CS7351 传感系统原理与设计

Principles and Design of Sensing Systems

Sensing System Security

陈东尧

上海交通大学

chendy@sjtu.edu.cn

2024年秋季

About Mid-term Exam

- Time
  - Next Thursday, at the Class
- Contents
  - The first two chapters
- Formality
  - 中文题目，中文或英文作答皆可
  - 5道填空题（共30分）；8道简答题（共70分）

Sensors we have Introduced

Type	How it works	Applications	Notes
IMU	• Accelerometer: Hooke's Law • Gyroscope: Coriolis Force • Magnetometer: Hall Effect	• Quantify motion into time-series data	• How to calibrate the sensor noise?
Camera	• Tools and techniques in computer vision	• Applications that need to "see"	• How to mitigate the energy and computation cost?
Bluetooth	• Received signal strength indicator (RSSI) • Triangulation	• Coarse-grained indoor localization • Ranging applications	• How to mitigate the sensing noises?
Satellite	• Trilateration • Time-of-flight localization	• Localize outdoor object on earth	• Why we need four satellites to locate an object? • What are the major noises?

Sensing System Security

Part of the contents are adapted from Tadayoshi Kohno, CSE 484 @ UW

Outline for this Chapter

- Why Learning Security
- Threat Modeling
- Exemplary Attacks

What's Wrong About this Picture?

Threat Modeling (Security Reviews)

威胁模型分析 (安全检查)

- Assets（保护对象）: What are we trying to protect? How valuable are those assets?
- Adversaries（攻击者分析）: Who might try to attack, and why?
- Vulnerabilities（漏洞探索）: How might the system be weak?
- Threats（攻击行为）: What actions might an adversary take to exploit vulnerabilities?
- Risk（风险分析）: How important are assets? How likely is exploit?
- Possible Defenses（保护措施）

Threat Modeling (Security Reviews)

威胁模型分析 (安全检查)

- Assets（保护对象）: What are we trying to protect? How valuable are those assets?
- Adversaries（攻击者分析）: Who might try to attack, and why?
- Vulnerabilities（漏洞探索）: How might the system be weak?
- Threats（攻击行为）: What actions might an adversary take to exploit vulnerabilities?
- Risk（风险分析）: How important are assets? How likely is exploit?
- Possible Defenses（保护措施）
- Benefits（获利分析）: Who might the system benefit, and how?
- Harms（受害者）: Who might the system harm, and how?

What's Wrong About this Picture?

What's Wrong About this Picture?

威胁模型分析 (安全检查)

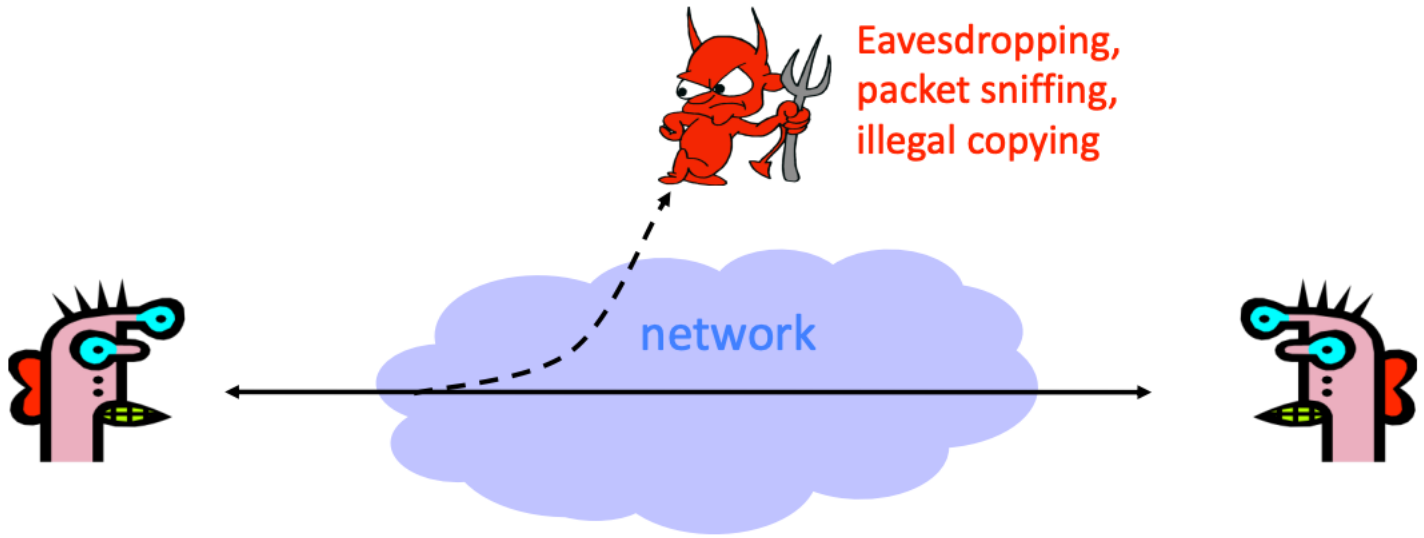
- Assets（保护对象）
- Adversaries（攻击者分析）
- Vulnerabilities（漏洞探索）
- Threats（攻击行为）
- Risk（风险分析）
- Possible Defenses（保护措施）
- Benefits（获利分析）
- Harms（受害者）

What is Security

- Common general security goals: “CIA”
  - Confidentiality -- 保密性
  - Integrity – 完整性（真实性）
  - Availability -- 可用性（可控性）

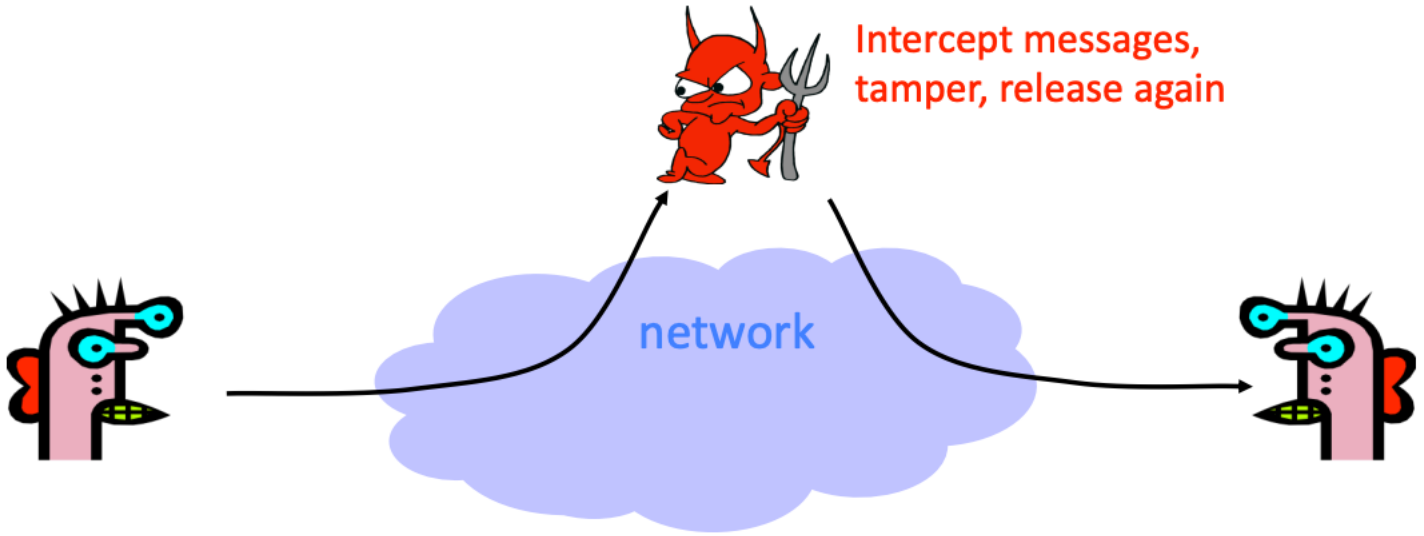
Confidentiality

- Confidentiality is concealment of information



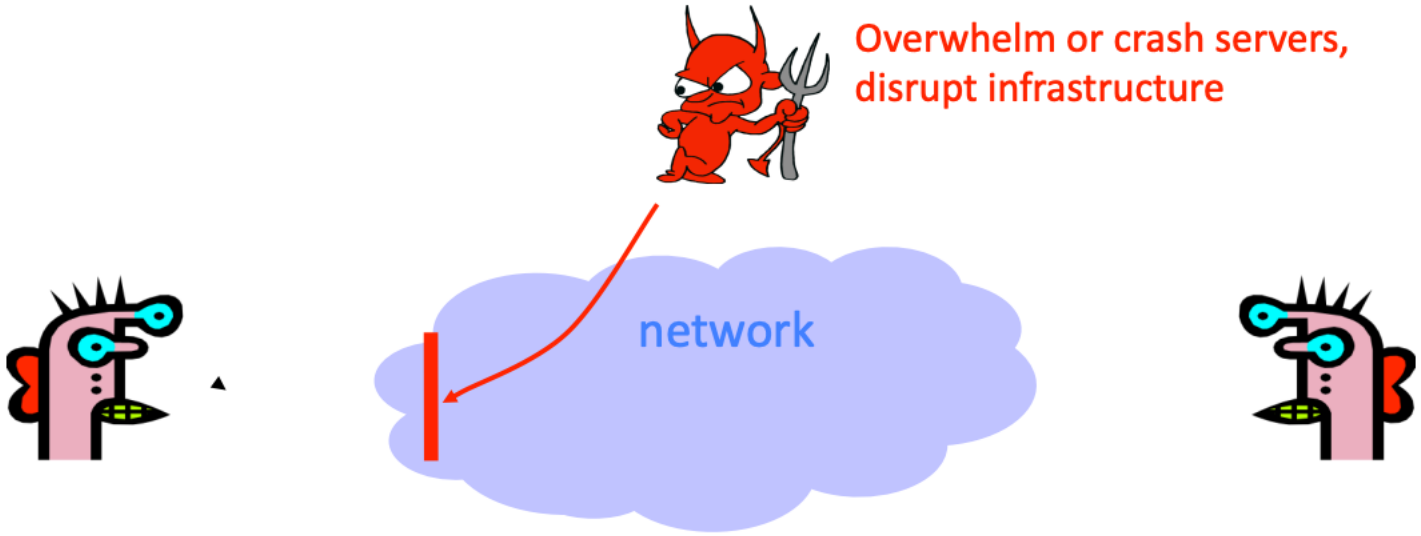
Integrity

- Integrity is prevention of unauthorized changes



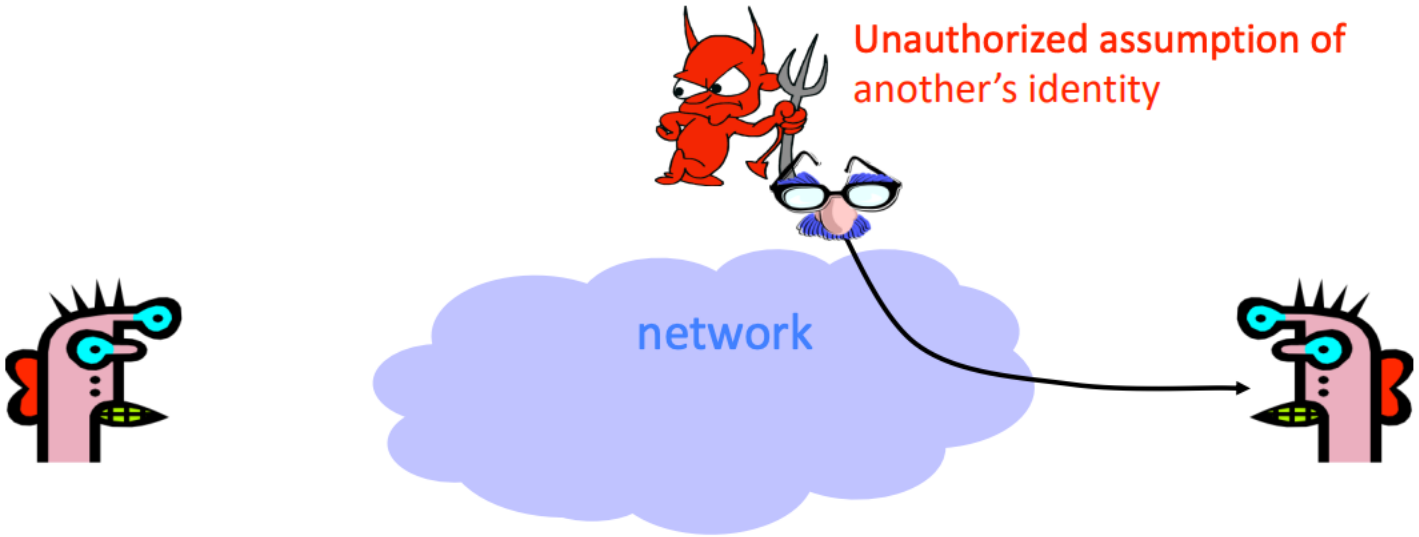
Availability

- Availability is ability to use information or resources



(Optional) Authenticity

- Authenticity is knowing who you're talking to



What is Security

- Or the extension: CPIAAU
  - **C**onfidentiality
  - **P**ossession or Control
  - **I**ntegrity
  - **A**uthenticity
  - **A**vailability
  - **U**tility

There is no such thing as PERFECT Security

- But, attackers have limited resources

There is no such thing as PERFECT Security

- But, attackers have limited resources

- Make them pay unacceptable costs/take on unacceptable risks to succeed!

There is no such thing as PERFECT Security

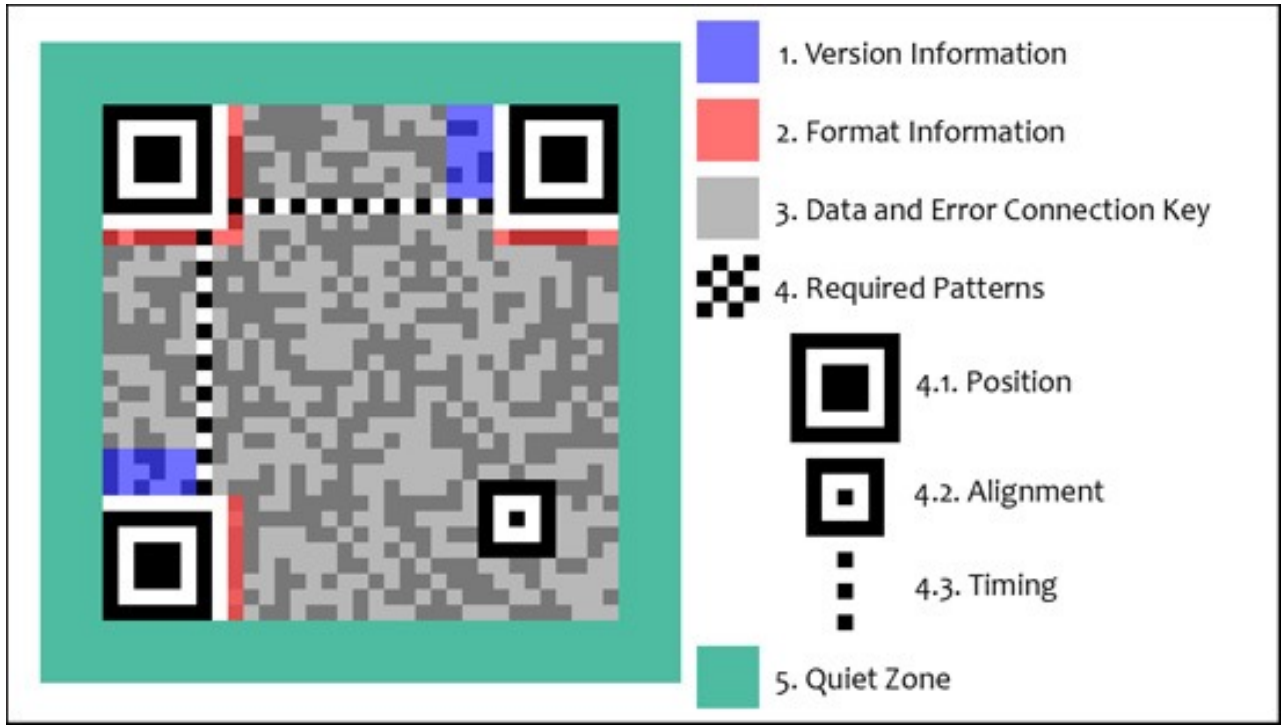
- But, attackers have limited resources
- Make them pay unacceptable costs/take on unacceptable risks to succeed!
- Analyze the Threat Model is ESSENTIAL!

Threat Model Analysis Example: QR Code

How QR Code Works

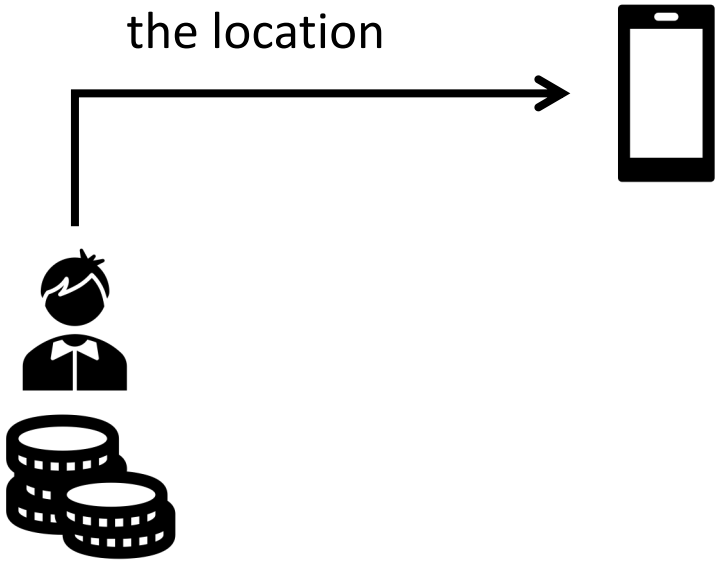
How QR Code Works

- It is designed to be robust
- Can be scanned with your camera at any angle, resilient to partial occlusion
- It also help conceal the clear text (明文) from human eyes

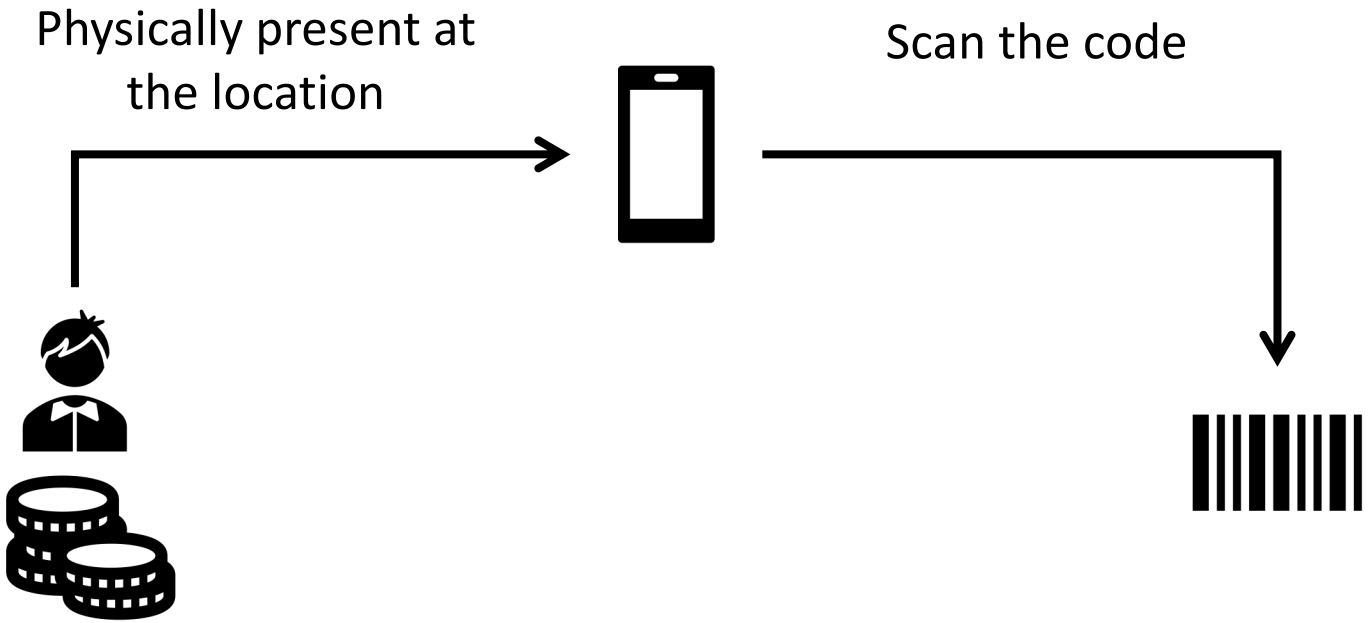


How QR Code Works

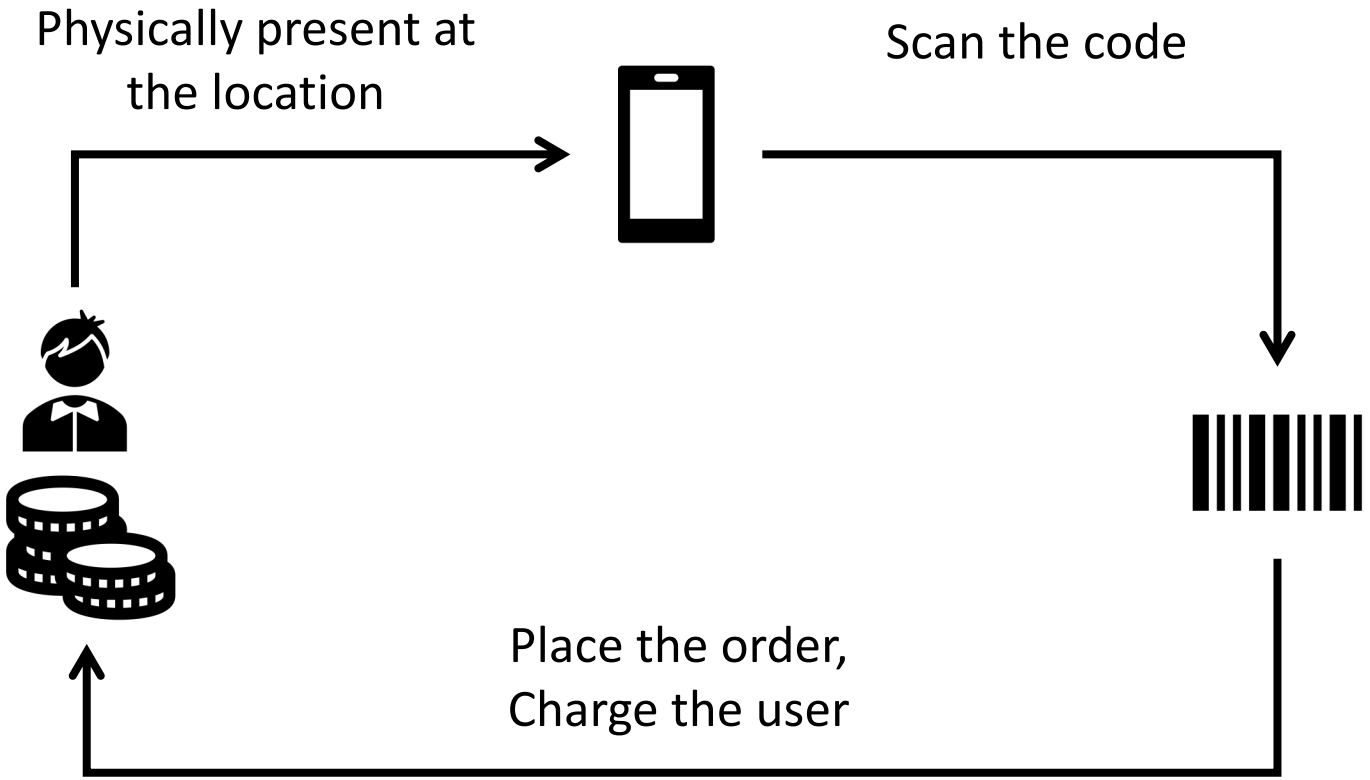
Physically present at the location



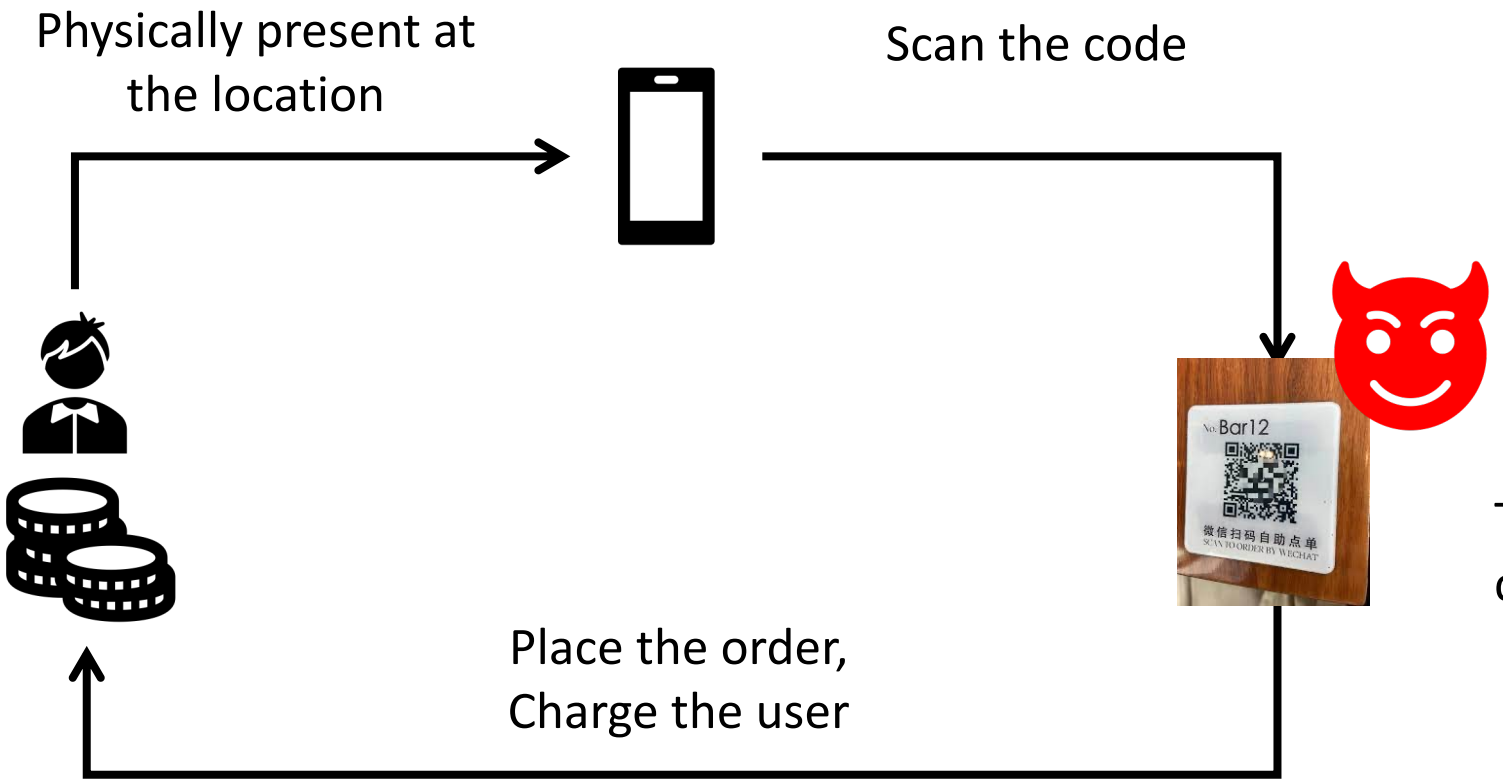
How QR Code Works



How QR Code Works

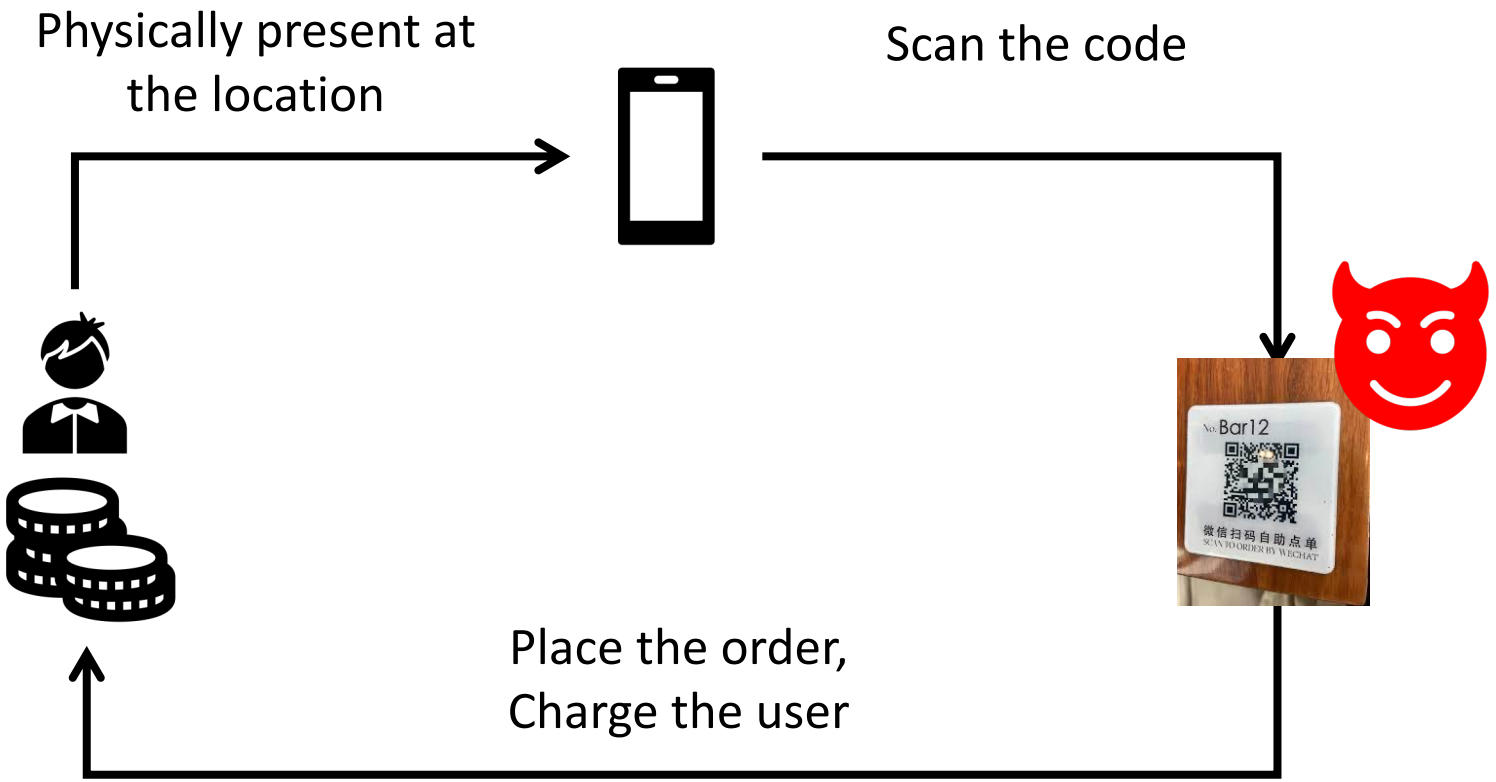


Attack: Quishing Attack!



The attacker can place a fake QR code that lead to a malicious link

Attack: Quishing Attack!

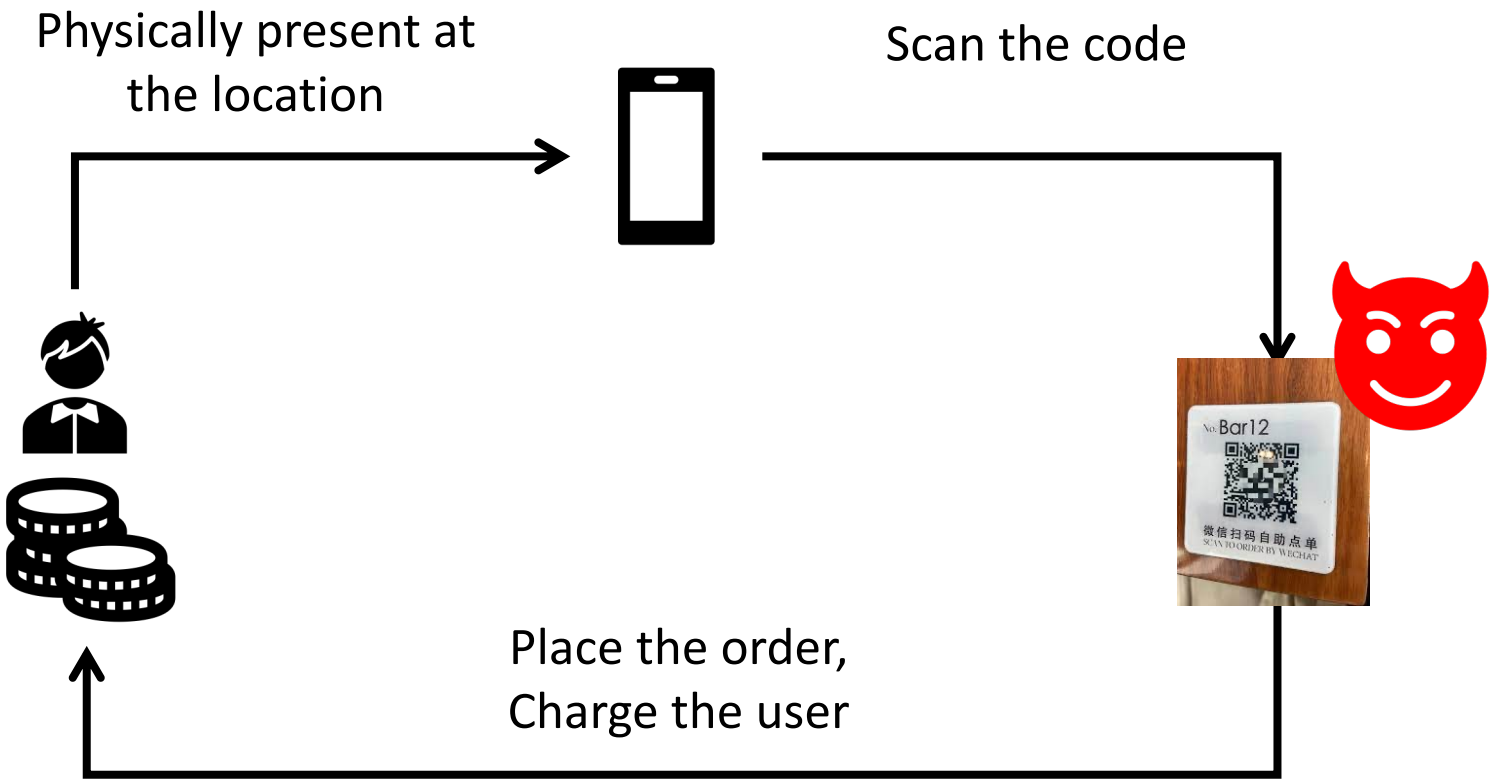


The attacker can place a fake QR code that lead to a malicious link

Target

- The target asset can be user's information, money, location, etc.

Attack: Quishing Attack!



The attacker can place a fake QR code that lead to a malicious link

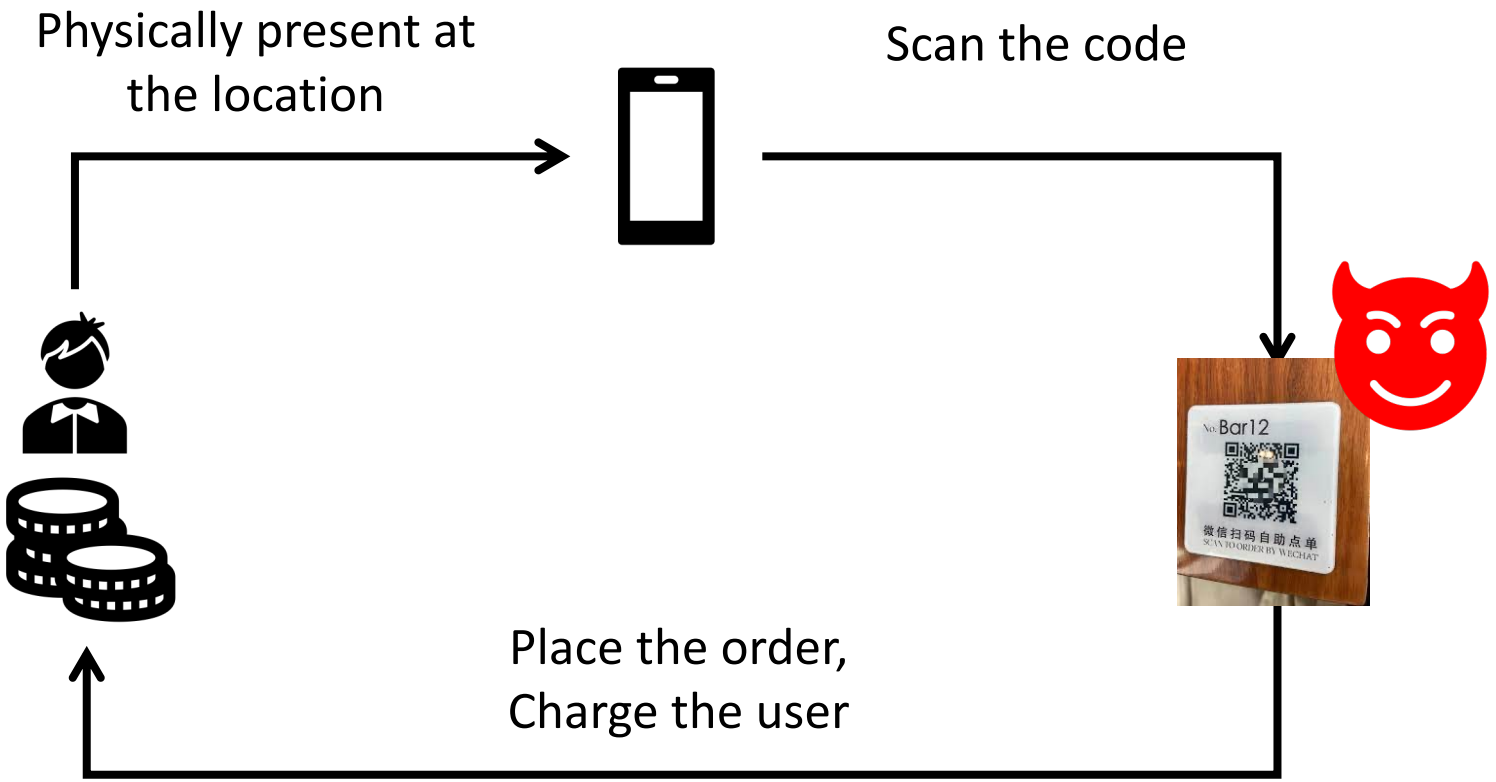
Target:

- The target asset can be user's information, money, location, etc.

Threats:

- The victim wouldn't aware from seeing the code
- The restaurant owner wouldn't notice this link, not before the checkout

Attack: Quishing Attack!



The attacker can place a fake QR code that lead to a malicious link

Target:

- The target asset can be user's information, money, location, etc.

Threats:

- The victim wouldn't aware from seeing the code
- The restaurant owner wouldn't notice this link, not before the checkout

Attacker

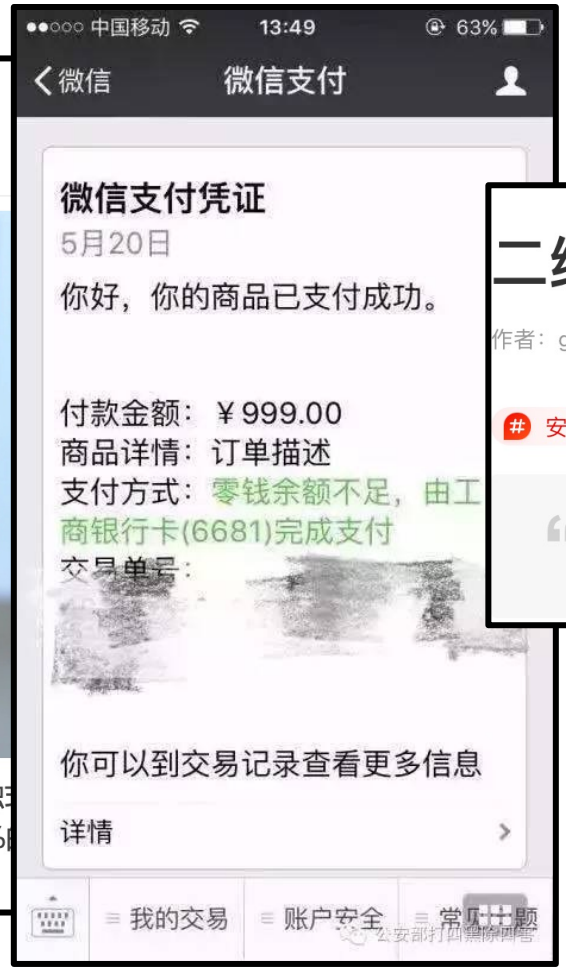
- Individual hacker
- Malicious organization
- …

The Attack is Already Exist!

扫描二维码时要小心

网喵 2022-05-31 23:33 0 条评论

二维码（QR）使用量的增长是由大流行推动的，在这种大流行中，非接触
常态。最近的数据显示，大约86%的智能手机用户至少扫描过一次二维码，36%
会每周扫描一次。



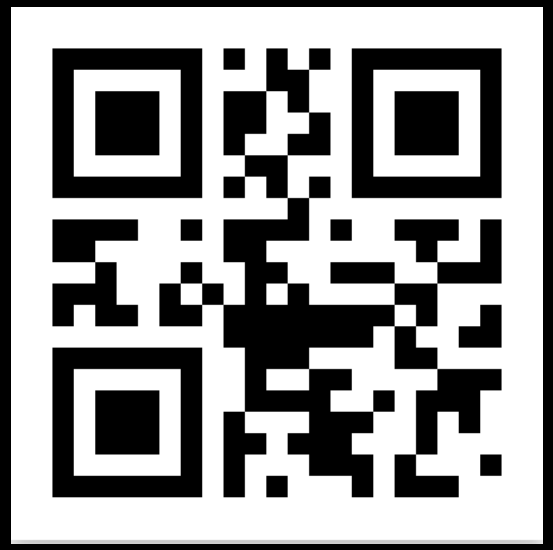
二维码：一种隐秘的安全威胁

作者：gejigeji 2020-10-10 11:34:47

安全

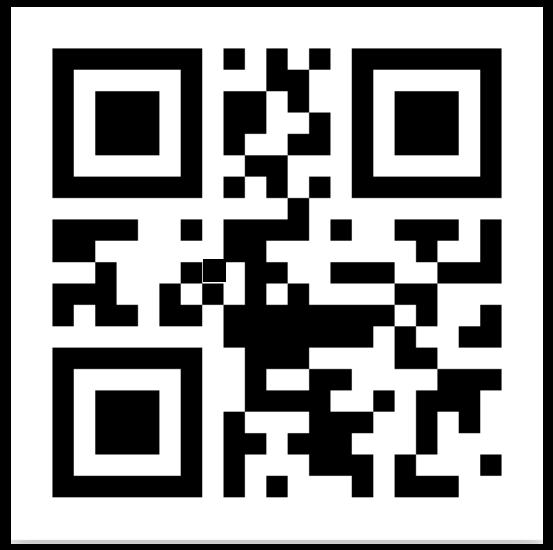
去年就有研究人员发现了一种新的网络钓鱼活动，该活动利用了旨在阻止此类攻击的安全解决方案和控制措施。

Try it for youself



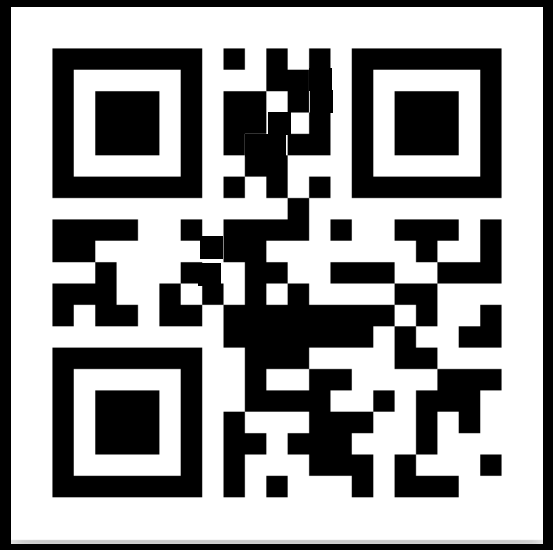
21 x 21 pixel QR Code

Try it for youself



Change 1 pixel

Try it for youself

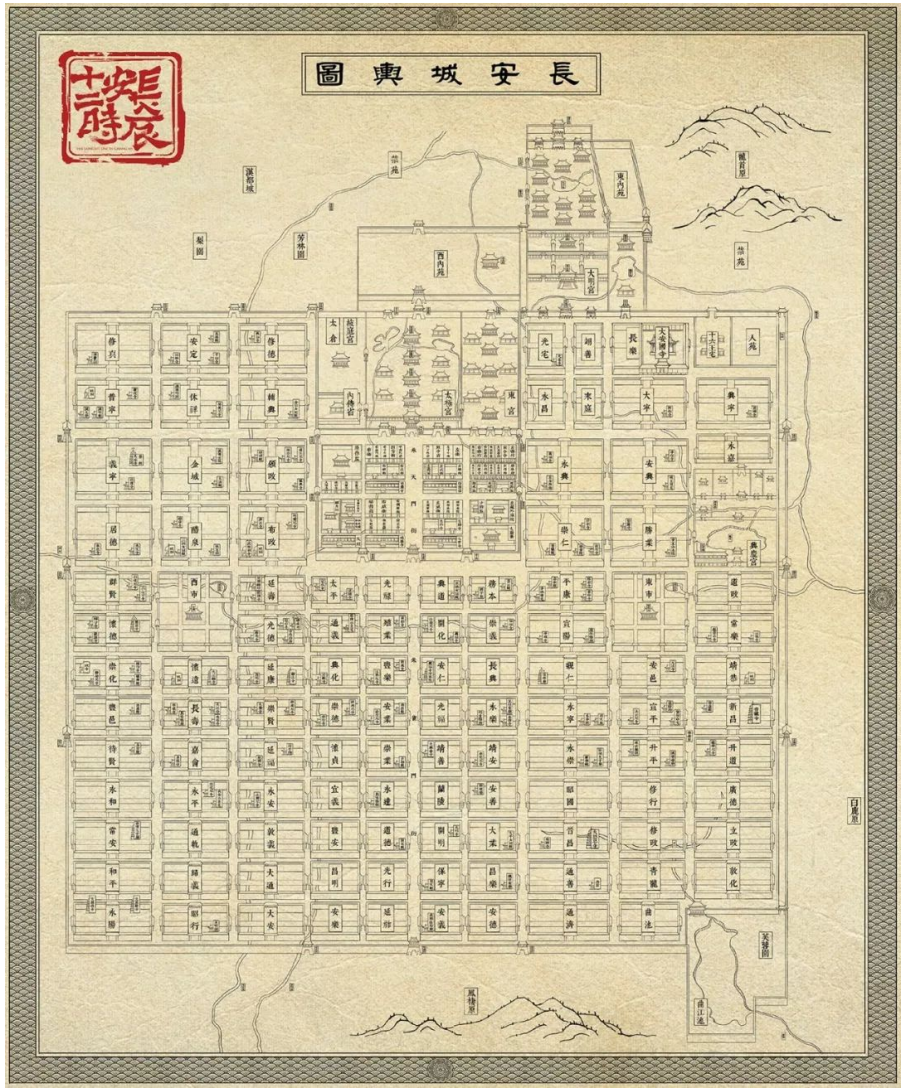


Change 6 pixels

Defenses

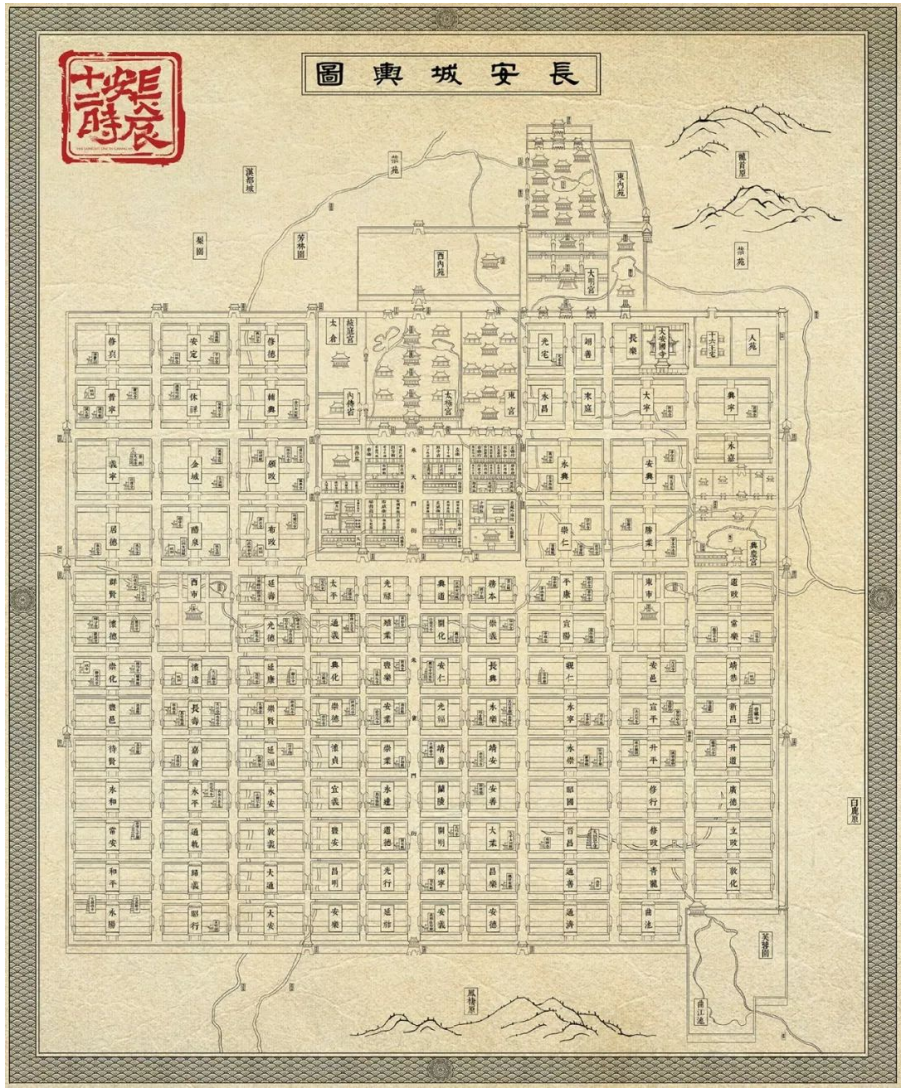
- You must physically at the place
- Timestamp the QR code
- You’re advised to examine the code
- After the scan, there has to be some steps before confirmation

Attacker's Asymmetric Advantage



Attacker's Asymmetric Advantage

- Attacker only needs to win in one place
- Defender's response:
  - Defense in depth
  - Think about the whole system

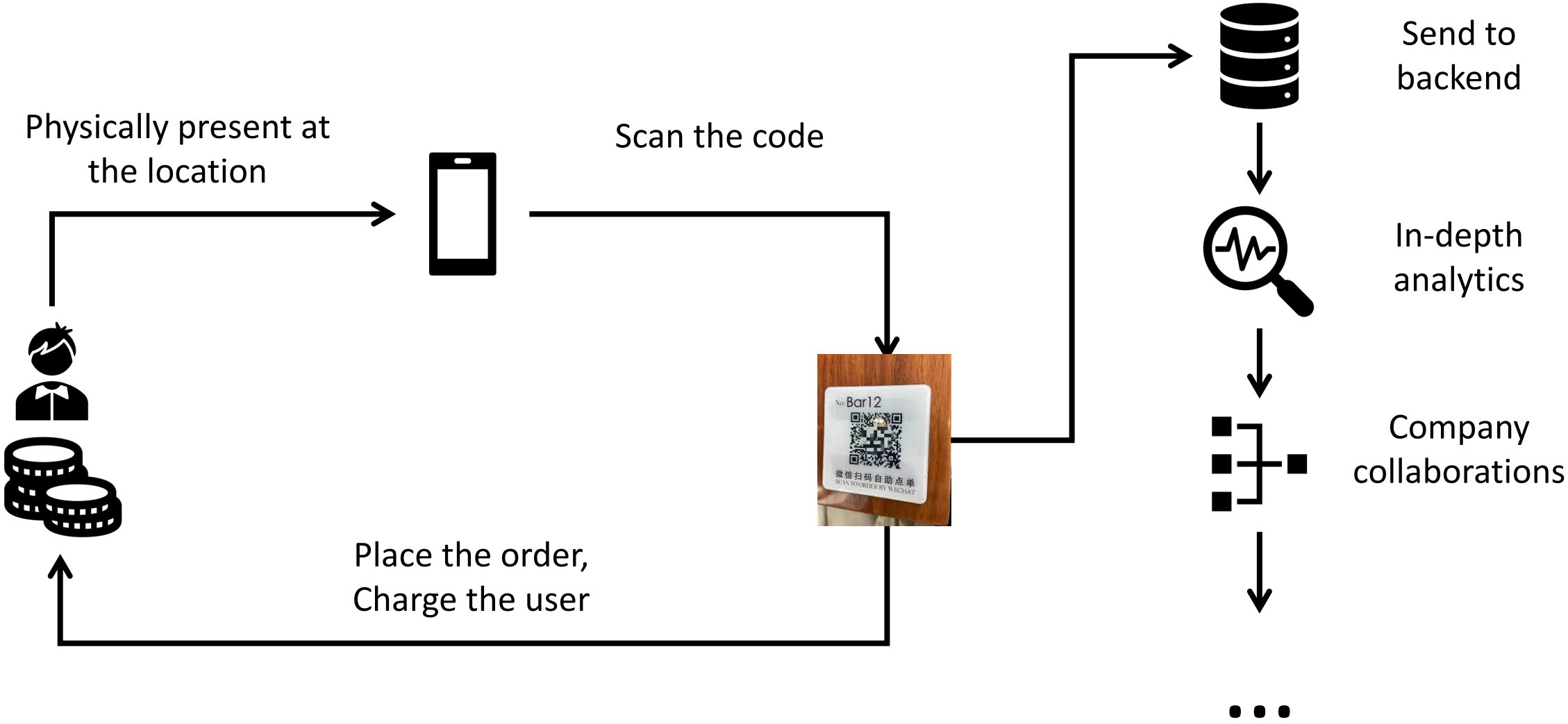


What's Wrong of this Picture?

Think about the Whole System

Whole System is Critical

More than Quishing Attack?



From Policy to Implementation

- After you've figured out what security means to your application, there are still challenges:
  - Requirements bugs and oversights
    - Incorrect or problematic goals
  - Design bugs and oversights
    - Poor use of cryptography
    - Poor sources of randomness
    - ...
  - Implementation bugs and oversights
    - Buffer overflow attacks
    - ...
  - Is the system **usable**?

Many Participants

- Many parties involved
  - System developers
  - Companies deploying the system
  - The end users
  - The adversaries (possibly one of the above)
- Different parties have different goals
  - System developers and companies may wish to optimize cost
  - End users may desire security, privacy, and usability
  - But the relationship between these goals is quite complex (e.g., will customers choose features or security?)

Better News

- There are a lot of defense mechanisms
  - We'll study some, but by no means all, in this course
- It's important to understand their limitations
  - "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem"

-- Bruce Schneier

https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html

What is Side-channel Attack?

- In computer security, a **side-channel attack (旁路攻击)** is any attack based on extra information that can be gathered because of the **fundamental way a computer system is implemented**

Light Commands: Laser-Based Audio Injection on Voice-Controllable Systems

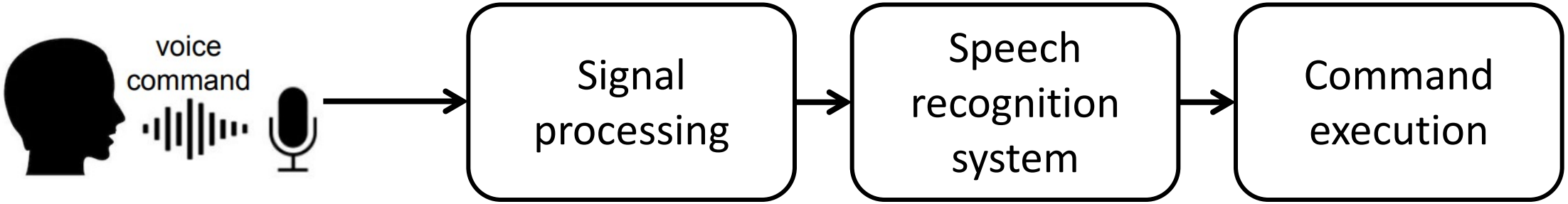
Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, Kevin Fu

USENIX 2020

Voice Controllable System (VCSs)

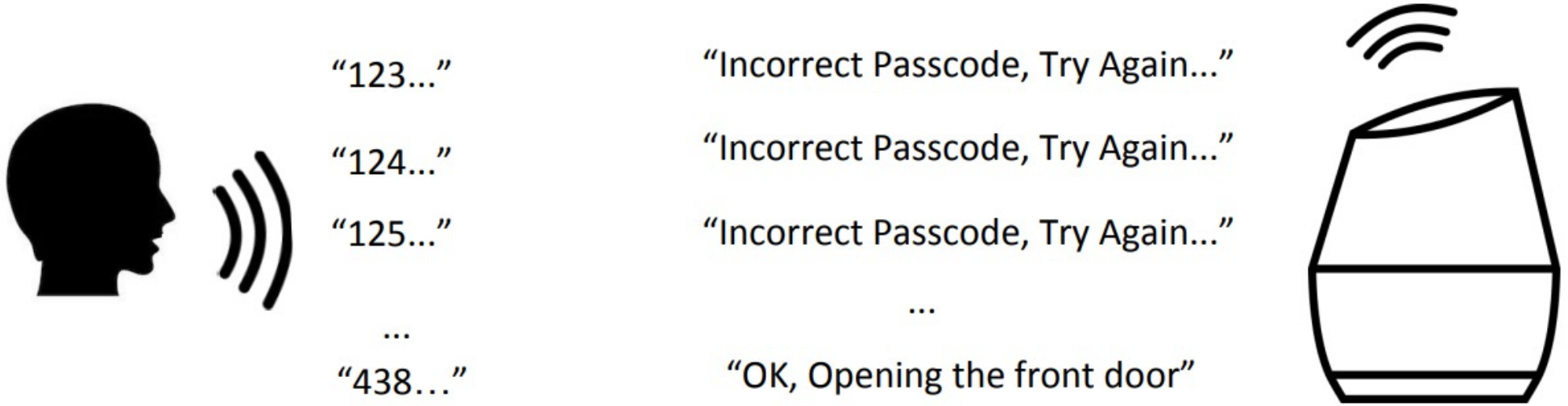
[Source: pandaily.com]

[Source: developers.google.com]



Security Concerns

- Sacrifice of security to promote usability
- Interfacing with 3rd Party Software
- Blind trust in microphone readings



The Problem

- Assumption:

  Microphones capture acoustic signals

The Problem

- Reality:

  Microphones capture acoustic signals & LIGHT signals

The Problem

- Two questions:
    1. How does laser injection affect VCSs?
    2. How can we protect VCSs against laser injection

Highlights of this paper

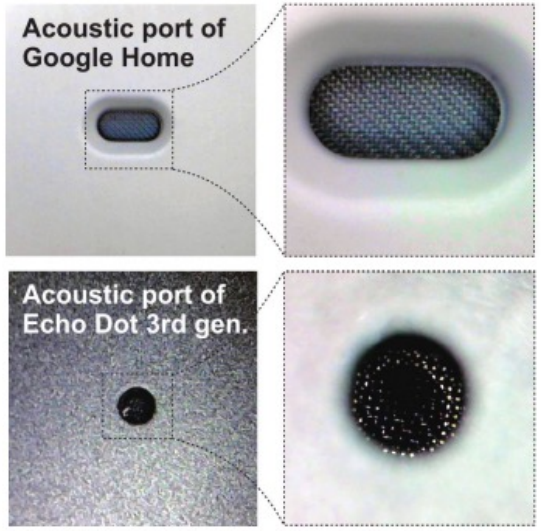
- Inject light commands via MEMS microphones
- Analyze limits of light-based VCS vulnerabilities
  - Success at 110 m with 5 mW laser pointer
  - Works through glass windows between buildings
- Demonstrate risks to smart speakers, phones, smart hones, and cars
- Suggest HW and SW countermeasures

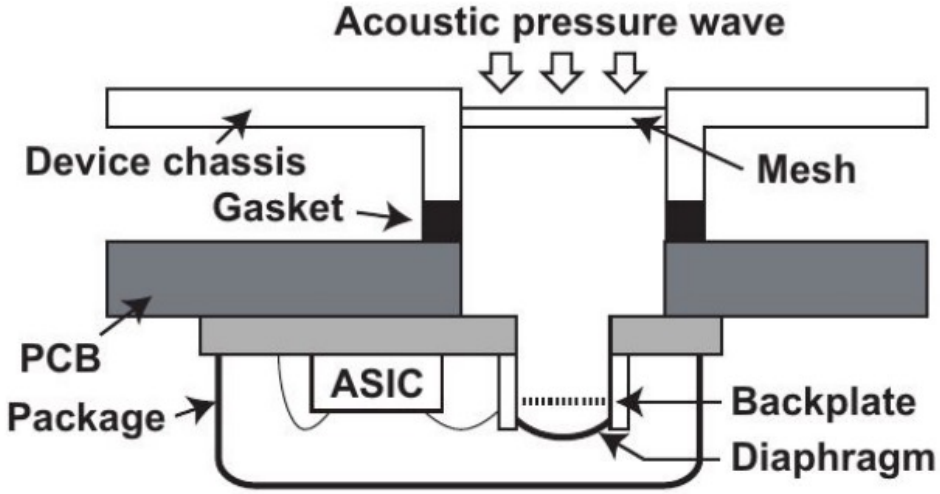
How it works?

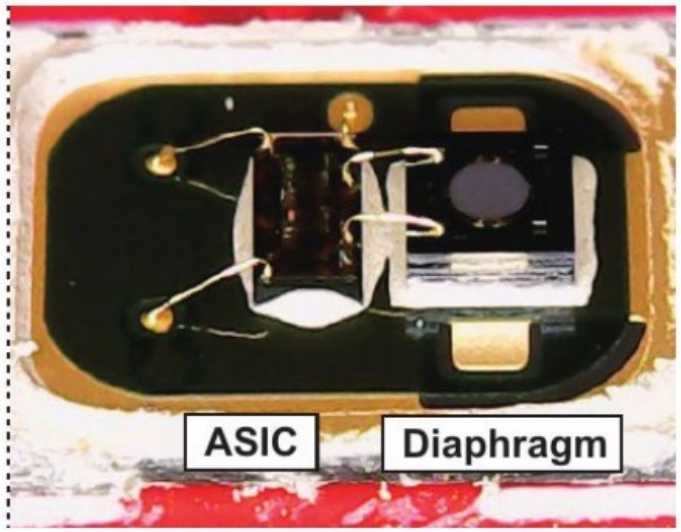
- Know the background of MEMS microphones

Background: MEMS Microphones

- Used in most Voice Controllable Systems
- The diaphragm and backplate (振动膜和背板) work as a capacitor
- When diaphragm moves, causes a change in capacitance
- The ASIC converts the capacitive change to voltage

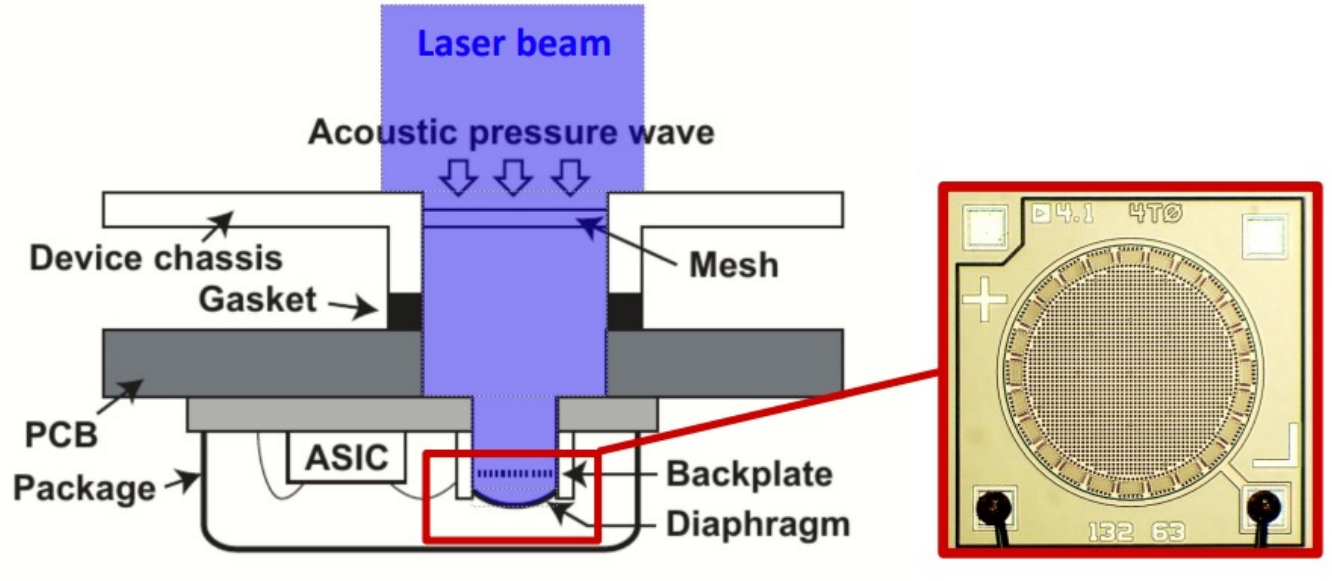






Background: MEMS Microphones

- MEMS microphones exhibit light sensitivity
- Output voltage affected by light irradiance (辐照度)
- Inject signal by modulating optical power

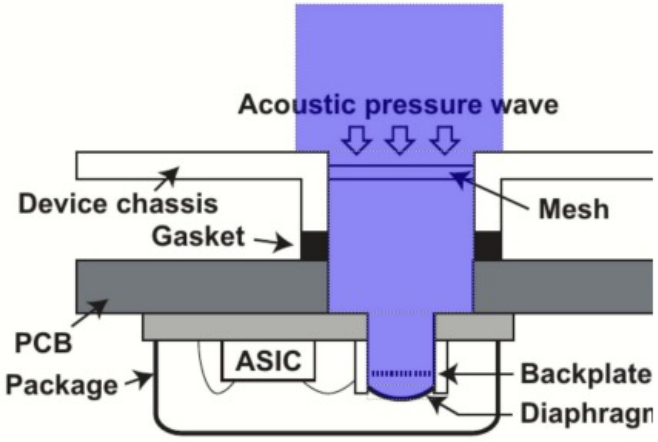


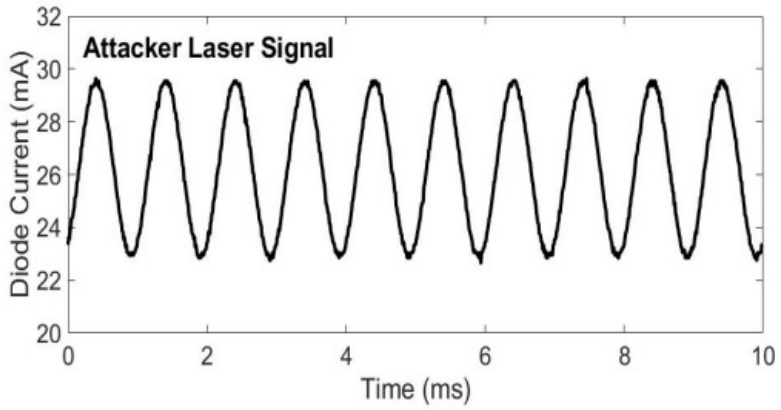
Irradiance:

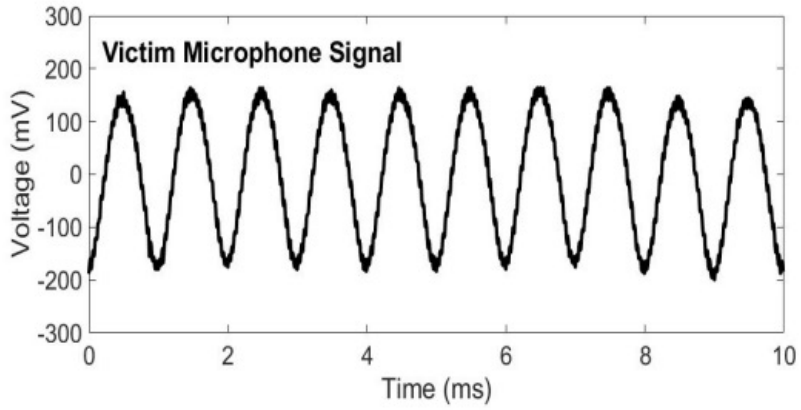
$$I = \frac{Optical\ Power\ (Watts)}{Beam\ Area\ \left(meters^2\right)}$$

Key Ideas

1. Amplitude modulated light generates a voltage signal on microphone output
2. Higher amplitude light == higher amplitude voltage
3. Very little distortion





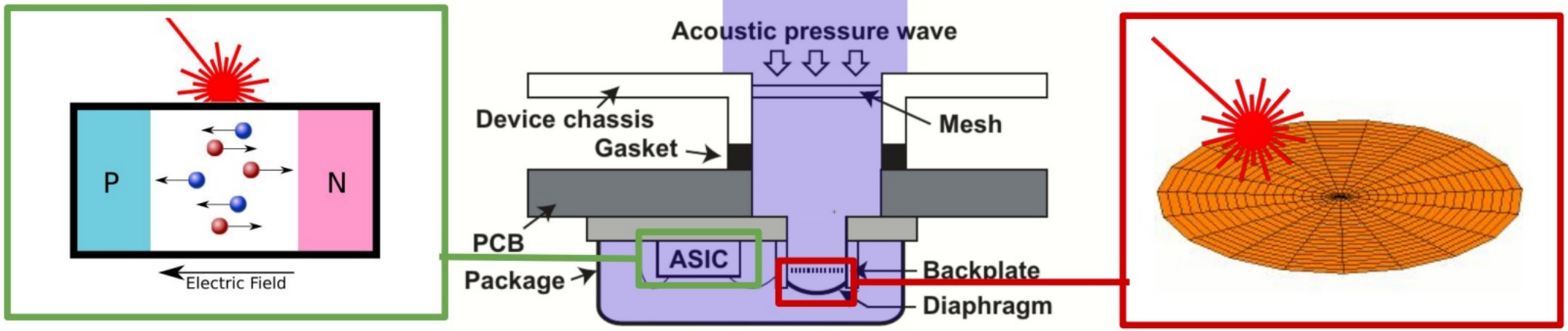


How is this Work?

- Combination of two physical effects: photoelectric (光电效应) on ASIC (专用集成电路) and photoacoustic (光声效应) on diaphragm

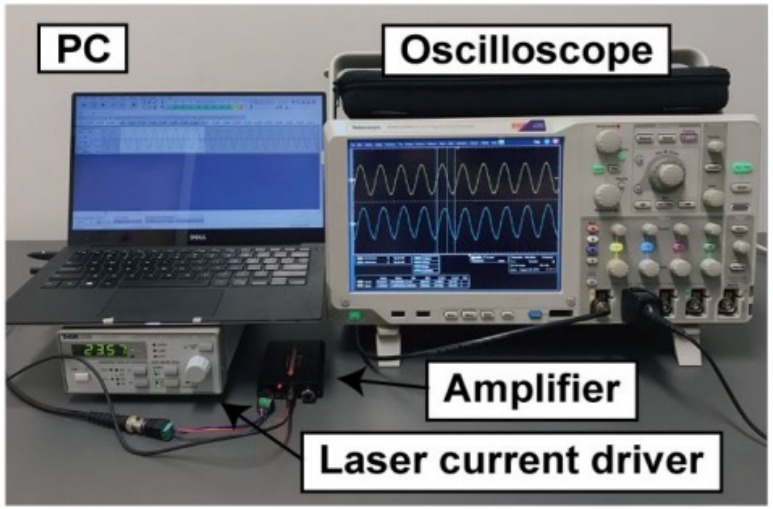
1. **Photoelectric** Effects on ASIC

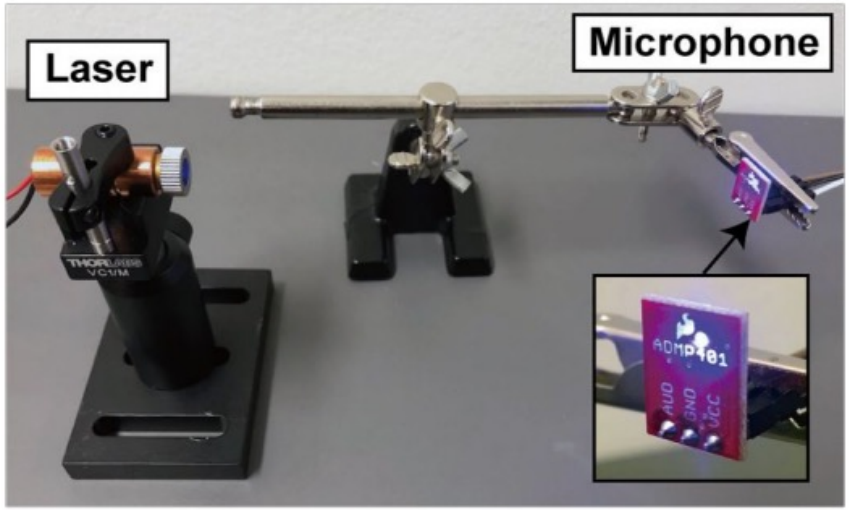
2. **Photoacoustic** Effects on Diaphragm

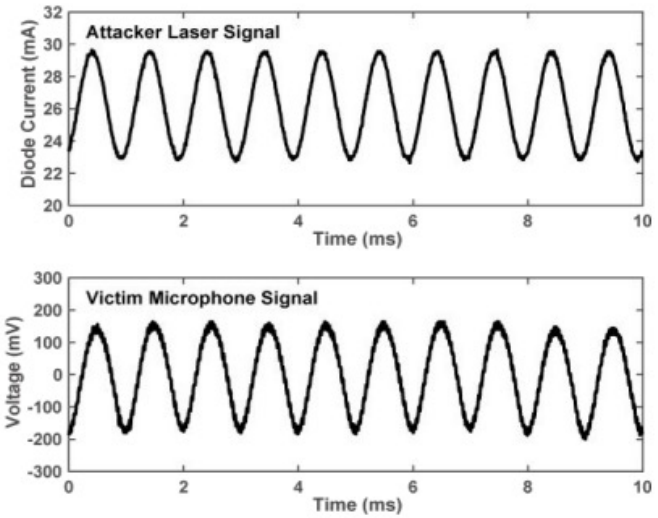


Signal Injection via Laser

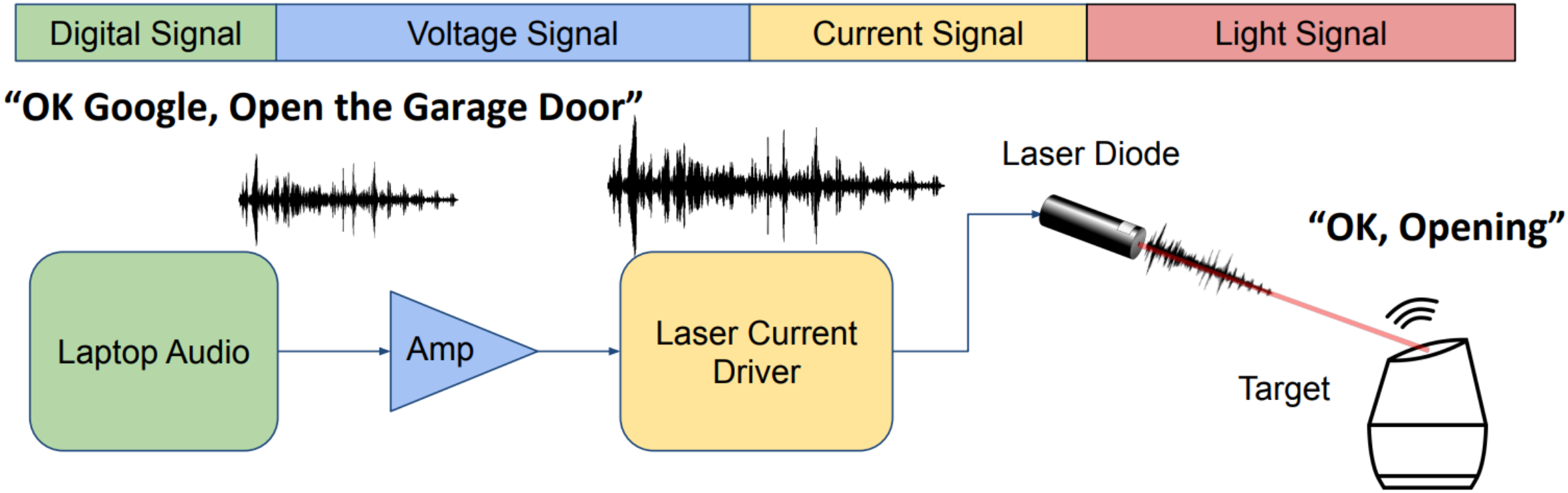
- Audio voltage signal from laptop
- Laser current driver converts to current signal – With DC Bias
- Laser output power is proportional to current





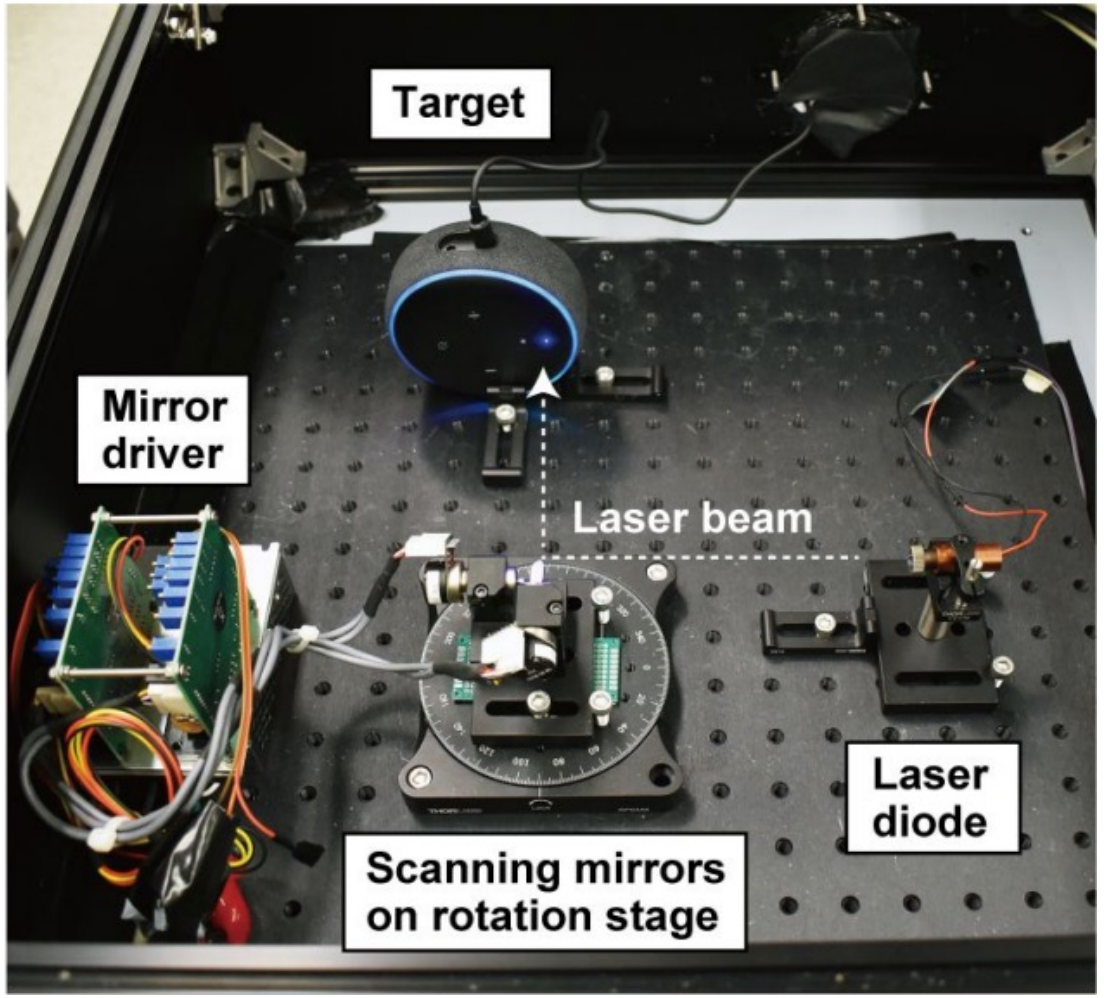


VCS Command Injection via Light



Measuring Vulnerability - Power

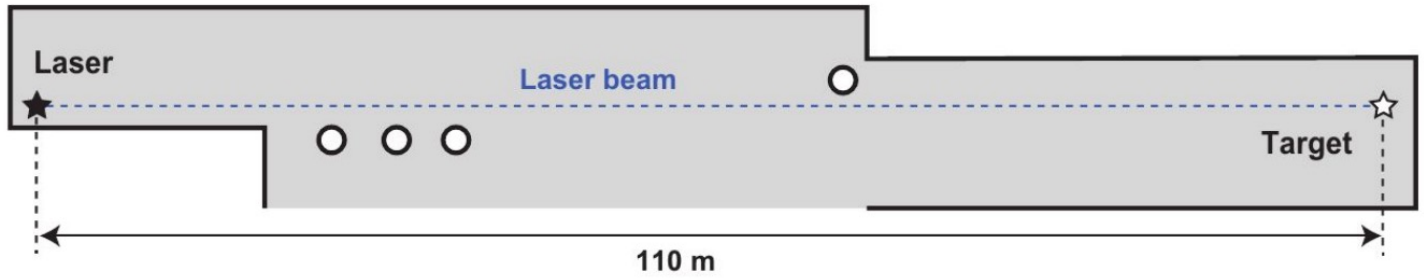
- Investigated 17 different devices
- Used scanning mirrors
- Measured minimum optical power to recognize commands



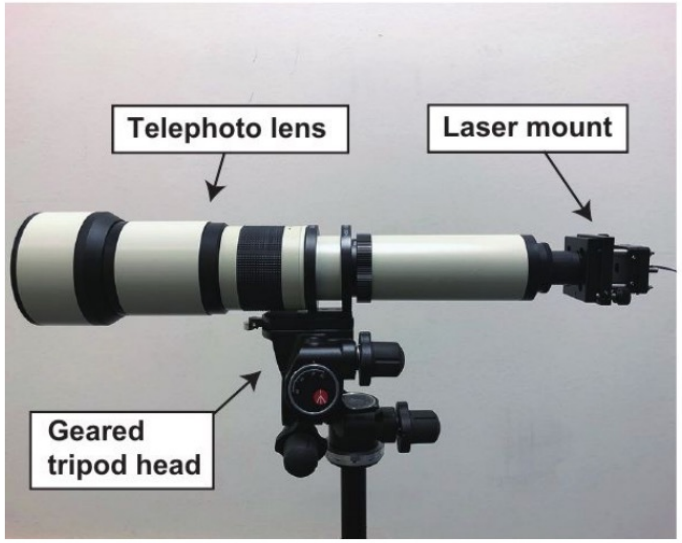
Measuring Vulnerability - Range

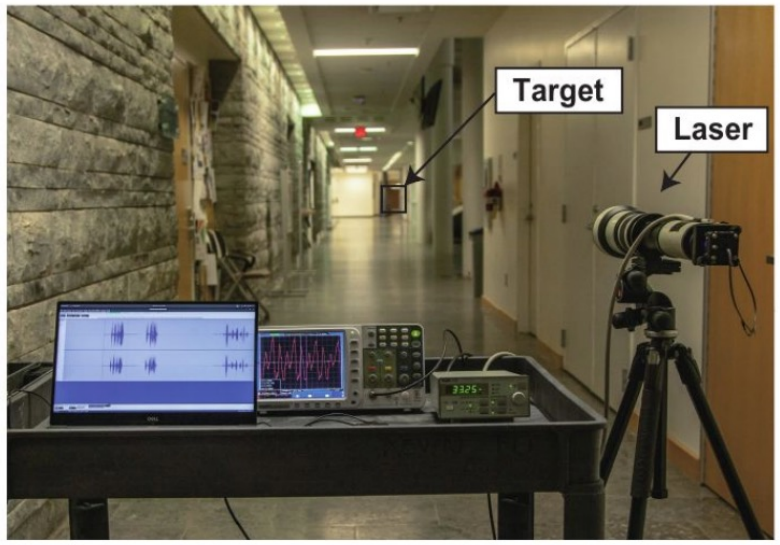
- Measuring the maximum range of the attack

$$\frac{\text{Optical Power (Watts)}}{\text{Beam Area } (\text{meters}^2)}$$



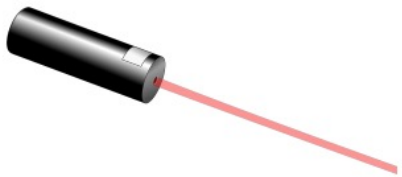
Optics!





Attack Results

Laser pointer power!



Device	Voice Recognition System	Minimun Laser Power at 30 cm [mW]	Max Distance at 60 mW [m]*	Max Distance at 5 mW [m]**
Google Home	Google Assistant	0.5	50+	110+
Google Home mini	Google Assistant	16	20	-
Google NEST Cam IQ	Google Assistant	9	50+	-
Echo Plus 1st Generation	Amazon Alexa	2.4	50+	110+
Echo Plus 2nd Generation	Amazon Alexa	2.9	50+	50
Echo	Amazon Alexa	25	50+	-
Echo Dot 2nd Generation	Amazon Alexa	7	50+	-
Echo Dot 3rd Generation	Amazon Alexa	9	50+	-
Echo Show 5	Amazon Alexa	17	50+	-
Echo Spot	Amazon Alexa	29	50+	-
Facebook Portal Mini	Alexa + Portal	18	5	-
Fire Cube TV	Amazon Alexa	13	20	-
EchoBee 4	Amazon Alexa	1.7	50+	70
iPhone XR	Siri	21	10	-
iPad 6th Gen	Siri	27	20	-
Samsung Galaxy S9	Google Assistant	60	5	-
Google Pixel 2	Google Assistant	46	5	-

5mW:
110+ meters

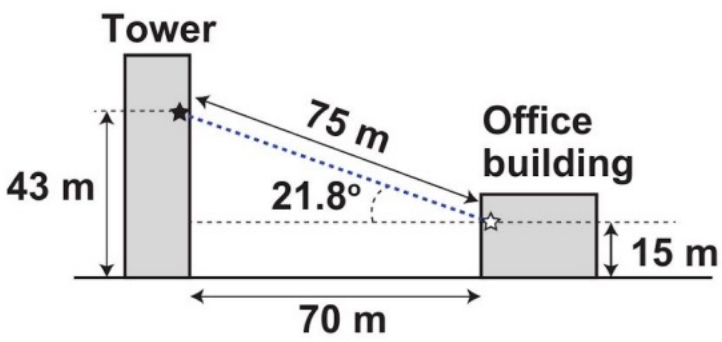
60mW:
50+ meters

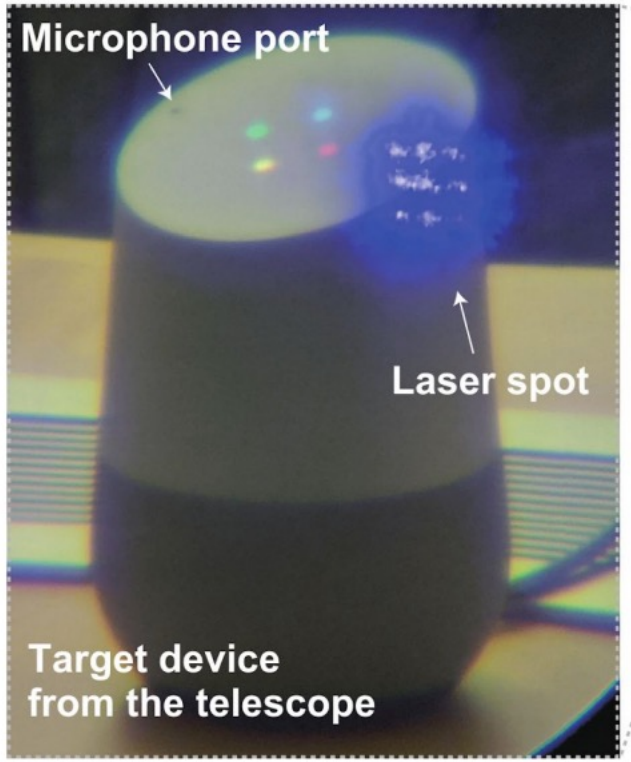
Phones/Tablets

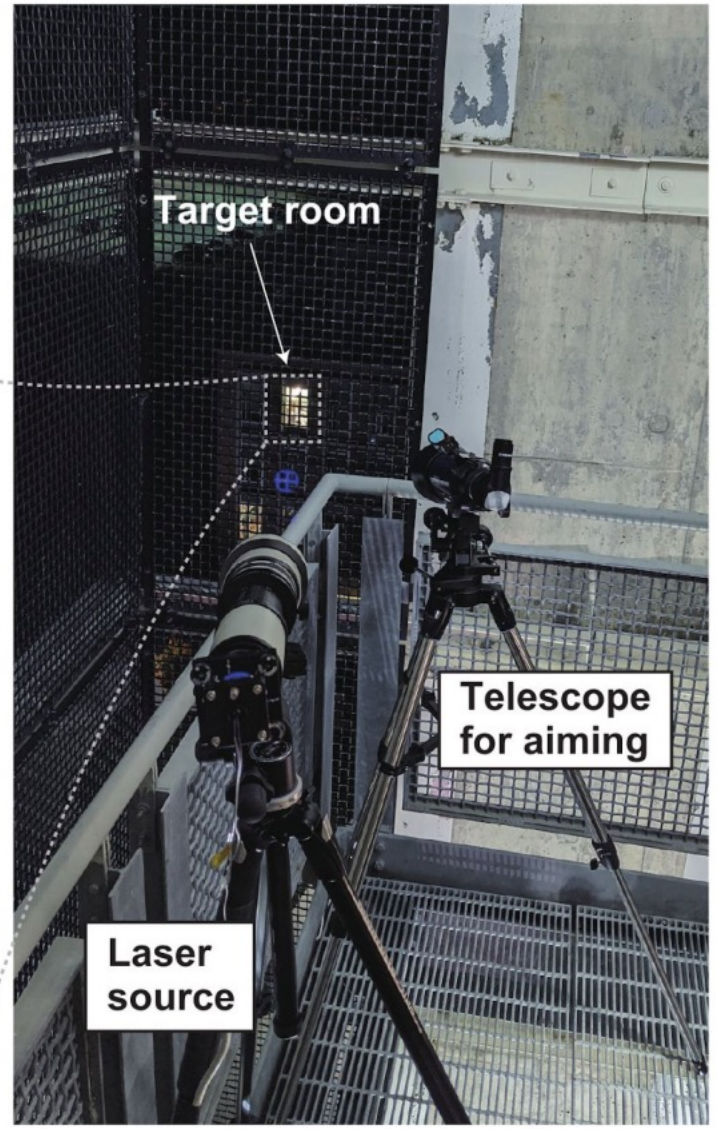
60mW:
5-20 meters

* Limited to a 50 m long corridor.
** Limited to a 110 m long corridor.

Cross-building Attack Scenario







Attack Demo 1

Attack Demo 2