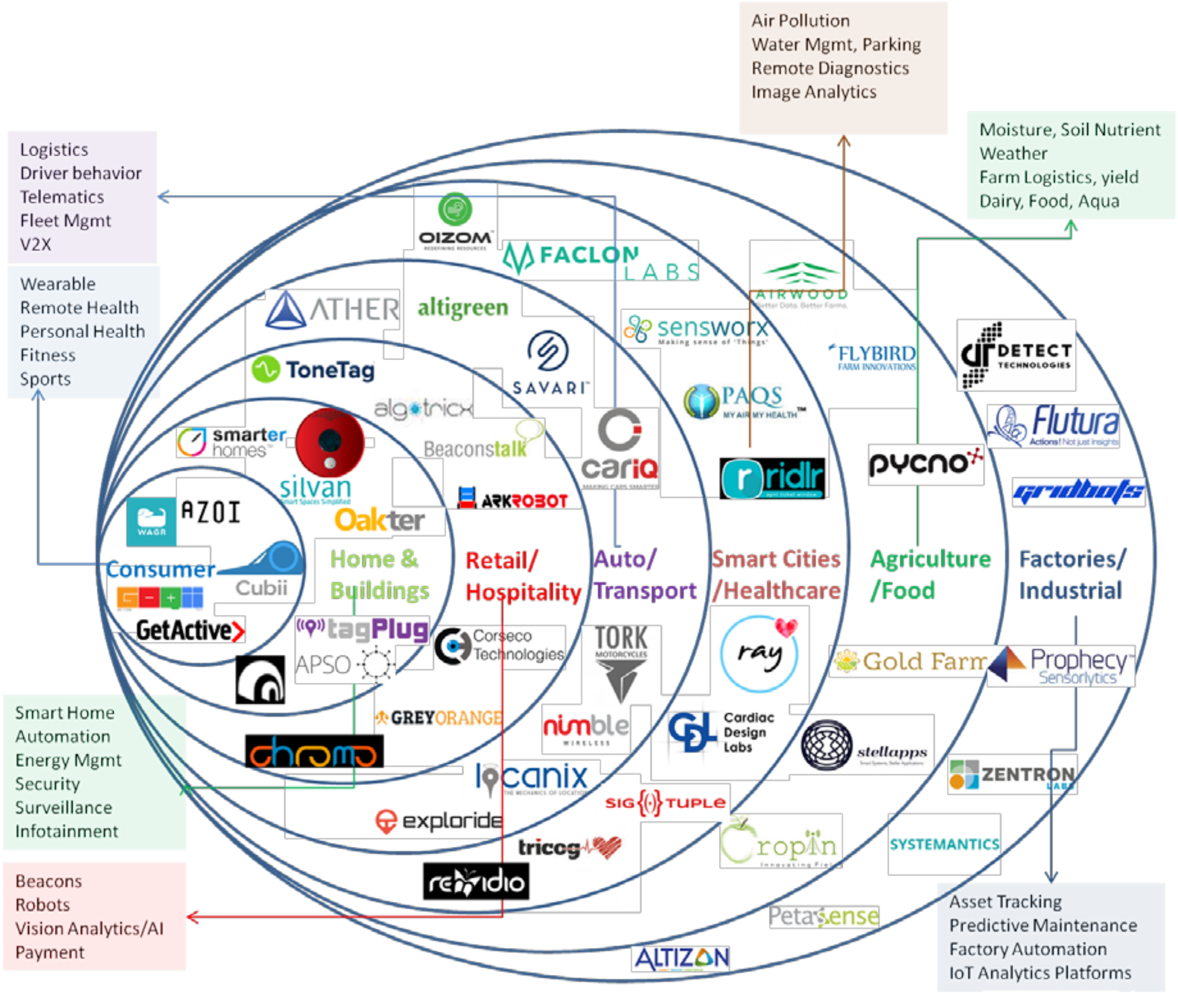


Air Pollution
Water Mgmt, Parking
Remote Diagnostics
Image Analytics

Moisture, Soil Nutrient
Weather
Farm Logistics, yield
Dairy, Food, Aqua

Logistics
Driver behavior
Telematics
Fleet Mgmt
V2X

Wearable
Remote Health
Personal Health
Fitness
Sports

Consumer

Home & Buildings

Retail/ Hospitality

Auto/ Transport

Smart Cities /Healthcare

Agriculture /Food

Factories/ Industrial

Smart Home
Automation
Energy Mgmt
Security
Surveillance
Infotainment

Beacons
Robots
Vision Analytics/AI
Payment

Asset Tracking
Predictive Maintenance
Factory Automation
IoT Analytics Platforms

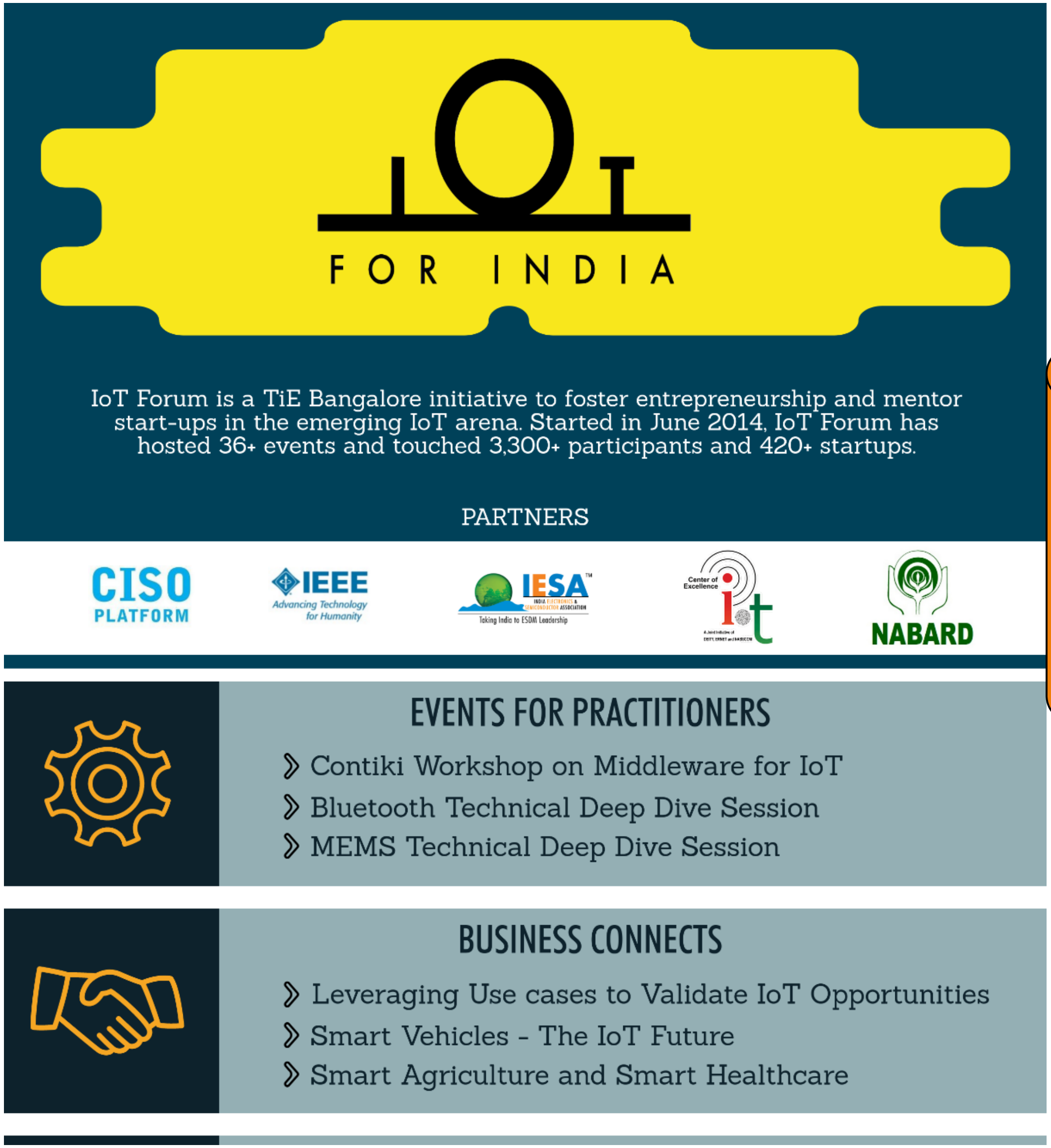
IoTSecurityTaskForce Fresh Thinking.

CISO Platform and IoTForum Intiative

Arvind Tiwary, Chair IoTForum

Bikash Barai, Co Founder CISO Platform

IoTForum: Raising the IoT Quotient of India


IoT
FOR INDIA

IoT Forum is a TiE Bangalore initiative to foster entrepreneurship and mentor start-ups in the emerging IoT arena. Started in June 2014, IoT Forum has hosted 36+ events and touched 3,300+ participants and 420+ startups.

PARTNERS

CISO PLATFORM
IEEE Advancing Technology for Humanity
IESA India Electronics & Semiconductor Association
Taking India to ESDM Leadership
Center of Excellence IoT
NABARD

EVENTS FOR PRACTITIONERS

- Contiki Workshop on Middleware for IoT
- Bluetooth Technical Deep Dive Session
- MEMS Technical Deep Dive Session

BUSINESS CONNECTS

- Leveraging Use cases to Validate IoT Opportunities
- Smart Vehicles - The IoT Future
- Smart Agriculture and Smart Healthcare

www.iotforindia.org

Task Force on IoT Security

IoT Forum & CISO platform join hands to create IoT Security Task force

Readying up the Nation for #IoTSecurity

The task force is chartered to develop threat models, controls and assist players in new techno-legal-commercial arrangements to improve IoT Security

Fresh thinking around Security for IOT

http://wiki.iotforindia.org/FreshThinking

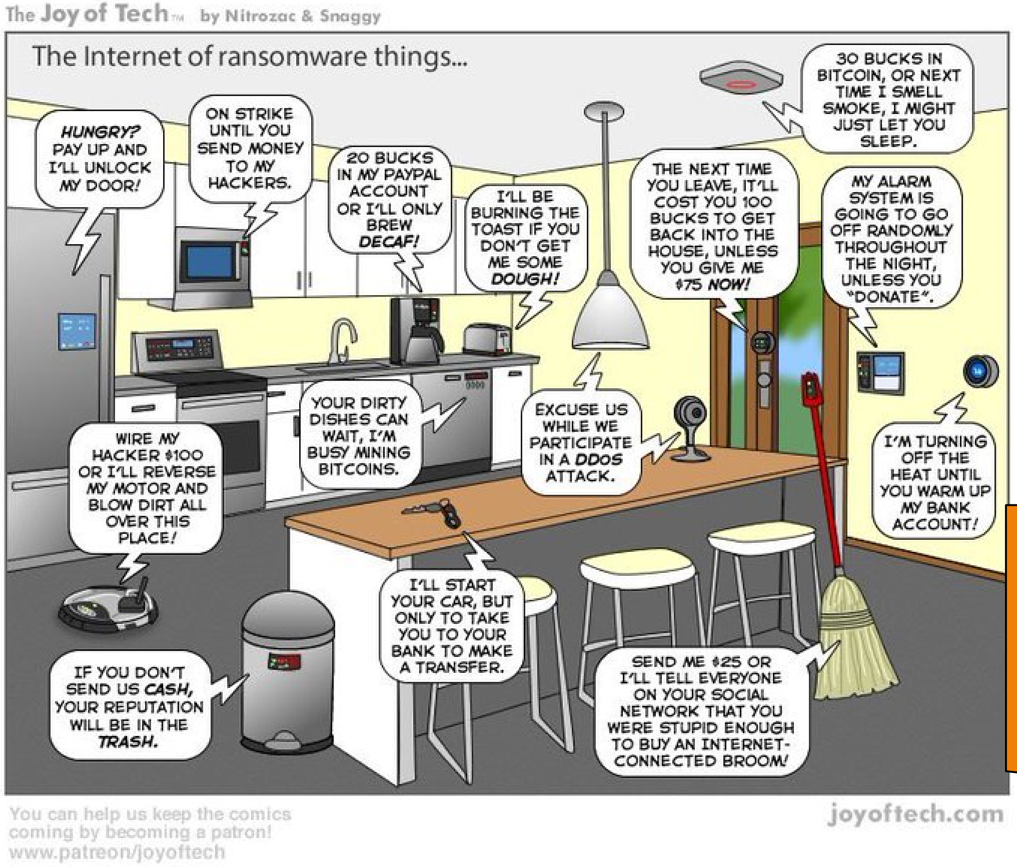
IOT Security

- **Over 13 Standards bodies have a advisory**
- **http://www.cisoplatform.com/profiles/blogs/survey-of-iot-security-standards**
- **FTC, NIST**
- **IoT Security Foundation,** Broadband Internet Technical Advisory Group (BITAG)**)**
- OWASP
- IETF
  - DICE MUD, OtrF, ACE
- IIC Industrial Internet Consortium,

Cybersecurity = risk is Money and reputation

IoT = risk is accident and human lives

Fresh Thinking: Is the Emperor Naked?


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

You don't change all the locks of each house in a city merrily because criminals can break 7 lever locks in less time

IOT Security

- **Program COMPLEXITY= Algorithm + Data Structure**
- **CyberSecurity Difficulty= Legal + Technical**
  - Internet was designed to withstand disruptive nuclear attack
  - IP and MAC spoofing make it fundamentally unsecure
- **Legal Basis**
  - Product Quality and Liability regime – USA
  - DDOS by House Owners is like Rioters are House owner responsibility?
  - Petty **Wannacry** type ransom ware is like carjacking in Joburg
    - Armoured car ?
- **Criminal Law**
  - Territorial
  - Individual, layers of Government
    - Precinct, City, State, Nation
  - Right of Self defence

We need attribution which can hold in a court of law and can be easily and routinely derived. not require weeks of research?

Principles of FreshThinking: Blaming the Victim is so old fashioned

For IoT Network
5 year Sandbox

- **Reduce effort and skill required to secure**
- **Increase probability of detection**
- **Decrees success rewards**
- **Impose costs on criminals. Pirates must be tamed**
  - Law is Territorial. Cyberspace criminals must be caught and booked under laws of piracy and high seas
- **Special High frequency crime mitigation procedures**
  - Instrument and infect hackers to provide evidence
  - Protocol between ISP of participating nations
- **Reduce burden and standard of care for network operators to act**
  - Throttle and block suspicious activity

CyberLaw for the Cyber City

- **Recognize pervasive criminal activity**
  - **SPAM,** Carjacking
- **Allow right to self defence**
- **Can instrument, infect and hack-back to identify and prove attacker**
- **The individual house owner is the victim and he should be able to count on neighbours, community and police and not be blamed or denied rights to chase and catch criminals**

No amount of passive defence can stop pervasive criminal succeeding once in a while
Broken Glass syndrome : Catch petty criminals deters big crime also

Managed SECURENET

FOR INDIA

- A new business opportunity
- Skills and effort required are increasing day by day
- Pool and outsource
- Hierarchy of Safety providers
- Office security, Facility Security, Township ,
- Police, CISF, BSF, Army

Legal Requirements

- **Fool Proof Identification of actor**
  - Not spoofable MAC and probabilistic pattern based
- **Establish Mens Rea (Intent)**
  - Deception based defence. Not accidental entrance
  - Cyber CCTV
- **Anton Pillar order capability**
  - Civil search and seizure
- **Execute a Letter of marque**
  - Piracy on high seas

Before SECURENET

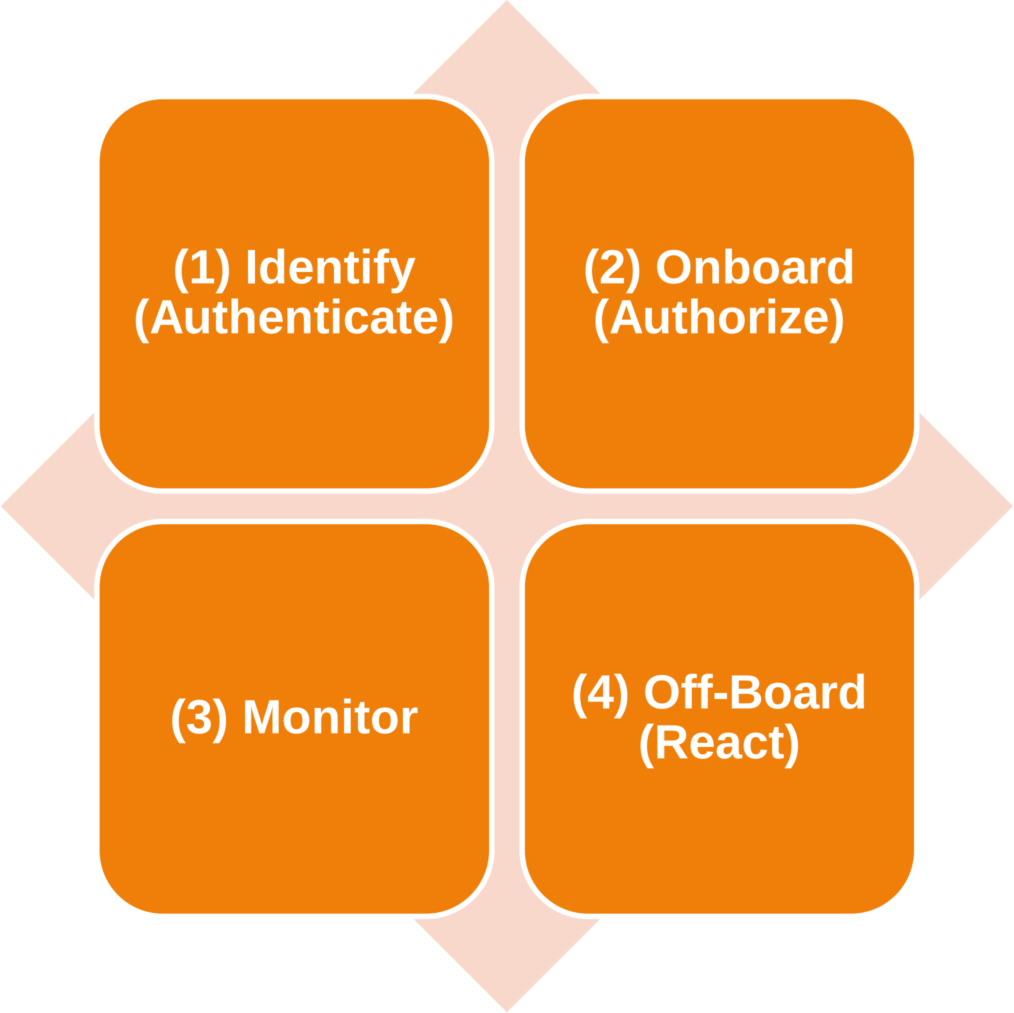
A Few Security Trends …

Security, Impossibility & Halting Problem

Isolation, Walled Gardens …

Zero Trust Model, Beyond Corp ..

4 Pillars of SECURENET



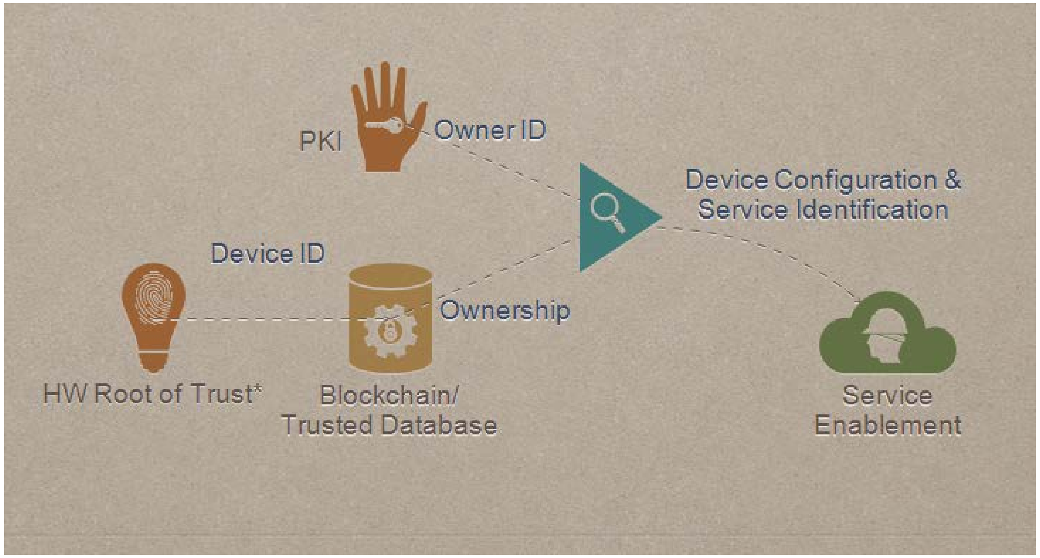
(1) Identify (Authenticate)

(2) Onboard (Authorize)

(3) Monitor

(4) Off-Board (React)

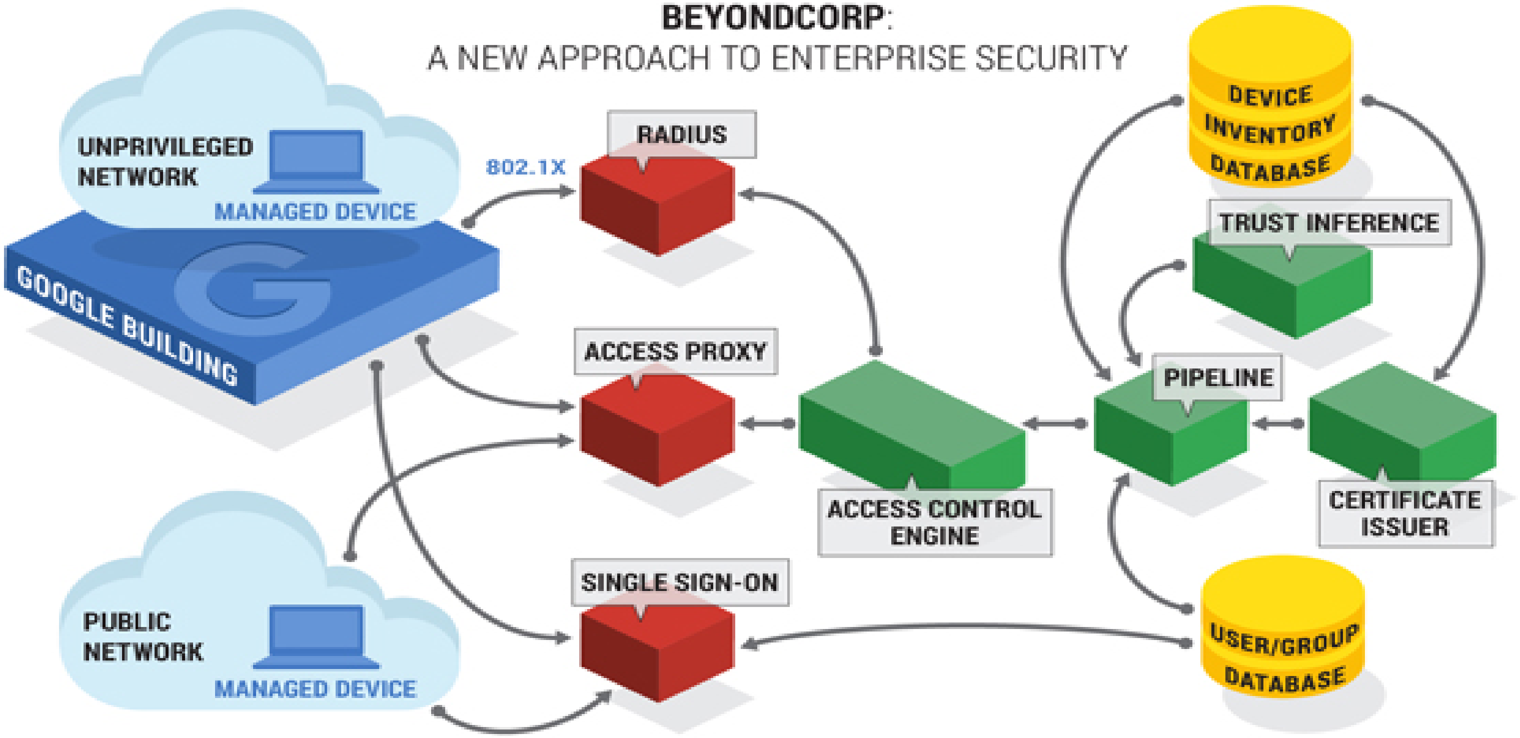
(1) Authenticate & (2) Authorize..


PKI
Owner ID
Device Configuration & Service Identification
Device ID
Ownership
HW Root of Trust*
Blockchain/ Trusted Database
Service Enablement

Identity/Authentication : Device, People, network Identity.. TPM, HW root of trust

Social/Behavior, Biometrics, Multi Factor etc

Authorization: Degrees of trust & scenario analysis, provision tiered authority



BeyondCorp components and access flow

(3) Monitor

- **Centralized/Network Access Proxy:**
  - At main entry point to subnet
  - Township entry/ Network Access Proxy

- **Decentralized:**
  - Local Anomaly detection for neighbourhood

- **OSINT, SIEM, SA, NTA/NBA, CASB, UBA, UEBA**

- **External & Hyper Local Threat Intelligence:**
  - Central Intelligence to Neighbourhood watch

(4) React/Offboard

- Offboard

- Reduce Access/Quarantine:

- Deception/Offensive Countermeasures/Active Defense

Delegated Police Authority

- **Semi Private and Semi Public Spaces**
- **Cyber City and Cyber Neighbourhood not Cyber Jungle**
- **Right of Self Defence**
  - Chase a thief into other property
  - Enter a house from where enemy fire is coming
  - Stop a speeding truck trying to ram thru a entry gate inspection
  - Place a marker to trace stolen goods
- **High Seas and Space Piracy laws**
  - Right for catching a cyberspace criminal
  - Letters of Marquee to bring criminals to justice

CROSS BORDER

- **PROTOCOL for Countries allowed to connect on SECURENET**
  - FAST , MINIMUM ACTION on suspect SITES automatically
  - MARTIME LAW is basis

In the days of fighting sail, a **letter of marque and reprisal** was a government license authorizing a person (known as a *privateer*) to attack and capture enemy vessels and bring them before admiralty courts for condemnation and sale.

A "letter of marque and reprisal" would include permission to cross an international border to effect a reprisal (take some action against an attack or injury) authorized by an issuing jurisdiction to conduct reprisal operations outside its borders.

Wikipedia

The United States Constitution grants to the Congress the power, among others, to issue "Letters of Marque and Reprisal.

FreshThinking : Don’t blame victim but hurt criminals

- SECURENET for IoT to test out new Techno Legal approach
- Technical ability to identify source and produce actionable forensic evidence
- Legal approach allowing cyber defence and chasing cyber pirates and hurting them and their assets
- Broken Glass principle

Security and safety is a stance.

An Active defence posture will cut down lots of wannabe hackers. New types of instrumentation and network wide correlation will increase skills and costs of attackers

Plan

- ✓ **Initial discussions IoTNext 2016 (4Q 2016)**
- ✓ **Public Airing 9 Sep 2017**
- ✓ **CISO Platform 14 Sep**
- ✓ **IoTNext Nov 9**
- ✓ **SACON Nov 11**
- **December / January**
  - TSDSI, DOT,TRAI,CDAC,
  - BSNL. Airtel, Jio, Vodafone, Ericson, Telco Stack
  - SoC, Chip mfgs
  - Lawyers, Free Internet
  - IEEE (Roof)
- **March 2018 Revisions based on feedback**

Critique, Alternative, Improvements

- **Volunteer Please…HARD PROBLEM**
- **Technical Tools and approaches**
  - Enterprise security at scale
  - Phishing and Super user hijack in IoT
    - Trigger words for Alexa, Google Home, Siri
  - MUD, DICE etc
- **Legal Tools and Approaches**
  - Semi private and Semi Public in Cyberspace
  - Right to self defence
  - Delegated policing powers

Join IoTSecurity Group
www.iotforindia/beta

✉ iot@tiebangalore.org

🌐 www.iotforindia.org

🐦 @iotforindia