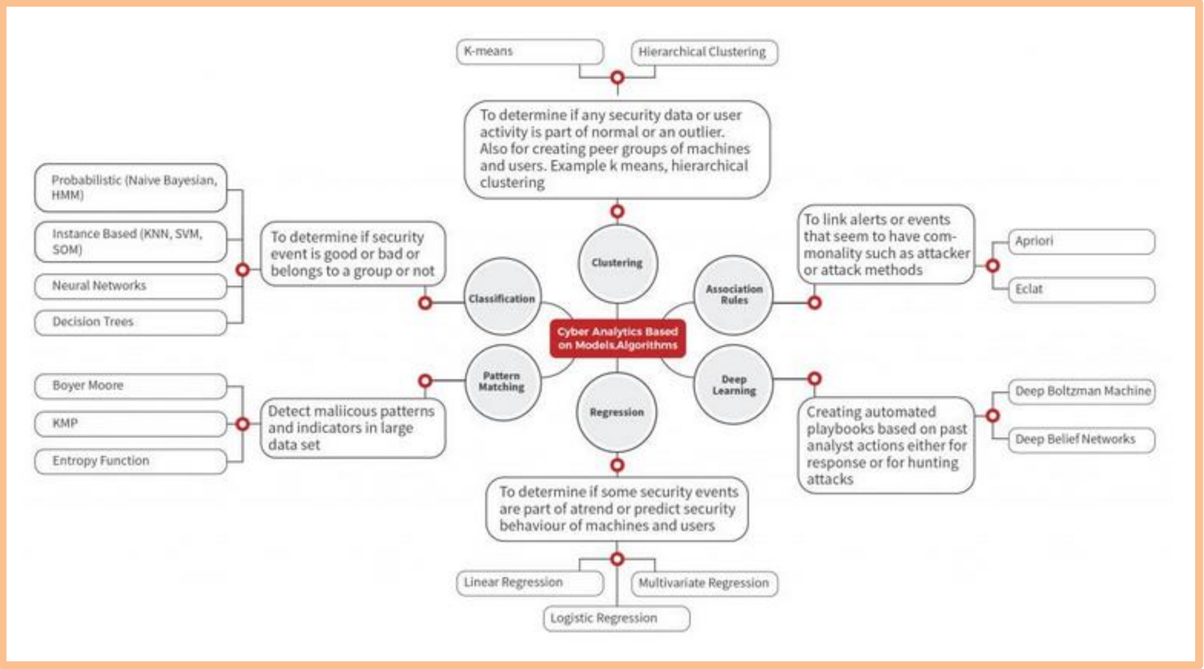
Figure 12 Objectives of AI/ML in Cybersecurity


Cyber Analytics Based on End Objectives
Prescriptive Analytics
Tell me best course of action for analysis or response
Descriptive Analytics
Tell me current security status with performance metrics and trends
Diagnostic Analytics
Tell me how & why something bad happened, like root causes of incidents, modus operandi of attacks
Detective Analytics
Show me hidden, unknown, bypassed threats - advanced malware, lateral movement etc
Predictive Analytics
Tell me what threats are likely to happen next, which assets or users are becoming riskier

There are three classes of machine learning techniques: (i) supervised, (ii) unsupervised and (iii) reinforcement. Unsupervised is useful for data mining as this will unearth the pattern in the data by various techniques such as clustering etc. Supervised learning requires a true model that would be learnt from existing data and then a new data can be predicted. In case of security, its primarily would be used for classification. Reinforcement learning, on the other hand can learn with time and does not require a complete training set to be available. The key is to use three different ML techniques as appropriate for the task in hand.

A common pattern of ML usage in cybersecurity is shown in Figure 13 ML options in

Figure 13 ML options in Cybersecurity


K-means
Hierarchical Clustering
To determine if any security data or user activity is part of normal or an outlier. Also for creating peer groups of machines and users. Example k means, hierarchical clustering
Probabilistic (Naive Bayesian, HMM)
Instance Based (KNN, SVM, SOM)
Neural Networks
Decision Trees
To determine if security event is good or bad or belongs to a group or not
Clustering
Classification
Association Rules
To link alerts or events that seem to have com-monality such as attacker or attack methods
Apriori
Eclat
Cyber Analytics Based on Models,Algorithms
Pattern Matching
Regression
Deep Learning
Boyer Moore
KMP
Entropy Function
Detect maliicous patterns and indicators in large data set
Creating automated playbooks based on past analyst actions either for response or for hunting attacks
Deep Boltzman Machine
Deep Belief Networks
To determine if some security events are part of atrend or predict security behaviour of machines and users
Linear Regression
Multivariate Regression
Logistic Regression

About IET India

The IET is one of the world's largest engineering institutions with over 168,000 members in 150 countries. It is also the most multidisciplinary – to reflect the increasingly diverse nature of engineering in the 21st century.

The IET is working to engineer a better world by inspiring, informing and influencing our members, engineers and technicians, and all those who are touched by, or touch, the work of engineers. The IET office started operations in India in 2006, in Bangalore. Today, we have over 13,000 members and have the largest membership base for the IET outside of the UK. Our strategy is to deliver activities that have an impact on overall competency and skill levels within the Indian engineering community and to play an influencing role with industry in relation to technology innovation and solving problems of public importance.

We plan to achieve this through working in partnership with industry, academia and government, focussing on the application of practical skills within the learning & career lifecycles (particularly early career), and from driving innovation and thought leadership through high impact sector activities.

The technologies that we have chosen to focus on are:

a. The Internet of Things (IoT)

b. Future of Mobility and Transport

To drive this focus forward, we have created volunteer-led panels for each.

The IET IoT Panel

One of the most important technologies that will connect all sectors will be Internet of Things (IoT). With 1.9bn devices expected to be connected in India alone, by 2023, IoT and related technologies assume relevance of significant proportions. Across sectors we will see energy, power grids, vehicles, homes, entire cities and manufacturing floors, computers and mobile devices being connected.

Leveraging its position as a multi-disciplinary organisation, IET India launched its IoT panel on February 20, 2015 with Dr Rishi Bhatnagar (President – Aeris Communication) as the Chairperson. The panel, being a first of its kind in India, focuses not only on technology but the application aspect of IoT in various segments.

The focus is to facilitate discussions that will help in making the inevitable connected world more efficient, smart, innovative and safe. It will focus on technology, security and regulatory concerns and the need for nurturing capabilities and talent for a quicker adoption of IoT in all spheres. The panel also constitutes sub panels / working groups focusing on the application of IoT in Agriculture, Retail, Energy and Healthcare domains. Each of these sub panels will work towards undertaking neutral pilots and studies and publishing white papers around the application of IoT in the respective domains.

The IET India IoT Panel will provide a platform for stakeholders to participate in becoming an authoritative, but neutral voice for the evolving movement of IoT in India. It aims to enable all the IoT practitioners (including people from the hardware – devices, portables, sensors, software, business) and IoT enablers (including people from regulatory area, training area, investors in IoT, end users) to work together on relevant areas to make this industry efficient as well as robust. The panel envisions laying a solid foundation by supporting policy makers, industry in the next step of adoption of IoT.

The panel works through Working Groups - Healthcare, Social Impact, Telecom, Smart Living, Skills, Standards, Regulatory & Legal, Cyber Security, Ganga Rejuvenation and Energy.

Read more on http://www.theiet.in/IoTPanel

If you are interested in volunteering for the IET or joining one of our panels, please write to us at india@theiet.in

Follow us on

@IETIndia

www.facebook.com/IETIndia

IET India