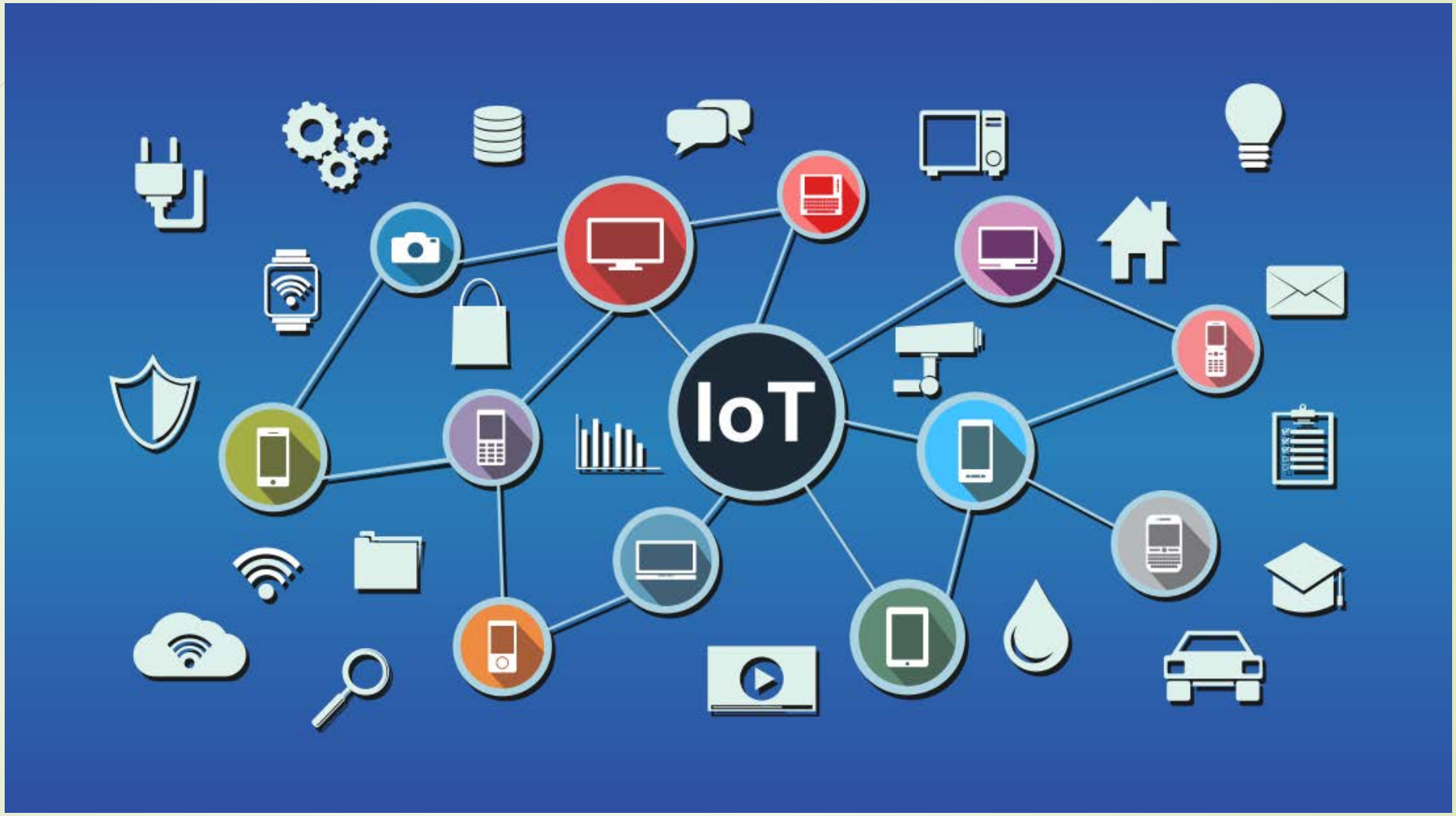
AutoAdd

Anoop Kumar Pandey
Senior Technical Officer
C-DAC Bangalore

Connected Things

Web Connected Things

Internet of (connected) Things



A system where the **Internet is connected to the physical world via ubiquitous sensors**. (Kevin Ashton 1999)

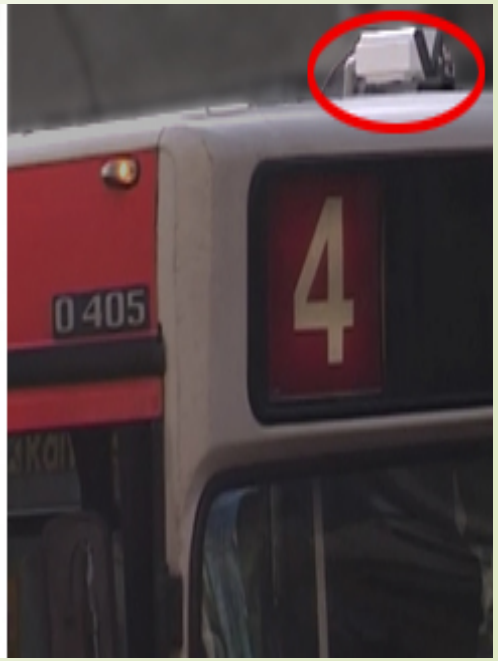
EkoBus


TGS2442
Ubeeum


EKOBUS 500


EkoBus
City: Pančevo
EkoBus
Tracker
Zone: Vojlovica, Pančevo


6:04 PM
Sensor data
Carbon monoxide CO: 2.8 ppm
Nitrogen dioxide NO2: 0.2 ppm
Carbon dioxide CO2: 205.5 ppm
Temperature: 3.99 C
Humidity: 87.3 %
Pressure: 103.95 kPa
Updated: 5 Dec 2010 14:58:50
Close
MENU


0 405
4

Amazon Alex / Echo

Google Home

Amazon Alexa Lighter Side

Source: Mark Parisi, Off The mark

Increased Risks!

Who is the culprit?

- Software Control
  - Everything turning in computer
  - Enormous power and flexibility, but brings insecurities
- Interconnection
  - Vulnerabilities in one lead to attacks against others
  - Ransomware attack
- Autonomy
  - Buying/selling stocks, driverless cars
  - Effects of attacks can take effect immediately, automatically, and ubiquitously.

Add a device to Network

- Manual bootstrap
  - Discovery
  - Registration
  - Key Setup
  - Configuration
- Can we minimize or eliminate user actions during bootstrap??

Let's *autoAdd*

- Add the device and let it bootstrap itself
- But Wait!!
  - How to know
    - The identity/authenticity of the device?
    - If device is compromised or not?
    - The identity of the network/domain?
    - If the domain is the correct one?

Prior Approaches

- TOFU (Trust on First Use) [RFC7435]
  - TOFU calls for accepting and storing a public key or credential associated with an asserted identity, without authenticating that assertion.
  - Subsequent communication that is authenticated using the cached key or credential is secure against an MiTM attack, if such an attack did not succeed during the vulnerable initial communication.

Prior Approaches

- Resurrecting Duckling [Stajano99theresurrecting]*
  - Imprinting
  - Device recognises as its owner the first entity that sends it a secret key
  - Stay faithful to its owner for rest of life (loyalty!!)
    - EoL: Reset the software or Dispose the device
    - Transfer of control to another owner

* https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf

Prior Approaches

- Enrollment over Secure Transport (EST) [RFC7030]
  - The client initiates a TLS-secured HTTP session with an EST server.
  - A specific EST service is requested based on a portion of the URI used for the session.
  - The client and server authenticate each other.
  - The client verifies that the server is authorized to serve this client.
  - The server verifies that the client is authorized to make use of this server and the request that the client has made.
  - The server acts upon the client request.

BRSKI

- Pledge discovers a communication channel to a Registrar.
- Pledge identifies itself. This is done by presenting an X.509 IDevID credential to the discovered Registrar (via the Proxy) in a TLS handshake. (The Registrar credentials are only provisionally accepted at this time)
- Pledge requests to Join the discovered Registrar using a voucher request.
- Registrar sends the voucher request to the MASA (manufacturer). URL of MASA can be in the voucher request or embedded in Registrar.
- MASA sends the voucher which is passed to pledge.
- Pledge verifies the voucher and imprints to the registrar by send voucher status telemetry.
- Registrar verifies the voucher and enrols the pledge to the domain

BRSKI

Pledge

Registrar

MASA

Voucher Request

Voucher Request

VR verification

Voucher issued

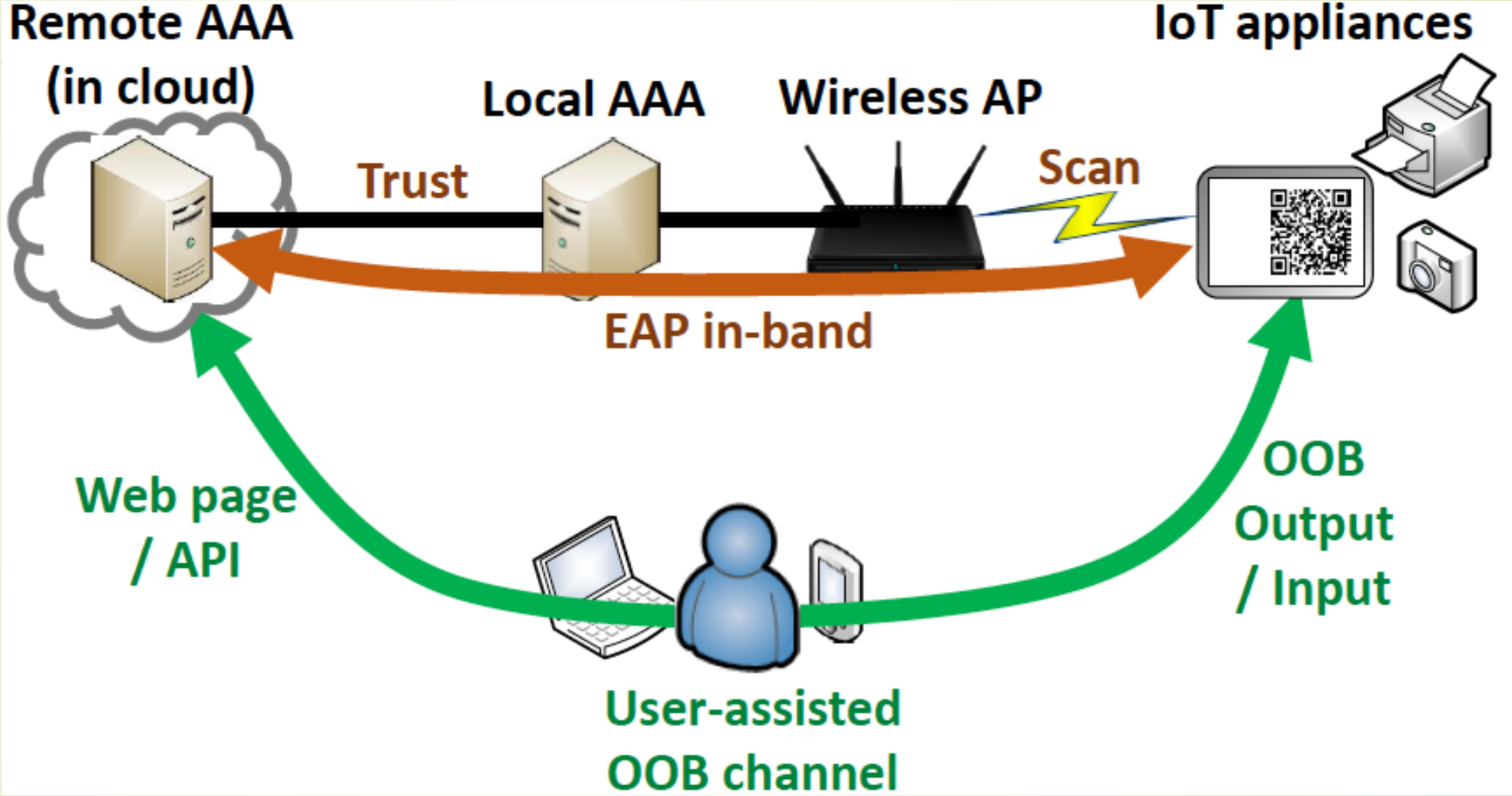
Voucher

Voucher verification

Status Telemetry

Voucher verification &
Enrolment using EST

EAP-NooB



Source: Mohit Shetty; https://www.cs.helsinki.fi/group/close/edge-computing-2016/lib/slides/tuomas_aura.pdf

AutoAdd

Manufacturer
or
Seller

Device

Registrar

MASA

Dig_Invoice = DigSignM {IDevID,
PubKey: [R1, R2, .., Rn]}

Embed DigiInvoice

DigiInvoice

Verify Manufacturer Signature

Signed Acceptance Note

Acceptance Note

Verify Registrar Signature
using public key in the digital invoice

Thank you.