Hardware security multidimensional attack and defense tool set

Jie Fu
Kunzhe Chai
Mingchuang Qin
From—360 Hacker Research Institute, 360 Security Technology
Abstract

• Hardware attack and defense tools.

• Master and implement a variety of hardware attack methods.

• Includes ultrasonic attacks, RFID attacks, power side channel attacks, and radio defense etc.

• Design idea, design concept
High frequency card reader and high frequency simulator

- proxmark3
- ChameleonMini
- HackNFC — designed by 360 Unicornteam
HACKNFC

- Man in the NFC
- Chip — PN7462
- Protocol—14443A
- NRF24L01
Open source

- Arduino programming design

- Simple, Practical

- Github:

Each function module will be made into Arduino library functions

PN7462 Controller Development Kit
OM27462CDK

PN7462 is the first all-in-one full NFC controller solution.

PN7462/CDK contains:

- PN7462/AM2 with standard 50x50mm antenna
- 2D-RFID antenna with matching configuration
- 2x100K ohm for individual antenna matching
- NFC sample card and tags
- 2 USB cables (power and data)
- PC/RFID card reader
- Quick start guide
- OM27462 NFC cards and debug adapter
- 10 PN7462 samples
- TVS power supply

This kit is part of an extensive product support package. It demonstrates all functionalities of the PN7462 family and enables the development of custom NFC applications as well as the antenna design.

All documentation, video tutorials, and software libraries can be downloaded from the product page.

www.nxp.com/products/PN7462CDK

PN7462 Controller Development Kit
OM27462CDK Quick Start Guide

1. Setting up the development board

The PN7462/AM2 Quick Start Guide contains information on:

- How to connect the development board
- How to use the PN7462/AM2 with an Xben Express environment
- How to receive various projects and examples in the development environment

2. Executing software examples

A collection of software examples shows how to implement the NFC contactless interface for the PN7462 family:

- PC RFID reader: working with NFC/CT and USB
- LM1070/PN7462 PC/RFID Reader User Manual
- NFC reader: working with NFC/CT and USB, with or without a SAP
- LM1070/77 PN7462 Door Access User Manual

3. Custom development

The LM1070/77 PN7462 Software User Manual describes the software architecture and all components to successfully create fully customised projects.

For additional information please visit: www.nxp.com/demosboard/OM27462CDK
ChameleonMini — how to emulate a mifare card
ChameleonMini

- Arduino programming design
- Simple, Practical

Each function module will be made into Arduino library functions
Why there is an error in the original SCH?

- Hardware Bug?
- Parameter adjustment
- The values in yellow are wrong
How to design a NFC hack tool?

- How to design more concealed
- How to get a long distance
- What features do you want
How to achieve a long reading distance?

- PN532
- Demodulation circuit
How to achieve a long reading distance?

- MFRC522
- Demodulation circuit
How to achieve a long reading distance?

• Chip — CLRC663
• General method
• Current monitoring
How to achieve a long reading distance?

- **Current monitoring**: 70mA - 100mA
How to achieve a long reading distance?

- Chip — CLRC663
- General method
- Current monitoring
- Optimize parameters
How to achieve a long reading distance?

- Remain L0, C0; Change C1, C2
- Antenna value 1uH - 2uH
Simple Arduino Reader
How to make the tool by yourself?

- Electronic circuit design software —— EAGLE, Altium Designer
NFC defender and 125Khz defender

- How to block NFC communication
NFC defender and 125KHz defender

- Detect and protect
NFC defender and 125KHz defender

- Detect and protect
NFC defender and 125KHz defender

- Detect and protect
Ultrasound attacks smart hardware

- What could voice do?
Ultrasound attacks smart hardware

• An electronic device with adjustable frequency of sound wave
Ultrasound attacks smart hardware

- Physical resonance
- An electronic device with adjustable frequency of sound wave
- Be patient — Looking for the frequency of resonance
Ultrasound attacks smart hardware

- Simplified — No Amplifier
- Speaker — Characteristic
- Microprocessor control
Hardware Power glitch attack

- Power fluctuation
- Clock disorder, program to run error
- Program bypass, decryption
Hardware Power glitch attack

- Power fluctuation
- Clock disorder, program to run error
- Program bypass, decryption
Ultra strong electromagnetic field circuit system breaker

• To attack a circuit system, such as an access control system, and do...
Ultra strong electromagnetic field circuit system breaker

To attack a circuit system, such as an access control system, and open the
Ultra strong electromagnetic field circuit system breaker
Ultra strong electromagnetic field circuit system breaker

How to make artificial lightning?
Make amazing artificial lightning
Hacker Research Institute

Thanks! && Any questions?

zhujiu1234@gmail.com