Hold The Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft

Kyungho Joo*  Wonsuk Choi*  Dong Hoon Lee
Korea University

* Co-first Authors
Outline

• Introduction
• Attack Model
• Our Method
• Evaluation
• Discussion
• Conclusion
Introduction

• Traditional system
  • Physically insert a key into the keyhole
  • Inconvenient
  • Vulnerable to key copying
Introduction

• Keyless Entry System
  • Remote Keyless Entry (RKE) System
  • Passive Keyless Entry and Start (PKES) System

• Attacks on Keyless Entry System
  • Cryptanalysis
  • Relay Attack
  • etc. (e.g., Roll-jam)
Introduction

• Countermeasures
  • Distance bounding protocol
    • Sensitive to timing error (Propagates at the speed of light)
  • UWB-IR Ranging System
    • Efforts are underway (IEEE 802.15.4z Task Group) [1-3]
    • Requires an entirely new system

• Motivation
  • Device Fingerprint: Exploits hardware imperfection
  • PHY-layer signal analysis

[1] UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks (M. Singh et al.)
[2] UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband (M. Singh et al.)
Introduction

• Contributions
  • New attack model
    • Combines all known attack methods; our attack model covers both PKES and RKE systems
    • Single/Dual-band relay attack, Cryptographic attack
  • No alterations to the current system
    • Easily employed by adding a new device that captures and analyzes the ultra-high frequency (UHF) band
      RF signals emitted from a key fob
  • Evaluations under varying environmental factors
    • Temperature variations, NLoS conditions (e.g., a key fob placed in a pocket) and battery aging
Introduction

• Passive Keyless Entry System
  • LF band (125~135 kHz, Vehicle)
    • 1 ~ 2 meter communication range
  • UHF band (433, 858 MHz, Key fob)
    • ~100 meter communication range
  • Shared cryptographic key between the key and the vehicle

1. Wake up (LF)
2. Ack (UHF)
3. ID with challenge (LF)
4. Key response

If Key in communication range
If ID is Correct
Introduction

• System Model
Outline

• Introduction / Background

• Attack Model

• Our Method

• Evaluation

• Discussion

• Conclusion
Attack Model

• Coverage
  • Attacks on PKES and RKE systems implemented with the LF/UHF band RFID communication

• Main Objectives of adversary
  • Unlocking a vehicle

• Out of Scope
  • Excluded other functions, such as an engine start message
  • Physical damage to a vehicle
Attack Model

- Single-band Relay Attack [*]
  - Manipulate LF band signal only
  - Wired / Wireless Attack

[*] Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars (Aurelien Francillon et al.)
Attack Model

- Dual-band Relay Attack (1. Amplification Attack)
  - Receives LF band signal and forward to the adversary at the key fob side
  - Injects LF band signal to the key fob
  - Amplifies UHF band signal and injects to the vehicle
Attack Model

- Dual-band Relay Attack (Ⅱ. Digital Relay Attack) [*]
  - Demodulate LF/UHF band signal
  - Relay binary information

[*] Car keyless entry system attack (Yingtao Zeng et al.)
Attack Model

• Cryptographic Attack [*]
  • Single adversary
  • Injects LF band signals to the key fob
  • Records valid responses and extract secret key
  • Exploits weaknesses of cryptographic algorithm

[*] Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars (Wouters et al.)
Outline

• Introduction / Background

• Attack Model

• Our Method

• Evaluation

• Discussion

• Conclusion
Our Method

• Overview (HODOR)

Phase I. Training

• Legitimate Signal Set
• Pre-processing
• Feature Extraction
• Generating Classifier
• Normalization Parameter Calculation (NPC)

Phase II. Attack Detection

• Pre-processing
• Feature Extraction
• Classifier
• Normalized Output

Newly Received Signal

Verify

Yes

No

Alarm

< Γ

16
Our Method

• Preprocessing

\[ c(t) \xrightarrow{\text{Band-Pass filter}} s[t] \xrightarrow{\text{Demodulator}} d[t] \xrightarrow{\text{RMS Normalization}} d_{RMS}[t] \]

• Feature Extraction

\[ d_{RMS}[t] \xrightarrow{\text{Bit Time}} f_{\text{peak}} \]

\[ \text{FFT} \]

\[ f \]

\[ A \]
Our Method

• Feature Extraction (Continue)

\[ d_{RMS}[t] \]

\[ s[t] \]

\[ SNR_{dB} \]

Kurtosis

Spectral Brightness

Carrier Frequency offset

Energy in high frequency band

Ideal Carrier Frequency
(i.e. 433MHz)

Actual Carrier Frequency
Our Method

• Training
  • Semi-supervised learning
    • Only requires legitimate data
    • Covers unknown attacks
    • OC-SVM, k-NN

Legitimate data

90% Training

Classifier

Output

\[ \mu \]

\[ \sigma \]

Normalization Parameter

\[ X10 \]
Our Method

• Attack Detection

Newly Received Signal → Preprocessing → Feature Extraction → Classifier → Normalization

Training Phase

μ, σ

{\text{\textit{f}_{\text{peak}}, SNR_{dB}, Kurtosis, Spectral Brightness, Carrier Frequency Offset}}

< \Gamma?

No

Yes

No
Outline

• Introduction / Background
• Attack Model
• Our Method
• Evaluation
• Discussion
• Conclusion
Evaluation

• Experimental Setup
  • Cars: KIA Soul, Volkswagen Tiguan
  • SDRs: HackRF One, USRP X310
  • SW: GNURadio
  • Loop Antenna, SMA Cable (Relay LF band signal)
Evaluation

• Selected Classification Algorithms
  • One-Class SVM (OC-SVM) with Radial Basis Function (RBF) kernel
  • k-NN with Standardized Euclidean Distance
  • MatLab implementation

• Performance Metric
  • Assume False Negative Rate (FNR) as 0%
  • Calculate False Positive Rate (FPR)
Evaluation

• Single-Band Relay Attack Detection

Experimental Setup
(LF band signal relay)

Results
(0% FPR in both algorithms)
Evaluation

- Dual-Band Relay Attack Detection
- Amplification Attack

Experimental Setup
(UHF band amplification)

Results
0% FPR in both algorithms

$k$-NN

$\Gamma_{PKES} = 4$

SVM

$\Gamma_{PKES} = 5$
Evaluation

- Dual-Band Relay Attack Detection
- Digital Relay/Cryptographic Attack

Experimental Setup
(Cryptographic Attack)

Results
(Average FPR k-NN: 0.65%, SVM:0.27%)

\(\Gamma_{PKES} = 4\)
Evaluation

• Environmental Factors

  • Non-Line of Sight (NLoS) conditions, Dynamic Channel Conditions

Backpack: FPR k-NN: 1.32%, SVM: 1.35%
Pocket: FPR k-NN: 1.71%, SVM: 1.67%
Underground: FPR k-NN: 5%, SVM: 4%
Roadside: FPR k-NN: 2%, SVM: 3%
Evaluation

• Environmental Factors
  • Signals from RKE system

Average FPR $k$-NN: 6.36%, SVM:0.65%
Average FPR $k$-NN: 0%, SVM:0%
Evaluation

- Execution time
  - Implementation on Raspberry Pi
    - 1.4Ghz Core, 1G RAM
  - Python Code

<table>
<thead>
<tr>
<th>Phase</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>k-NN</td>
</tr>
<tr>
<td>Feature</td>
<td>$f_{\text{peak}}$</td>
</tr>
<tr>
<td></td>
<td>$f_{\text{offset}}$</td>
</tr>
<tr>
<td>Extraction</td>
<td>$\text{SNR}_{\text{dB}}$</td>
</tr>
<tr>
<td>(FSK / ASK)</td>
<td>$\text{Kurtosis}$</td>
</tr>
<tr>
<td></td>
<td>$\text{Spec. Brightness}$</td>
</tr>
<tr>
<td>Attack Detection</td>
<td>$C_{PKES}$</td>
</tr>
<tr>
<td>(FSK / ASK)</td>
<td>$C_{RKE}$</td>
</tr>
</tbody>
</table>

Total Execution Time

K-NN: 163.8ms and SVM: 159.038ms
Evaluation

- Feature Importance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>SNR</td>
<td>Kurtosis</td>
<td>$f_{peak}$</td>
<td>Spec. Brightness</td>
</tr>
<tr>
<td>2</td>
<td>Kurtosis</td>
<td>SNR</td>
<td>Kurtosis</td>
<td>Kurtosis</td>
</tr>
<tr>
<td>4</td>
<td>$f_{peak}$</td>
<td>$f_{peak}$</td>
<td>SNR</td>
<td>SNR</td>
</tr>
</tbody>
</table>
Outline

• Introduction / Background
• Attack Model
• Our Method
• Evaluation
• Discussion
• Conclusion
Discussions

• **HODOR and Security**
  - Threshold is a trade-off parameter in HODOR
  - Small threshold leads to the false alarm; a large threshold leads to the false-negative (attack success)

• **Feature Impersonation**
  - Adversary must impersonate the whole feature at the same time
  - Impersonating a specific feature leads to a distortion in other features

• **Practicality**
  - Develop additional features and algorithms that properly operate even in extreme environments
Future Work

• Robustness
  • Comprehensive experiments against feature variations
    • IEC certified facilities (Temperature, Humidity, Impact)
  • Incremental/ Decremental learning
    • Cope with a feature variation (a.k.a Concept drift)

• Scalability
  • Feature collision
  • Defense against strong attacker equipped with signal-generator

• Performance optimization
  • Low sample rate, memory usage
Conclusion

• Proposed a sub-authentication system
  • Supports manufacturer-installed support systems to prevent keyless entry system car theft

• Effectively detect simulated attacks that are defined in our attack model
  • Reducing the number of erroneous detection occurrences (i.e., false alarms)

• Found a set of suitable features in a number of environmental conditions
  • Temperature variation, battery aging, and NLoS conditions
HODOR! (Thank you!)

Q&A

This work was supported by Samsung Electronics
Appendix

• Remote Keyless Entry System
  • Unidirectional
  • UHF band (433MHz, 868MHz)
    • ~100 meter communication range
  • FSK or ASK Modulation
  • Shared cryptographic key between the key and the car

![Diagram showing the process of unlocking a vehicle using a key fob](image_url)
Appendix

• Playback Attack Detection

Experimental Results

(SDR with 5MS/s)

Experimental Results

(USRP with various sample rate)