On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them

EDUARD MARIN, DAVE SINGELÉE, FLAVIO D. GARCIA, TOM CHOTHIA, RIK WILLEMS AND BART PRENEEL

KU LEUVEN - COSIC AND IMINDS

UNIVERSITY OF BIRMINGHAM, SCHOOL OF COMPUTER SCIENCE

UNIVERSITY HOSPITAL GASTHUISBERG, CARDIOLOGY

ACSAC 2016
December 4-9, Los Angeles
Introduction
State-of-the-art

Pacemakers and Implantable Cardiac Software Radio Attacks and Zero-Po
Daniel Halperin†
University of Washington

Shane S. Clark
University of Massachusetts Amherst
Kevin Fu, PhD
University of Massachusetts Amherst

Abstract—Our study analyzes the security and privacy vulnerabilities of an implantable cardioverter defibrillator (ICD) used to treat heart patients. We evaluated the security of a commercial ICD over-the-air communication protocol to determine if it could be exploited to perform timing attacks.

Pacemakers and Implantable Cardiac Software Radio Attacks and Zero-Po
Daniel Halperin†
University of Washington

Shane S. Clark
University of Massachusetts Amherst
Kevin Fu, PhD
University of Massachusetts Amherst

Abstract—Our study analyzes the security and privacy vulnerabilities of an implantable cardioverter defibrillator (ICD) used to treat heart patients. We evaluated the security of a commercial ICD over-the-air communication protocol to determine if it could be exploited to perform timing attacks.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.

Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
Chunxiao Li
Department of EE
Princeton University
chunxiao@princeton.edu

Anand Raghunathan
School of ECE
Purdue University
raghunathan@purdue.edu

Niraj K. Jha
Department of EE
Princeton University
jha@princeton.edu

Abstract—Wearable and implantable medical devices are being increasingly used to diagnose and treat diabetes and other chronic diseases. In this work, we demonstrate successful security attacks and countermeasures on the proposed delivery systems to mitigate the proposed security threats.

On the Feasibility of Cryptography for a Wireless Insulin Pump System
Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede and Bart Preneel
KU Leuven, ESAT-CAOS and iMinds
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

ABSTRACT
This paper presents the security and privacy properties of the use of an insulin pump and its peripherals. We evaluate the wireless channel using Commercial Off-The-Shelf (COTS) software-based radios to intercept the messages sent between these devices, and fully reverse-engineer the wireless communication protocol using a black-box approach, and document the message format and the protocol state-machine in use. The upshot is that no standard cryptographic mechanisms are applied and hence the system is shown to be completely vulnerable to radio- and presence injection attacks.
Device programmer – 2nd generation ICD

Device programmer – 2nd generation ICD

Short-range communication channel (<10 cm)
Device programmer – latest generation ICD

Short-range communication channel (<10 cm)

Long-range communication channel (2-5 m)
ICD activation procedure
Contributions

- Feasibility of reverse-engineering
- How an adversary could activate the ICD
- Active and passive wireless attacks
- Short-term and long-term countermeasures
Laboratory setup

- Universal Serial Radio Peripheral (USRP)
- Data Acquisition System (DAQ)
- Antennas
- Device programmers
- Base stations
- 10 different ICDs models
Methodology

- Proprietary wireless communication protocol
- Weak adversary who can only intercept the messages
- Black-box reverse-engineering
- Labour-intensive and challenging process
Methodology

- Proprietary wireless communication protocol
- Weak adversary who can only intercept the messages
- Black-box reverse-engineering
- Labour-intensive and challenging process
Wireless communication parameters

- Transmission frequency
- Modulation
- Symbol rate
  - Hilbert transform
  - FM demodulator
Intercept the signals
Data whitening

- Technique to avoid long strings of “1s” and “0s”
- Data obfuscation
- LFSR sequence is constant across sessions and reused in all ICDs

(a) "A" 00101011 10111101 00011010 01010001
(b) "AA" 00101011 11101000 00011010 01010001
(c) "AAA" 00101011 11101000 01101001 01010001
(d) "AAAA" 01010111 11101000 01101001 01111101
(e) LFSR seq 01001010 10001001 000001000 00011100
(f) ASCII 01100001 01100001 01100001 01100001

A A A A

More details in the paper
How can adversaries activate the ICD?

- Hijacking an active session
- Wake up the device from “sleep” mode
- Standby mode
- Using legitimate external devices

![Diagram showing the relationship between Adversary, Device programmer, and ICD]
How can adversaries activate the ICD?

- Hijacking an active session
- **Wake up the device from “sleep” mode**
- Standby mode
- Using legitimate external devices
ICD state machine

- Sleep mode
- Interrogation mode
- Reprogramming mode

2 hours
Wake up the device from sleep mode

- Short-range channel
- Vulnerable to replay attacks
- Crowded places (e.g. public transport)
How can adversaries activate the ICD?

- Hijacking an active session
- Wake up the device from “sleep” mode
- **Standby mode**
- Using legitimate external devices
ICD state machine

- Sleep mode
- Interrogation mode
- Reprogramming mode
- Standby mode

- 5 min
- 2 hours
How can adversaries activate the ICD?

- Hijacking an active session
- Wake up the device from “sleep” mode
- Standby mode
- Using a legitimate base station
  - Home monitoring
  - Inexpensive, portable and can be easily purchased

1st step: Use the base station to put the ICD in “standby” mode

2nd step: Use the USRP to send messages over the long-range channel
Privacy attacks

- Passive adversary: eavesdropping
- Active adversary: send messages to request specific data
- Sensitive health and personal data
  - Name, address, etc
  - Treatment and therapy details
  - Telemetry data
  - Unique ICD SN
- Track patients
DoS attacks

- Jamming the wireless channel
- Keep the ICD active while being in standby mode
  - No need of being in close proximity
  - Message sent over the long-range communication channel
  - Same for all ICDs
Short-term countermeasures

- Already-implanted ICDs
- Only modifications in external devices
- “Shutdown” command
  - Proactive or reactive jamming
- Drawbacks:
  - Disrupt other ongoing sessions
  - Patients need to stay close to the external device for 5 minutes
Offline vs online solutions

- Off-line key agreement protocol
  - Store master key in all device programmers (high risk!!)
  - Diversified keys in ICDs
- On-line key agreement protocol
  - Master key in the cloud
  - Device programmers need to be online all the time (not realistic!!)

Middle ground solution: semi-offline key agreement protocol
Semi-offline key agreement protocol
Conclusions

- Responsible disclosure
- Security through obscurity is a dangerous approach
- Feasibility of reverse engineering the protocol by a weak adversary
- Short-term and long-term countermeasures
- Balance between security and availability