SDC 20
SNIA INDIA

Storage Developer Conference
December 4-5, 2020
BY Developers FOR Developers

Preventive Safety from unauthorized IoT devices

Mitigating Security Threats By Unauthorized Devices in an IOT network, Using Distributed Ledger

Rekha MS, Shilpa PV
DellEMC

Shilpa PV

Software Senior Engineer at Dell EMC having 6 years of experience in web and enterprise applications using AngularJS, Java, hibernate etc., Currently working in Dell Change management.

Rekha MS

Senior Software Senior Engineer at Dell EMC having 10 years of experience in development of web and enterprise applications using Core Java, J2EE, technologies such as JDBC, Servlets etc. automation using python. Research-oriented, motivated, proactive, self-starter with strong technical, analytical and interpersonal skills.

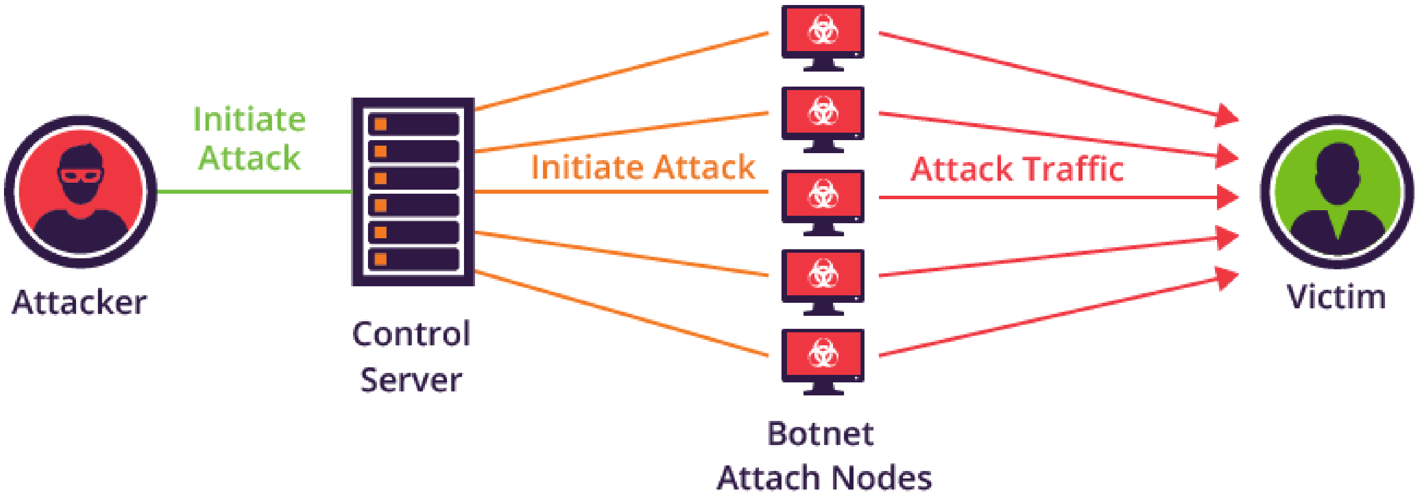
Agenda

- How IOT devices become participants in cyber attacks(DDOS)?
- A scenario by which compromised IOT devices can be used to launch a DDOS
- IOT network architecture and adoption of DLT
- Threat scenarios
- Key components of the solution
- Advantages of DLT

How do IOT devices become participants in cyber attacks (DDOS)?

- An attacker scans for devices on the internet
- Most IOT devices have default credentials

Scenario: IOT devices used for launching DDOS



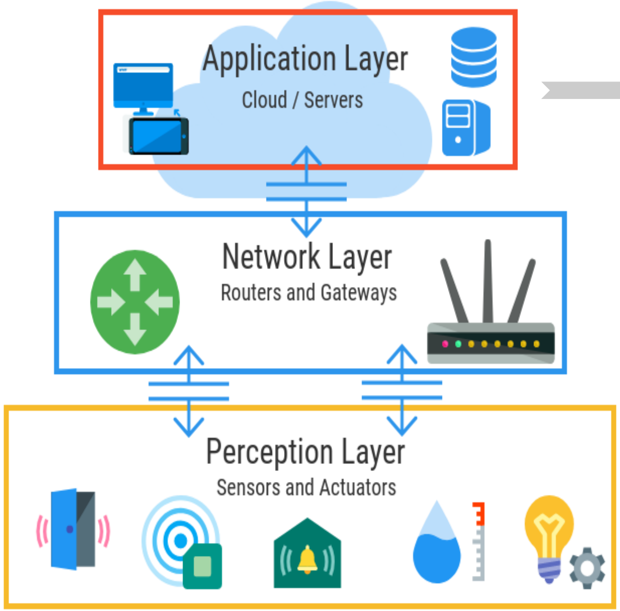
Mirai DDoS Attacks

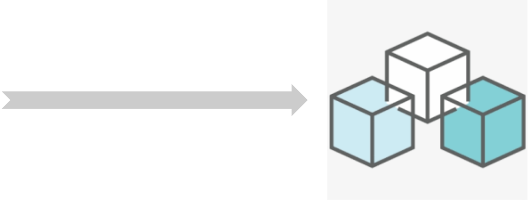
- Mirai first struck **OVH**, one of the largest European hosting providers, on Sept 19, 2016.

- Later the attack happened on **Minecraft servers**.
- The big strike on Oct 12 was launched on **DYN**, a facilities company that among other things provides **DNS solutions** to a lot of big businesses.

- The impact of this major attack was felt by users when hugely popular websites such as **Netflix**, **Amazon**, **Airbnb**, **Twitter**, **Reddit**, **PayPal**, **HBO**, and **GitHub**, were left inaccessible.

IOT architecture





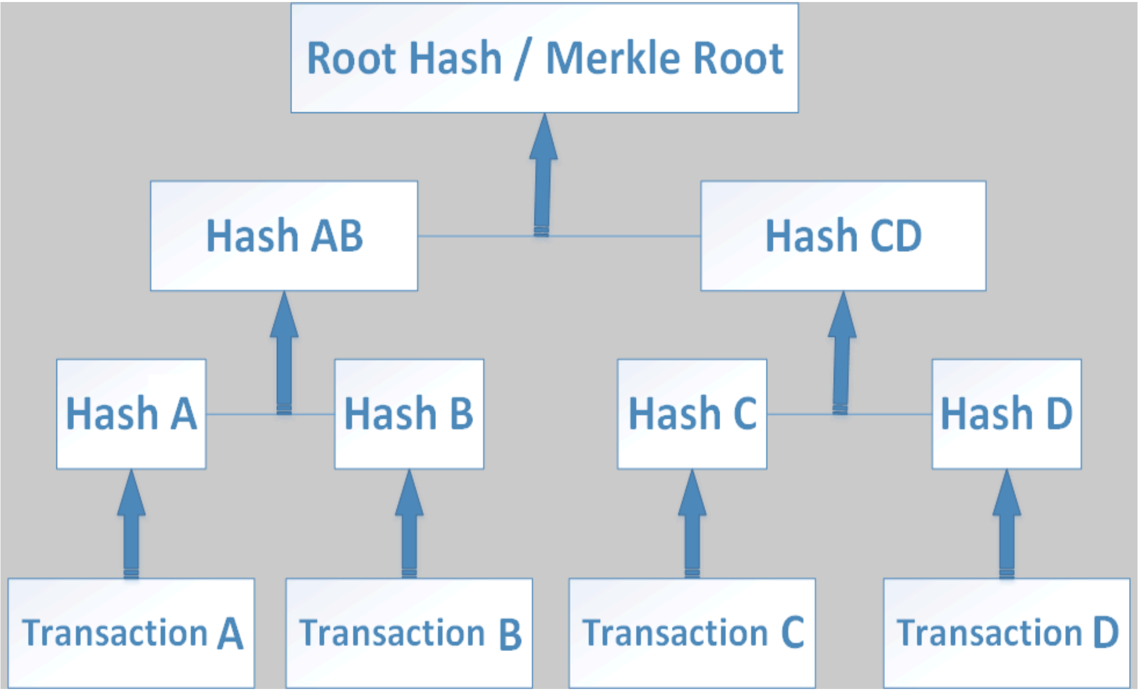
Ledger in Enterprise Nodes

Threats posed by rogue devices

Scenario 1 : An unauthorized device can be introduced in the network

Scenario 2: An authorized device can be infected with malware

Two-factor authentication



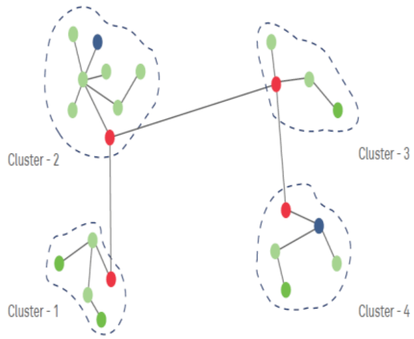
Token based authentication :

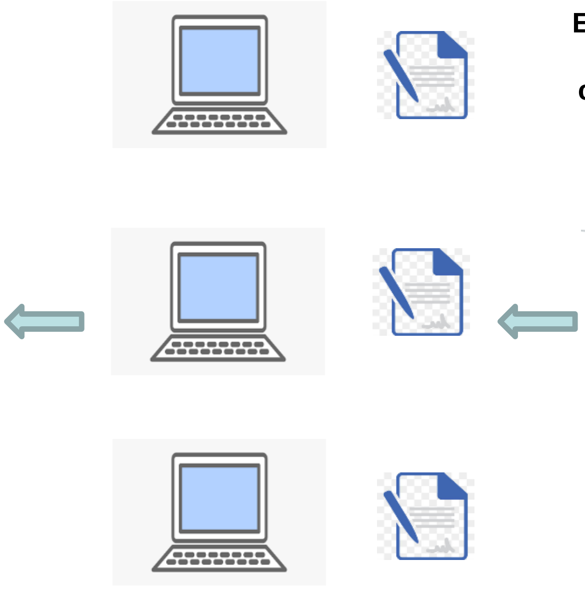
Devices communicate by sharing their tokens or unique hash. Firmware ID, Device ID and Device Name or IP address of IOT device is used to generate a unique device identity

Root Hash authentication:

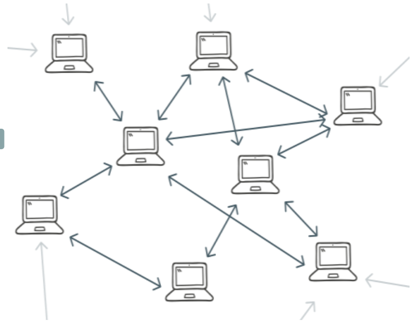
Each device stores the final whitelist root hash which is cumulative hash of the current state of the network.

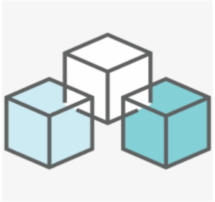
Adding a new device to the network





Enterprise nodes validate and update device whitelist and circulate hash to IOT devices and gateways





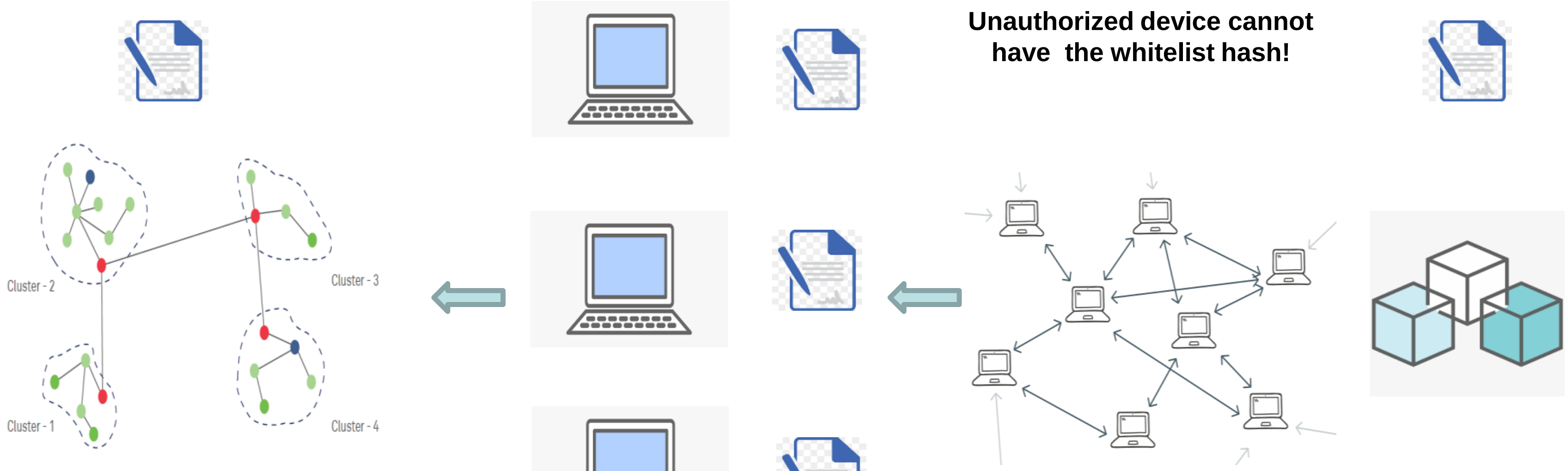
IOT clusters

IOT Gateways storing the hash of the whitelist

Enterprise Nodes

Scenario 1 : Unauthorized device

Unauthorized device cannot have the whitelist hash!

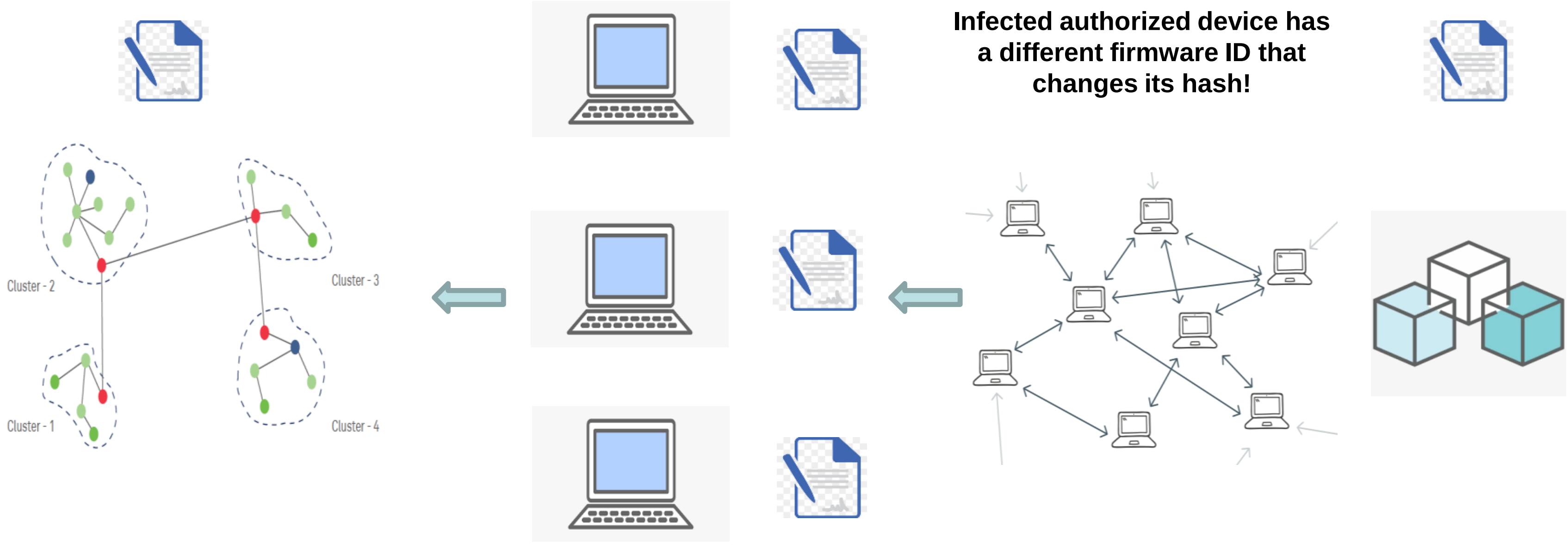


IOT clusters

IOT Gateways storing the hash of the whitelist

Enterprise Nodes

Scenario 2 : Infected Authorized device



Infected authorized device has a different firmware ID that changes its hash!

IOT clusters

IOT Gateways storing the hash of the whitelist

Enterprise Nodes

Advantages of Distributed Ledger

- ➢ Secure
- ➢ Tamper Proof
- ➢ Transparent
- ➢ Accessible
- ➢ Synchronized

THANK YOU

Please take a moment
to rate this session.

Your feedback matters to us.

For any queries or suggestions, please reach out to

rekha_ms@dell.com

shilpa_pv@dell.com