CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

University Institute of Engineering

AIT-CSE

Privacy and Security in IoT - CSD- 433

Topic – Security Concerns in IoT Applications

Lecture – 1.4

Delivered by

Er. Gaurav Soni (E9610)

Assistant Professor, AIT-CSE

DISCOVER . LEARN . EMPOWER

Privacy and Security in IoT

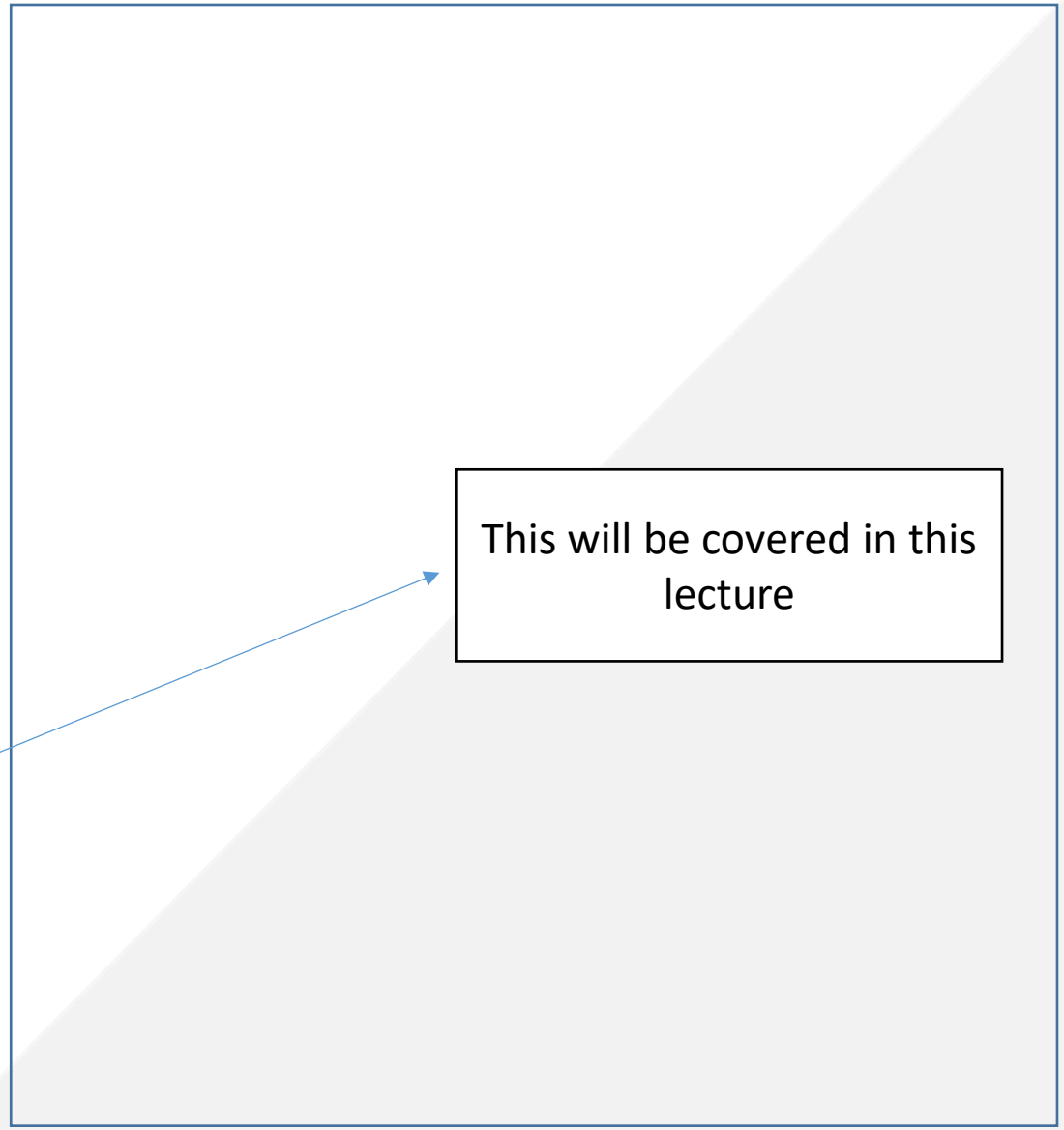
Course Objectives

CO Number	Title
CO1	To identify various privacy and security requirements in Internet of Things
CO2	To learn cryptographic techniques for a secure IoT system
CO3	To understand various Trust Models used in IoT

Privacy and Security in IoT

Course Outcome

CO Number	Title	Level
CO1	After successful completion of this course students will be able to understand the security requirements in IoT.	**Understand**
CO2	After successful completion of this course students will be able to understand the authentication credentials and access control.	**Understand**
CO3	After successful completion of this course students will be able to implement security algorithms to make a secure IoT system.	Implement



SECURITY CONCERNS IN IoT APPLICATIONS

- For IoT applications, security and privacy are two important challenges.
- To integrate the devices of sensing layer as intrinsic parts of the IoT, effective security technology is essential to ensure security and privacy protection in various activities such as personal activities, business processes, transportations, and information protection.

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

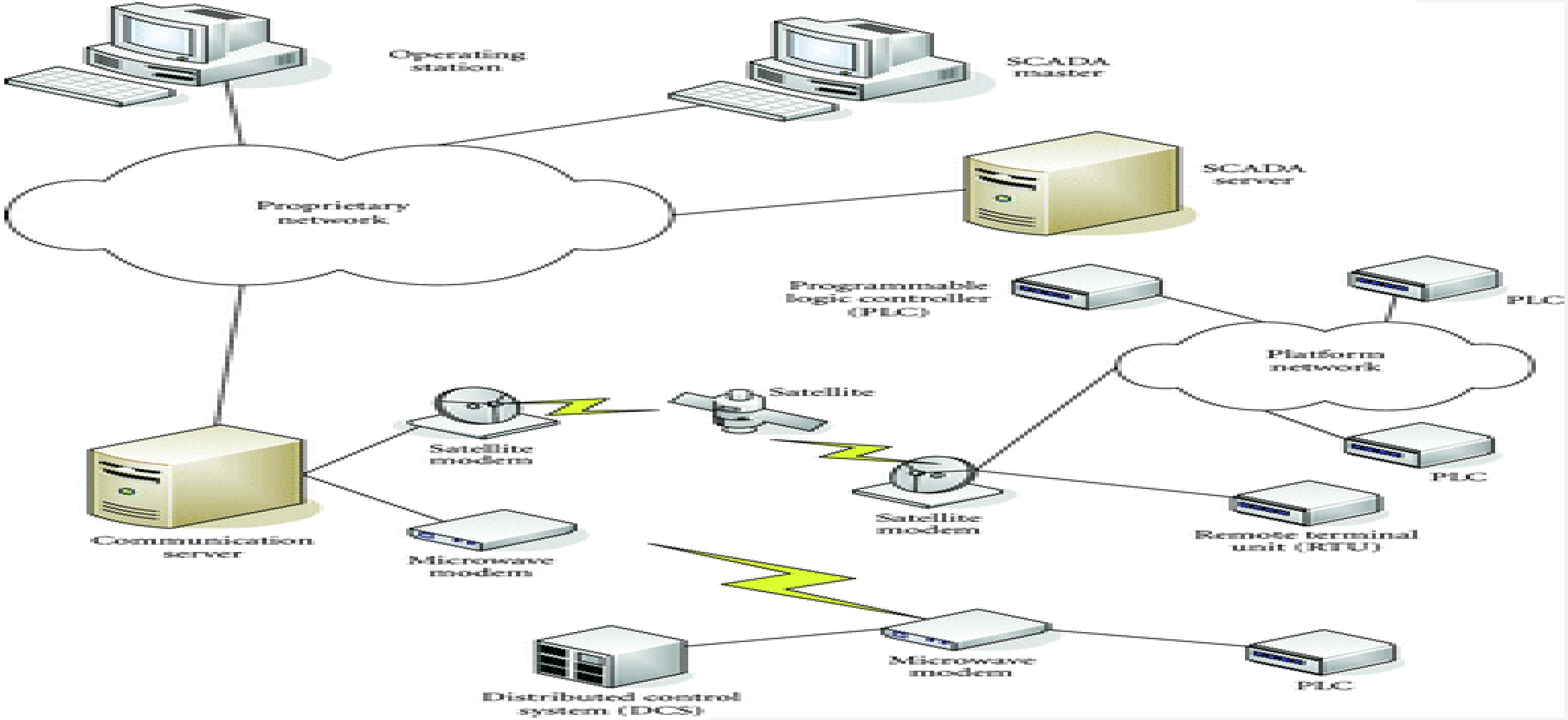
- Security Concerns in SCADA Systems
- Security Concerns in Enterprise Information Systems
- Security Concerns in Social IoT
- Confidentiality and Security for IoT-Based Healthcare

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

Security Concerns in SCADA Systems

- A SCADA could contain multiple elements: supervisory systems, PLCs, human machine interface, remote machine telemetry units, communication infrastructure, and various process and analytical instrumentation.
- From a security viewpoint, an attacker could target each of the above elements to compromise a SCADA system.

ASSOCIATED SECURITY CHALLENGES IN SCADA SYSTEM



SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

Security Concerns in SCADA Systems are as follows:

Authentication and access control.

- To ensure secure communication, strong authentication must be implemented to allow access to main functionalities.

Identification of SCADA vulnerabilities.

- The software in SCADA should be regularly updated to tackle the security vulnerabilities.

Physical security.

- In SCADAs, physical security protection must be carefully evaluated for each component and each component is recommended to meet industrial standards.

System recovery and backups. The SCADAs should be designed to be able to rapidly recover from disaster or compromised status.

ASSOCIATED SECURITY CHALLENGES IN SCADA SYSTEM

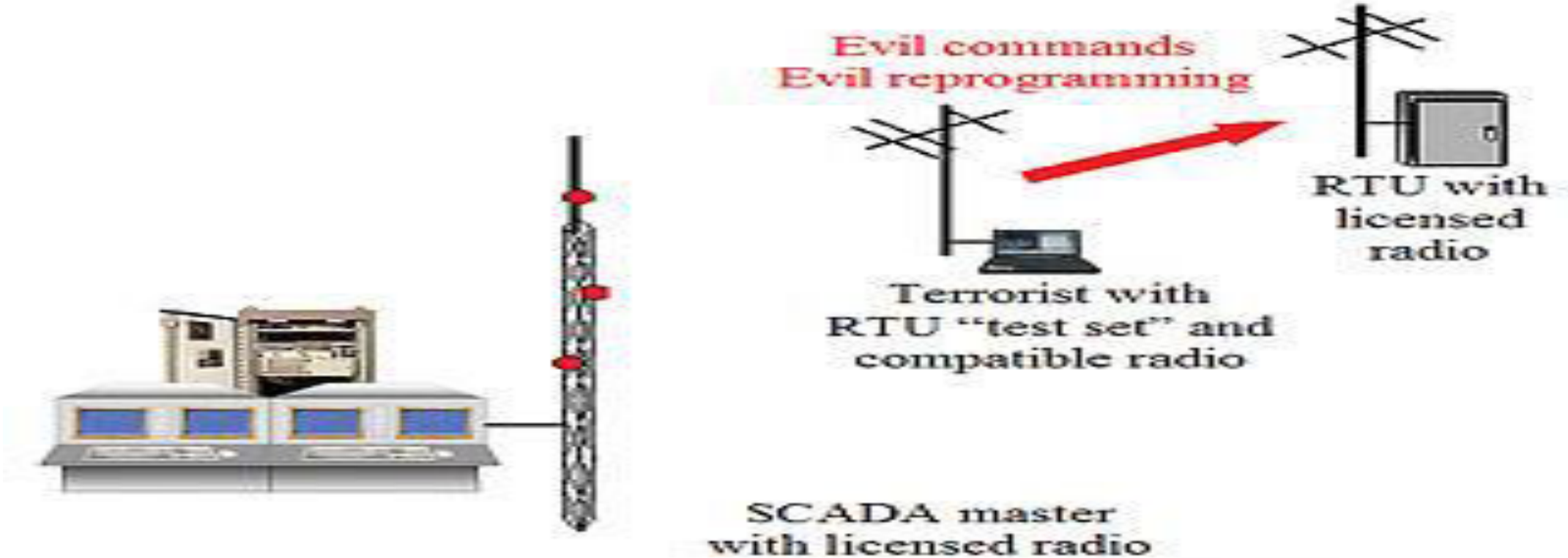


Figure 2.0 – Direct attack on an RTU site

ASSOCIATED SECURITY CHALLENGES IN SCADA SYSTEM

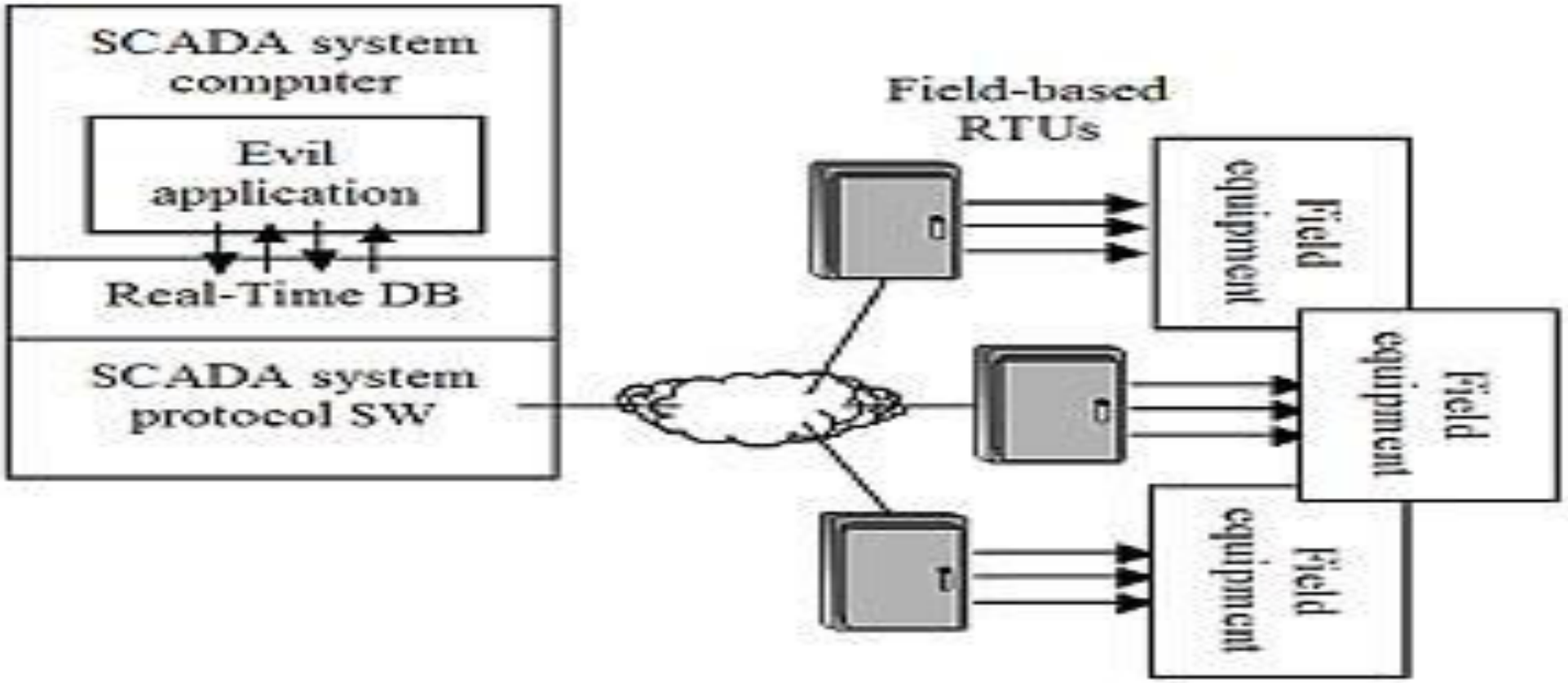


Figure 4.0 – Malicious application software

ASSOCIATED SECURITY CHALLENGES IN SCADA SYSTEM

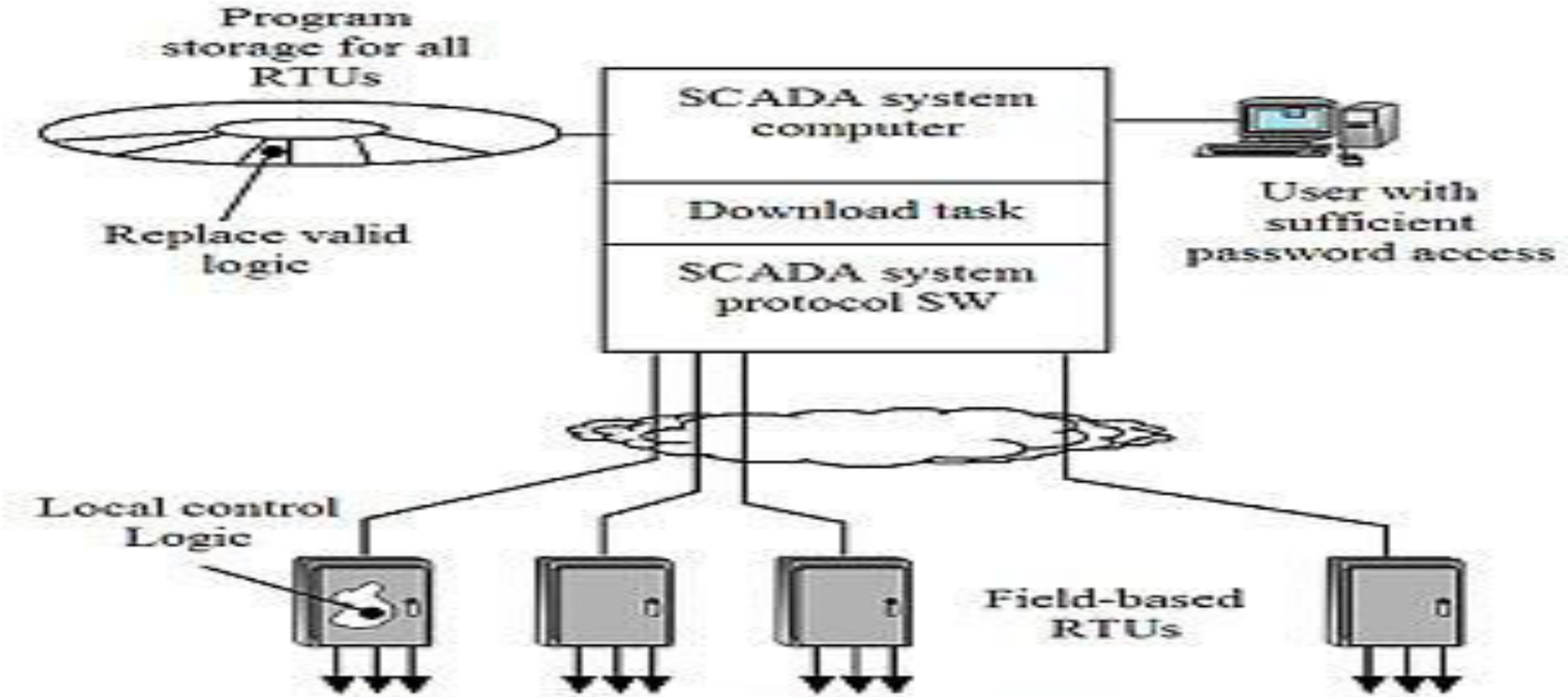


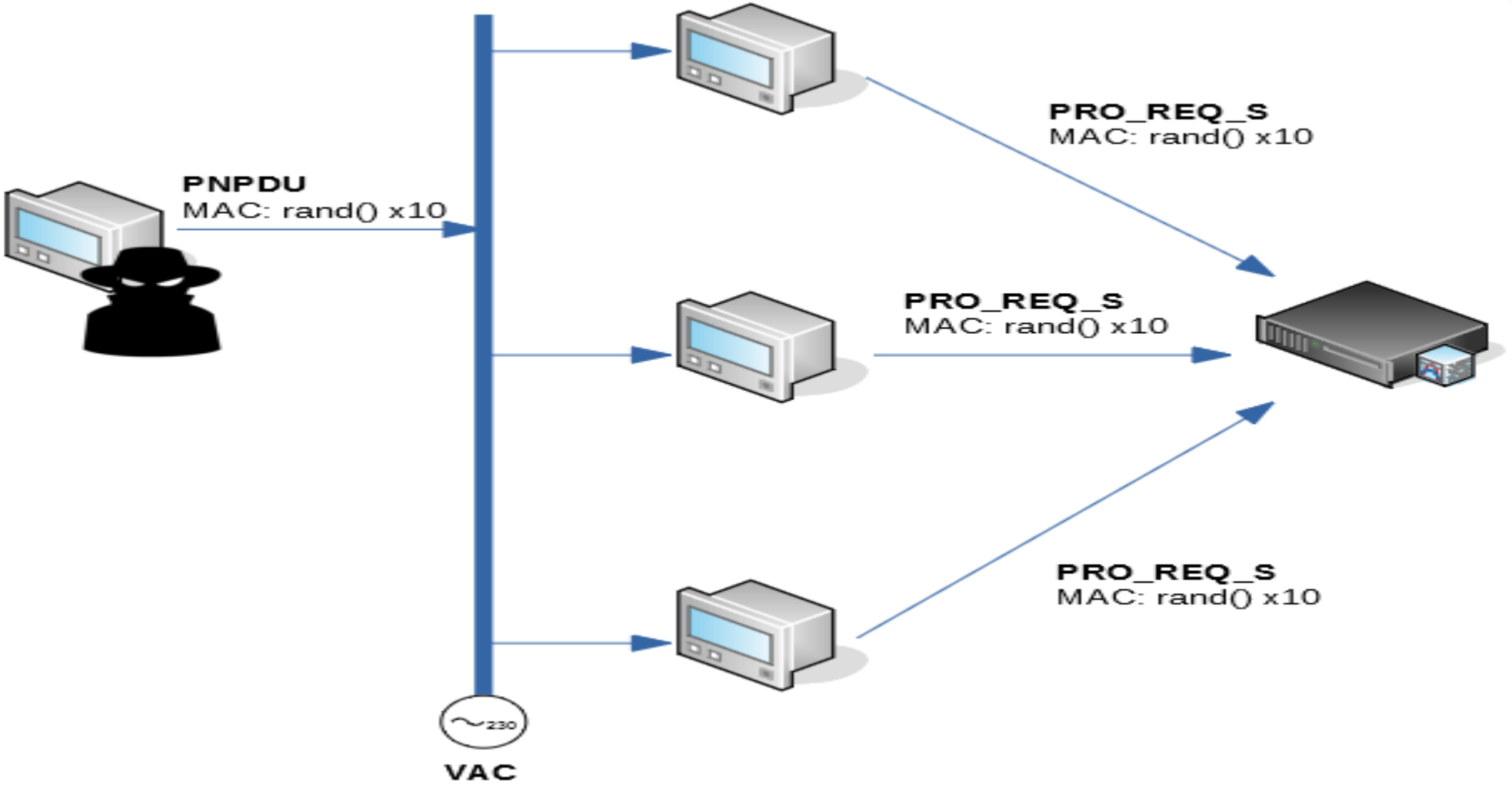
Figure 5.0 – Malicious RTU reprogramming

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

Security Concerns in Social IoT

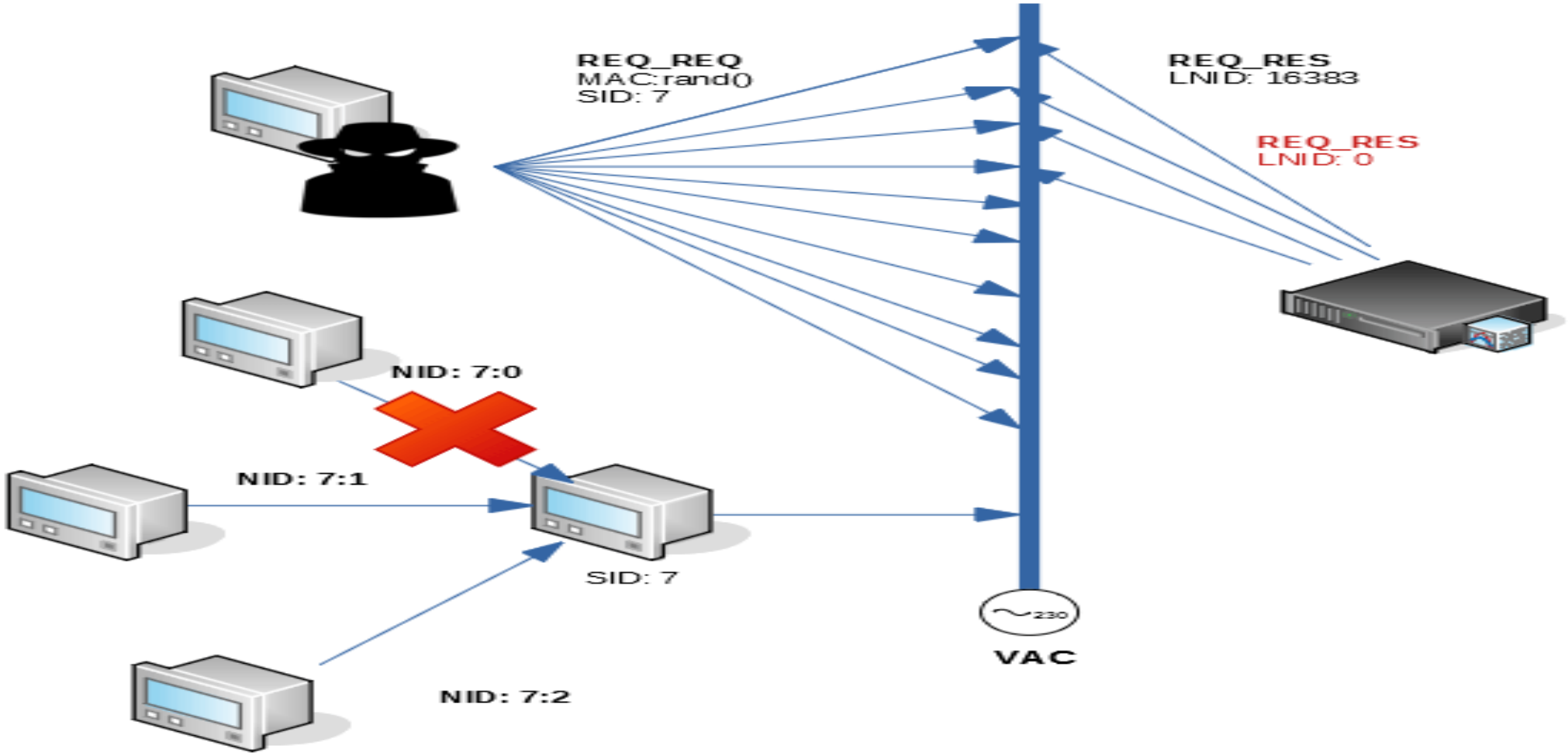
- Social IoT is the spread and diffusion of IoT applications into societal level eg: wearable devices, smart TV, smart meter, and smart home
- Ethical issues such as privacy, data access right, the degree of openness of data will all influence how the security architecture for social IoT to be constructed
- When more and more devices are connected together, How to effectively design the traffic so that data over social IoT could be transferred securely in a reliable way will also become challenging.

SECURITY ATTACKS IN SMART ENERGY METERS
(Flood of promotion requests)



SECURITY ATTACKS IN SMART ENERGY METERS

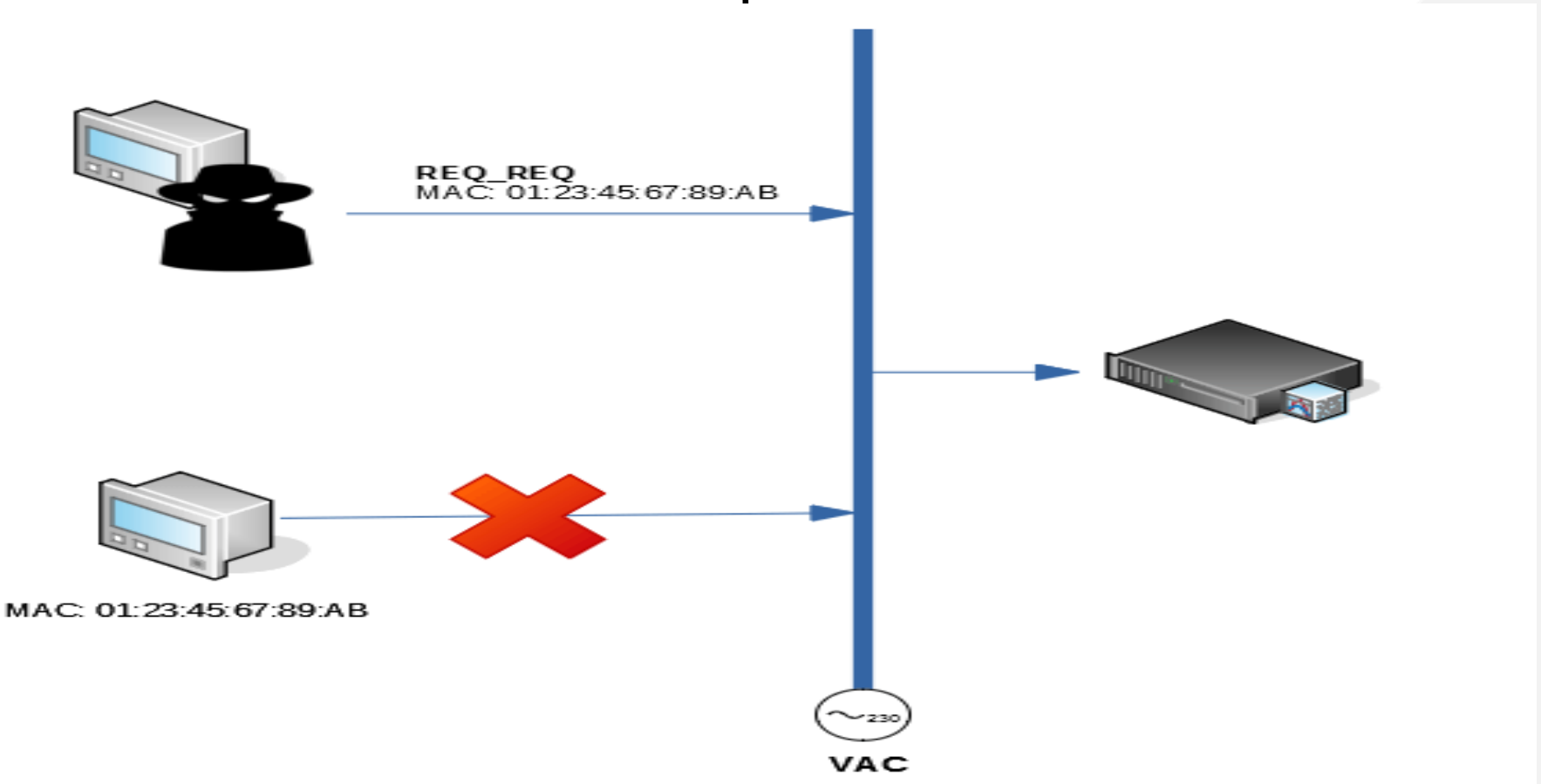
Overflow in the node log



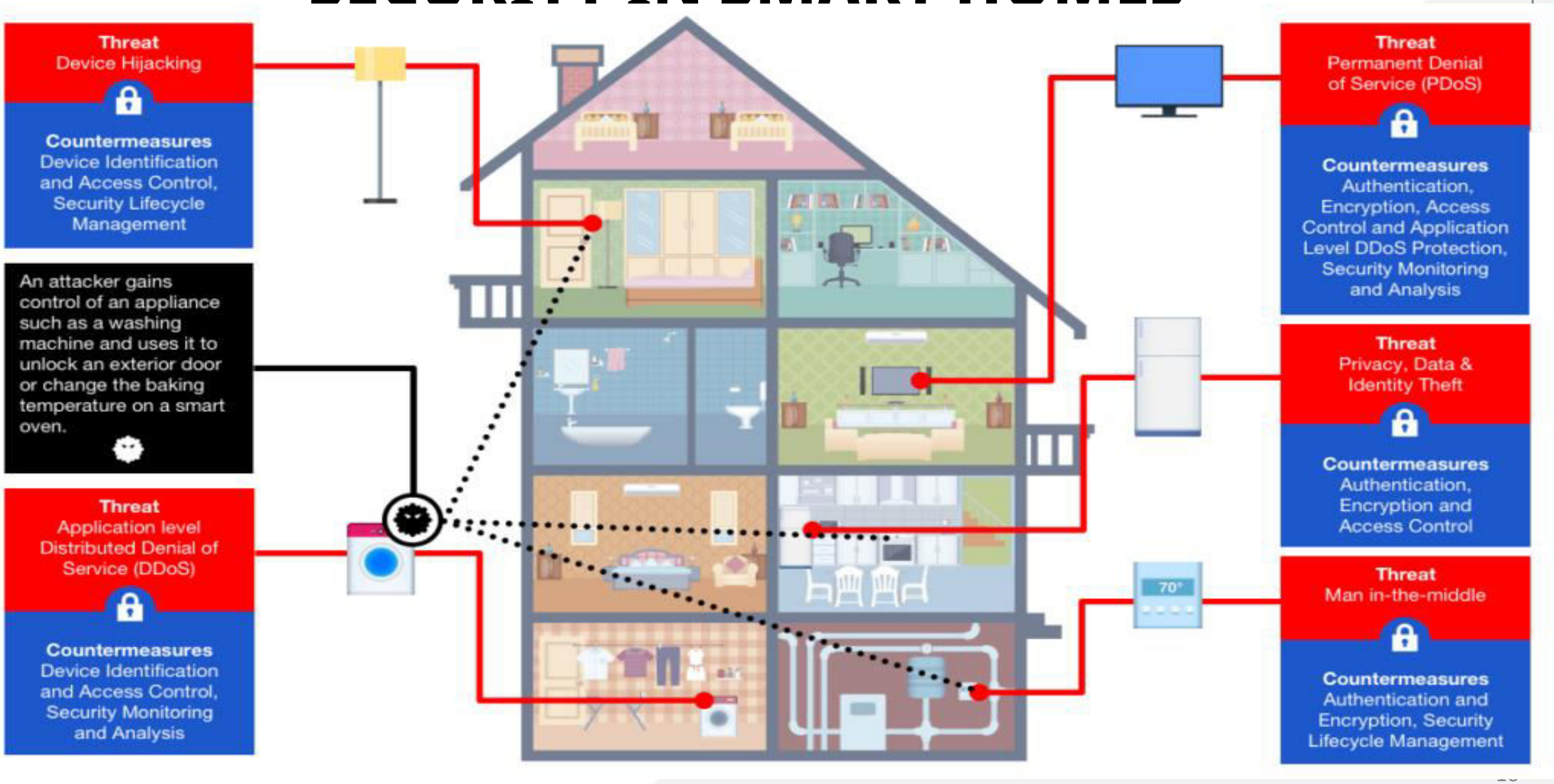
SECURITY ATTACKS IN SMART ENERGY METERS

(Identity theft in the node registry)

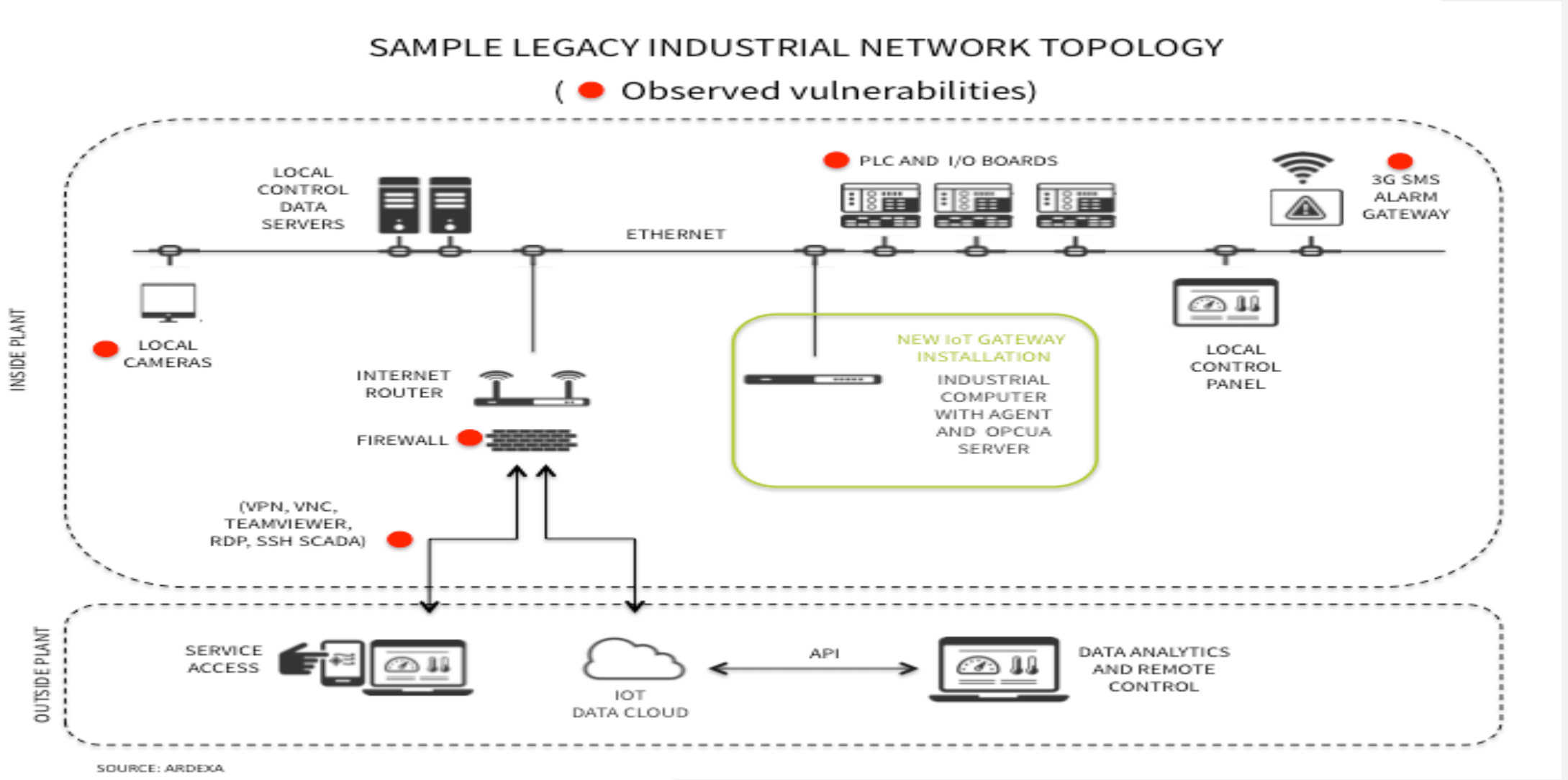
\



SOME APPLICATIONS AND ASSOCIATED SECURITY IN SMART HOMES



SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES



IoT security incidents in recent years

Month/Year	Incident Case	
Aug. 2016	Mirai, a malware targeting IoT devices, first detected	Used as a Bot that performed DDoS attacks on numerous websites. Released as open-source software, subsequently resulting in the creation of multiple variants.
Dec. 2016	Industroyer, a malware targeting circuit breakers at power plants, detected	Caused a wide-scale power outage in Ukraine.
May 2017	Ransomware WannaCry wreaks worldwide havoc	Significantly affected the IoT (OT) environment, with many infections in the manufacturing industry being reported. Infections to security cameras also noted in Australia.
Sep. 2017	BlueBorne, a type of vulnerability enabling the remote operation of Bluetooth devices, detected	Could affect as many as 5.3 billion Bluetooth devices, including IoT devices.
Nov. 2017	Reaper, a malware targeting IoT devices, infects several million network devices	Unlike Mirai, which targets initial passwords, this malware uses a variety of vulnerabilities to make IoT devices into Bots.
May 2018	Infection of VPNFilter, a malware targeting IoT devices, spreads	Over 500,000 infections reported in 54 countries worldwide.

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

Security Concerns in Enterprise Information Systems

- IoT-enabled enterprise systems incorporate sensors into the enterprise systems and will involve more security challenges than the traditional enterprise systems because the data and information carried by the sensors might go beyond the enterprise system physically
- This new architecture of enterprise systems require the security concerns to focus more on the sensor layer as well as the middleware layer because in both there might be issues of data breach at these layers

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

Confidentiality and Security for IoT-Based Healthcare

The current healthcare-specific security standards include following four parts:

- Authentication, identification, signature, nonrepudiation;
- Data integrity, encryption, data integrity process, permanence;
- System security, communication, processing, storage, permanence;
- Internet security, personal health records, secures Internet services.

In IoT-based healthcare system, the security issues include:

- Security for patient confidentiality,
- Security that enables electronic health records (authentication, data integrity),
- Transmission security,
- Security in healthcare data access, processing, storage, etc.

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES

main aims and focus is presented in Fig. 6.

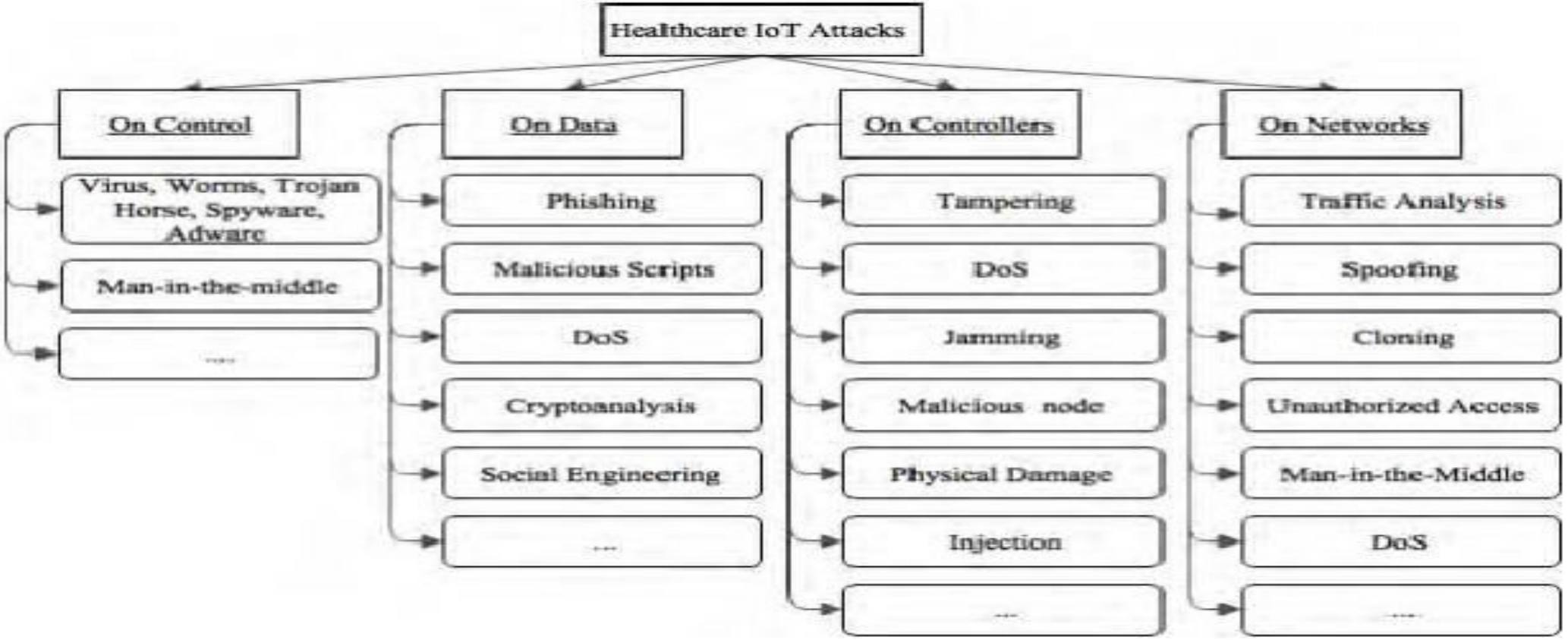
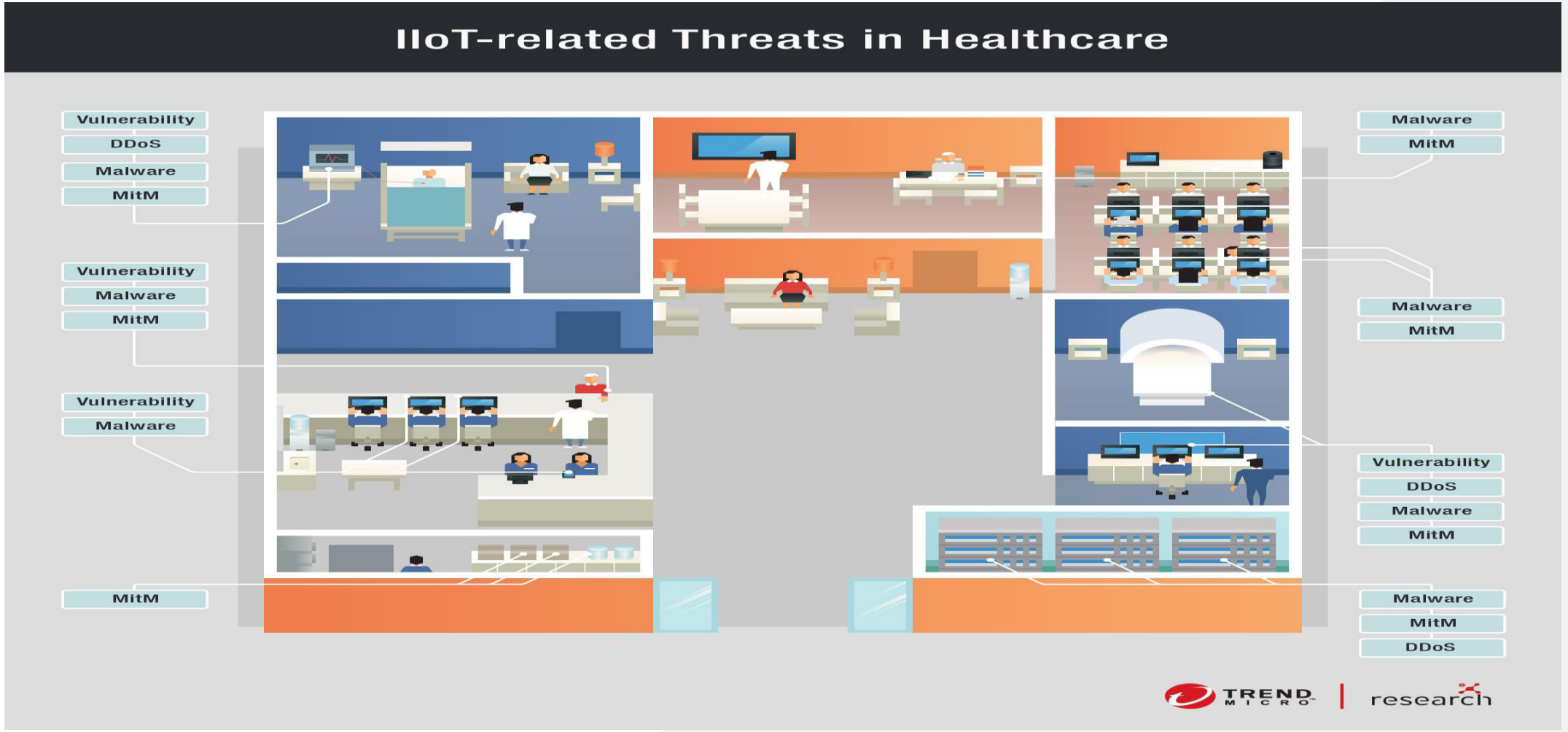


Figure 6. Classification of healthcare IoT attacks

Such attacks on vulnerabilities can prevent the devices

SOME APPLICATIONS AND ASSOCIATED SECURITY CHALLENGES



References

1. Li Da Xu, Securing Internet of Things, Algorithms, and Implementations, Elsevier
2. https://www.iotforall.com/iot-application-security/.
3. https://www.youtube.com/watch?v=djUHvCyPYhY

Home Assignment

1. Find more IoT applications other than we discussed in lecture and explore associated security challenges.

THANK YOU

For queries
Email: gaurav.e9610@cumail.in