CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Internet-of-Things ("IoT") Security

A reality check

Aloysius Cheang
27 February 2019

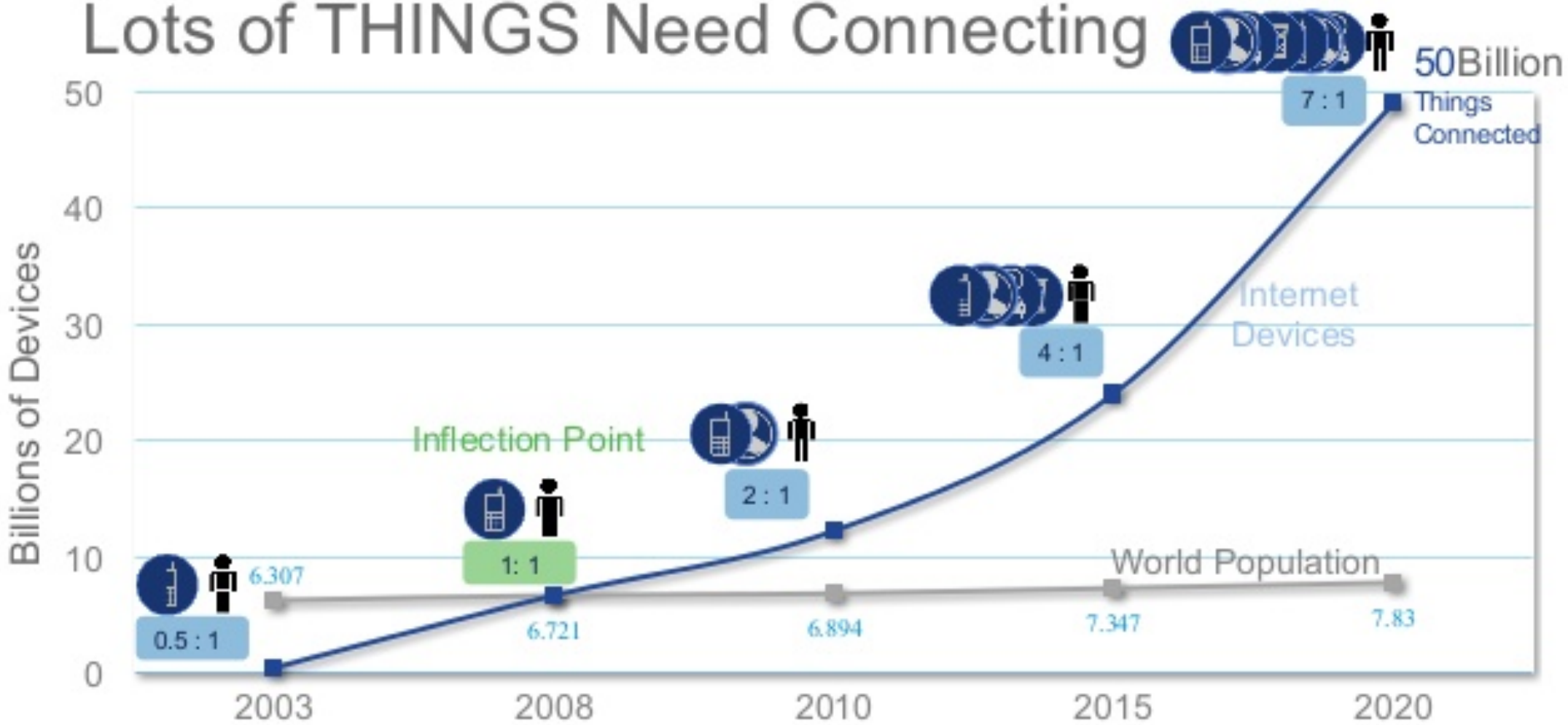
Agenda

- Foreword
- Risks and threats
- What we can do to close the gap (in security)
- Q&A

FOREWORD

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

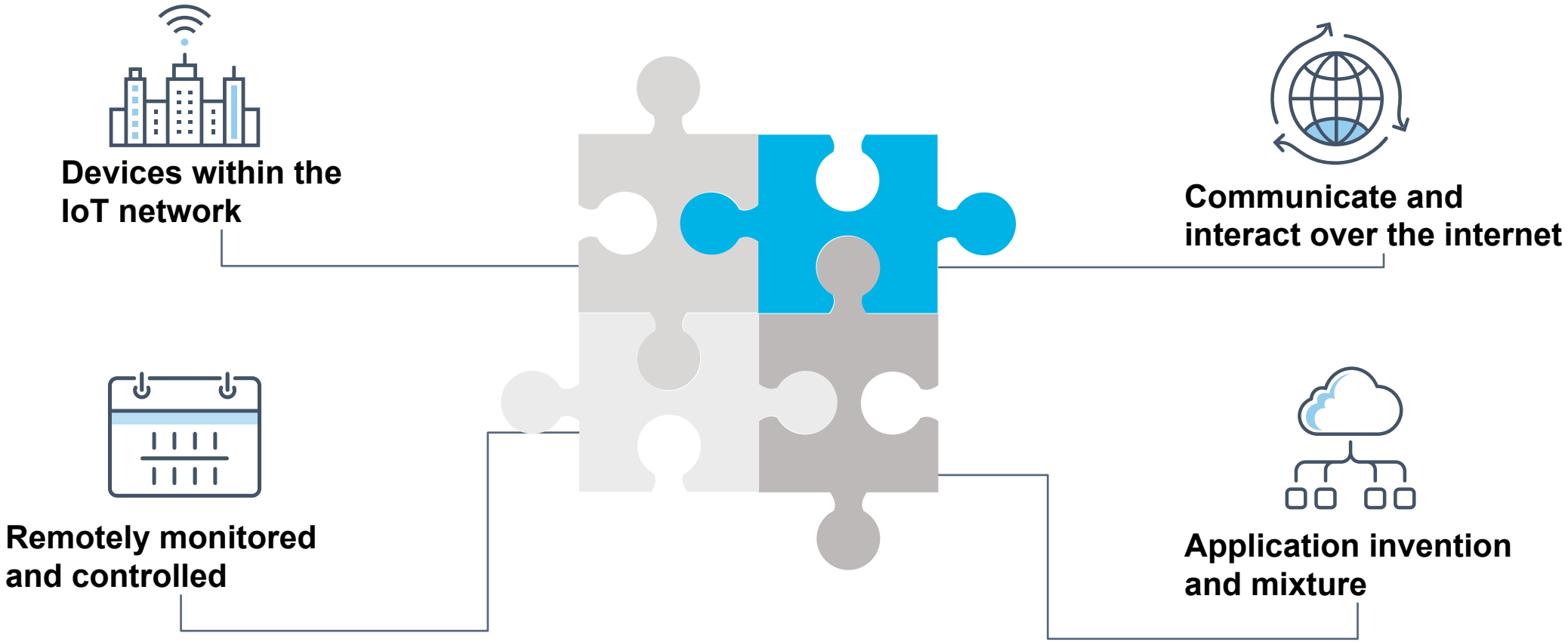
Lots of THINGS Need Connecting



Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

Background

IoT enables anything that is embedded with electronics, software, sensors, actuators, and connectivity to be connected to each other and make life easier and simpler, but together with the convenience, new security challenges also arise around the usage of IoT devices.



IoT technology has grown rapidly around the world in the past years. The growth will just keep going and it is expected to have billions of IoT devices installed and operated in 2025.

Building Cyber Leadership

Cyber is Global

RISKS AND THREATS

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

It starts with compromising “smart” devices that are built with no security in mind…

EDITION: AS

ZDNet

VIDEOS EXECUTIVE GUIDES SECURITY CLOUD INNOVATION CXO HARDWARE MORE NEWSLETTERS ALL WRITERS

MUST READ: 5G warning: Don't let governments ruin our plans with greed and red tape, warn networks

Over nine million cameras and DVRs open to APTs, botnet herders, and voyeurs

Re-branded IP cameras and DVRs sold by over 100 companies can be easily hacked, researchers say.

By Catalin Cimpanu for Zero Day | October 9, 2018 -- 15:35 GMT (23:35 GMT+08:00) | Topic: Security

OT – a gap in the security industry

TSMC lost US$171 million off its revenue and much more of spoiled chips that need to be disposed

CNN BUSINESS Markets Tech Media Success Perspectives Video

Computer virus cripples top Apple supplier TSMC

by Sherisse Pham @Sherisse

August 6, 2018: 8:54 AM ET

Hit another bump on the road for Industrial 4.0 (IIoT adoption)

MENU CSO FROM IDG CSO Events Resources/Whitepapers Opinions Blogs CSOM CISO Leaders

DHS warns of another dangerous flaw in Advantech WebAccess SCADA software

Liam Tung (CSO Online) on 24 October, 2018 08:53

0 Comments 36

The US DHS Industrial Control Systems CERT (ICS-CERT) has warned organizations using Advantech's ICS products to install an update that kills a remotely exploitable flaw in its WebAccess software.

WebAccess is the Taiwanese company's browser-based SCADA software for monitoring remote field devices. It's known among security researchers as a type of SCADA Human Machine Interface (HMI) system and has been the focus of security research in part because of its use of Microsoft's implementation of distributed computing protocol, Remote Procedure Call (RPC).

Managing legal and regulations internationally – mounting risk and costs!

Contact | Stay Connected | Privacy Policy | FTC en español

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » News & Events » Press Releases » ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk

ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk

SHARE THIS PAGE

FOR RELEASE

February 23, 2016

TAGS: deceptive/misleading conduct | Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

Taiwan-based computer hardware maker ASUSTeK Computer, Inc. has agreed to settle Federal Trade Commission charges that critical security flaws in its routers put the home networks of hundreds of thousands of consumers at risk. The administrative complaint also charges that the routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal information on the internet.

EVENTS CALENDAR

In English

En Español

Related Cases

ASUSTeK Computer Inc., In the Matter of

Related Actions

Getting eerily as they start to hit public transportation – flashes of 9-11

Evening Standard.

News Comment Football *Six Nations 2019* Insider GO London Lifestyle Show

News › Crime

Gatwick airport drone flight disruption: Army called in as drone pilot plays cat and mouse with police sparking mayhem for Christmas getaway passengers

Follow live updates on the latest at Gatwick Airport here +++ Chaos at Gatwick after drones flown over airport last night and in the early hours +++ Police hunting for pilots who sparked mass delays +++ Over 100,000 passengers caught up in mayhem +++ 760 flights either cancelled or delayed today by drones

JONATHAN PRYNN |, JUSTIN DAVENPORT |, NICHOLAS CECIL |, JOHN DUNNE |, BENEDICT MOORE-BRIDGER |
Thursday 20 December 2018 12:14

New terminology coined (achievement unlocked!)

Victim of your own circumstances

Shooting cars at your key infrastructures

Chinese Hackers Find Over a Dozen Vulnerabilities in BMW Cars

May 23, 2018 Mohit Kumar

Lemmings

by Psynosis...are these guys psychic?

And now you can kill …with a click

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

From Weapons of Mass Disruption to Weapons of Mass DESTRUCTION ?!

- The number of Internet of Things (IoT) devices is large, diverse, and inadequate. The number of malicious programs on IoT devices is rapidly increasing. The IoT devices are dominated by monitors and IP cameras, and the rest are various network devices and routers, or VoIP phone and printer, etc.
- IoT devices have become the main target of cyber attacks and the main source of security threats due to the proliferation of malicious programs on IoT devices.
- Hackers may use the IoT devices to establish relay stations, invade drones to steal sensitive information, and invade wearables and medical devices to obtain biological information.
- IoT can even be used to threaten lives! An armchair weapon of mass destruction!

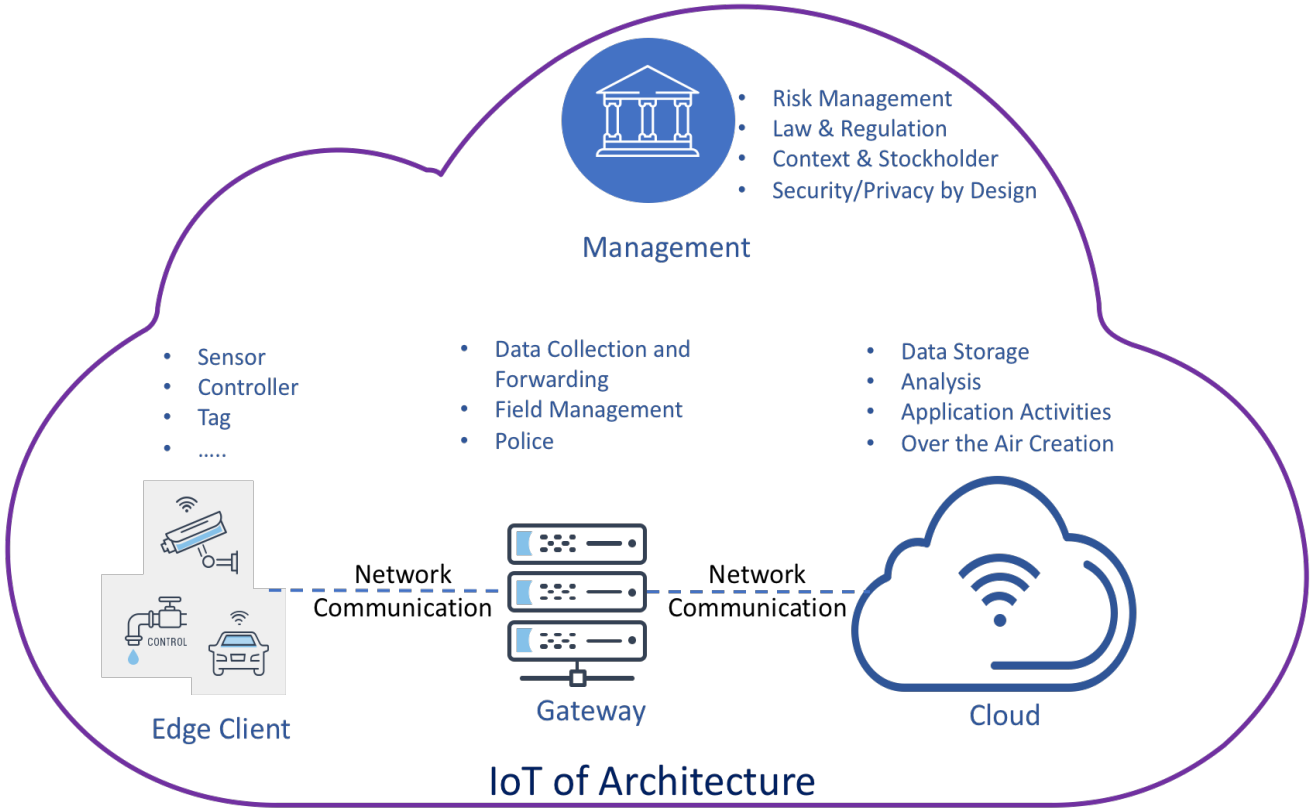
CHALLENGES

Framework and Components

Due to the complexity of the IoT architecture, it is not ideal to include all security issues related to each architecture in the world in the framework. Instead, this framework focus on the most common core components of the IoT architecture, which are: Edge Client, Gateway and Cloud.

Common use cases of the core IoT components:

- **<u>Edge Client</u>**
  Senses and collects data, then send the collected data to the Gateway
- **<u>IoT Gateway</u>**
  Acknowledges and confirms the reception of the data with Edge Client, then perform identification on the data before sending it to the Cloud
- **<u>Cloud</u>**
  Receives the data from Gateway, then saves the data into its storage. After analyzing the data, output will be broadcasted to the Edge Client through Gateway



Security Challenges

Privacy
Several IoT devices are used to collect and analyze sensitive data. The devices might not be secure enough to protect the users against security incidents such as data leakage.

Hardware Security
Hardware security is often neglected during the development of IoT. The IoT network becomes vulnerable if security mechanisms against hardware attacks such as physical intrusion or physical tapping of the IoT devices.

Vulnerability
Due to the massive connectivity of IoT, if one of the nodes is vulnerable to malicious attack, attackers might take advantage over the weakness link and attack the IoT network through the vulnerable node.

IoT Networking
Being remote controllable is often a key feature of IoT products. If network security mechanisms such as authentication is absent on the IoT device, malicious attacks can simply perform a remote attack toward the IoT network.

Mobile Device
Mobile devices are becoming an indivisible part of our life and is often connected to the IoT network.

Upgrade/ Update
System upgrade or update are common features for IoT devices. Without a strong authentication and verification mechanism, malicious users can leverage on the system update/upgrade interface to control the software, hardware or firmware of the IoT devices.

IoT Architecture
An IoT network consists of numerous IoT nodes which can be sensors, gateways or mobile devices. With the increasing number of nodes being connected to the IoT network, the chance of having a vulnerable node or malicious node within the network also increases.

Data Transmission
Distances between IoT nodes varies. They can be next to each other, or they can be installed in different continents. As data transmissions between IoT nodes usually rely on wireless connections, without sound authentication and identification mechanism, security incidents such as data leakage may occur.

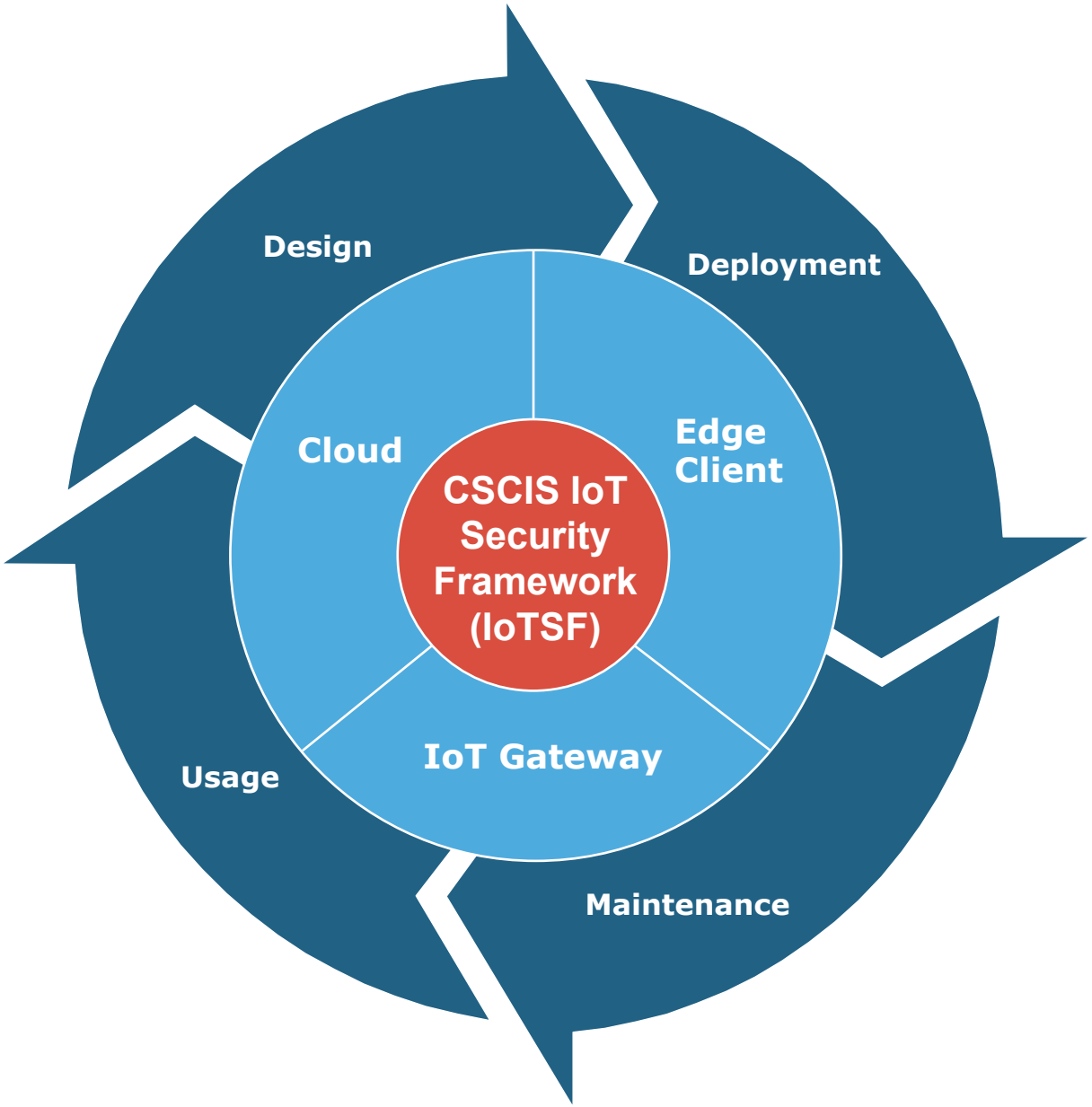
The above challenges are the most common and critical security challenges associated with IoT. If they have not been considered during the development IoT, the IoT ecosystem will become vulnerable if more and more vulnerable IoT devices start to kick in. As such, we proposes the CSCIS IoTSF to provide recommendations and best practices for IoT developers.

What we can do to close the gap (in security)

Objective

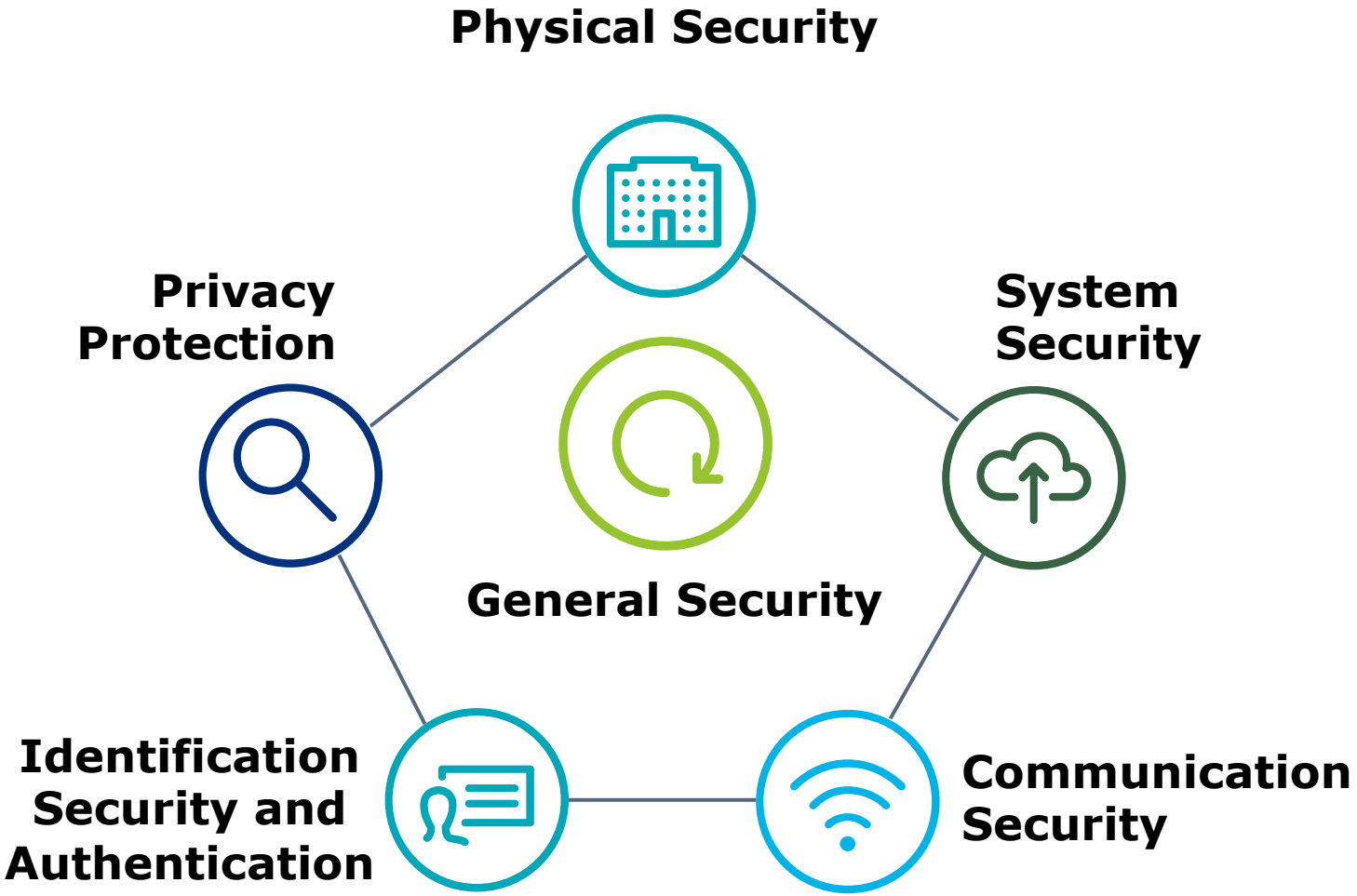
We aims to:

- Create a more secure IoT ecosystem through a well-defined IoT security framework on IoT components including edge clients, gateways and cloud.
- The framework provides recommendations and best practices for development and application of IoT and educate both the IoT developers and users on how to secure their IoT.
- The CSCIS IoT Security Framework (IoTSF) will help to strengthen the security of IoT by contributing recommendations and best practices on design, deployment, maintenance and usage of IoT devices.



CSCIS IoT Security Requirements

- Security recommendations and best practices on IoT are necessary to help secure the IoT ecosystem as well as building trust on IoT utilization
- CSCIS not only aims to provide recommendations and best practices for IoT development. But at the same time, educate the IoT users on the security requirements of their IoT devices and how they can utilize the security mechanisms to have a more secure IoT experience.
- CSCIS has identified 21 IoT security requirements and they can be categorized into 6 different categories, which are: general security, physical security, system security, communication security, identification security and authentication, and privacy protection.



Key security controls

Security by design

Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating different security policies and techniques and design architecture by compartments to encapsulate elements in case of attacks throughout the development, manufacture, and deployment.

Risk and Threat Identification and Assessment

Identify the IoT ecosystem context including key network/information systems and intended use /environment of a given IoT device then using a defense-in-depth approach to Identify significant risks among the IoT ecosystem.

Management of Security Vulnerabilities and Incidents

Establish procedures for analyzing and handling security incidents and participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.
Based on the mentioned information-sharing platforms, create and coordinate and a publicly disclosed mechanism for vulnerability reports.

Key security controls (Cont.)

Third-Party relation-ships

It is necessary for IoT hardware manufacturers and IoT software developers to adopt cybersecurity supply chain risk management policies and communicate the cyber security requirements to their suppliers and partners.

Cryptographic Management

Proper and scalable management mechanism and requirements should be implemented and enforced for cryptographic key generation, exchange, storage, usage, replace and discard.
While adopting cryptographic algorithms for data process and communication, use well known ones that recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided.

CSCIS IoT Security Requirements Mapping

Component Category	Security Requirement	IoT Components		
		Edge Client	Gateway	Cloud
General Security	Security by Design	○	○	○
	Risk and Threat Identification and Assessment	○	○	○
	Management of Security Vulnerabilities and Incidents	○	○	○
	Third-Party Relationships	○	○	○
	Cryptographic Management	○	○	○
Physical Security	Physical Interface	○	○	N/A
	Physical Layer	○	○	N/A
System Security	Operating System	○	○	N/A
	Sensitive Data Storage	○	○	○
	Web-Based Management Interface	○	○	○
	Application Programming Interface	○	○	○
	System Logging	○	○	N/A
Communication Security	Network Port	○	○	N/A
	Sensitive Data Transmission	○	○	○
	Communication Interface	○	○	N/A
	Communication Protocol	○	○	○
Identification and Authentication	Authentication	○	○	○
	Password	○	○	○
	Authorization	○	○	○
Privacy Protection	Assessment of Sensitive Information	○	○	○
	Assessment of Impacts on Sensitive Information	○	○	○

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Q&A

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES