



TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

IT4735

Internet of Things and Applications

Giảng viên: TS. Phạm Ngọc Hưng
Viện Công nghệ Thông tin và Truyền thông
hungpn@soict.hust.edu.vn

Nội dung

- Chương 1. Tổng quan về IoT
- Chương 2. Hệ thống IoT và các công nghệ
- Chương 3. Lập trình IoT
- Chương 4. An toàn và Bảo mật IoT
- Chương 5. Xây dựng ứng dụng IoT

Chương 4. An toàn và Bảo mật IoT

- 4.1. Tổng quan về bảo mật IoT
- 4.2. Các dạng tấn công vào hạ tầng IoT
- 4.3. Các vấn đề mất an toàn bảo mật trong IoT

4.1. Tổng quan về bảo mật IoT

- Các vấn đề trong bảo mật IoT:
 - Thiết kế ban đầu cho mạng truyền thông riêng sau đó được chuyển sang mạng IP và Internet
 - Cập nhật firmware cho thiết bị IoT khó khăn
 - Xuất phát từ những yêu cầu bảo mật cơ bản, sau đó xuất hiện các lỗi bảo mật kèm theo các yêu cầu bảo mật phức tạp hơn.
 - Các thiết bị bảo mật kém từ các thiết kế ban đầu đã được sử dụng trên thực tế

Tổng quan về bảo mật IoT

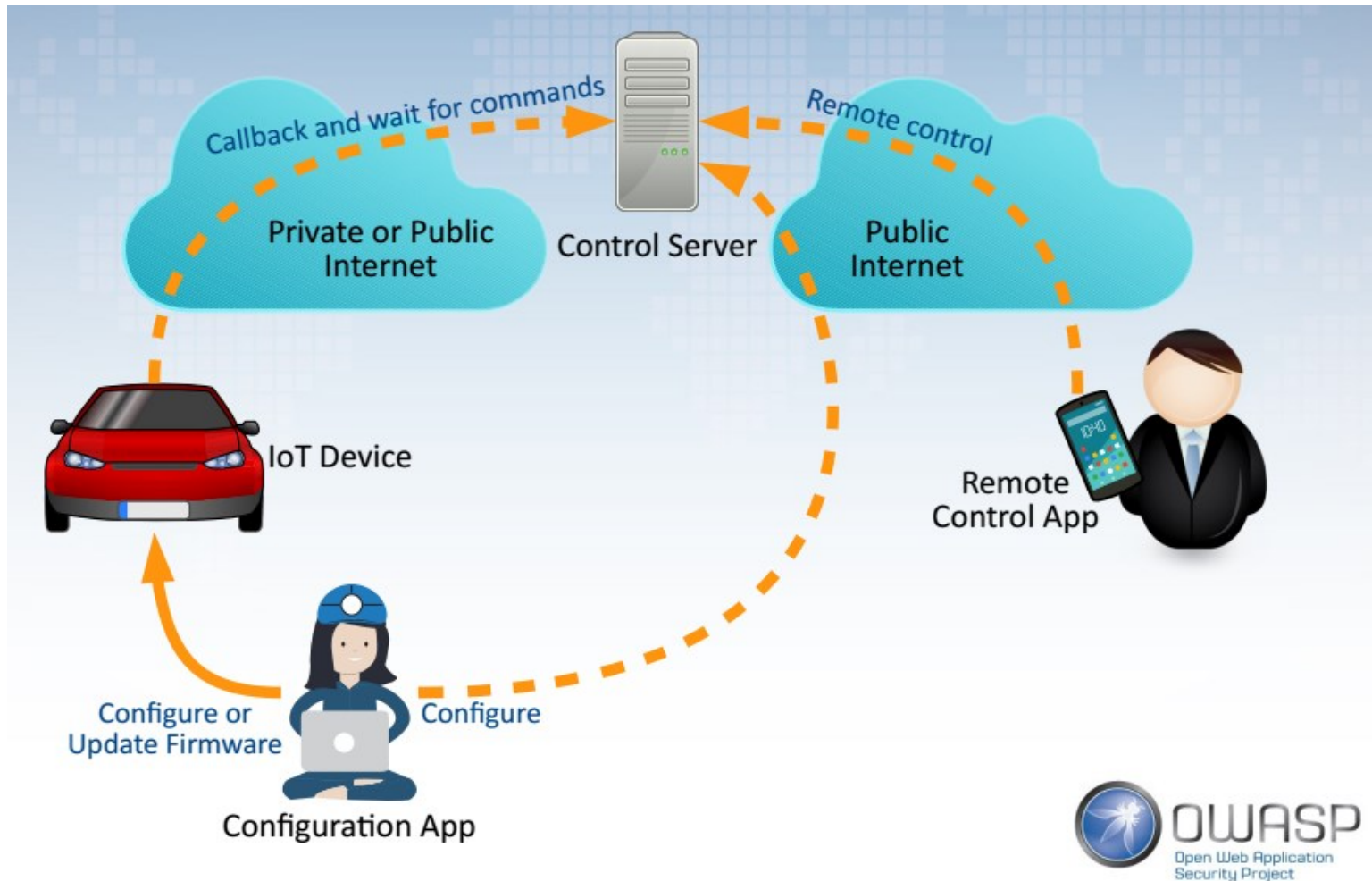
- Phân loại nguy cơ bảo mật IoT:
 - Capture:
 - Disrupt
 - Manipulate

Tổng quan về bảo mật IoT

- Các yêu cầu bảo mật IoT:
 - Confidentiality
 - Availability
 - Integrity
 - Authenticity

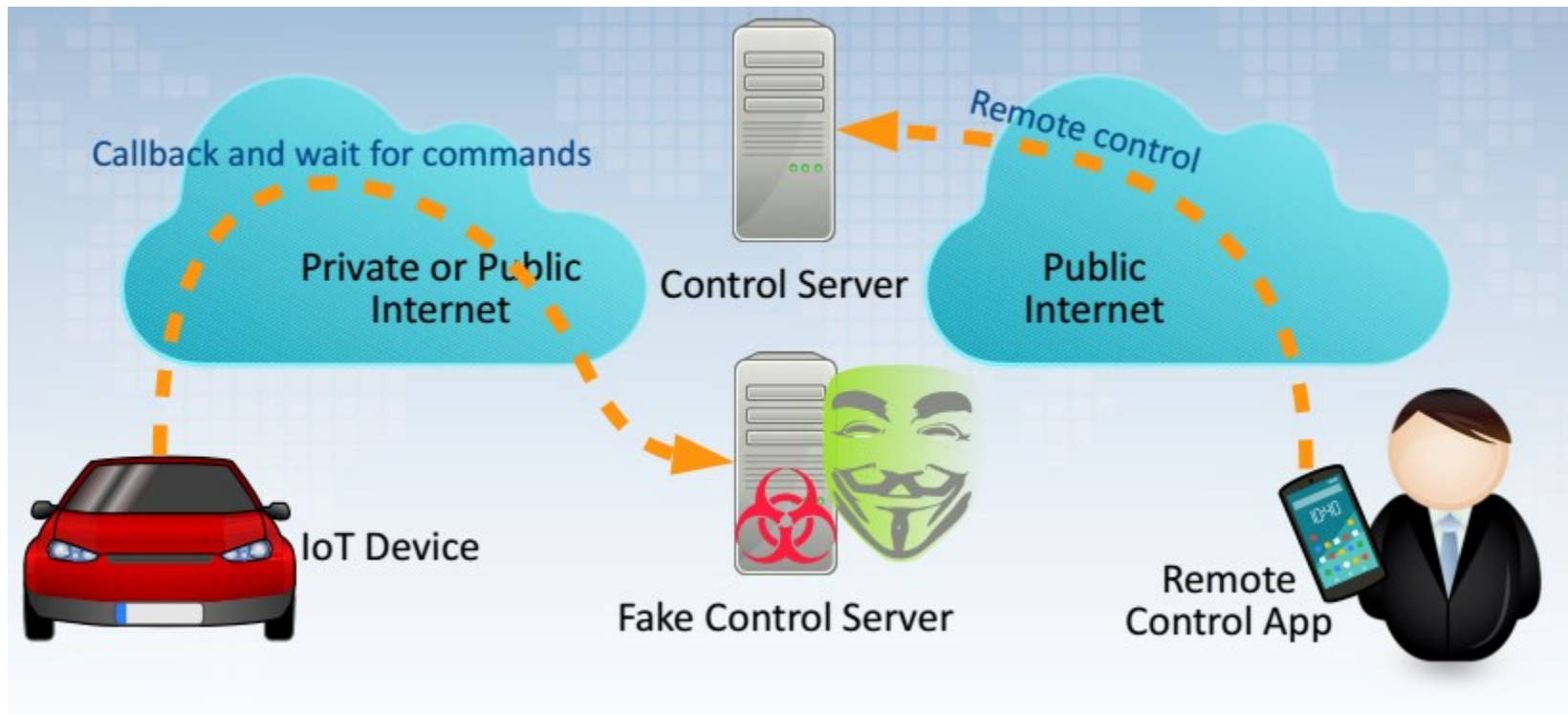
4.2. Các dạng tấn công hạ tầng IoT

- Hạ tầng IoT thông dụng



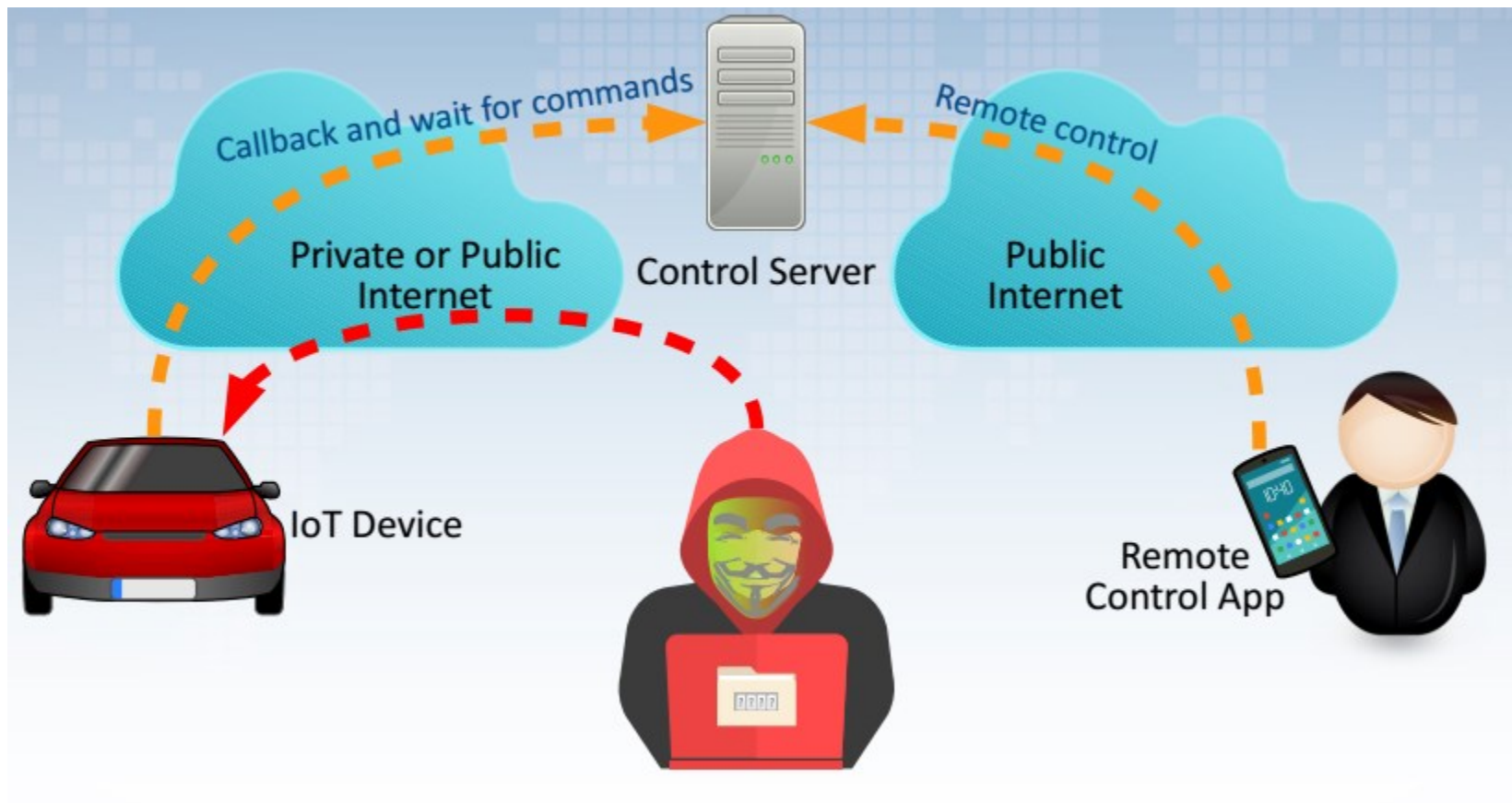
Một số dạng tấn công

- Fake Control Server



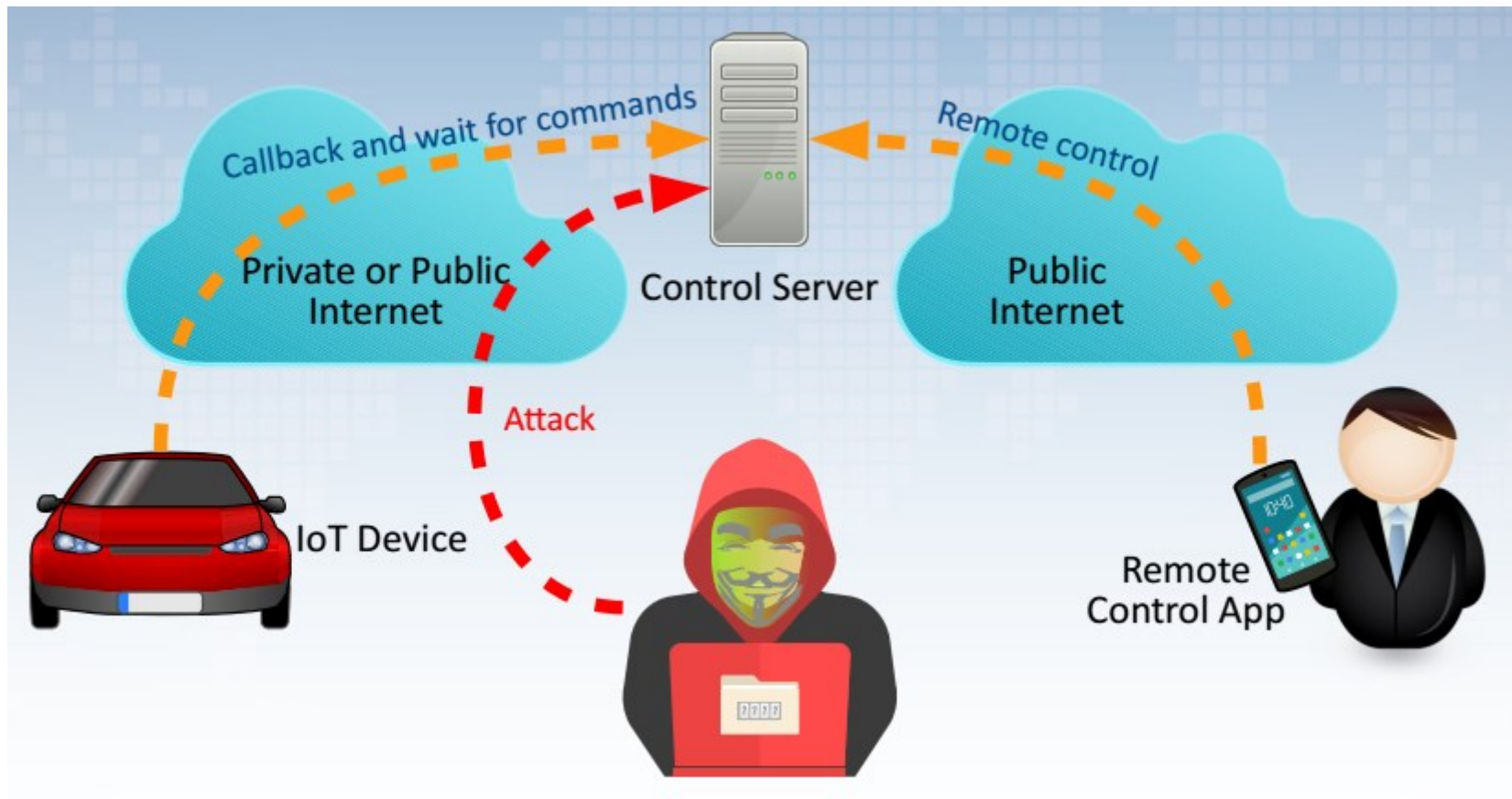
Một số dạng tấn công

- Attack on device open ports



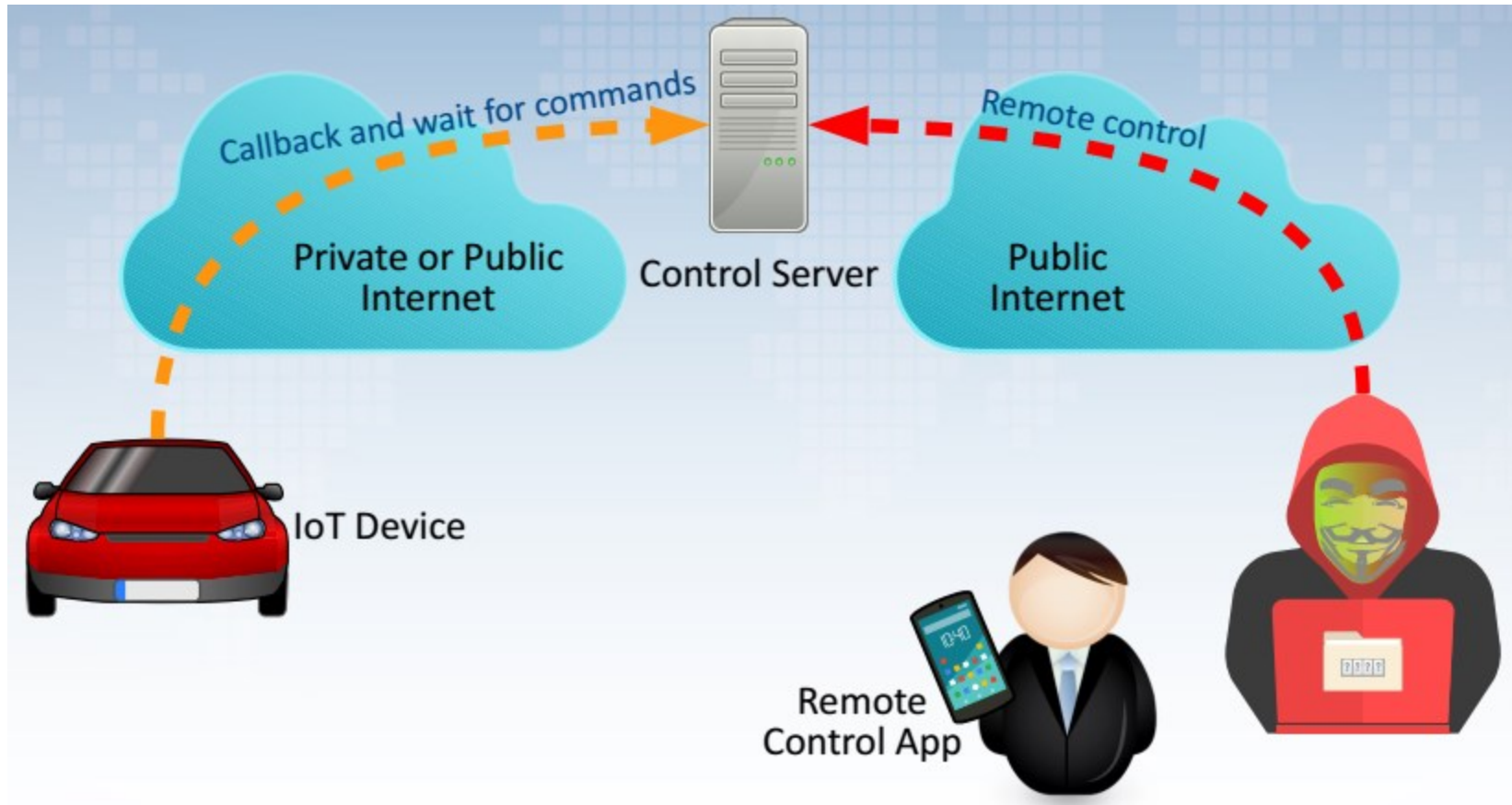
Một số dạng tấn công

- Attack on server open ports



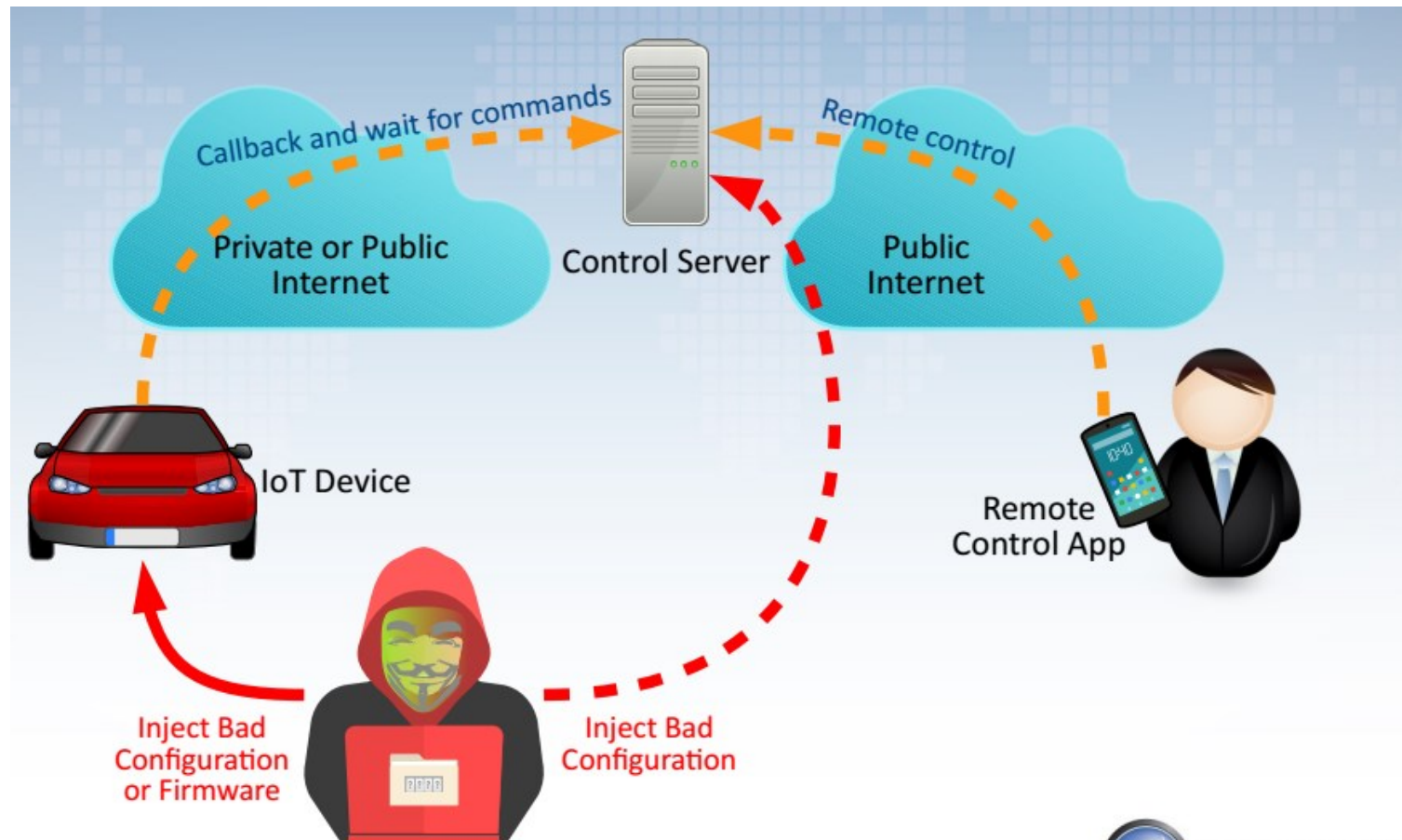
Một số dạng tấn công

- Steal Credential



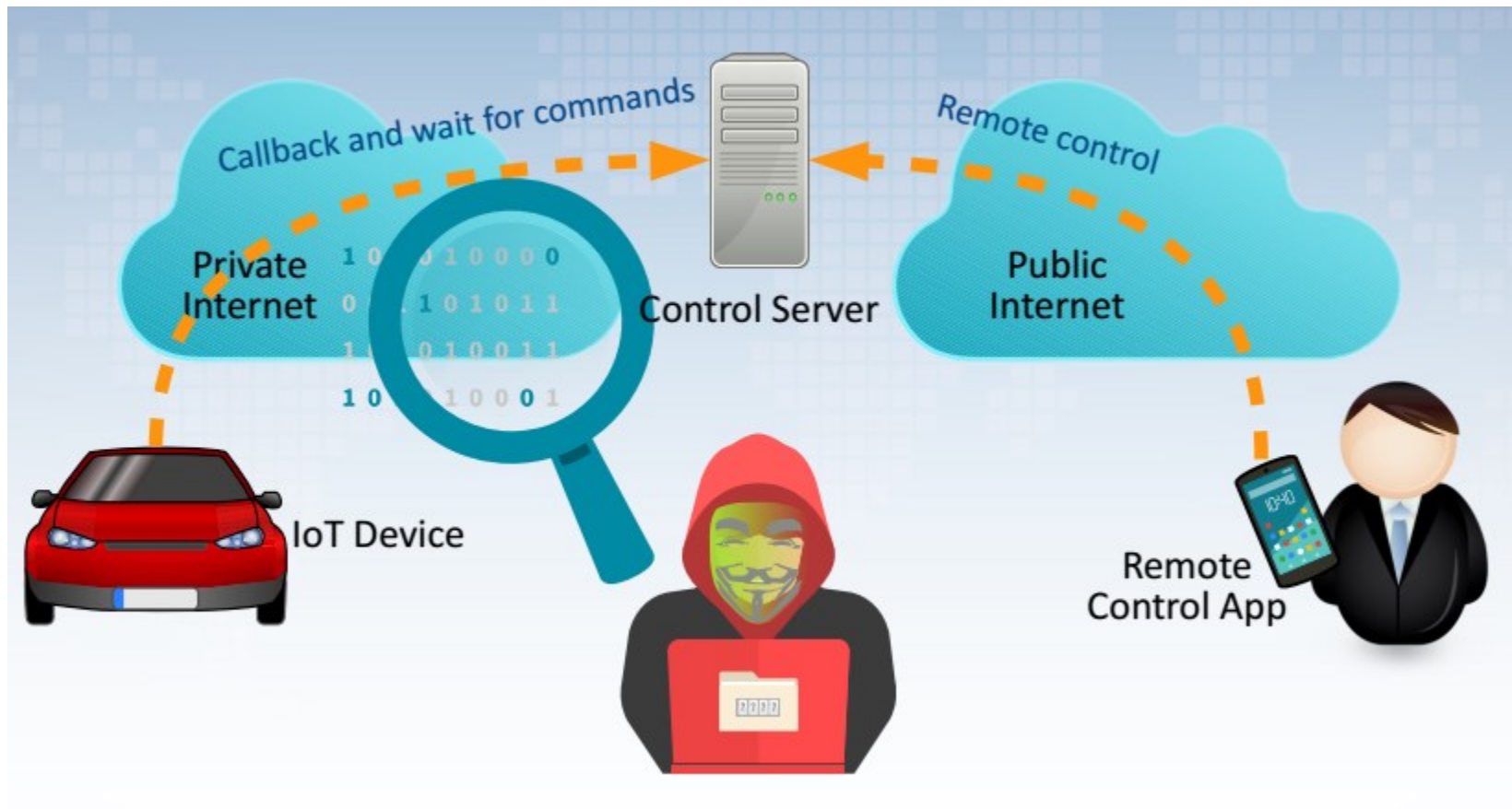
Một số dạng tấn công

- Inject bad configuration or firmware



Một số dạng tấn công

- Sniff data on private network



4.3. Các vấn đề mất an toàn bảo mật IoT

- I1. Insecure Web Interface (Giao diện quản trị không an toàn)
- I2. Insufficient Authentcaton/Authorizaton (Xác thực không đủ an toàn)
- I3. Insecure Network Services (Các dịch vụ mạng thiếu bảo mật)
- I4. Lack of Transport Encrypton/Integrity Verifcaton (Thiếu mã hóa tầng giao vận)
- I5. Privacy Concerns (Các vấn đề liên quan quyền riêng tư)
- I6. Insecure Cloud Interface (Giao diện Cloud thiếu bảo mật)
- I7. Insecure Mobile Interface (Giao diện mobile thiếu bảo mật)
- I8. Insufficient Security Configurability (Cấu hình bảo mật không an toàn)
- I9. Insecure Software/Firmware (Phần mềm không an toàn)
- I10. Poor Physical Security (Thiếu bảo mật tầng vật lý)

1. Giao diện quản trị không an toàn

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10
TOP



1

Insecure Web Interface

covers IoT device administrative interfaces

Obstacles



Default usernames and passwords



No account lockout

XSS, CSRF, SQLi vulnerabilities



Solutions



Allow default usernames and password to be changed



Enable account lockout



Conduct web application assessments

2. Cơ chế xác thực không an toàn



The infographic is titled "OWASP INTERNET OF THINGS VULNERABILITY CATEGORIES" and "TOP 10". It features a world map in the background with icons for a house, a computer, and a camera. The main section is a dark blue box with a teal header. The header text is "Insufficient Authentication/Authorization" in white, with "covers all device interfaces and services" below it. To the right of the header is a teal circle with the number "2". On the left side of the box is an icon of a person in a suit with a large orange circular arrow around them. The box is divided into two columns by a vertical dotted line. The left column is titled "Obstacles" and lists three items: "Weak passwords" (with a padlock icon), "Password recovery mechanisms are insecure" (with a network icon), and "No two-factor authentication available" (with a person and a red X icon). The right column is titled "Solutions" and lists three items: "Require strong, complex passwords" (with a password field icon), "Verify that password recovery mechanisms are secure" (with a shield icon), and "Implement two-factor authentication where possible" (with a person and a magnifying glass icon).

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10 TOP

Insufficient Authentication/Authorization
covers all device interfaces and services **2**

Obstacles

- Weak passwords
- Password recovery mechanisms are insecure
- No two-factor authentication available

Solutions

- Require strong, complex passwords
- Verify that password recovery mechanisms are secure
- Implement two-factor authentication where possible

3. Các dịch vụ mạng không an toàn

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10
TOP



3

Insecure Network Services

covers all network services including device, cloud, web and mobile



Obstacles

Solutions

	Unnecessary ports are open	Minimize open network ports	
	Ports exposed to the internet via UPnP	Do not utilize UPnP	
	Network services vulnerable to denial of service	Review network services for vulnerabilities	

4. Thiếu sử dụng mã hóa tầng giao vận

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10
TOP



Obstacles

Sensitive information is passed in clear text
SSL/TLS is not available or not properly configured
Proprietary encryption protocols are used

Solutions

Encrypt communication between system components
Maintain SSL/TLS implementations
Do not use proprietary encryption solutions

Lack of Transport Encryption
covers all network services including
device, cloud, web and mobile

4



5. Các vấn đề về quyền riêng tư

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10
TOP



5

Privacy Concerns

covers all components of IoT solution



Obstacles

- ➔ Too much personal information is collected
- ➔ Collected information is not properly protected
- ➔ End user is not given a choice to allow collection of certain types of data

Solutions

- ➔ Minimize data collection
- ➔ Anonymize collected data
- ➔ Give end users the ability to decide what data is collected

6. Giao diện Cloud không an toàn



7. Giao diện Mobile không an toàn

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10
TOP



7

Insecure Mobile Interface

covers mobile application interfaces



Obstacles



Weak passwords
are present



No two-factor authentication
implemented



No account lockout
mechanism



Implement account
lockout after failed
login attempts



Implement two-factor
authentication



Require strong,
complex passwords

Solutions

8. Thiếu cấu hình bảo mật

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

10
TOP



Insufficient Security Configurability

covers the IoT device

8

Obstacles

Password security options are not available

Encryption options are not available

No option to enable security logging



Solutions



Make security logging available



Allow the selection of encryption options



Notify end users in regards to security alerts

9. Phần mềm không an toàn

OWASP
INTERNET OF THINGS
VULNERABILITY CATEGORIES

TOP
10



9

Insecure Software/Firmware
covers the IoT Device



Obstacles



Update servers are not secured



Device updates transmitted without encryption



Device updates not signed

Solutions



Sign updates



Verify updates before install



Secure update servers

10. Thiếu bảo mật tầng vật lý

