Popping a Smart Gun

plore@tuta.io

DEF CON 25
What is a smart gun?
Why I care
Armatix iP1: watch and pistol
Normal operation

1. *squeeze*

2. Hey!

3. Here’s a token

4. “Good, now I can fire”

25 cm
(Demo of normal operation)
Motivation: a good challenge

Forum post on Armatix iP1 review, November 2015:

Could you imagine what the guys at Defcon could do with this POS?
So... let’s pop it three ways!

- Defeat proximity restriction
- Denial of service
- Fire without authorization
Normal range

5.35 kHz

916.5 MHz

25 cm
5.35 kHz burst
Relay devices (custom hardware)

nRF24
2.4 GHz xcvr

5.35 kHz
BPF & amp

5.35 kHz
tuned coil

Pistol side

Watch side

PIC16F MCU

Coil driver
Relay devices (custom hardware)

• Cost (each):
  – $5 nRF24 module
  – $2 PCB
  – $1 microcontroller
  – $2 other parts

Total cost: $20
(Demo of relay attack)
Latency of relay

Pistol NFC start

Slave NFC start

630 us overall latency
Relay defense

• Enforce *very* tight timing requirements
• Don’t use RF/NFC at all for proximity
• This is a difficult problem
  – Applicable to many products/industries
Denial of service

• Scenario 1:
  – Adversary wants to prevent gun from being fired by authorized user

• Scenario 2:
  – Parent wants backup kill-switch in house in case gun not locked up properly

• Scenario 3:
  – Other device unintentionally interferes
RF weaknesses

5.35 kHz

916.5 MHz
Not necessarily intentional

• 900 MHz ISM band used by many products
  – Baby monitors
  – Wireless microphones
  – Wireless video game controllers
  – Wireless headphones
  – Utility telemetry systems
  – Cordless phones

• EMC testing *should* catch these problems
900 MHz transceiver

The TR1000 hybrid transceiver is ideal for short-range wireless data applications where robust operation, small size, low power consumption and low cost are required. The TR1000 employs Murata’s amplifier-sequenced hybrid (ASH) architecture to achieve this unique blend of characteristics. All critical RF functions are contained in the hybrid, simplifying and speeding design-in. The receiver section of the TR1000 is sensitive and stable. A wide dynamic range log detector, in combination with digital AGC and a compound data slicer, provide robust performance in the presence of on-channel interference or noise. Two stages of SAW filtering provide excellent receiver out-of-band rejection. The transmitter includes provisions for both on-off keyed (OOK) and amplitude-shift keyed (ASK) modulation. The transmitter employs SAW filtering to suppress output harmonics, facilitating compliance with FCC 15.249 and similar regulations.

### Absolute Maximum Ratings

<table>
<thead>
<tr>
<th>Rating</th>
<th>Value</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply and All Input/Output Pins</td>
<td>-0.3 to +4.0</td>
<td>V</td>
</tr>
</tbody>
</table>
Slicer and Manchester coding
Watch auth token to pistol

Sync
Constant data
Dynamic data
Constant data
Dynamic data
Checksum
Test signal

33 us active

300 us inactive
Test signal over watch signal
Scenario 1: Interference > Signal

Slicer level set based on interference peaks

Slicer level too high

No signal bits recovered

= interfering signal

= watch signal
Scenario 2: Interference $\approx$ Signal

Interference fills gaps in signal

- No edges where there should be edges
- Manchester decoding fails

= interfering signal

= watch signal
Scenario 3: Interference < Signal

Interference appears before byte start

.: Byte sync incorrect
.: Byte decode fails

= interfering signal
= watch signal
Custom test transmitter

Transceiver (Murata TR1000)

MCU (PIC16F18313)

Antenna (Linx 916-SP2)

(Yes, I know that through-hole components usually go on the other side of a stripboard like this)
Effective range

916.5 MHz

3+ m
(Demo of denial of service)
DOS defense

• Use more transmitter power
• Use error-correcting codes
• Use more-robust modulation
Unlocking mechanism

- Firing pin with blocking lugs
- Pin blocker
- Channel for pin to be unblocked
- Cam
- Trigger
- MCU
- Electromagnet
- Ferrous material

(Looking longitudinally)
Trigger partially pulled

(Firing pin closer to being unblocked)

(Cam moves up)

(Trigger partially pulled, presses on cam)

(Looking longitudinally)

MCU
Scenario 1: Firing NOT authorized

Electromagnet NOT active

MCU

Firing pin remains blocked; Gun cannot fire

(Looking longitudinally)
Scenario 2: Firing authorized

Electromagnet rotates pin block remainder of distance

Firing pin matches hole; Pin is unblocked; Gun can fire

(Looking longitudinally)
Mechanism in frame

Top view of pistol frame

Electromagnet
Mechanism in slide

Profile view of slide

Bottom view of slide

Ferrous material

Cam presses here
Magnet attack

External magnet pulls ferrous material;
Pin unblocked;
Gun can fire

(Looking longitudinally)
Magnets

- N52 neodymium magnets
- 32 mm × 5 mm
- $19 on Amazon for a four-pack (only three are required)
- Cost
  - $14.25 magnets
  - $0.20 scrap dowel
  - $0.05 stainless screw
  - Total: ≈$15
Completed magnet tool
Magnet alignment

Align magnet here
Magnets on pistol
(Demo of magnet attack)
Magnet defense

• Don’t use magnets, solenoids, etc.
  – Nothing involving a DC magnetic field
  – Consider motor-driven mechanism

• Detect external magnetic field and activate secondary lock
  – Kind of like a relocker in a safe
Final Thoughts

plore@tuta.io

@_plore
BACKUP SLIDES
What is a smart gun?

• Firearm that can be fired only by an authorized user

• Various authorization techniques
  – Magnetic ring
  – RFID
  – Biometrics (e.g., fingerprint reader)
Smart gun models

• Examples that have been prototyped
  – iGun shotgun (RFID ring)
  – Kloepfer pistol (fingerprint)
  – Magna-Trigger/Magloc retrofit (magnets)
  – Safe Gun retrofit (fingerprint)

• Only one model currently for sale in the US
  – Armatix iP1 (NFC/RF watch)
New Jersey Smart Gun Law

• “New Jersey Childproof Handgun Law”
• Takes effect 3 years after qualifying guns available at retail
• Guns legally sold if and only if they “can only be fired by an authorized or recognized user”
• Owners of gun stores have received threats over plans to sell the Armatix iP1

3 https://www.washingtonpost.com/local/california-smart-gun-store-prompts-furious-backlash/2014/03/06/43432058-a544-11e3-a5fa-55f0c77bf39c_story.html
Armatix iP1

- Custom semi-auto pistol design
- Fires .22 LR cartridge
- Hammer fired
- Introduced ca. 2015
- “Smart” authorization via paired wristwatch
Design overview

• Two system components
  – Pistol
  – Watch
• Watch authorizes pistol to fire
• Watch must be near the pistol (<25 cm)
• Communication
  – Pistol → watch: 5.35 kHz inductive
  – Pistol ↔ watch: 916.5 MHz
Armatix iP1 operation

1. Enter PIN on watch
2. Wear watch within 25 cm of pistol
3. Squeeze grip on pistol
4. Fire pistol
Armatix iP1: pistol field strip
Size comparison

Glock 17      Armatix iP1      Ruger SR22
Design internals

• MSP430 microcontroller
• Murata TR1000
  – 916.5 MHz transceiver
  – OOK modulation
• Ferrite-core coil for NFC
• FCC equipment cert database is amazing
  – Interior photos, EMC test results, etc.
Unlock sequence

- Pistol sends 5.35 kHz CW chirp for 1.5 ms
  - No data; just carrier
  - Range of about 25 cm
- Watch receives chirp and sends unlock response on 916.5 MHz
- Pistol ACKs 100 ms later on 916.5 MHz
- If watch sent correct code, pistol enables firing
- Watch retries once after 400 ms if no ACK
- LED on pistol grip
  - Green = auth token, can fire
  - Red = no token, cannot fire
Operation overview

• Pair watch and pistol
  – Long PIN to do this (only needed once)

• Sync watch and pistol
  – Auth tokens are time-dependent
  – Clock drifts badly, so need to do this often

• Enable firing on watch
  – 5-digit PIN (4 values per digit; 1024 possibilities)
  – Activates watch for 2-8 hours (selectable)

• Squeeze pistol backstrap

• Pistol sends 5.35 kHz chirp to watch

• Watch sends auth code to pistol via RF

• Pistol enables firing by unblocking firing pin
Watch/pistol comms

- OOK, Manchester coding
- 30 kbit/s raw, 2 kbytes/s net
- 8-bit checksum
- 8 data bits plus one start bit
  - Least-significant bit first
- 19-byte frame from watch to pistol
- 13-byte frame from pistol to watch
Watch and Pistol on 916.5 MHz

Watch sends token

Pistol ACKs token

100 ms
Pistol reply to watch

Sync

Constant data

Battery level

Checksum
Watch and pistol on spectrum analyzer

-40 dBm

0 Hz span – 100 ms/div
How to defeat proximity

• Relay 5.35 kHz burst
  – First device:
    • Listen for 5.35 kHz chirp
    • Send indication that chirp occurred over backhaul
  – Second device:
    • Listen for trigger on backhaul about chirp
    • Generate 5.35 kHz chirp near watch
    • Watch thinks it’s hearing from pistol, sends auth token at 916.5 MHz

• 916.5 MHz reply strong enough for at least 3 m
  – TX power from watch roughly -20 dBm
  – Could be similarly proxied over backhaul for limitless range
Defeat proximity restriction

• Watch normally needs to be <25 cm from the pistol
• We want to fire the pistol when separated from the watch by more distance
• Distance limited by physics of 5.35 kHz near-field coupling
  – The 916.5 MHz signal goes much farther
Proximity-defeat results

• Works reliably to at least 3 m
  – 12x range improvement

• Limit now is 916.5 MHz radio link
  – Could work arbitrarily far with a 916.5 MHz relay

• Relay adds about 630 us latency
  – System tolerates it
Proximity-defeat HW

• Custom hardware, pulse listener:
  – Tuned coil placed near pistol
  – 5.35 kHz bandpass filter/amplifier
  – Microcontroller (PIC16F) sampling and watching for burst from pistol
  – 2.4 GHz transmitter (nRF24) to trigger generator

• Custom hardware, pulse generator:
  – Tuned coil placed near watch
  – Microcontroller generating 5.35 kHz chirp
  – Simple Class C amp driving coil (MOSFET connected to GPIO)
  – 2.4 GHz receiver to receive trigger signal
Latency of relay

400 us latency due to radio, SPI, etc

Radio TX start

Slave NFC start
Latency of relay

630 us overall latency

Pistol NFC start

Slave NFC start
How sensitive to interference?

• OOK modulation is highly susceptible to interference
  – 916.5 MHz module datasheet used in iP1 warns that slicer will be “blinded” by strong noise pulses
  – Slicer will also be fooled by lone pulses in bit timeslot that are less than 6 dB down from the normal bit peaks
• Signal from watch measured at -40 dBm @ 10 cm
  – Typical distance between pistol and watch
  – Implies actual TX power of about -20 dBm
• Ballpark: interference signal at least -50 dBm at pistol will prevent reception of signal from watch
  – ...even when pistol is very close to watch

Not necessarily intentional

• 900 MHz ISM band used by many products
  – Baby monitors
  – Wireless microphones
  – Wireless video game controllers
  – Wireless headphones
  – Utility telemetry systems
  – Cordless phones
• EMC testing *should* catch these problems
Theory

• Constant carrier has effect only up to about 1 m
• Why pulsed carrier?
  – Short range: our pulse is stronger than normal pulses, so slicer level is set too high
  – Mid range: our pulse about the same strength as normal pulses, so bit interference high (edges missing, so bits can’t be decoded)
  – Long range: our pulse comes before packet/byte sync, prevents packet/byte sync, corrupting packet
5.35 kHz NFC

• Very sensitive to false signals
  • Will respond to other bursts when source close
  • But...

• Short range
  – Inductive coupling
  – Low power, low receiver sensitivity

• Limited impact
  – False signal simply causes another token to be issued by the watch
916.5 MHz RF

• Also very susceptible
• Transmitting a 916.5 MHz pulsed signal
  – Corrupts data from watch
  – Prevents pistol from getting auth token
    • Pistol cannot fire without auth token
• We’re basically doing EMC testing
  – Not necessarily intentional interference
  – Don’t call it jamming
Unmodulated carrier spectrum
Modulated transmitter spectrum
Transmitter over watch signal
Transmitter stepping on watch signal

Transmitter pulses

Normal watch pulses
Results

• Gun does not fire while transmitter is active
  – 100% effective up to 3 m
  – Some effect even up to 10 m depending on pistol orientation
  – Higher TX power would increase range
• For these tests, watch was on wrist of non-shooting hand (about 10 cm from pistol)
Scenario 2: Firing IS authorized

Electromagnet active; pulls on ferrous material

(Looking longitudinally)
Electronic attack

• Impersonate watch?
• Replay attack?
  – Perhaps including forcing pistol/watch time to specific moment
• Some other exploit?
• Investigated, but then...
Mechanical operation

• Hammer always falls
• Firing pin blocked unless authorized
• If authorized, electromagnet is energized as long as backstrap remains pulled
• Half-pull of trigger moves cam in receiver that moves linkage in slide
  – Partially unblocks firing pin
• The half-pull moves a ferrous material within range of the electromagnet
  – Electromagnet pulls linkage the remainder of the way, unblocking the firing pin
Mechanical attack

• Use a Big-Ass™ Magnet
• Put the magnet next to the pistol so that it will fill in for the electromagnet
• Needs to be strong, but not *too* strong
  – Too strong will stop everything from moving
• A stack of three 1.25” diameter, 0.2” height N52 neodymium magnets works well
Magnet attack in package

You can do this without even taking the magnets out of their retail packaging

Magnet axis at angle relative to grip
Magnet attack in package
Magnet attack in package

Firing pin visible through “loaded chamber” inspection port when dry-fired after successfully bypassed with magnet or authorized normally.
(Firing pin not visible after unauthorized/unbypassed attempt to fire, indicating it was blocked)
Magnet attack results

• Works great!
  – Fire the pistol without the watch
  – Fire the pistol even without any batteries

• Caveats:
  – Magnet can prevent trigger from resetting
  – Occasional issue with light primer strikes
Tools for reverse engineering

• Wealth of information on government sites
  – Patents
    • Detailed drawings and explanations of mechanical design
    • Search not just on company name but also on names of inventors for the company’s principal patents
  – FCC certification database
    • Interior photos
    • RF emissions
    • https://www.fcc.gov/oet/ea/fccid
See also

• “A Review of Gun Safety Technologies” (Greene 2013)
  – Greene gets some details wrong about the iP1
Custom test transmitter BOM

• 916.5 MHz transmitter
  – Murata TR1000 (same module Armatix used)
  – Could have used a similar 916 MHz chip, e.g., SiLabs Si4430 ($5) or the ON Semi AX5243 ($1)

• Antenna
  – Linx ANT-916-SP
  – Could have used a couple short pieces of wire ($0.05)

• Generator for the modulation waveform
  – PIC16F18313 microcontroller ($1)

• Stripboard breadboard ($1)

• Total cost: $5 (optimal component choices) to $20 (as-built)