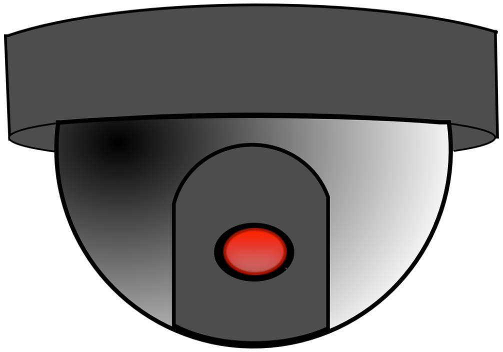


Controlling Connected Thing's Vision

Real-Time Communication (RTC) Conference – 2017
Illinois Institute of Technology, Chicago

Aman Singh
Palindrome Technologies Inc.

Joint work with
Internet Real-Time (IRT) Lab - Columbia University
Interdeciplinary Center for Security, Reliability and Trust (SnT) - University of Luxembourg

/agenda

- Connected Things
- Why ?
  - Strengths | Weaknesses | Opportunities | Threats
- Communication Model
- Security Issues
- Things & Software-defined-Networking (SDN)
- Thing Controller
- Trust Model

/connected_things

- Network of devices / objects / things
  - Understand and Control of physical processes

Sense | Log | Interpret -- Communicate | Process | Act

- Classification (Consumer vs. Commercial)
  - Smart Home / Car
  - Smart Cities
  - Smart Business
  - Smart Factories (Industry 4.0)

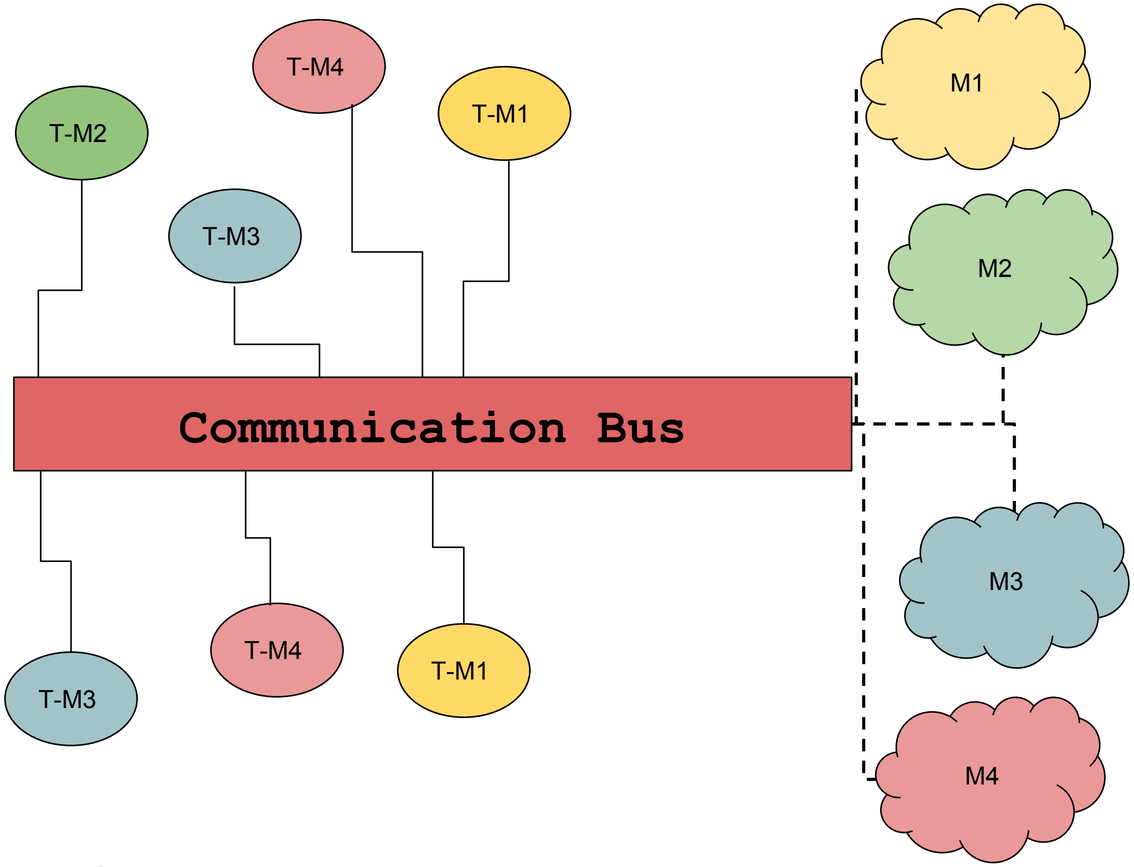
/why ?

Strengths	Weaknesses
• Ubiquitous sensing • Increased productivity • Speed and accuracy of information	• Expanded attack surface • Uncertainity of data handling due to high volume • Data spread across multiple jurisdictions
Opportunities	**Threats**
• Real-time operational efficiency • New functionalities • Economic growth revenues • Rethink end-to-end security and resiliency	• Unanticipated attacks • Emergent, disruptive behavior • Immature knowledge base related to IoT security

*President's National Security Telecommunications Advisory Committee (NSTAC) – Report on IoT

/communication_model

- Spatio-temporal event system
- Messaging model
  - Publish/ Subscribe
  - Request/ Response

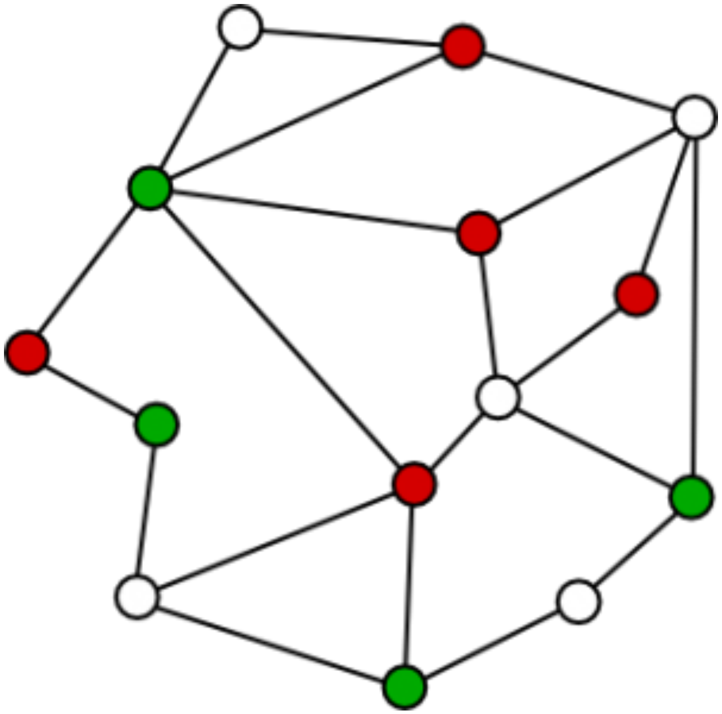


*e.g. - https://www.iotivity.org/

/security_issues

- Device management
  - Security updates
- Weak default configurations
  - Credentials
  - Protocol configurations
- Device runtime integrity
  - Secure-boot
- Complex network access management

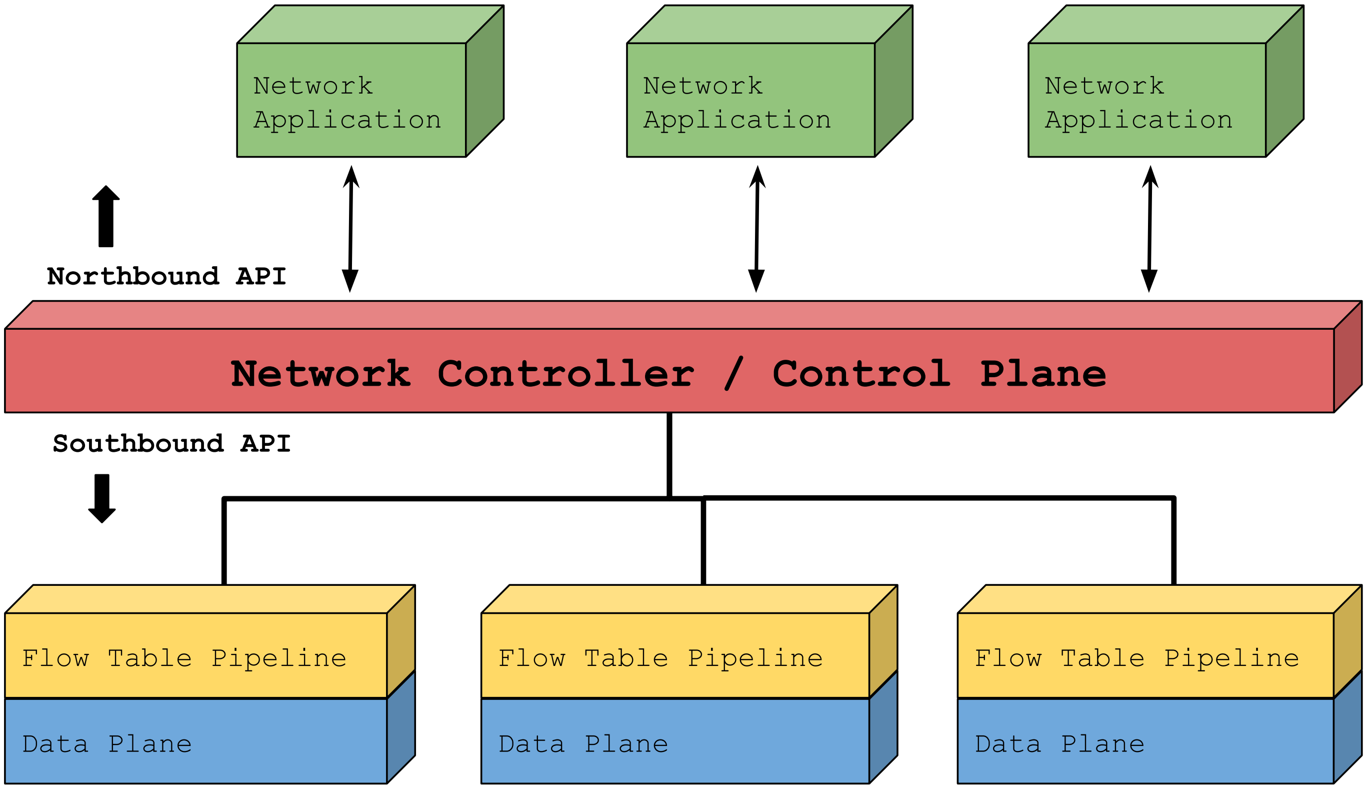
*https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project



Things & Software-defined-Networking (SDN)

/sdn

- Decouple data and control plane
  - Enables flexible network programming model based upon spatio-temporal event system



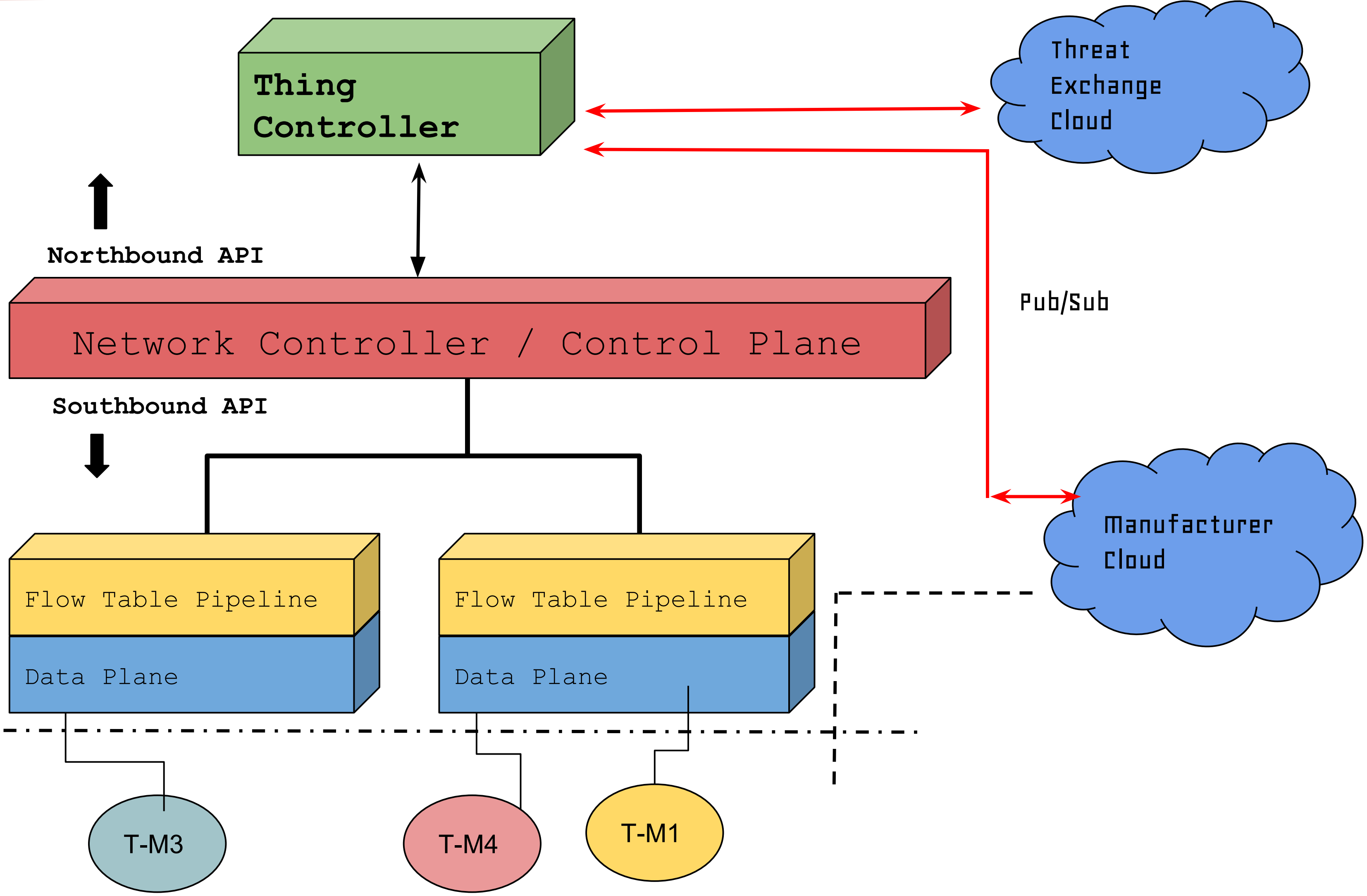
/network_first_approach

- Network State
    - Inventory – Static
    - Behavior - Dynamic
- Logical Groups
    - Same manufacturers
    - Device categories
    - Time-based
- User vs. Thing
  - Home / Enterprises

/thing_controller (1)

- Thing registry
  - Maintains all the registered things in the network
  - Configuration/ Software stack / Open ports
- Static Communication Profiler
  - Gathers communication rules from manufacturers
    - Thing 1 (iot.cs.columbia.edu / 8443 / tcp)
    - Thing 2 (iot.palindrome.io / 1331 / udp)
- Dynamic Communication Profiler
  - Communication behavior => rules
  - Device categories

/thing_controller (2)



/security_model

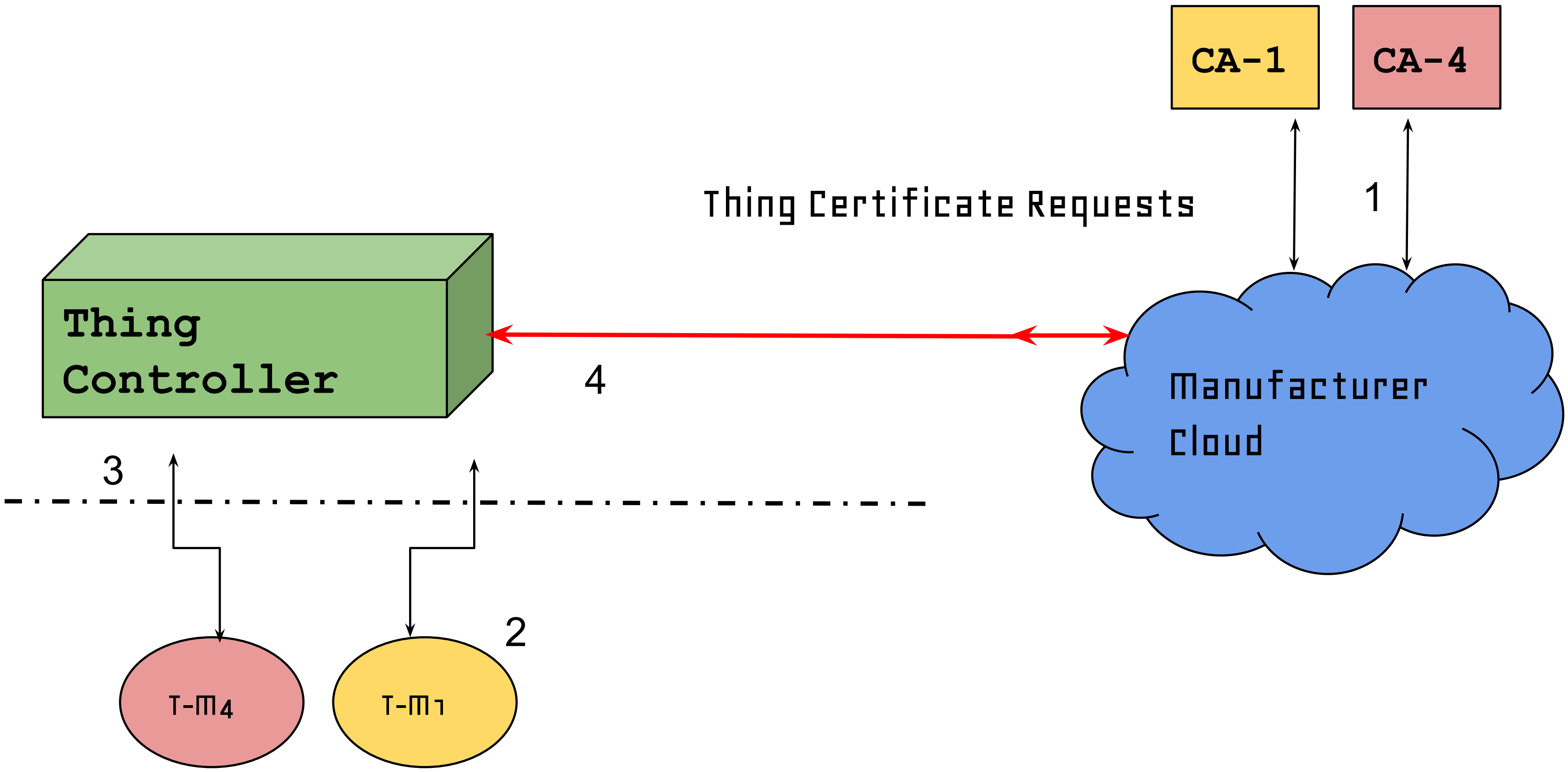
“Exploring new security models, especially at the ecosystem level, where security decisions can be made autonomously and at speed and scale: The dynamism of the IoT introduces new adaptability requirements to existing security practices. For example, as part of security-by-design, it is necessary for components and systems to be able to learn and detect new vulnerabilities dynamically, and if necessary, isolate themselves. “

*President's National Security Telecommunications Advisory Committee (NSTAC) – Report on IoT / 2.2.1.4

/thing_state_machine

- Thing-as-a-process
  - Registration
  - Not-Authorized
    - Thing controller access
    - Manufacturer cloud access
  - Operational
  - Quarantine
    - Deviates from deployed rules

/trust_model


CA-1
CA-4
Thing Certificate Requests
1
Thing Controller
4
Manufacturer Cloud
3
2
T-M4
T-M1

/registration

- Thing provides manufacturers device profile URL
  - Extensible Authentication Protocol (EAP)
    - X.509 Extension / EAP-TLS Authentication
  - Dynamic Host Configuration Protocol (DHCP)
    - Option field
  - Link Layer Discovery Protocol (LLDP)
    - Type-Length-Value (TLV) extension
  - Domain Name Service – Service (SRV) Records
    - Thing controller service

/prototype

- Manufacturer Usage Description (MUD)* profiles

```
"ietf-access-control-list:access-lists": {
     "acl": [
       {
         "acl-name": "mud-54684-v6to",
         "acl-type": "ipv6-acl",
         "access-list-entries": {
           "ace": [
             {
               "rule-name": "cl0-todev",
               "matches": {
                 "ipv6-acl": {
                   "ietf-acldns:src-dnsname": ”iot.cs.columbia.edu",
                   "protocol": 6,
                   "source-port-range": {
                     "lower-port": 8443,
                     "upper-port": 8443
                   }
                 },
                 "tcp-acl": {
                   "ietf-mud:direction-initiated": "from-device"
                 }
               },
               "actions": {
                 "permit": [
                   null
                 ]}}]}}
```

*https://tools.ietf.org/html/draft-ietf-opsawg-mud-11

/THANK YOU

email: aman.singh@palindrometech.com