Computer Science, College of William and Mary

IMDGuard

Securing Implantable Medical Devices with the External Wearable Guardian

Fengyuan Xu, Zhengrui Qin, Chiu C Tan, and Qun Li

April 13, 2011

Outline

Outline

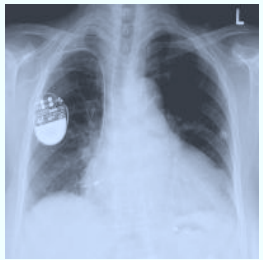
What is Implantable Medical Devices (IMDs))

IMDs are a group of medical devices implanted inside patients' bodies to provide daily monitoring or treatments, such as measuring insulin level, regulating heart rhythm, and providing visual sight.

Intracranial Sensor

Cardiac Defibrillator

Pacemaker

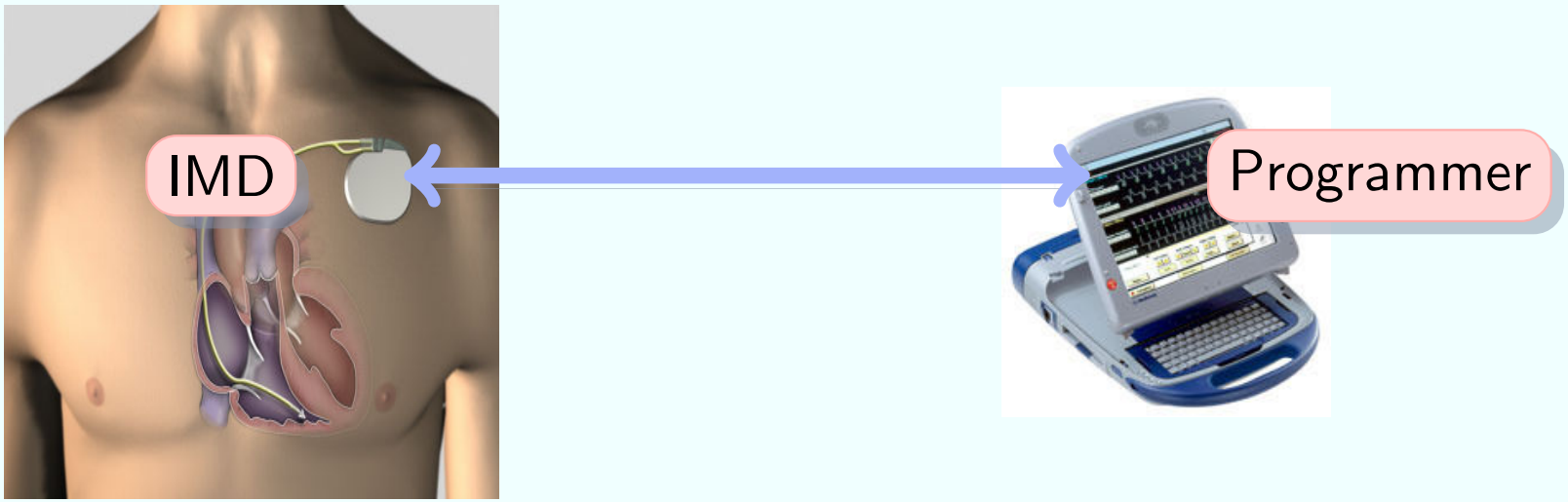


X-ray Image of Installed Pacemaker

Trend of Modern IMDs

- **Multifarious function.** It has been integrated into many IMDs that the flexible therapy configuration, physical condition monitoring, and diagnostic data stage.
- **Wireless capability.** It is common to find out current IMDs shipped with wireless communication interface. The frequency band used by IMDs has been approved by U.S. Federal Communications Commission and European Telecommunications Standards Institute.
- **Large demands.** 25 million US citizens depend upon IMDs, reported in 2001. This demand is excepted to continue increasing 8.3 percent annually through 2014.

Current Communication Model

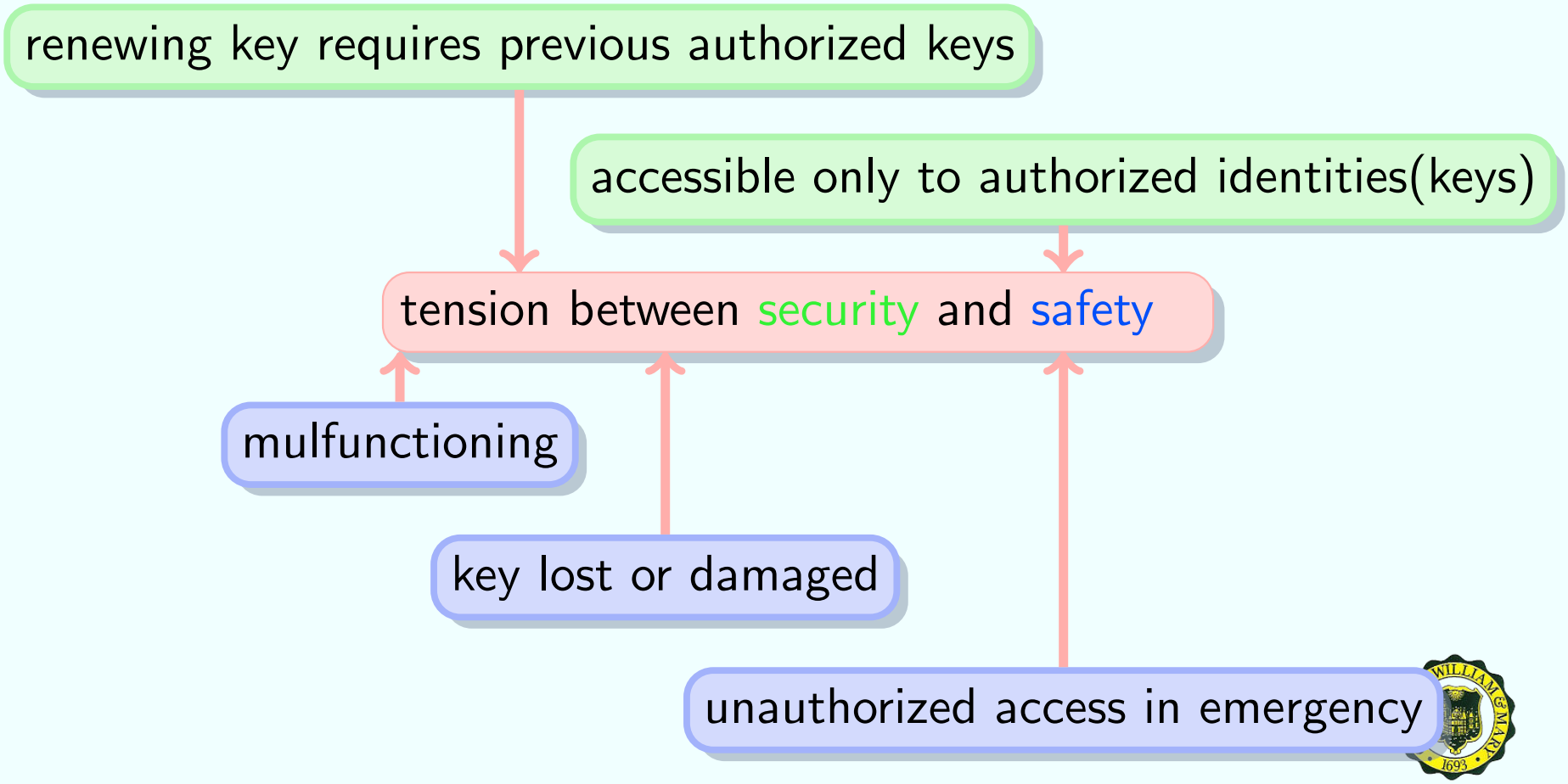


Potential Attacks

All wireless interactions occurred daily on patients' IMDs currently are not protected, which can be leveraged by vandals.

A recent study demonstrated that, by using equipments available on the markets, an IMD is able to be reprogrammed, putting the patient's life in danger.

Motivation


renewing key requires previous authorized keys
accessible only to authorized identities(keys)
tension between security and safety
mulfunctioning
key lost or damaged
unauthorized access in emergency

Motivation

renewing key requires previous authorized keys

identities(keys)

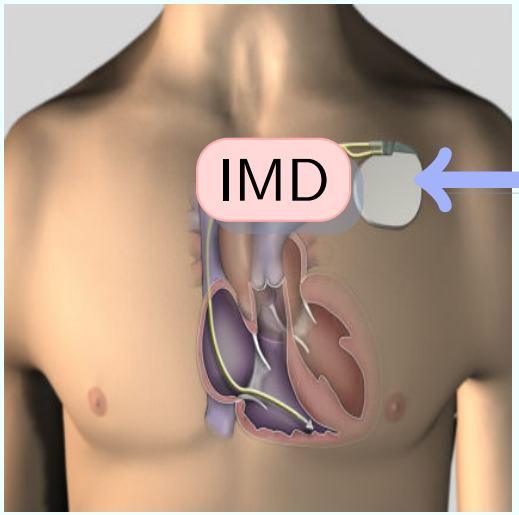
How to design a security scheme for IMDs that protects IMDs in regular situations,but safely allow access in any emergency without assistance from the patient?

mulfun

key lost or damaged

unauthorized access in emergency

New Infrastructure

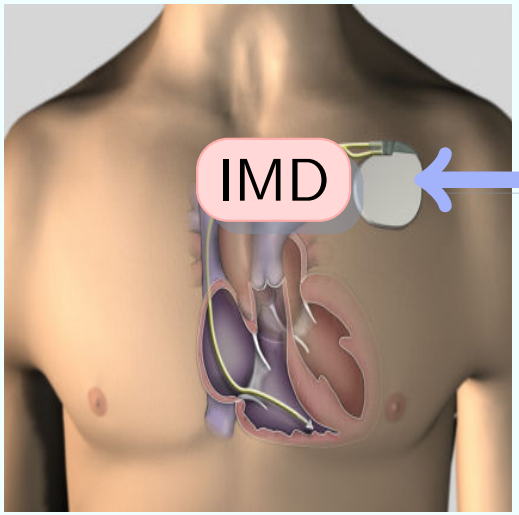


authorized

unauthorized

unauthorized in emergency

New Infrastructure



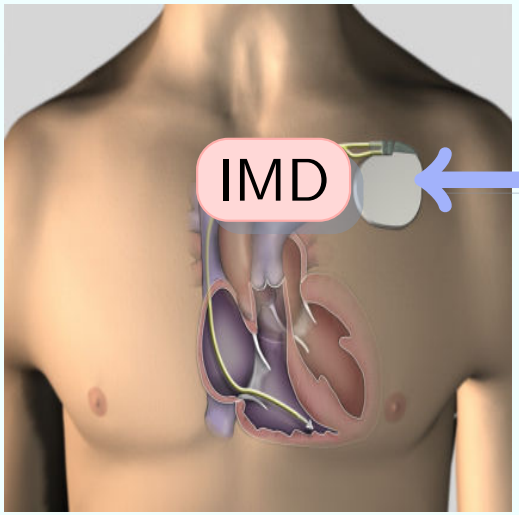
authorized

unauthorized

unauthorized in emergency

Guardian

New Infrastructure

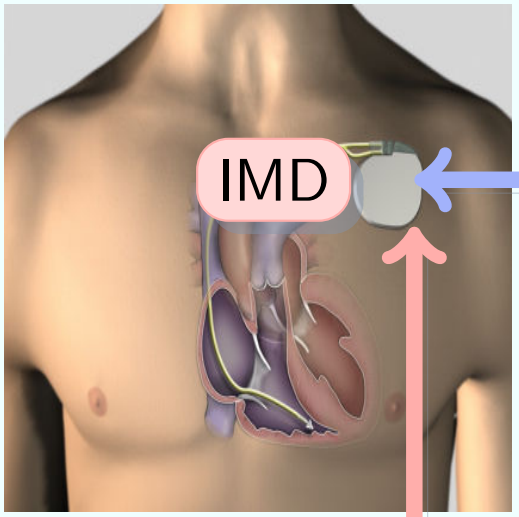


Programmer

- authorized
- unauthorized
- unauthorized in emergency

Guardian

New Infrastructure



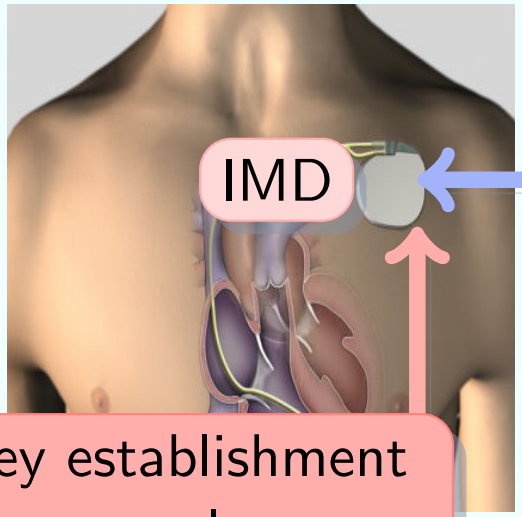
authorized

unauthorized

unauthorized in emergency

Guardian

First Challenge



IMD

Programmer

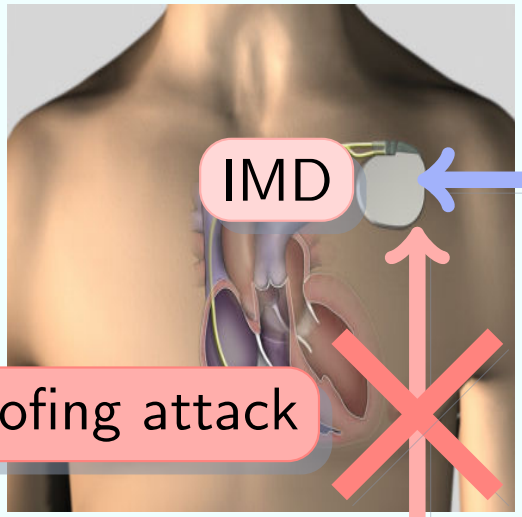
key establishment or renewal

Guardian

requirements:

- do not require prior shared secrets
- secure in any circumstance

Second Challenge



IMD

spoofing attack

Guardian

Programmer

authorized

unauthorized

unauthorized in emergency

Outline

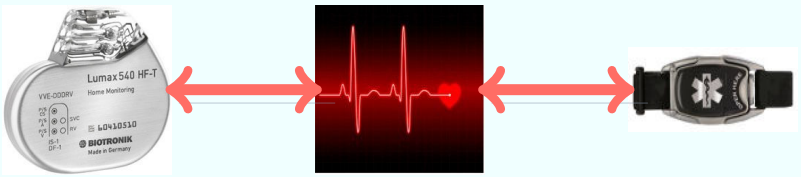
Adversary Model

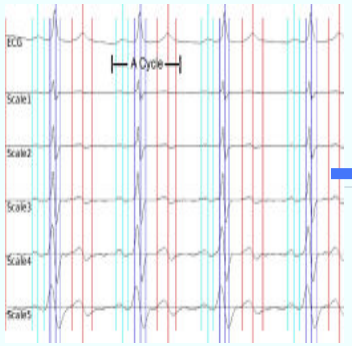
- Consider an adversary whose goal is trying to program to or retrieve data from the IMD without being caught.
- Assume the adversary cannot physically measure the patient's real-time ECG signals without being detected.
- Assume there is no adversary in an emergency situation.

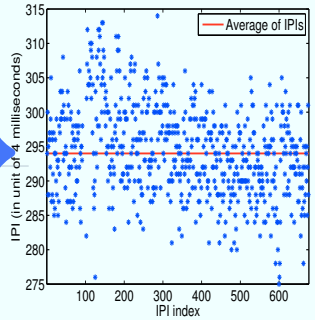
Overview

- IMDGuard is a novel security scheme for IMD-Guardian-Programmer infrastructure.
- IMDGuard incorporates two techniques tailored to provide desirable protections for IMDs.
  1. **ECG-based secure key extraction.** It allows the IMD securely pairs to an legitimate Guardian without any prior shared secrets.
  2. **Spoofing-resistant access control.** It provides security to the IMD in normal cases, and only grants accessibility to any programmer in *real emergency*.

Secure Key Establishment Scheme Based on ECG Signals







i quantization

ii reconciliation

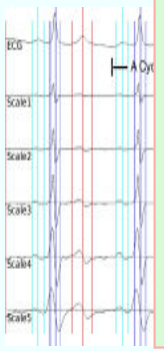
00101010101
01010100101
00110101101
10101011011

ECG Delineation **IPI fluctuation** **Secret Key**

Secure Key Establishment Scheme Based on ECG Signals

Quantization:

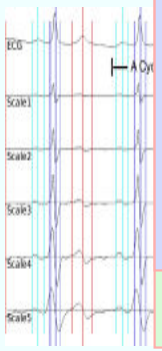
- We map each IPI fluctuation into a n-bit binary string.
- Occurrences of different n-bit binary string mappings are equally likely.
- In order to reduce the mismatched bits of two sides, we pick proper n and apply gray code.



01010101
10100101
10101101
01011011

ECG Delineation IPI fluctuation **Secret Key**

Secure Key Establishment Scheme Based on ECG Signals



Quantization:

Reconciliation:

- Exchange a bit information so that both sides can agree on a secret composed of identical binary strings.
- Remove the leaked information to condense the entropy of generated secret.

code.

01010101
10100101
10101101
01011011

ECG Delineation **IPI fluctuation** **Secret Key**

Secure Key Establishment Scheme Based on ECG Signals

Quantization:

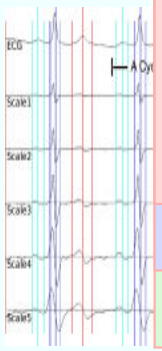
Reconciliation:

Features:

- No need to change IMDs' hardware design.
- Ensured information-theoretic security.
- Robust against man-in-the-middle attacks.

the entropy of generated secret.

code.



01010101
10100101
10101101
01011011

ECG Delineation IPI fluctuation

Secret Key

Spoofing-resistant Access Control

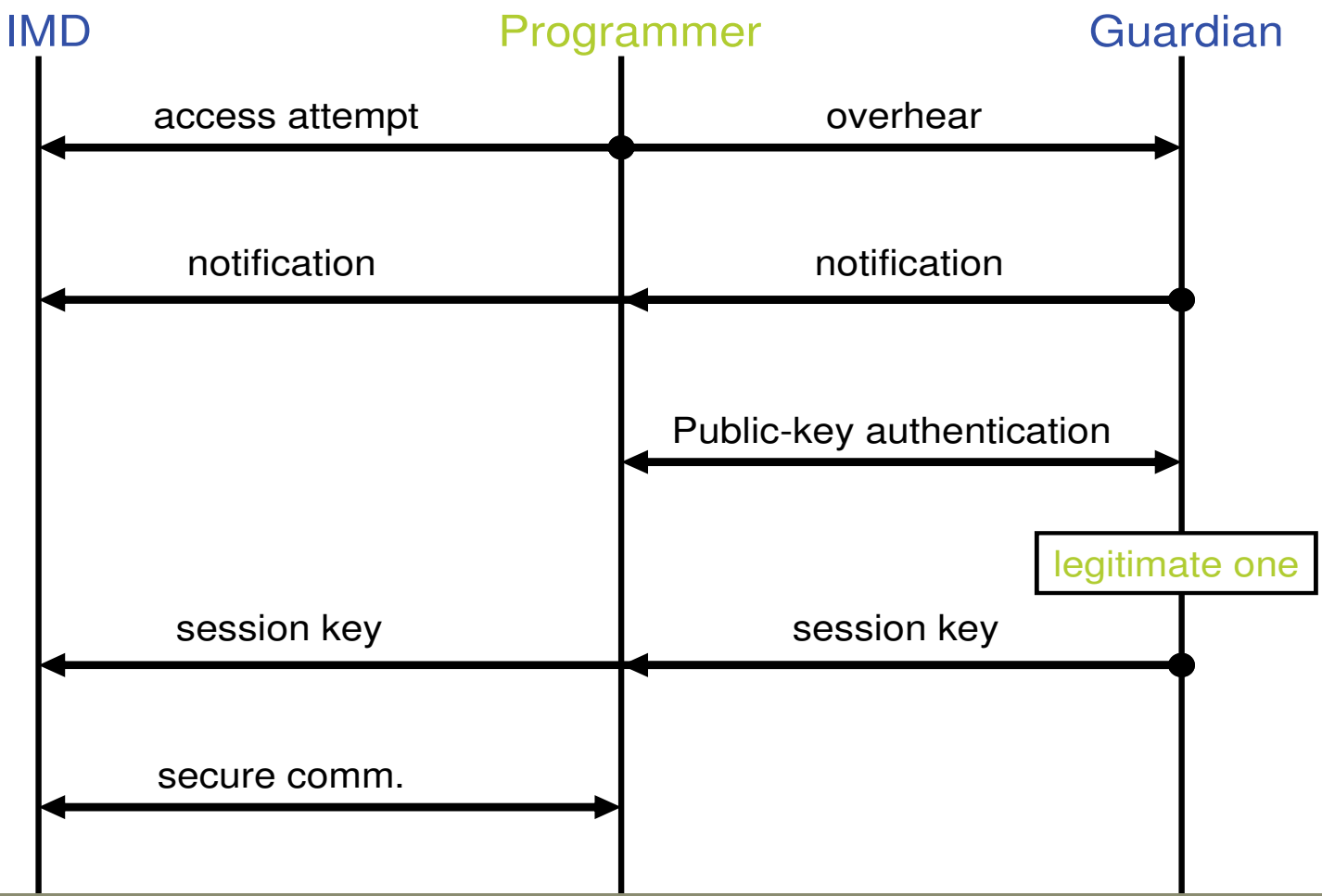
Motivation

- It is unknown how powerful the adversary is.
- Collaboration is possible between the IMD and Guardian.

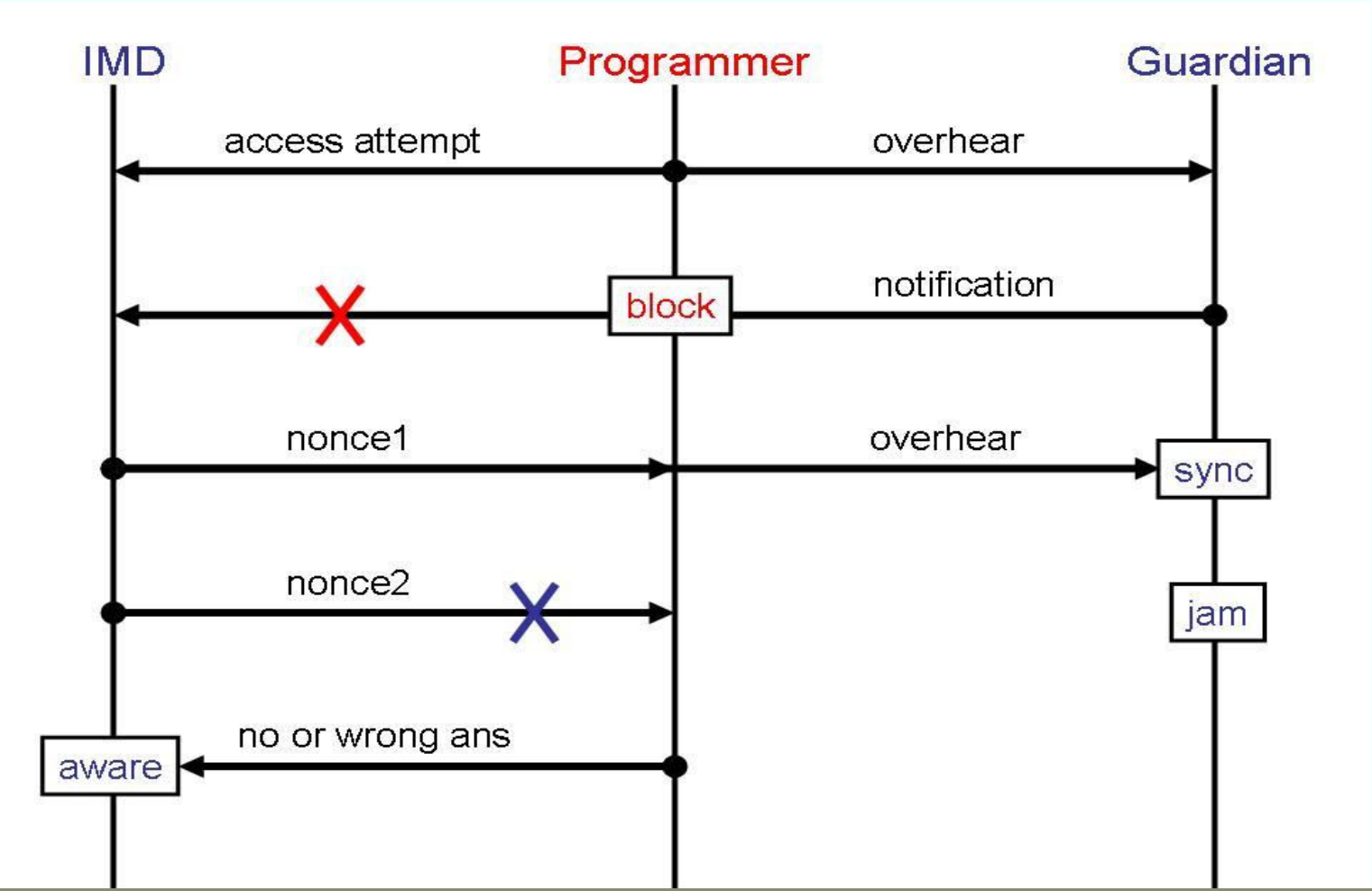
Strategy

Guardian jams IMD's message to block illegal interactions when encountering spoofing attacks.

When There is no Spoofing Attacks



Defensive Jamming against Spoofing Attacks



Prototype Implementation

Total code size of IMDGuard prototype		
Module	ROM(*bytes*)	RAM (*bytes*)
IMD	20656	1056
Programmer	20754	1060
Guardian	20614	1050
ECC	42190	1931
Key Extraction	10078	887
ECG Delineation	18720	9652

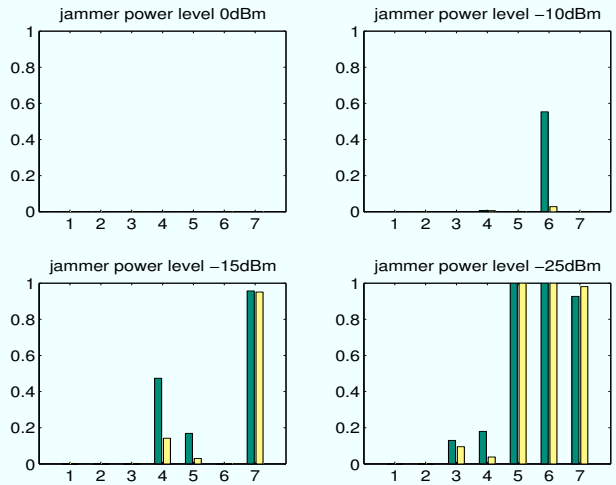
Outline

Key Establishment

1. **Variance.** The historic records of the same person do not help adversary to guess the generated key, neither do that of other people.
2. **Efficiency.** On average a secret key can be extracted in 45 seconds.
3. **Randomness.** Generated keys can pass National Institute of Standards and Technology (NIST) Randomness testing suite.

Access Control Protocol

Defensive Jamming Effectiveness



Prototype Timing Information

Overhead in Time (ms)		
Situation	Operation	Overhead
Authentication	Signing(20bytes)	1550
	Verification(20bytes)	2221
	Others	50
Guardian Removed	Challenge Transfer	512
	Others	14
Guardian Jamming	Session Deny	1501

Outline

Conclusion

1. We are the first to propose a rigorously information-theoretic secure extraction scheme, and evaluate its performance on resource constrained embedded systems.
2. We are the first to finalize and implement a comprehensive secure protocol for the IMD-Guardian-Programmer infrastructure.
3. We perform extensive experiments on our prototype to evaluate the validity and performance of IMDGuard.

Thank You

Any question