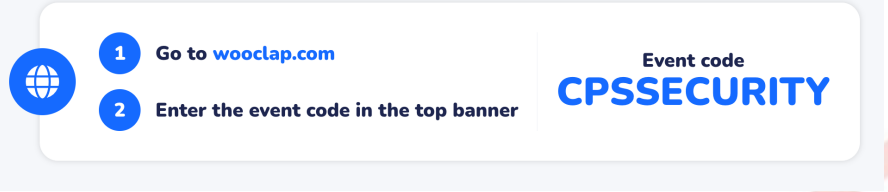
CE/CZ4055 Cyber Physical System Security

Attack Surfaces of Cyber Physical Systems

Anupam Chattopadhyay

SCSE, NTU



NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- *Attack Surfaces Classification*
- Attack Examples
- TVR Analysis
- Discussion

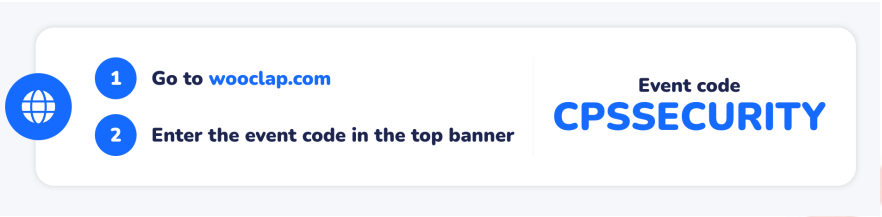
NANYANG TECHNOLOGICAL UNIVERSITY

Contents

Attack Surfaces Classification

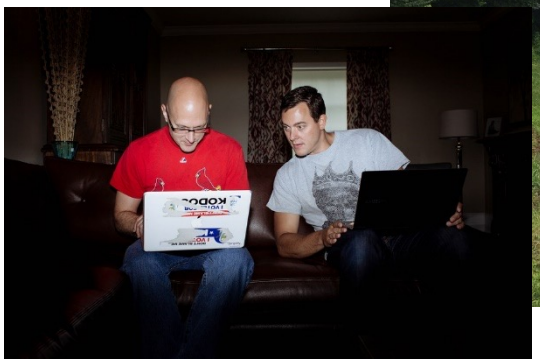
- Example of Autonomous Vehicle (AV)
- AV as CPS: CPS-driven Attack Classification
- IoT Protocol Layer-wise Classification
- Other Classifications

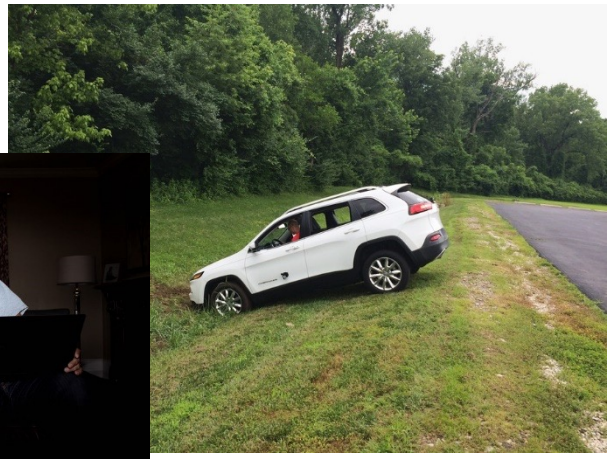
- Attack Examples
- TVR Analysis
- Discussion



NANYANG TECHNOLOGICAL UNIVERSITY

Real Threat



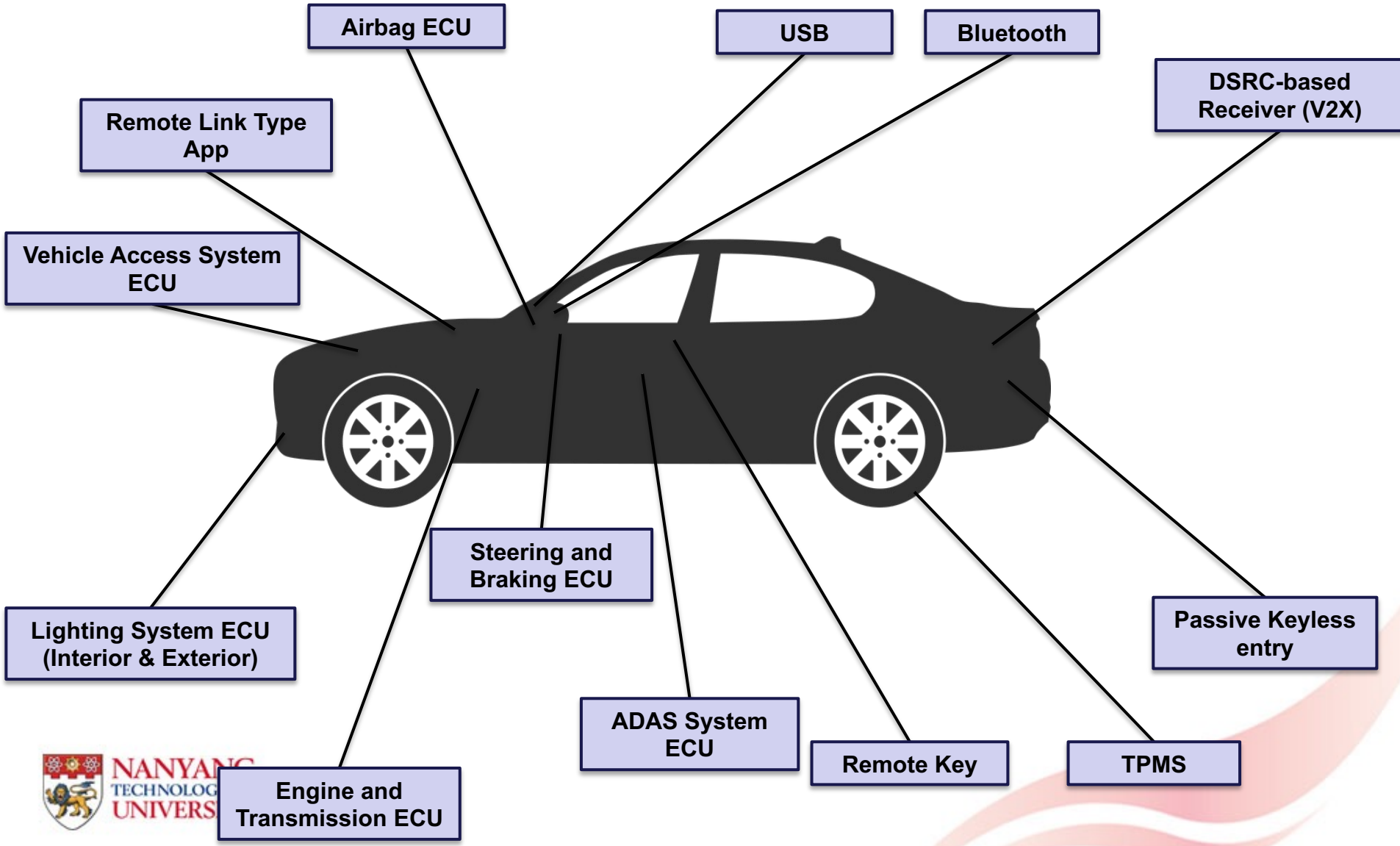


- Hackers took control of a Jeep Remotely, 2015
- Smart Home hacked in live demo, 2017
- Belarusian Railway servers hacked with ransomware, 2022

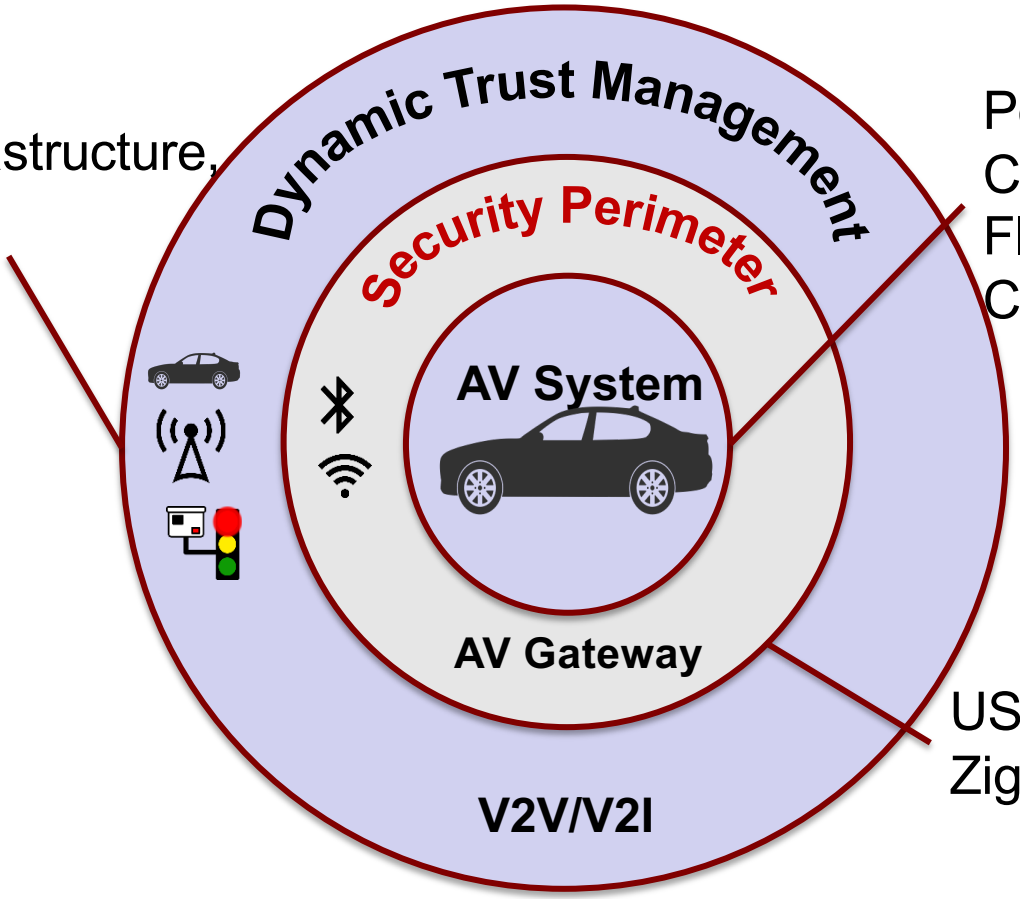
- IoT Security Market at $2.2B, 2019
- Projected to grow at 32.3% to $20.8B, 2027

NANYANG TECHNOLOGICAL UNIVERSITY

AV Attack Surfaces



Security Perimeter



NANYANG TECHNOLOGICAL UNIVERSITY

Examples of Security Perimeters

- Artificial Perimeters
- Natural Perimeter
- IT Security
  - Firewall
  - Access Control
- OT Security
  - Access Control
  - Surveillance

Contents

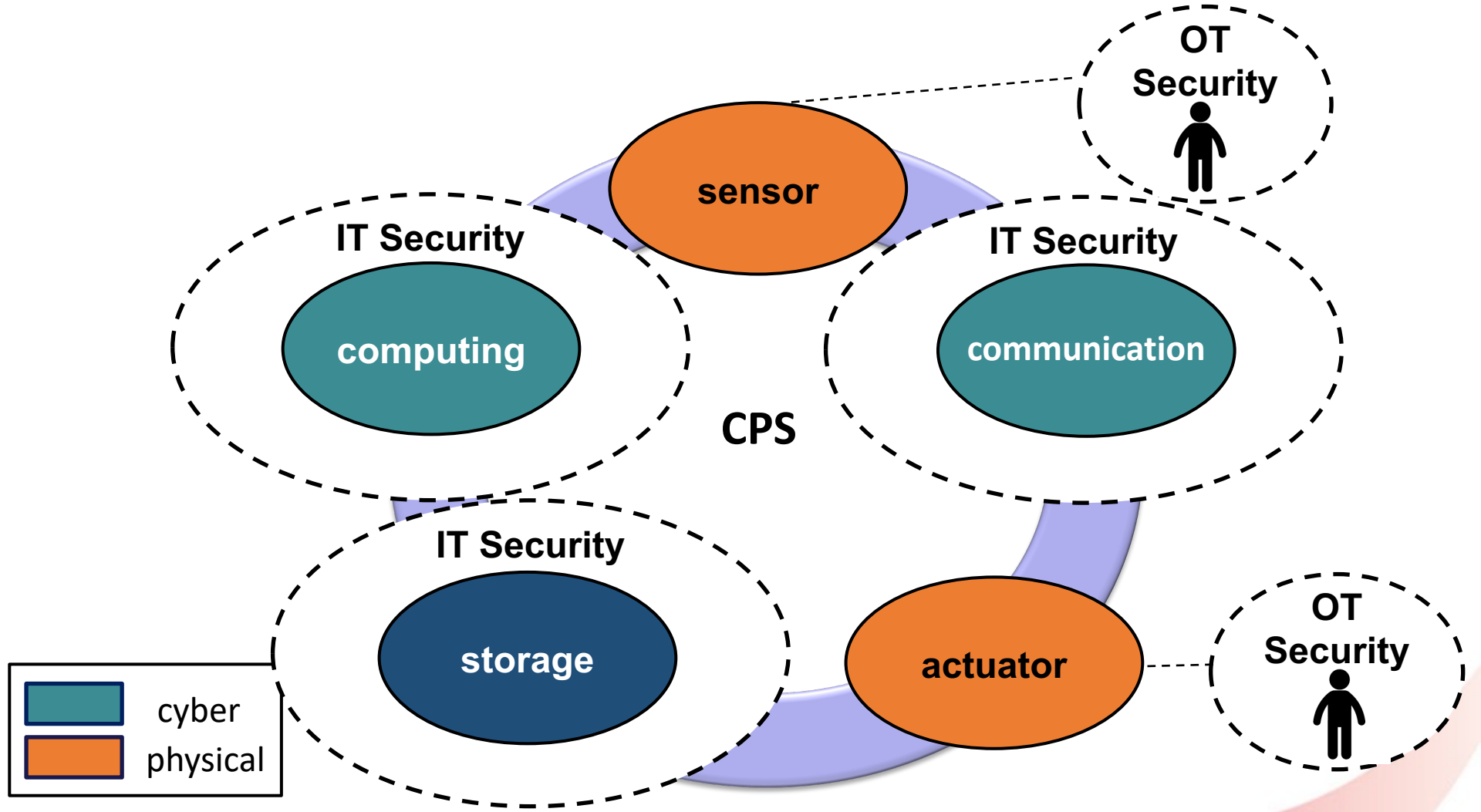
Attack Surfaces Classification

- Example of Autonomous Vehicle (AV)
- AV as CPS: CPS-driven Attack Classification
- IoT Protocol Layer-wise Classification
- Other Classifications

- Attack Examples
- TVR Analysis
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

AV as CPS

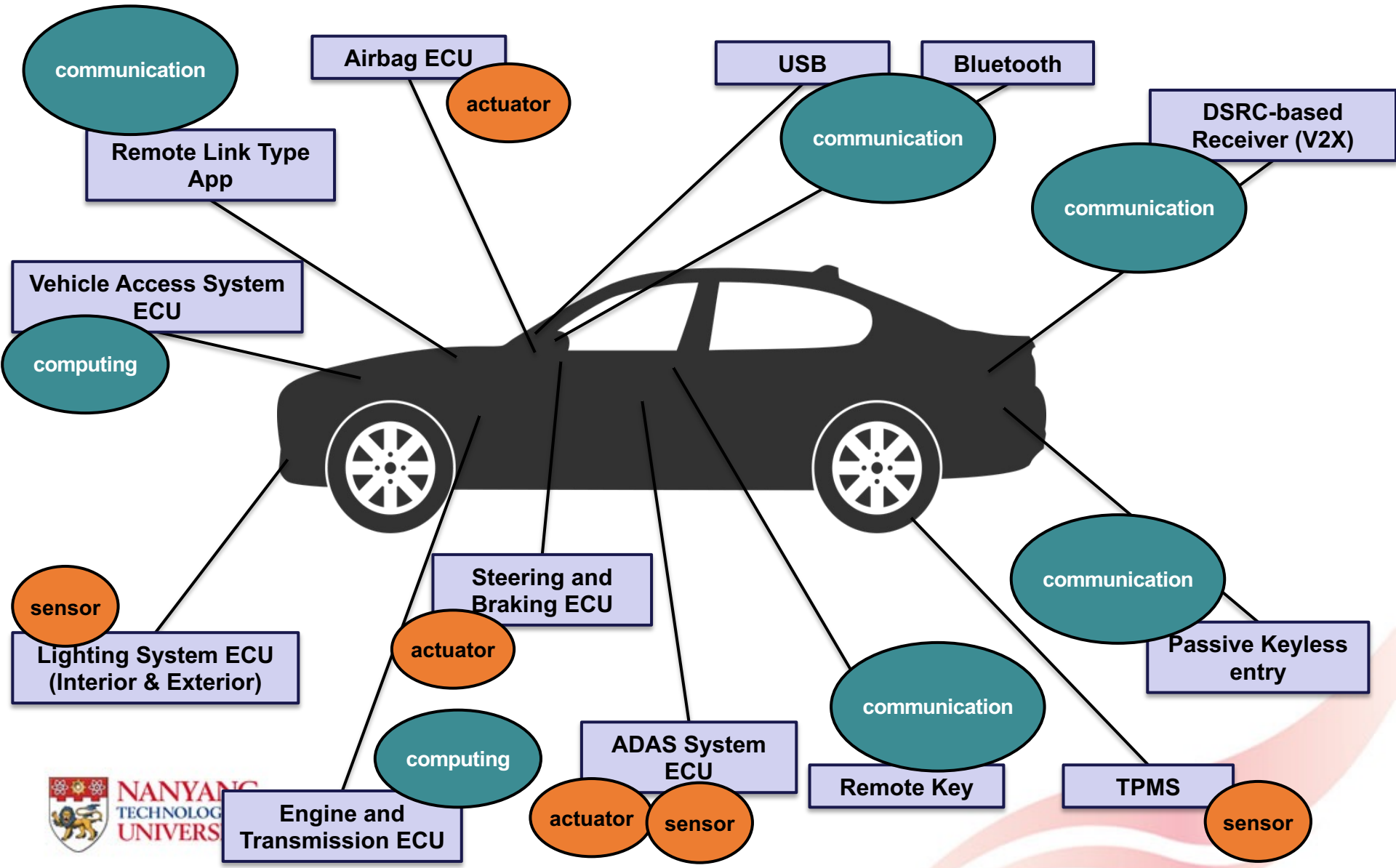


NANYANG TECHNOLOGICAL UNIVERSITY

Types of Attack Surfaces

- CPS-based Classification
  - Control/Computing
  - Storage
  - Communication
  - Sensor/Actuator

AV Attack Surfaces



Contents

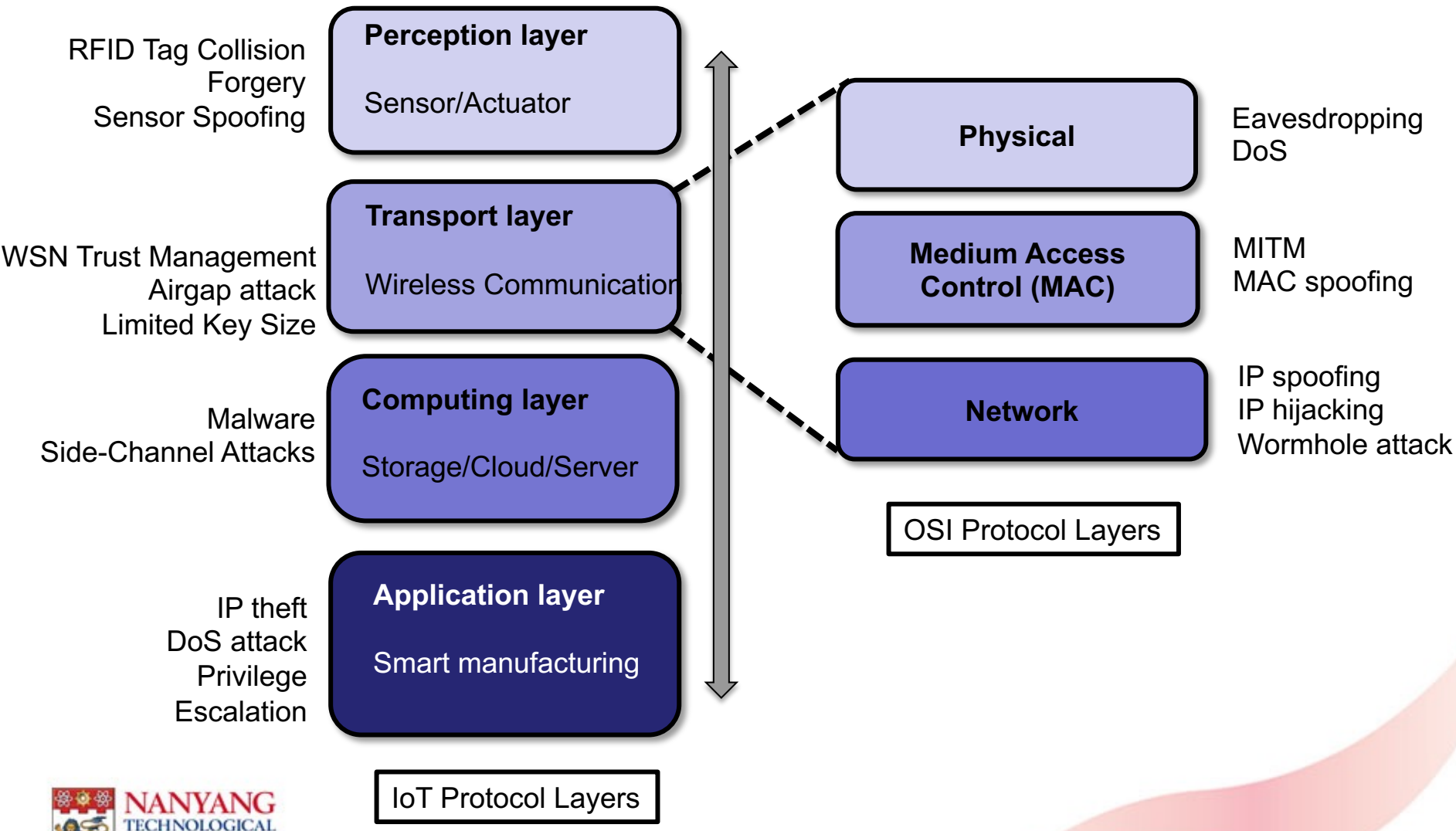
Attack Surfaces Classification

- Example of Autonomous Vehicle (AV)
- AV as CPS: CPS-driven Attack Classification
- IoT Protocol Layer-wise Classification
- Other Classifications

- Attack Examples
- TVR Analysis
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

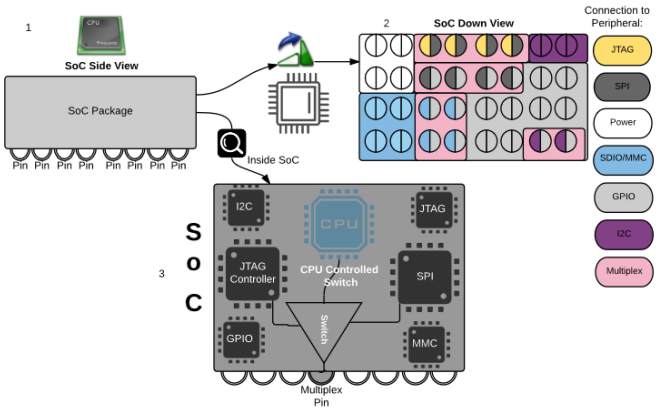
Attack Surfaces across IoT Layers

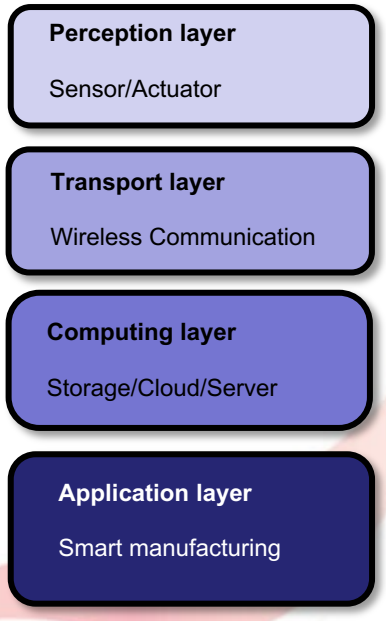


NANYANG TECHNOLOGICAL UNIVERSITY

Computing Layer: PLC Pin Control Attack

- Pin Multiplexing
  - Altering the pin connection to different peripherals
  - E.g., switching between memory and a sensor access
- Pin Configuration
  - Altering the Input and Output pin behavior



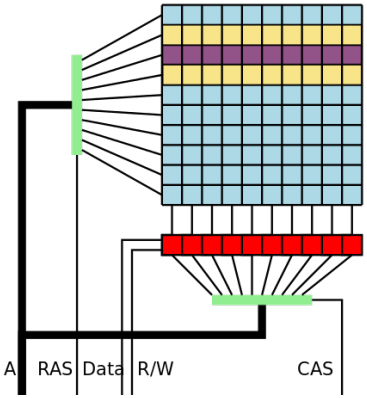


NANYANG TECHNOLOGICAL UNIVERSITY

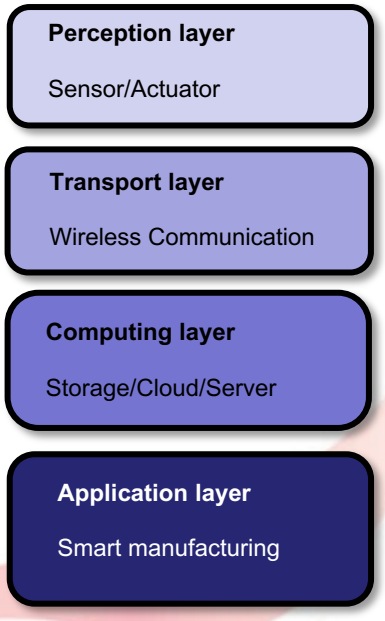
A. Abbasi, M. Hashemi, "Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack", Blackhat Europe 2016

Computing Layer: Rowhammer/Remanence

- Rowhammer: Highly repeated access to the same row/column can disturb the charge in neighboring (victim) row/column



- Remanence: Deleted Data is not really deleted
  - Application: Auto-backup
  - OS: Entry from file access table removed
  - HDD: Remanence based on the device property
- Data overwriting is needed to secure sensitive data after usage

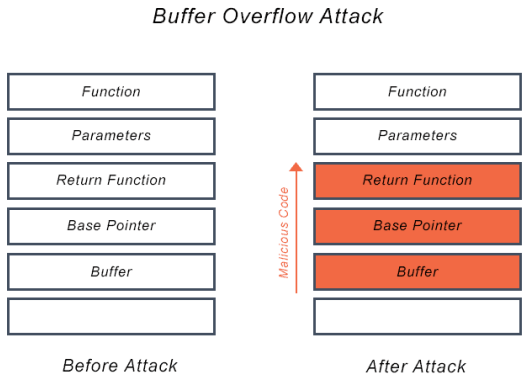


NANYANG TECHNOLOGICAL UNIVERSITY

Computing Layer: Software Attack

- Exploited Buffer Overflow vulnerability in the PKCS#11 driver
  - In a classic *buffer overflow exploit*, the attacker sends data to a program, which it stores in an undersized stack buffer. The result is that information on the *call stack is overwritten*, including the function's return pointer. The data sets the value of the return pointer so that when the function returns, it transfers control to malicious code contained in the attacker's data.

```
...
char buf[BUFSIZE];
cin >> (buf);
...
```

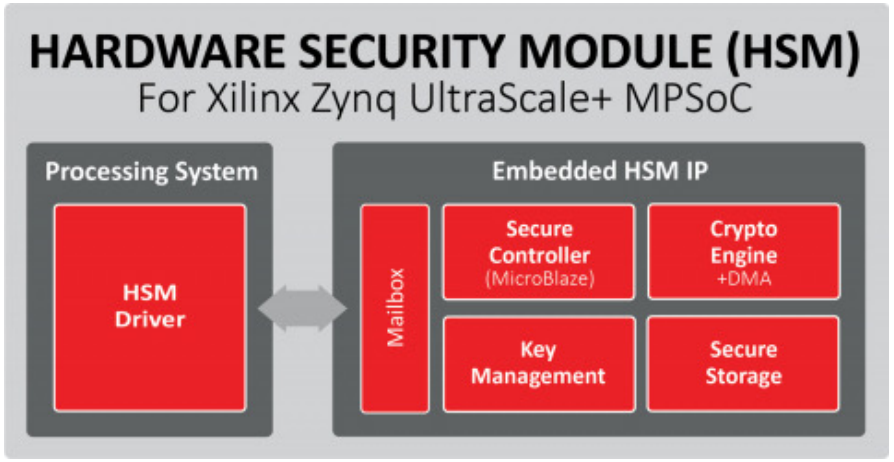


NANYANG TECHNOLOGICAL UNIVERSITY

J. Bedrune and G. Campana, "Everybody be cool, This is a Robbery!", Blackhat USA, 2019

Computing Layer: Protection

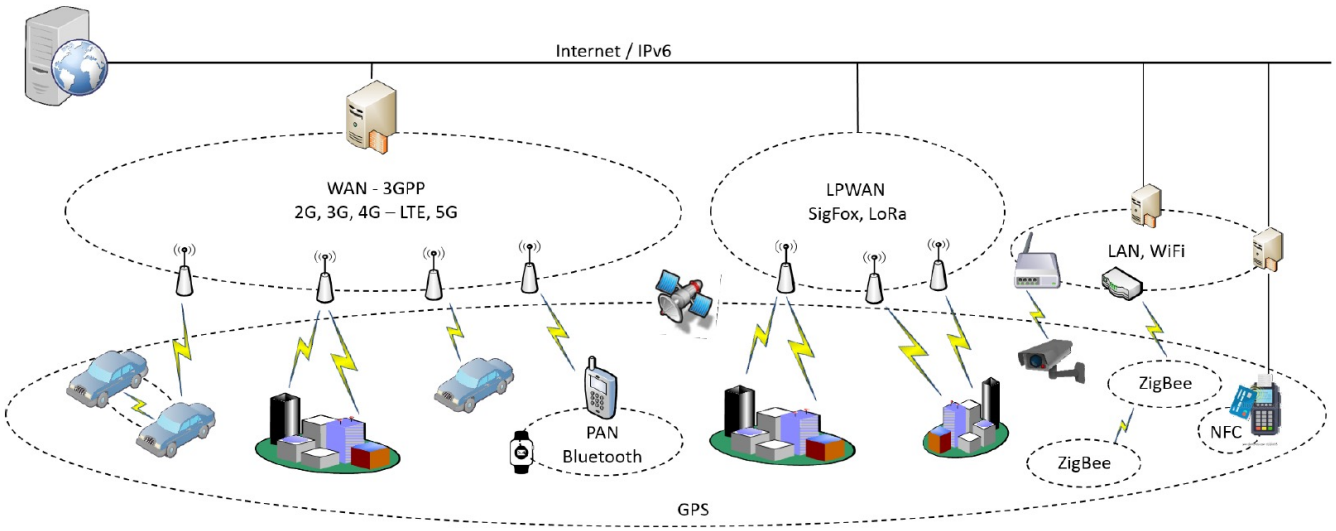
- Hardware security module (HSM) is a special-purpose computing unit with associated software/firmware attached to a system for providing cryptographic functions and cryptographic key management.



NANYANG TECHNOLOGICAL UNIVERSITY

Communication Layer Attacks

- Modern IoT systems utilize heterogeneous communication media



Perception layer

Sensor/Actuator

Transport layer

Wireless Communication

Computing layer

Storage/Cloud/Server

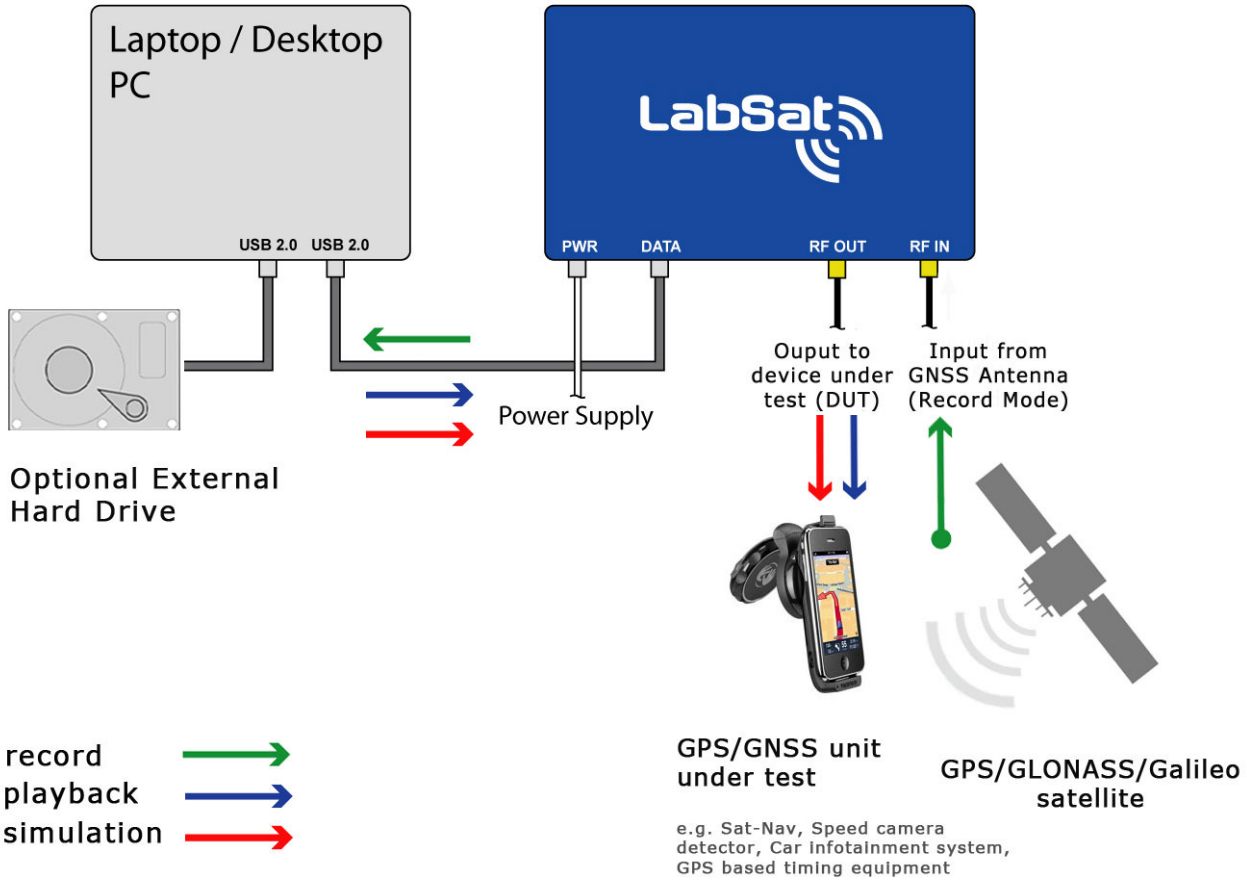
Application layer

Smart manufacturing

NANYANG TECHNOLOGICAL UNIVERSITY

A. Burg, A. Chattopadhyay, K.-Y. Lam, "Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things", Proceedings of IEEE, 2018

Sensor Layer: GPS spoofing



Perception layer

Sensor/Actuator

Transport layer

Wireless Communication

Computing layer

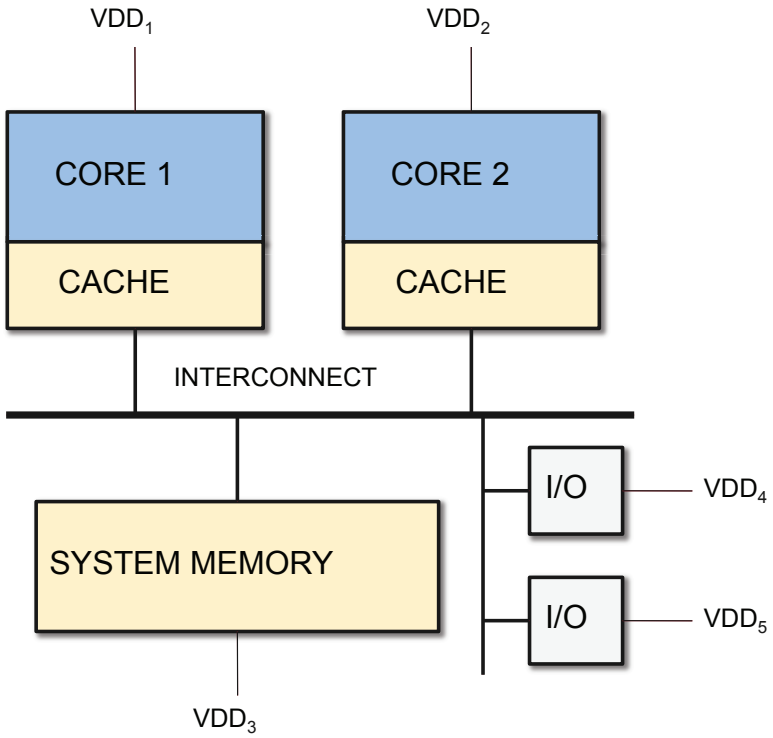
Storage/Cloud/Server

Application layer

Smart manufacturing

NANYANG TECHNOLOGICAL UNIVERSITY

Application Layer: Constraint-based Attack



- Drive a single core at a lower voltage using a malware
  - Feasible due to isolated SoC components

Perception layer
Sensor/Actuator

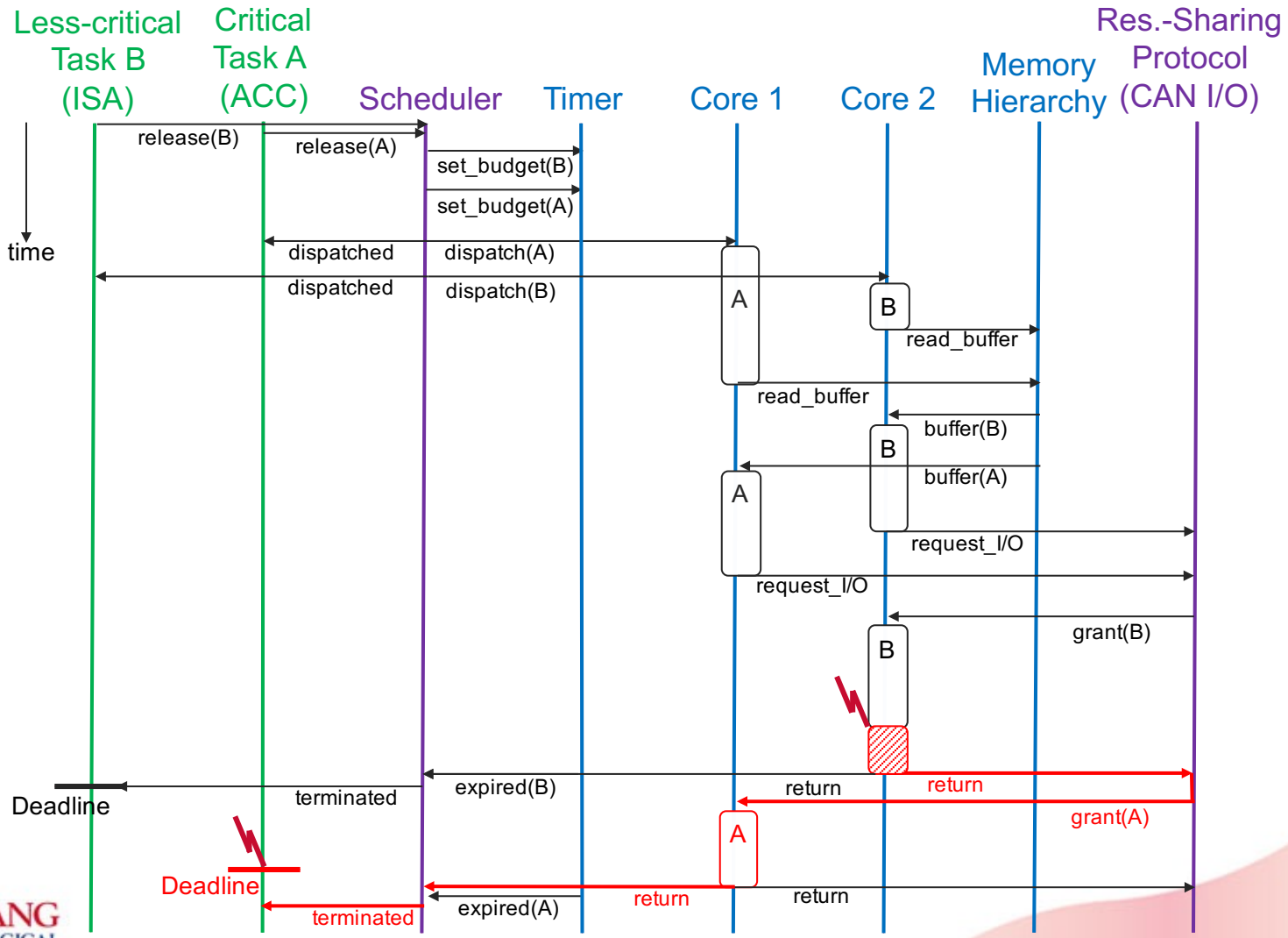
Transport layer
Wireless Communication

Computing layer
Storage/Cloud/Server

Application layer
Smart manufacturing

NANYANG TECHNOLOGICAL UNIVERSITY

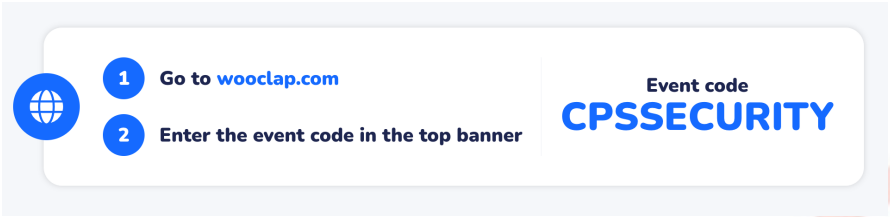
Application Layer: Constraint-based Attack
(contd.)



A. Easwaran, A. Chattopadhyay, S. Bhasin, "A systematic security analysis of real-time cyber-physical systems", ASP-DAC 2017

Contents

- *Attack Surfaces Classification*
  - Example of Autonomous Vehicle (AV)
  - AV as CPS: CPS-driven Attack Classification
  - IoT Protocol Layer-wise Classification
  - Other Classifications
- Attack Examples
- TVR Analysis
- Discussion



NANYANG TECHNOLOGICAL UNIVERSITY

MITRE ATT&CK® knowledge Base

- For Enterprise Systems but, can also apply to CPS/IoT
- Maintain an up-to-date cyber threat intelligence

1. Reconnaissance
   - E.g., Gather Victim Network Information
2. Resource Development
   - E.g., Establish accounts
3. Initial Access
   - E.g., Hardware Additions
4. Execution
   - Scheduled Task/Job
5. Persistence
   - Create or Modify System Process
6. Privilege Escalation
   - Access Token Manipulation

https://attack.mitre.org/

MITRE ATT&CK® knowledge Base

(contd.)

7. Defense Evasion
   - Domain policy modification
8. Credential Access
   - Forced authentication
9. Discovery
   - File/Directory Discovery
10. Lateral Movement
    - Remote services
11. Collection
    - Data from Information Repositories
12. Command and Control
    - Data Encoding
13. Exfiltration
    - Transfer data to cloud account
14. Impact
    - System Shutdown

Contents

- Attack Surfaces Classification
- *Attack Examples*
- TVR Analysis
- Discussion

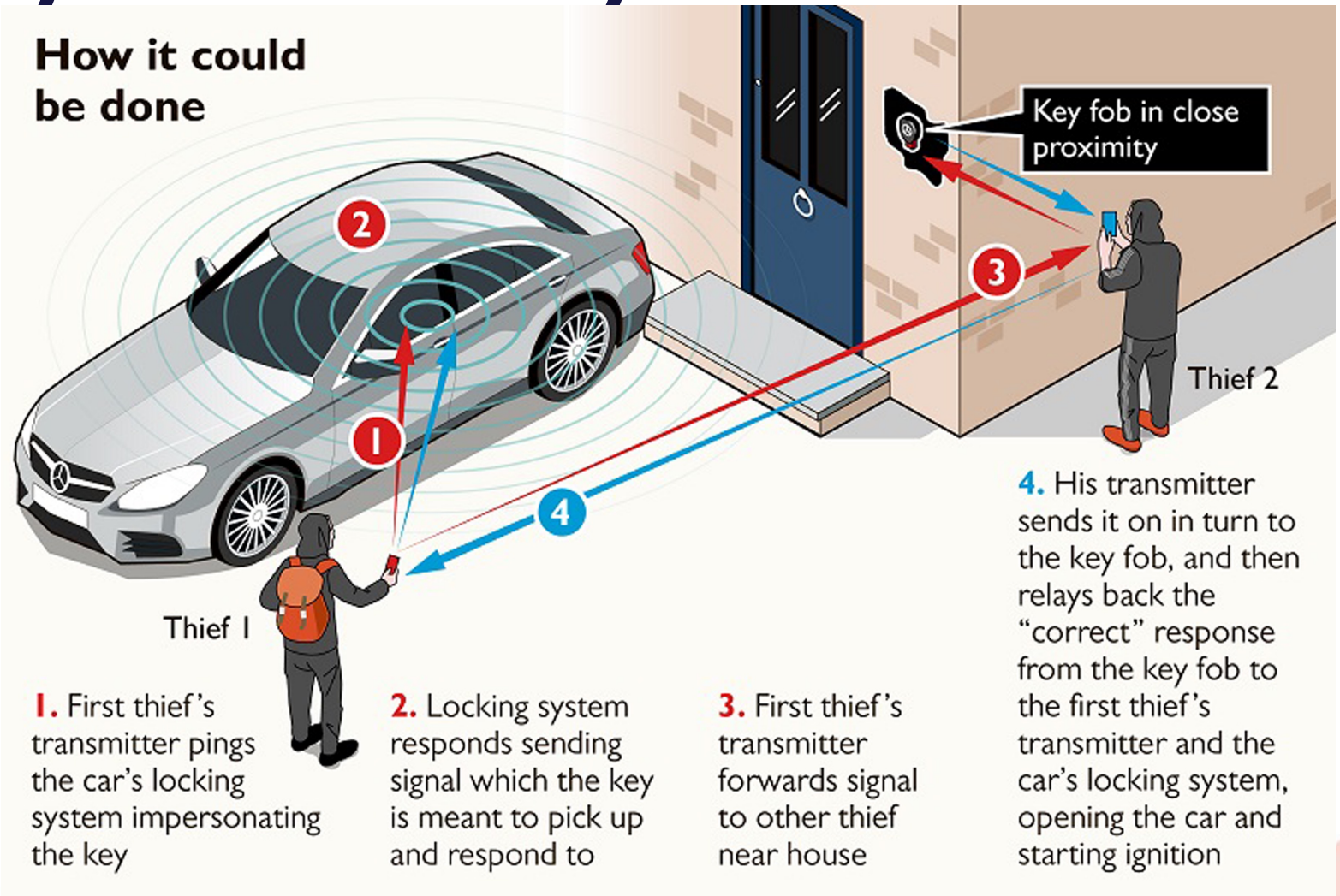
NANYANG TECHNOLOGICAL UNIVERSITY

1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

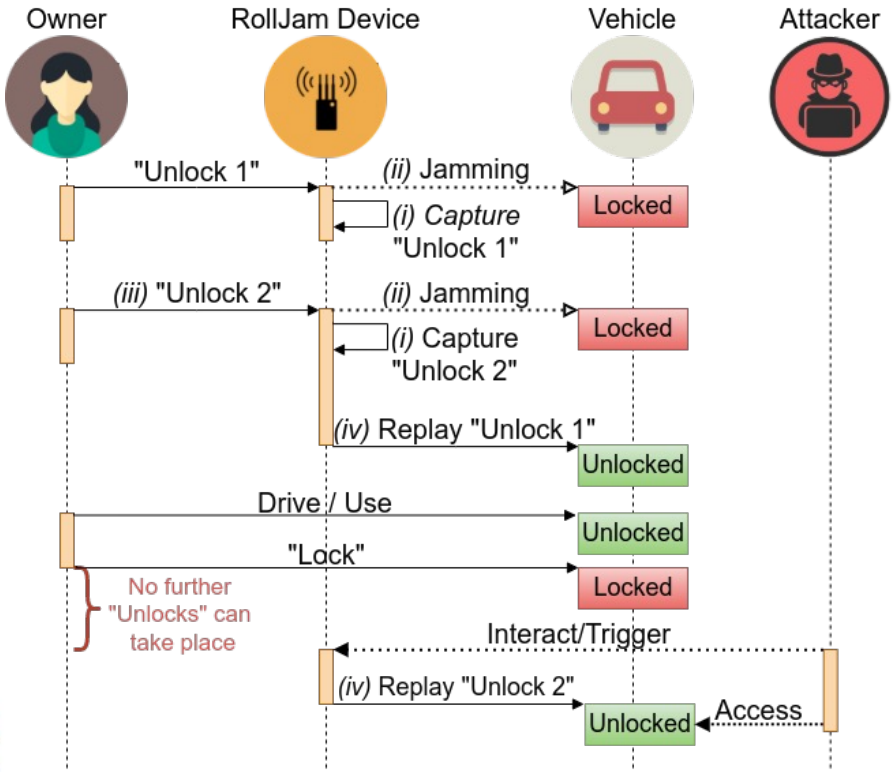
Keyless Car Entry



Keyless Car Entry (Prevention/Attack)

- Rolling code can be used to prevent simple ‘replay attack’.
- Yet, defeated with RollJam attack.

Audi A6 uses HCS301
Chip with Rolling Code



NANYANG TECHNOLOGICAL UNIVERSITY

Smart Bulb Attack

1. The *hacker controls the bulb's color* or brightness to trick users into thinking the bulb has a glitch. The bulb appears as 'Unreachable' in the user's control app, so they will try to 'reset' it.
2. The only way to *reset the bulb* is to delete it from the app, and then instruct the control bridge to re-discover the bulb.
3. The bridge discovers the *compromised* bulb, and the user adds it back onto their network.
4. The hacker-controlled bulb with updated firmware then uses the ZigBee protocol vulnerabilities to trigger a heap-based buffer overflow on the control bridge, by sending a large amount of data to it. This data also enables the hacker to *install malware on the bridge* – which is in turn connected to the target business or home network.
5. The malware connects back to the hacker and using a known exploit (such as EternalBlue), they can *infiltrate the target IP network* from the bridge to spread ransomware or spyware.

E. Ronen et al, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction" S&P 2017

Contents

- Attack Surfaces Classification
- Attack Examples
- *TVR Analysis*
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

TVR (Threat-Vulnerability-Risk) Assessment

- **Threat:** Anything that would contribute to the tampering, destruction or interruption of any service or item of value.

- Human
  - Hackers
  - Theft (electronically and physically)
  - Non-technical staff (financial/accounting)
  - Backup operators
  - Technicians, Electricians

- Non-Human
  - Floods, Lightning strikes, Fire
  - Plumbing, Electrical, Air (dust)
  - Viruses
  - Heat control

TVR (Threat-Vulnerability-Risk) Assessment *(contd.)*

- **Vulnerability:** Ability to gather information and cause breach of security triad (confidentiality-integrity-availability) despite safeguards in place
  - Determined through penetration testing

- Combined approach to determine Vulnerability
  - Attacker Effort and Exposure
  - Vulnerability requires major/significant resources to exploit, with heavy/little potential to affect many components.

TVR (Threat-Vulnerability-Risk) Assessment *(contd.)*

- **Risk:** Impact of the attack on the corporation in terms of economic/reputation loss
  - Man-months of shutdown
  - Accidental loss of sensitive data
  - Loss of brand image

- Trade-off between over-protection and risk quantification

Contents

- Attack Surfaces Classification
- Attack Examples
- TVR Analysis
- *Discussion*

NANYANG TECHNOLOGICAL UNIVERSITY

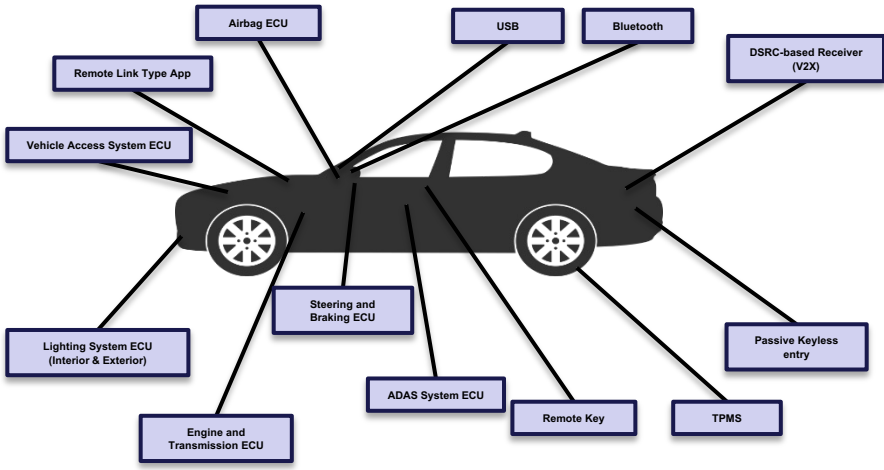
1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

What did we learn?

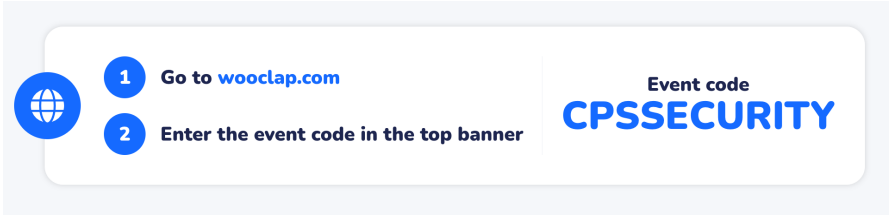
- **What is an Attack Surface?**
  - CPS-based Classification
  - IoT-Layers Classification
  - Attack Examples



- **Threat-Vulnerability-Risk Assessment**

NANYANG TECHNOLOGICAL UNIVERSITY

The End



NANYANG TECHNOLOGICAL UNIVERSITY