Security and Privacy in the Internet of Things

Elisa Bertino
CS Department, Cyber2SLab, and CERIAS
bertino@purdue.edu

PURDUE UNIVERSITY

CERIAS

The IoT – Wikipedia

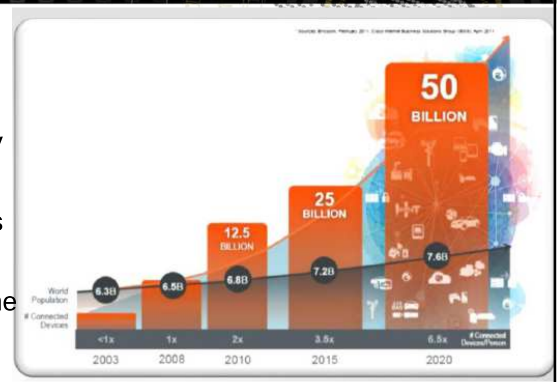
- The **Internet of Things** (**IoT**) is the network of physical objects or "things" embedding electronics, software, and network connectivity, which enables these objects to collect and exchange data.
- The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems.
- When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities.

Applications
- Media
- Environmental Monitoring
- Infrastructure Management
- Energy Management
- Medical and Healthcare Systems
- Building and Home Automation
- Transportation

PURDUE UNIVERSITY

IoT Diffusion - Forecast

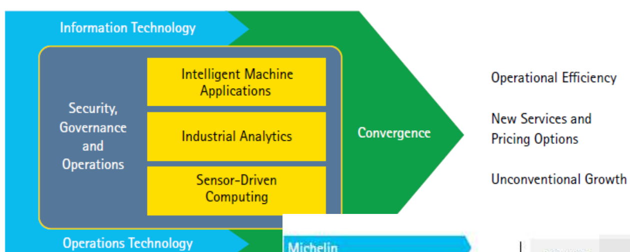
- 50 billion connected devices by 2020
- More than 6 connected devices per person
- $1.7 trillion in value added to the global economy in 2019

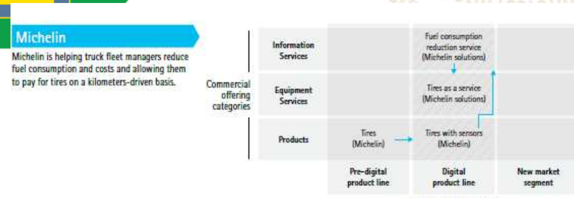


- By 2020 IoT will be more than double the size of the smartphone, PC, tablet, connected car, and the wearable market combined
- Technologies and services generated global revenues of $4.8 trillion in 2012 and will reach $8.9 trillion by 2020, growing at a compound annual rate (CAGR) of 7.9%

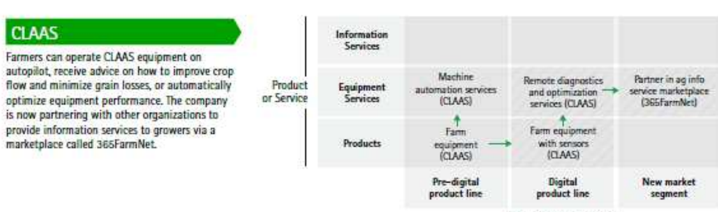
PURDUE UNIVERSITY

Industrial IoT (IIoT)





Diagrams and examples from Accenture "Driving the Unconventional Growth through the Industrial Internet of Things", 2015, downloaded from https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf



PURDUE UNIVERSITY

IoT - Risks

IoT dramatically expands the attack surface

- IoT systems do not have well defined perimeters
- IoT systems are highly dynamic and continuously evolve because of mobility
- IoT are highly heterogeneous with respect to:
  - ❑ Communication
  - ❑ Platform
  - ❑ Devices
- IoT systems may include physically unprotected portions
- IoT systems are highly autonomous and control other autonomous systems
- IoT systems may include “objects” not designed to be connected to the Internet
- Human interaction with all the devices is not scalable

PURDUE UNIVERSITY

CERIAS

IoT - Risks

The OWASP Internet of Things Top 10 - 2014

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
   Including authentication bypass vulnerabilities in firmware
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interfaces
7. Insecure Mobile Interfaces
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

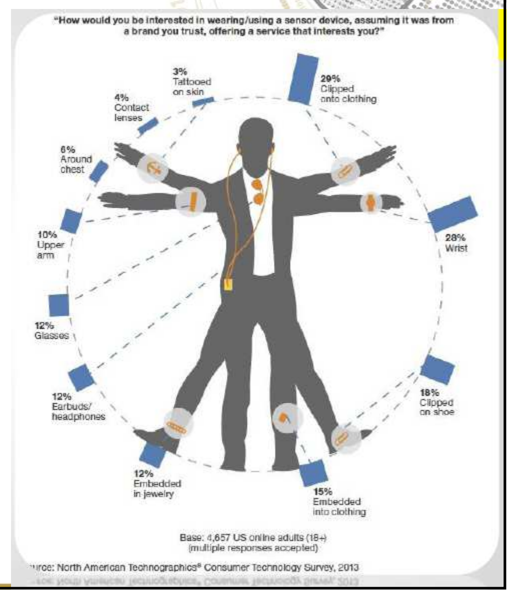
PURDUE UNIVERSITY

CERIAS

IoT – Privacy Risks

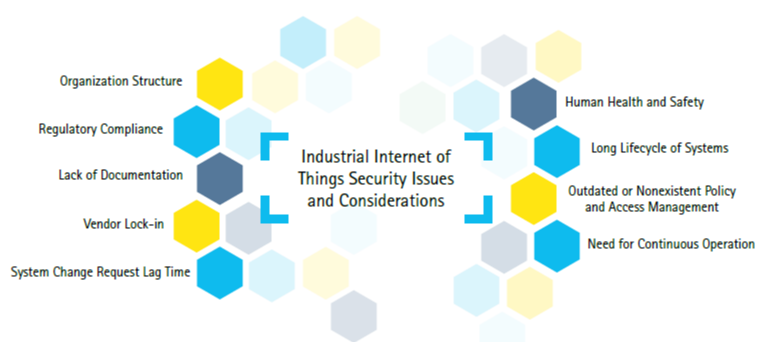
Individuals as sources of multiple data sets

- Wearable devices collect huge amounts of personal data as well data about the user environment
- Major privacy concerns arise for health-related data from the use of medical devices and fitness applications
- Privacy-sensitive information can be easily disclosed to third parties
- Threats arise for enterprise perimeters



PURDUE UNIVERSITY

Specific Security Challenges of IIoT



PURDUE UNIVERSITY

Diagram from Accenture "Driving the Unconventional Growth through the Industrial Internet of Things", 2015, downloaded from https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf

CERIAS

A Holistic Approach is Required

All technical elements need to be considered

- The IoT Devices
- The Cloud
- The Mobile Applications
- The Network Interfaces
- The Software
- Use of Encryption
- Physical Security
- USB Ports

PURDUE UNIVERSITY

CERIAS

Question:

We have a lot of data security techniques

Can we apply them to the IoT?

PURDUE UNIVERSITY

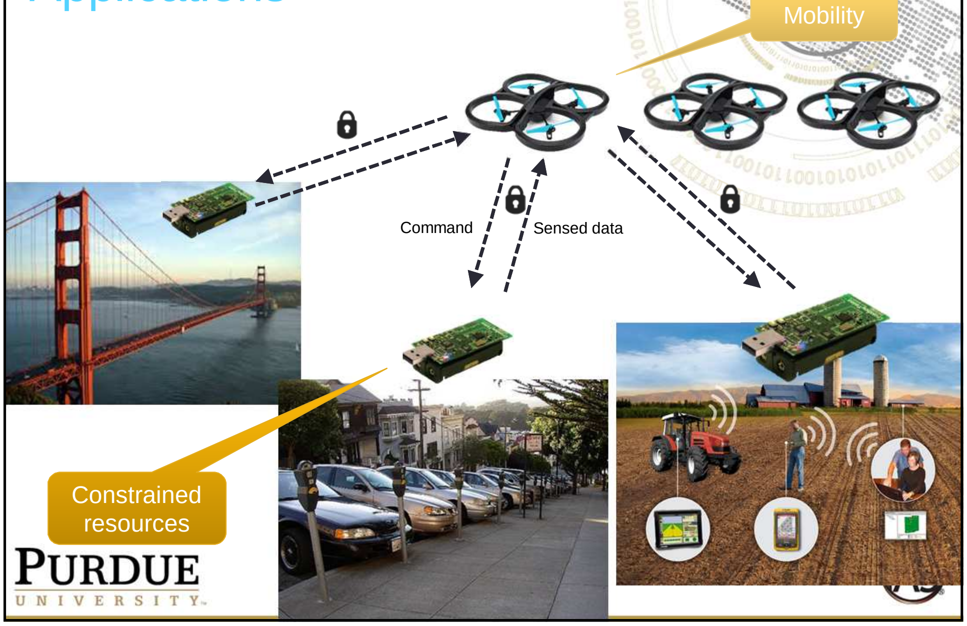
CERIAS

Encryption Protocols

Efficient key management schemes for mobile devices

J. Won, A. Seo, E. Bertino

Secure Communication for Drone-based Applications



Challenges: Security and Efficiency

- Sensors (smart objects) and drones are battery-powered
  - The drones cannot be equipped with high capacity battery due to their weight
  - Sensor's battery is usually not replaced during their life time
    - Sensors use Low Power Listening (LPL) for energy saving

  → The drone may wait until the sensor wakes up.

- Asynchronous computing power
  - The sensors have very low computing power (TelosB: 4MHz)
  - The drones have PC or smartphone-like computing power (> 1GHz)

  → The drone must wait until the sensor completes key establishment in order to receive an encrypted message from the sensor

PURDUE UNIVERSITY

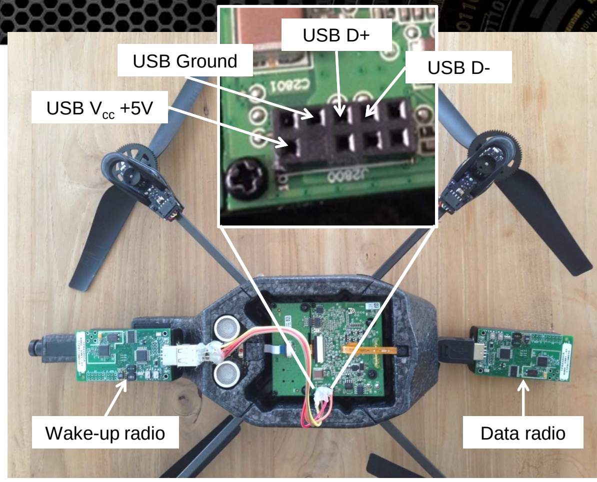
CERIAS

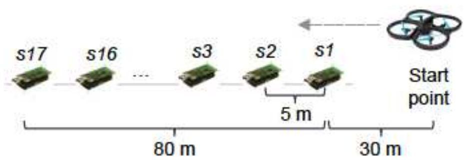
The solution

- Pairing-free Certificateless Signcryption Tag Key Encapsulation Mechanism (pCLSC-TKEM)
  - satisfies all security requirements
  - minimizes computational overhead on sensor (w ECC and w/o pairing, small number of EC point multiplications)
- Dual channel strategy
  - The drone has two radios
    - Wake-up channel: continuously sends wake-up signals including drone's public key
    - Data channel: used only for data exchange
  - allows multiple sensors to concurrently execute pCLSC-TKEM

PURDUE UNIVERSITY

CERIAS



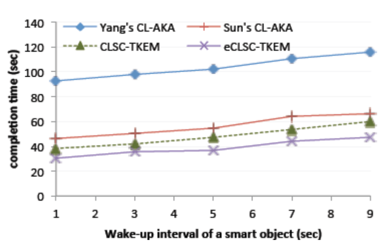


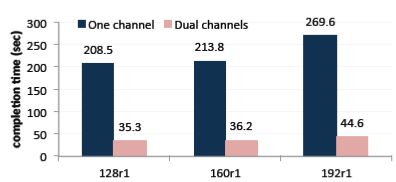
Altitude: 10m
Comm. range: 30m

Experimental Results

Protocol	secp128r1	secp160r1	secp192r1
Yang's CL-AKA [26]	32.84	36.22	50.43
Sun's CL-AKA [24]	15.10	16.98	23.84
CLSC-TKEM [21]	13.37	13.87	18.77
eCLSC-TKEM	9.25	9.61	13.03

Comparison of the on-line computation time of a smart object (unit: second)





Impact of dual channel strategy

On-going Work

- Encryption protocols for one-to-many communications
- Attestation techniques
- *White-box cryptography*
- Access control for drones and Internet of Drones (IoD)
- Scalable distributed encryption key management

PURDUE UNIVERSITY

CERIAS

Security Framework for IOT

Prepare and Prevent

nesCheck
- static analysis and dynamic instrumentation for nesC memory safety [to be submitted]

OptAll
- security provisioning based on game theory [ICDCS 2016]

Monitor and Detect

Kalis
- knowledge-driven adaptable IDS for IoT [to be submitted]

Heimdall
- whitelist-based anomaly detection defense for IoT routers [to be submittted]

Diagnose and Understand

Fine-Grained Analysis
- node- vs link-related packet dropping attacks
- interference location [SECON'14] [ACM ToSN'16]
- statistical model based on variance [SP4SC (IEEE FiCloud'16)]

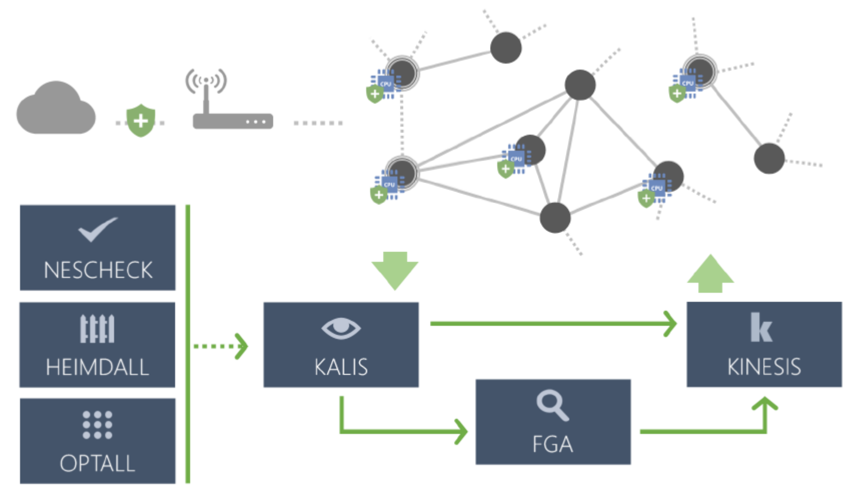
React, Recover and Fix

Kinesis
- automated response system [ACM SenSys'14] [ACM ToSN'16]

PURDUE UNIVERSITY

CERIAS

Security Framework for IOT



PURDUE UNIVERSITY

CERIAS

Monitor and Detect

Kalis

D. Midi, A. Mudgerikar,

A. Rullo, E.Bertino

PURDUE UNIVERSITY

CERIAS

kalis

Knowledge-driven Adaptable IDS for IoT

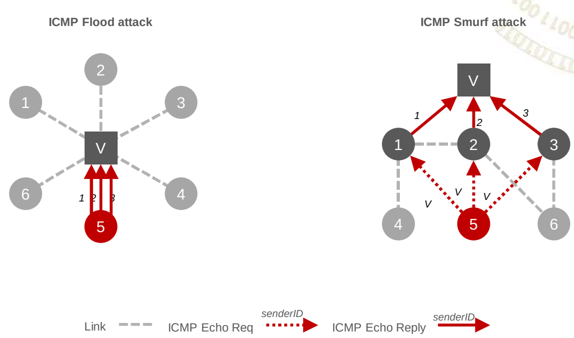
- to detect attacks in real time across heterogeneous IoT systems
- running different communication protocols and with different security goals
- adapting detection strategy to specific network features

APPLICATIONS: Intrusion detection in domestic and corporate scenarios, …

PURDUE UNIVERSITY

CERIAS

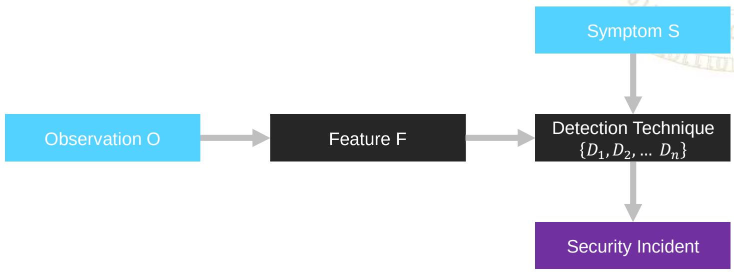
Leveraging Knowledge



PURDUE UNIVERSITY

CERIAS

Knowledge-driven Intrusion Detection



PURDUE
UNIVERSITY

CERIAS

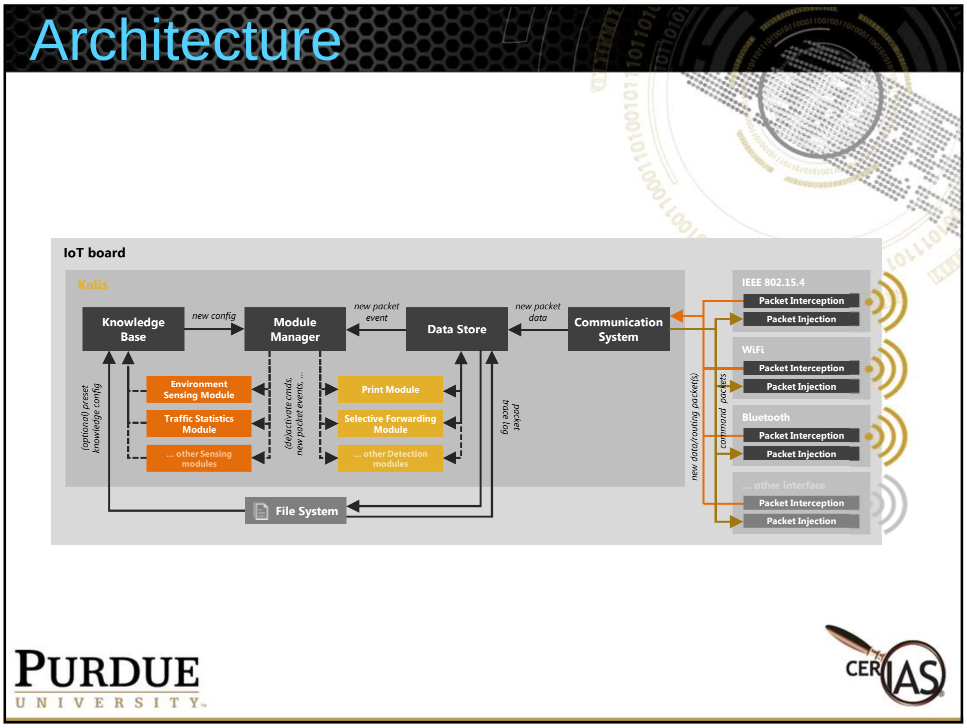
Leveraging Knowledge: Taxonomy by Features

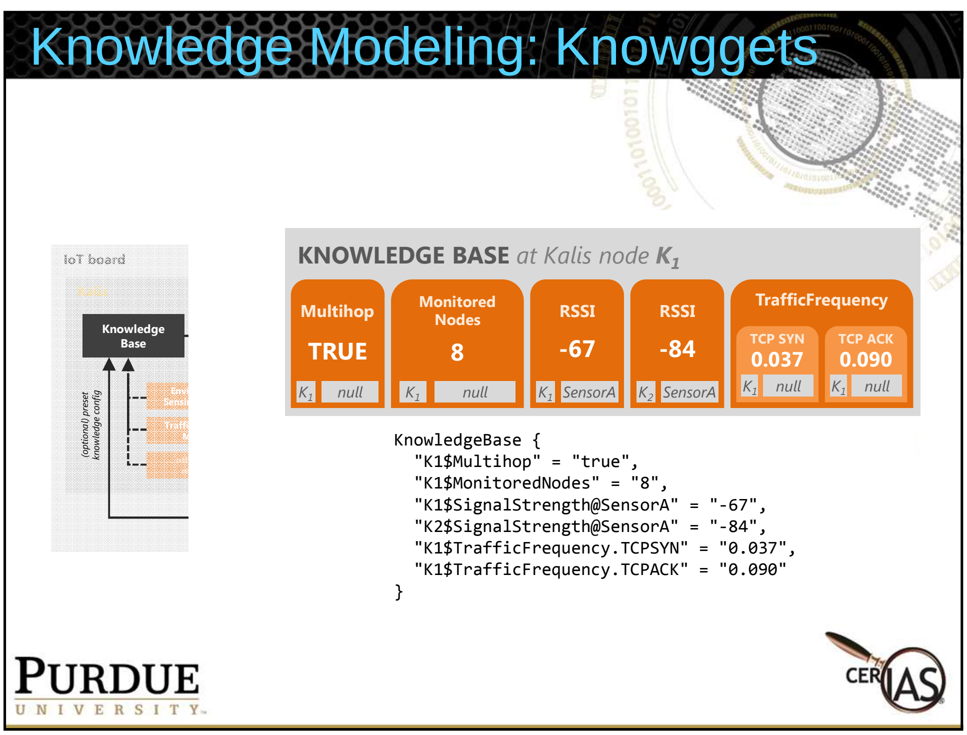
	FEATURES (by class)																											
	deployment		mobility		communication			topology		coverage		composition		QoS		routing protocol			location		availability of prevention techniques							
ATTACKS	one time	iterative	static	mobile	radio	inductive	sound	single-hop	multi-hop	redundant	non redundant	heterogeneous	homogeneous	timeliness	reliability	max power	min energy	shortest path	human av	non human av	crypto puzzle	cryptography	code attestation	tamper-resistant	FHSS	code spreading	identity verification	dynamic routing
selective forwarding	•	•	○	○	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	×	•	•	•	×	•	•	•	×
replication	•	•	○	○	•	•	•	×	•	•	•	•	•	•	•	•	•	•	•	×	•	•	•	×	•	•	•	•
sinkhole	•	•	○	○	•	×	•	×	•	•	×	•	•	•	•	○	○	○	•	×	•	•	•	×	•	•	•	•
sybil	•	•	○	○	•	×	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	×	•	×	•	•	•	•
wormhole	•	•	○	○	•	×	×	×	•	•	•	•	•	•	•	•	•	•	•	×	•	•	•	×	•	•	•	•
HELLO flood	×	•	○	○	•	×	•	×	•	•	•	•	•	•	•	•	•	•	•	•	×	•	×	•	•	•	×	•
ACK spoofing	•	•	•	•	•	×	•	×	•	•	•	•	•	•	•	○	○	×	•	•	•	•	•	•	•	•	•	•
data alteration	•	•	•	•	•	×	•	•	•	•	•	•	•	•	×	•	•	•	•	×	•	×	×	×	•	•	•	•
data repetition	•	•	•	•	•	×	•	•	•	•	•	•	•	•	•	•	•	•	•	×	•	•	×	×	•	•	•	•
transmission delay	•	•	○	○	•	×	•	•	•	•	•	•	•	×	•	•	•	•	•	×	•	•	×	×	•	•	•	•
jamming	•	•	•	•	•	×	•	•	•	•	•	•	•	•	•	•	•	•	•	×	•	•	•	•	×	×	•	•
collision	•	•	•	•	•	×	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
flooding	•	•	•	•	•	×	•	×	•	•	•	•	•	•	•	•	•	•	•	•	×	•	•	•	•	•	•	•
self-propagating code injection	•	•	•	•	•	•	•	•	•	•	•	×	•	•	•	•	•	•	•	•	•	•	×	•	•	×	•	•
TCP SYN flood	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
smurf attack	•	•	•	•	•	•	•	○	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ICMP flood	•	•	•	•	•	•	•	×	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
fraggle attack	•	•	•	•	•	•	•	○	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

• attack possible   × attack not possible   ○ detection technique depends on feature

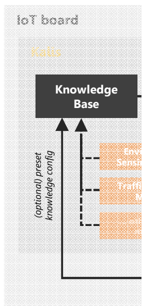
PURDUE
UNIVERSITY

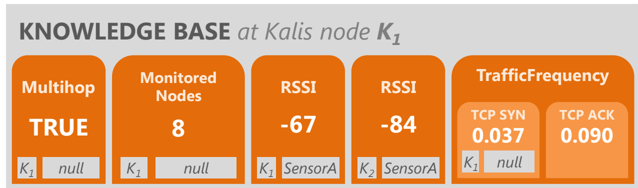
CERIAS


Architecture
IoT board
Kalis
Knowledge Base
new config
Module Manager
new packet event
Data Store
new packet data
Communication System
(optional) preset knowledge config
Environment Sensing Module
Traffic Statistics Module
... other Sensing modules
(de)activate cmds, new packet events, ...
Print Module
Selective Forwarding Module
... other Detection modules
packet trace log
File System
new data/routing packet(s)
command packets
IEEE 802.15.4
Packet Interception
Packet Injection
WiFi
Packet Interception
Packet Injection
Bluetooth
Packet Interception
Packet Injection
... other interface
Packet Interception
Packet Injection
PURDUE
UNIVERSITY
CERIAS


Knowledge Modeling: Knowggets
IoT board
Knowledge Base
(optional) preset knowledge config
KNOWLEDGE BASE at Kalis node K1
Multihop
TRUE
K1 null
Monitored Nodes
8
K1 null
RSSI
-67
K1 SensorA
RSSI
-84
K2 SensorA
TrafficFrequency
TCP SYN
0.037
K1 null
TCP ACK
0.090
K1 null
KnowledgeBase {
"K1$Multihop" = "true",
"K1$MonitoredNodes" = "8",
"K1$SignalStrength@SensorA" = "-67",
"K2$SignalStrength@SensorA" = "-84",
"K1$TrafficFrequency.TCPSYN" = "0.037",
"K1$TrafficFrequency.TCPACK" = "0.090"
}
PURDUE
UNIVERSITY
CERIAS

knowledge modeling: knowggets






```
KnowledgeBase {
  "K1$Multihop" = "true",
  "K1$MonitoredNodes" = "8",
  "K1$SignalStrength@SensorA" = "-67",
  "K2$SignalStrength@SensorA" = "-84",
  "K1$TrafficFrequency.TCPSYN" = "0.037",
  "K1$TrafficFrequency.TCPACK" = "0.090"
}
```

PURDUE UNIVERSITY

CERIAS

Configuration Grammar

⟨config⟩ ::= ⟨modules⟩ ⟨knowggets⟩

⟨modules⟩ ::= 'modules = {' ⟨module-list⟩ '}'

⟨module-list⟩ ::= ⟨module-def⟩ ',' ⟨module-list⟩
| ⟨module-def⟩

⟨module-def⟩ ::= ⟨module-name⟩ ['(' ⟨param-list⟩ ')']

⟨param-list⟩ ::= ⟨key-value-pair⟩ ',' ⟨param-list⟩
| ⟨key-value-pair⟩

⟨knowggets⟩ ::= 'knowggets = {' ⟨knowgget-list⟩ '}'

⟨knowgget-list⟩ ::= ⟨key-value-pair⟩ ',' ⟨knowgget-list⟩
| ⟨key-value-pair⟩

⟨key-value-pair⟩ ::= ⟨key⟩ '=' ⟨value⟩

```
modules = {
  TopologyDetectionModule,
  TrafficStatsModule (
    activationThresh=1,
    detectionThresh=2
  )
}
knowggets = {
  mobility = false
}
```

PURDUE UNIVERSITY

CERIAS

Implementation

- Java on Odroid xu3 board
  - *IEEE 802.15.4:* TelosB sensor mote with TinyOS
  - *WiFi:* Tcpdump with libpcap
- Dynamicity in the implementation
  - Java Reflection for dynamic module activation
  - Event-driven implementation for async execution
  - Publish-subscribe pattern for async event propagation
- Collective Knowledge Synchronization
  - Through *discovery-through-advertisement* pattern

PURDUE UNIVERSITY

CERIAS

Experimental Setup

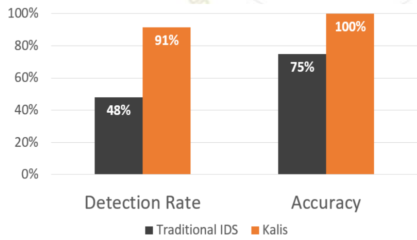
- Small WSN+ real-world IoT devices
  - 6 TelosB motes, TinyOS app sending data message every 3 seconds over CTP
  - Kalis node placed near middle section of WSN
  - Nest Thermostat, August SmartLock, Lifx smart lightbulb, Arlo security camera, Amazon Dash Button
- Recording/replay of actual traffic traces
  - Enhanced with packets representing symptoms (50 instances/attack scenario)
- Comparing Kalis vs. traditional IDS
  - Emulated as Kalis node w/o knowledge base, all modules always active

PURDUE UNIVERSITY

CERIAS

Experimental Results

- Metrics
  - Detection rate
  - Classification accuracy
  - CPU usage
  - RAM usage
- Attack scenarios
  - ICMP Flood, single-hop network
  - Replication, static vs. mobile network



	Trad. IDS	Kalis	
CPU usage (%)	0.22%	0.19%	(−16.00%)
RAM usage (kb)	23961.06	13978.62	(−41.66%)

PURDUE UNIVERSITY

CERIAS

Reactivity to Environment Changes

- Selective Forwarding attack on ZigBee
  - ZigBee network, one attacker
  - No a-priori knowgget, no detection module active by default
- Topology Discovery sensing module
  - Immediately detects multihop network
  - Activates Selective Forwarding detection module
  - Achieve 100% detection rate from first attack

PURDUE UNIVERSITY

CERIAS

Research Directions

- Management of IoT devices including identity management
  - Identify and locate devices
  - Authenticate devices
  - Maintain device hw/sw (including patching), protection against firmware and software attacks
- Data management in IoT
  - Confidentiality
  - Availability
  - Integrity
- Privacy in IoT
  - Controlled data acquisition
  - Anonymity
- IoT Safety
- Design, test, configure, and monitor IoT systems

PURDUE UNIVERSITY

CERIAS

How to Reason about IoT Data Security and Privacy

Based on

- Jeff Voas "Primitives and Elements of Internet-of-Things (Iot) Trustworthiness" Draft NIST IR 8063 http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8063\
- Slides of ACM CODASPY 2016 Keynote Talk by Jeff Voas

PURDUE UNIVERSITY

CERIAS

Primitives

1. **Sensor** A *sensor* is an electronic utility that digitally measures physical properties such as temperature, acceleration, weight, sound, etc.
2. **Aggregator** An *aggregator* is a software implementation based on mathematical function(s) that transforms groups of raw data into *intermediate* data.
3. **Communication channel** A *communication channel* is a medium by which data is transmitted (e.g., physical via USB, wireless, wired, verbal, etc.).
4. ***eUtility*** A *e*Utility (external utility*)* is a software or hardware product or service.
5. **Decision trigger** A *decision* trigger creates the final result(s) needed to satisfy the purpose, specification, and requirements of a specific NoT.

PURDUE UNIVERSITY

CERIAS

Sensor

1. Sensors are physical.
2. Sensors may have little or no software functionality and computing power; more advanced sensors may have software functionality and computing power.
3. Sensors will likely be heterogeneous, from different manufacturers, and collect data, with varying levels of data integrity.
4. **Sensors will have operating geographic locations that may change.**
5. **Sensors may provide surveillance. Cameras and microphones are sensors.**
6. **Sensors may have an owner(s) who will have control of the data their sensors collect, who is allowed to access it, and when.**
7. **Sensors will have pedigree – geographic locations of origin and manufacturers. Pedigree may be unknown and suspicious.**
8. **Sensors may fail continuously or fail intermittently.**
9. **Sensors may be cheap, disposable, and susceptible to wear-out over time;** here, building security into a specific sensor will rarely be cost effective. However there will differentials in security, safety, and reliability between consumer grade, military grade, industrial grade, etc.

PURDUE UNIVERSITY

CERIAS

Sensor

10. **Sensors may return no data, totally flawed data, partially flawed data, or correct/acceptable data.**
11. **Sensors are expected to return data in certain ranges, e.g., [1 … 100]. When ranges are violated, rules may be needed on whether to turn control over to a human or machine when ignoring out-of-bounds data is inappropriate.**
12. **Sensor repair is likely handled by replacement.**
13. Sensors may be acquired off-the-shelf.
14. Sensors release data that is event-driven, driven by manual input, or released at pre-defined times.
15. **Sensors may have a level of data integrity ascribed (Weights).**
16. **Sensors may have their data encrypted to void some security concerns**
17. **Sensor data may be leased to multiple IoT systems. A sensor may have multiple recipients of its data.**
18. **The frequency with which sensors release data impacts the data's currency and relevance. Sensors may return valid data at an incorrect rate/speed.**
19. **Sensor data may be 'at rest' for long periods of time; sensor data may become *stale.***
20. A sensor's resolution may determine how much information is provided.
21. **Security is a concern for sensors if they or their data is tampered with or stolen.**
22. **Reliability is a concern for sensors.**

PURDUE UNIVERSITY

CERIAS

Aggregator

1. Aggregators are likely virtual due the benefit of changing implementations quickly and increased malleability. A situation may exist where aggregators are physically manufactured.
2. Aggregators are assumed to lack computing horsepower, however this assumption can be relaxed by changing the definition and assumption of virtual to physical, e.g. firmware, microcontroller or microprocessor. Aggregators will likely use weights to compute intermediate data.
3. Aggregators have two actors that make them ideal for consolidating large volumes of data into lesser amounts: Clusters, and Weights. Aggregator is the *big data processor* within IoT.
4. Intermediate data may suffer from some level of *information loss*.
5. For each cluster there should be an aggregator or set of potential aggregators.
6. Aggregators are executed at a specific time and for a fixed time interval.
7. Aggregators may be acquired off-the-shelf.
8. Security is a concern for aggregators (malware or general defects) and for the sensitivity of their aggregated data.
9. Reliability is a concern for aggregators (general defects).

PURDUE UNIVERSITY

CERIAS

Thank you!!

Any question?

PURDUE UNIVERSITY

CERIAS