Popping a Smart Gun

plore@tuta.io

DEF CON 25

PRELIMINARY SLIDES
FINAL DECK AVAILABLE AFTER DEF CON

What is a smart gun?

- Gun that can be fired only by authorized parties
- Various authorization/authentication approaches
  - Biometrics (e.g., fingerprint reader)
  - RFID ring
  - Etc.
- See “A Review of Gun Safety Technologies” for a more thorough discussion (Greene 2013)
  - Greene gets some details wrong about the smart gun we will discuss today

In the movies

Skyfall

Smart guns

- 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)

Why I care

PRELIMINARY SLIDES
FINAL DECK AVAILABLE AFTER DEF CON

Armatix iP1: watch and pistol

Design overview

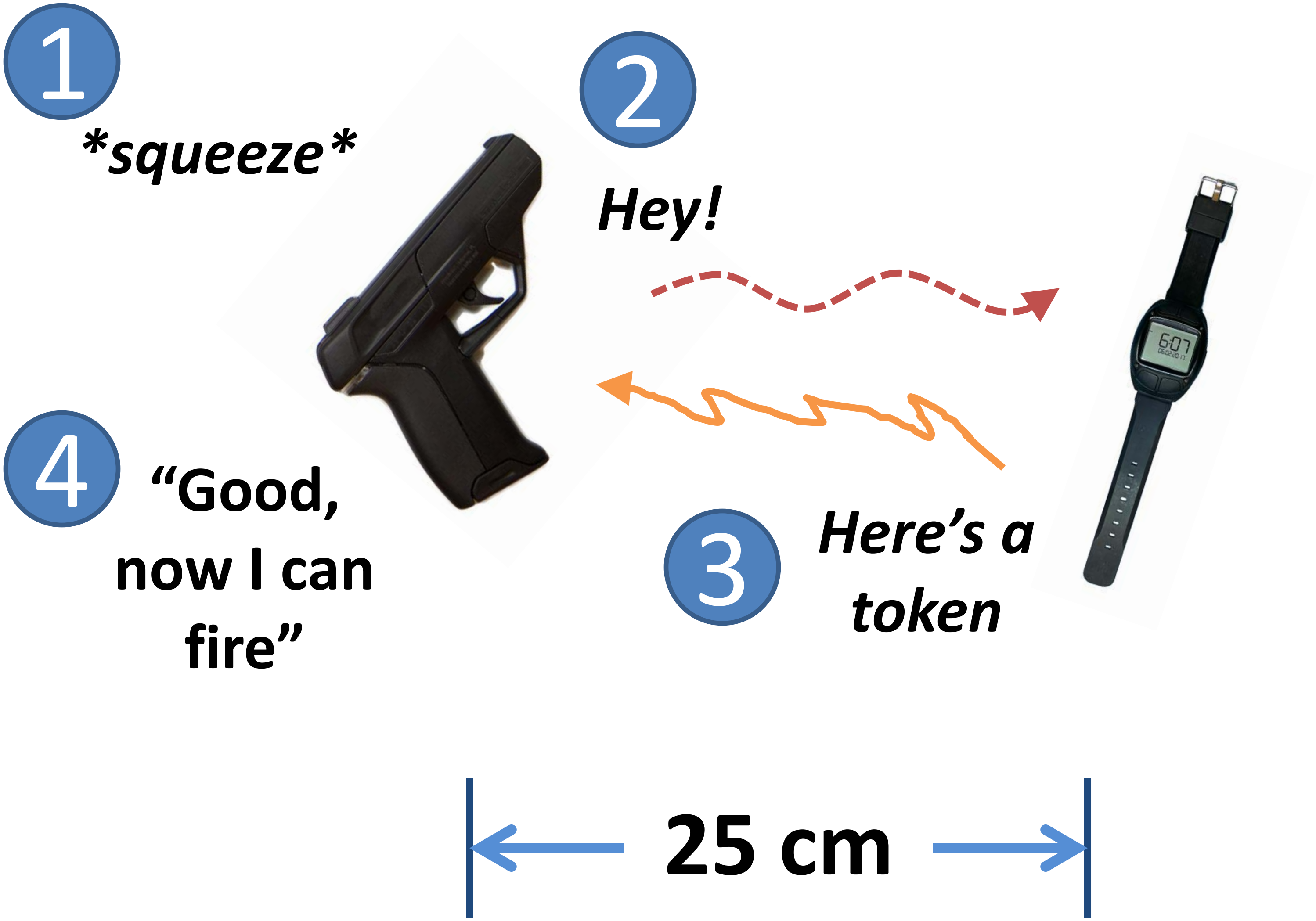
- Two system components
  - Pistol
  - Watch
- Watch authorizes pistol to fire
- Watch must be near the pistol (<25 cm)
- Communication
  - Pistol → watch: 5.35 kHz inductive
  - Pistol ←→ watch: 916.5 MHz

Armatix iP1 operation

1. Enter PIN on watch
2. Wear watch within 25 cm of pistol
3. Squeeze grip on pistol
4. Fire pistol

(Demo of normal operation)

Normal operation



1 *squeeze*

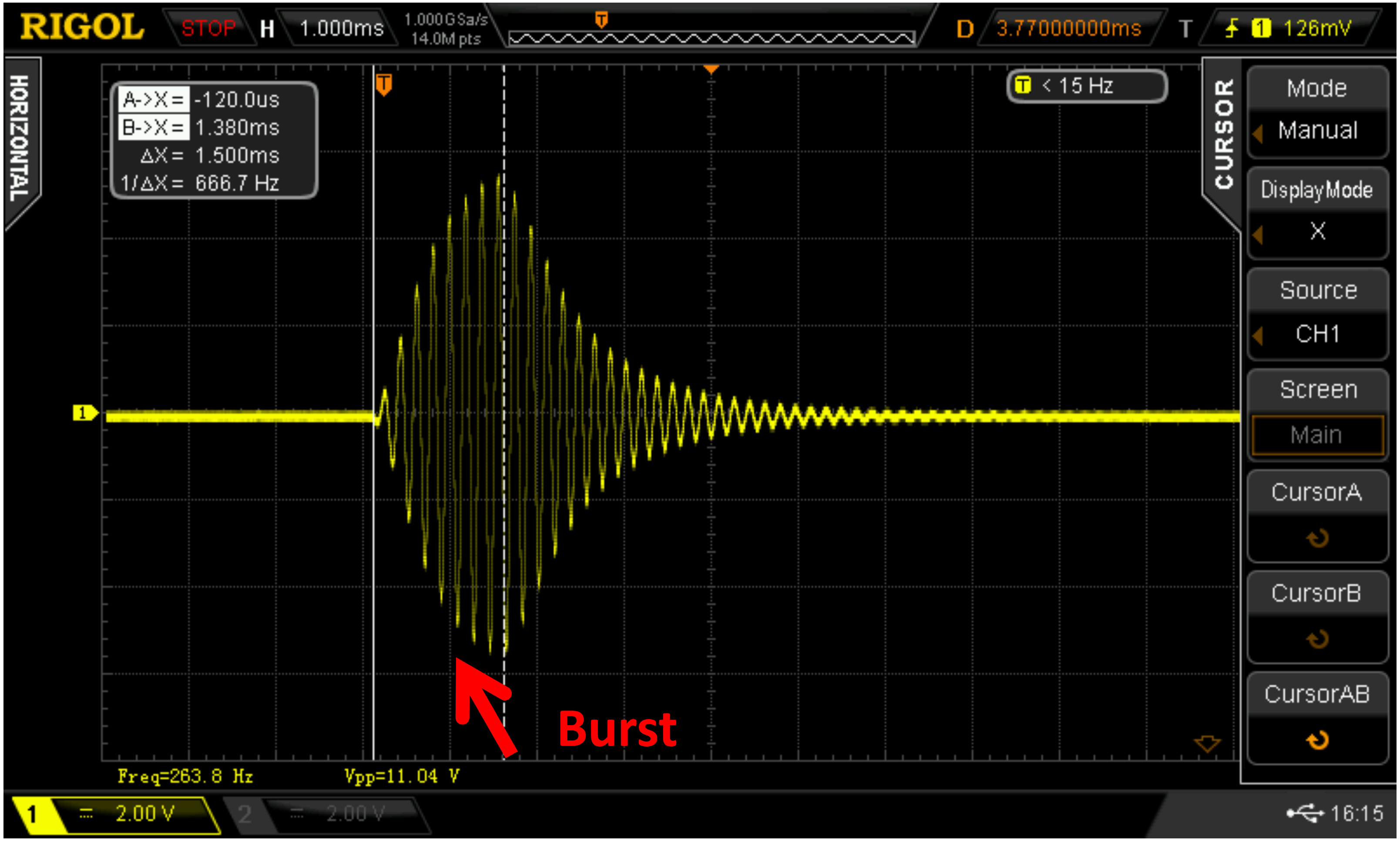
2 Hey!

3 Here’s a token

4 “Good, now I can fire”

25 cm

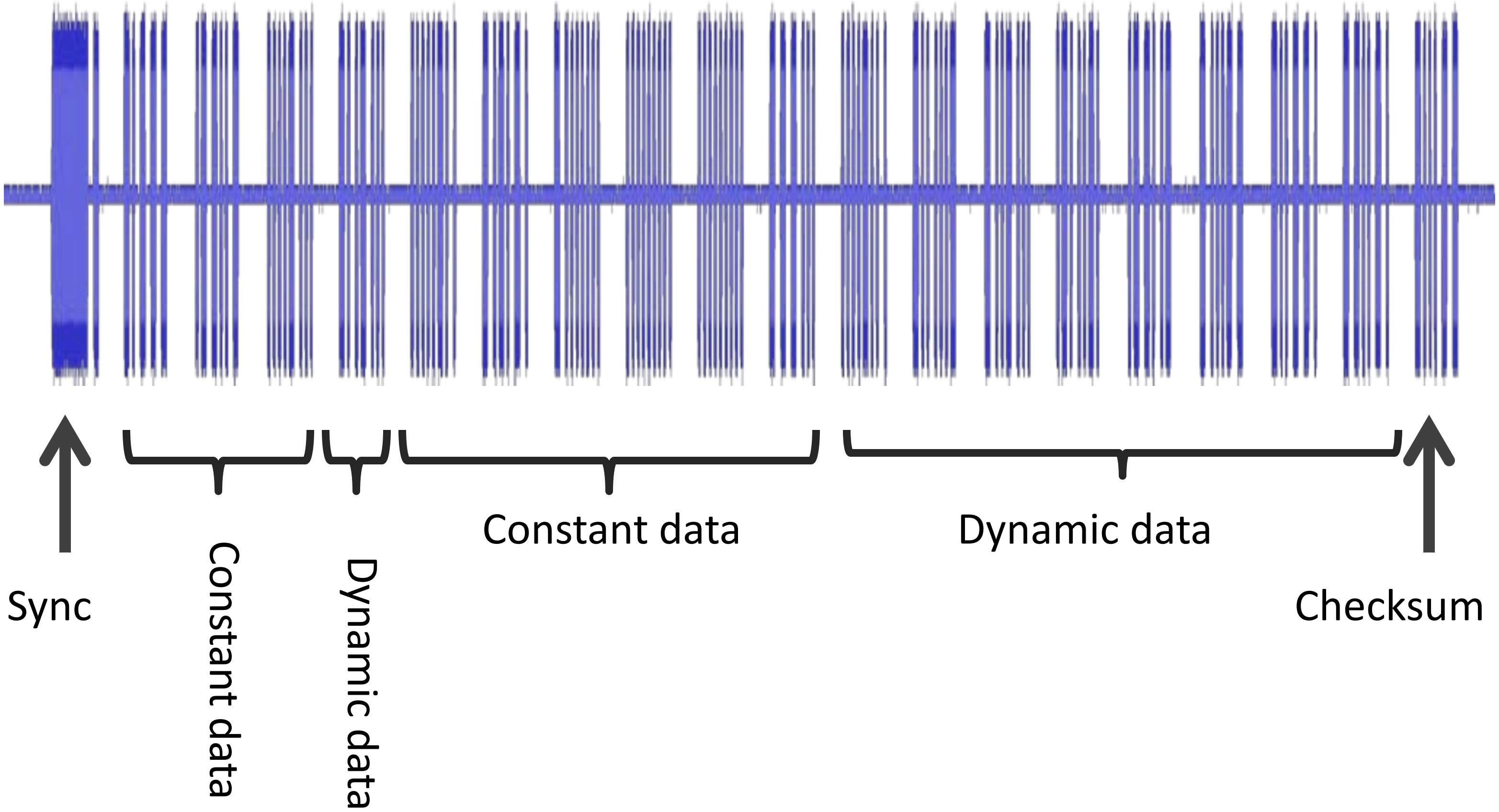
5.35 kHz burst



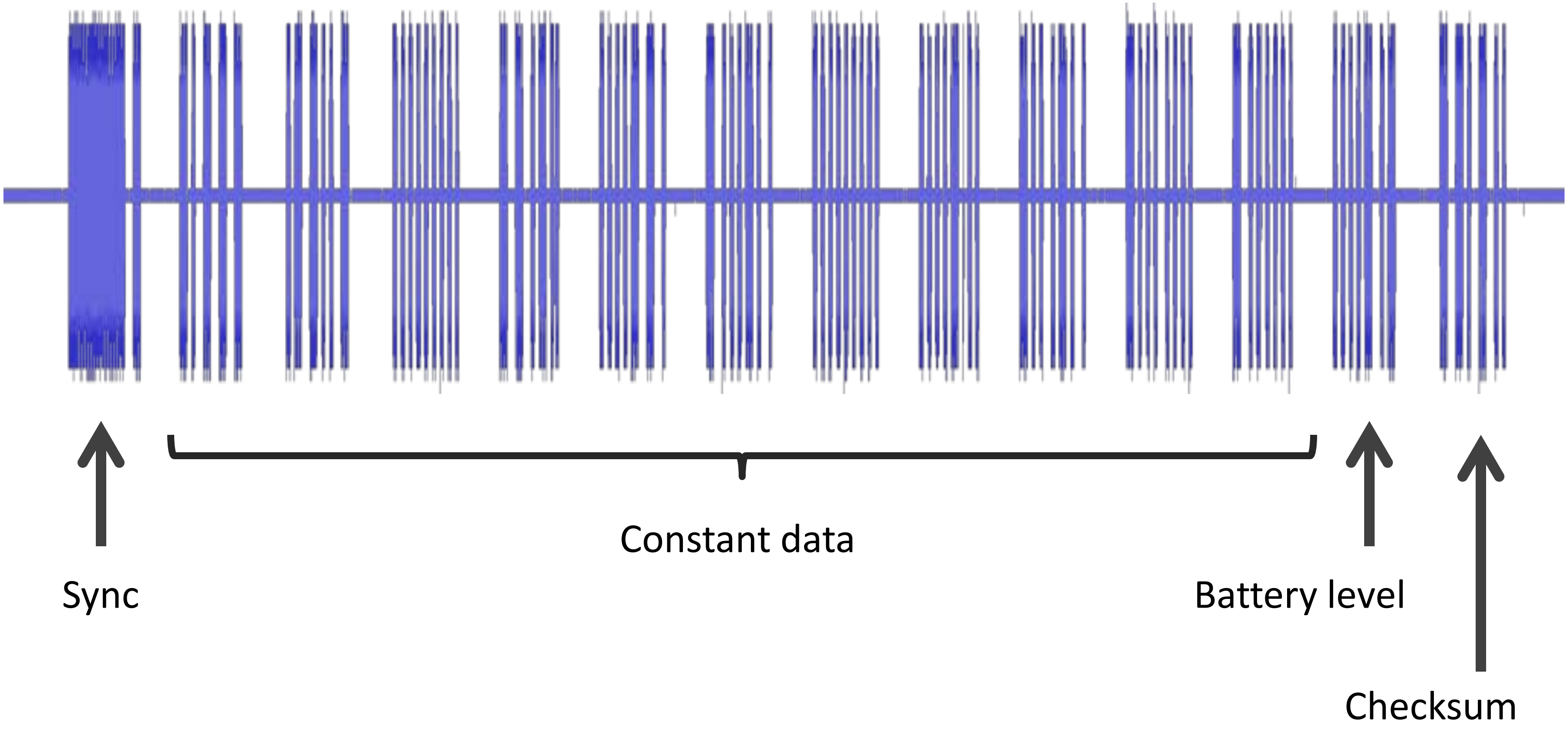
```
H 1.000ms   1.000GSa/s
            14.0M pts
D 3.77000000ms   T 1 126mV

A->X= -120.0us
B->X=  1.380ms
  ΔX=  1.500ms
1/ΔX=  666.7 Hz

T < 15 Hz

Mode: Manual
DisplayMode: X
Source: CH1
Screen: Main

Freq=263.8 Hz        Vpp=11.04 V

1  2.00 V    2  2.00 V                16:15
```

Burst

Watch auth token to pistol



Pistol reply to watch



Sync

Constant data

Battery level

Checksum

So… let’s break it!

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

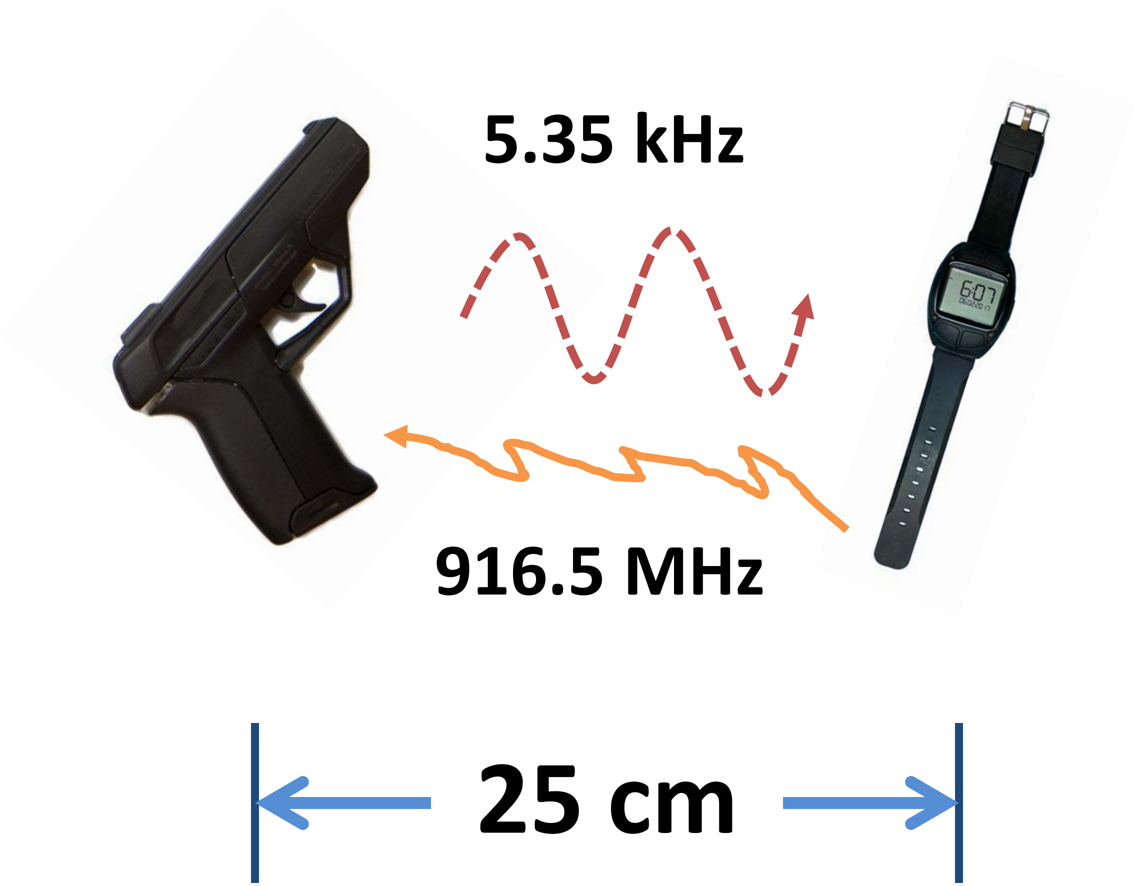
Fire from more than a foot away

DEFEAT PROXIMITY RESTRICTION

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

Normal range

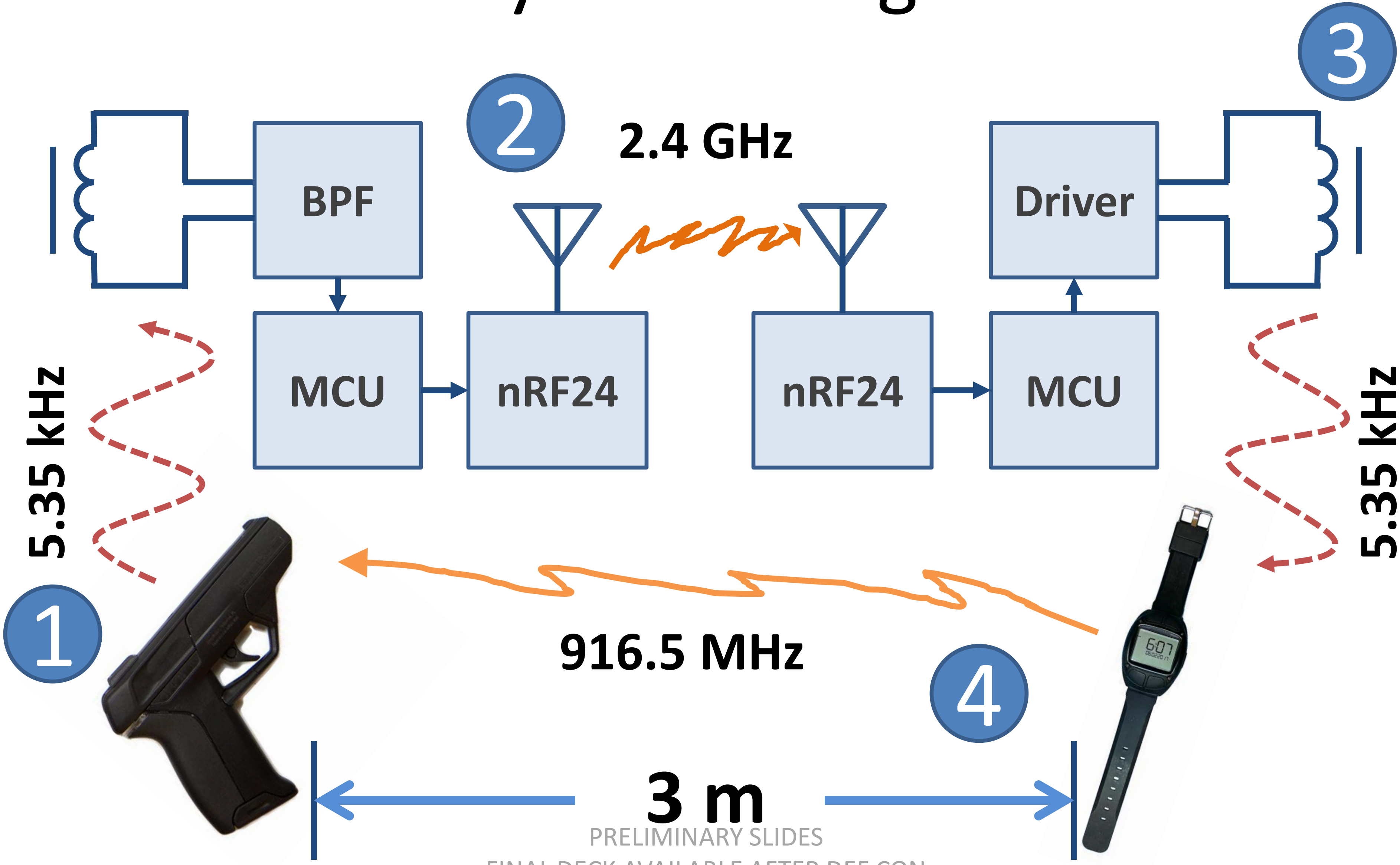


5.35 kHz

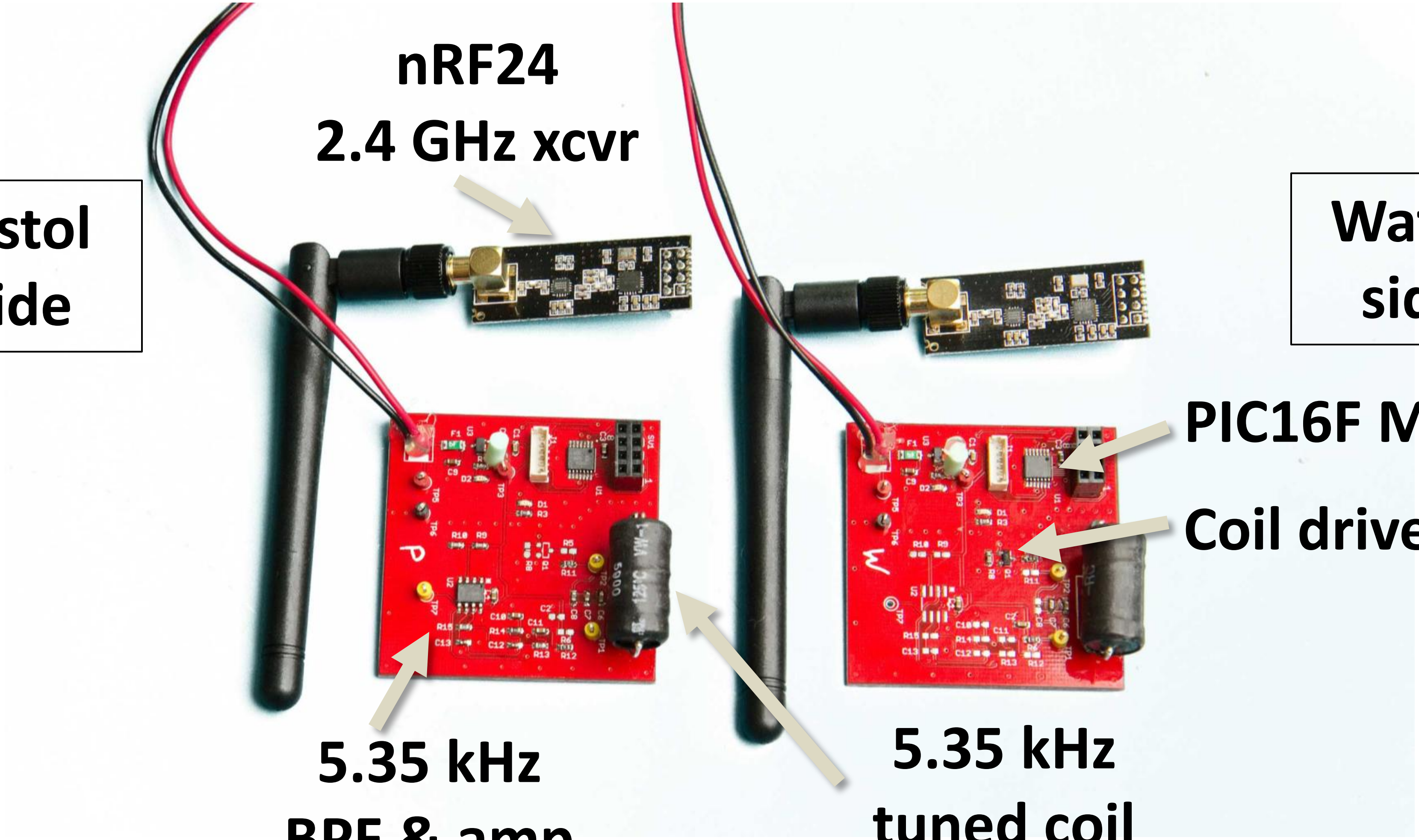
916.5 MHz

25 cm

Relay block diagram



Relay devices (custom hardware)



Pistol side

nRF24
2.4 GHz xcvr

Watch side

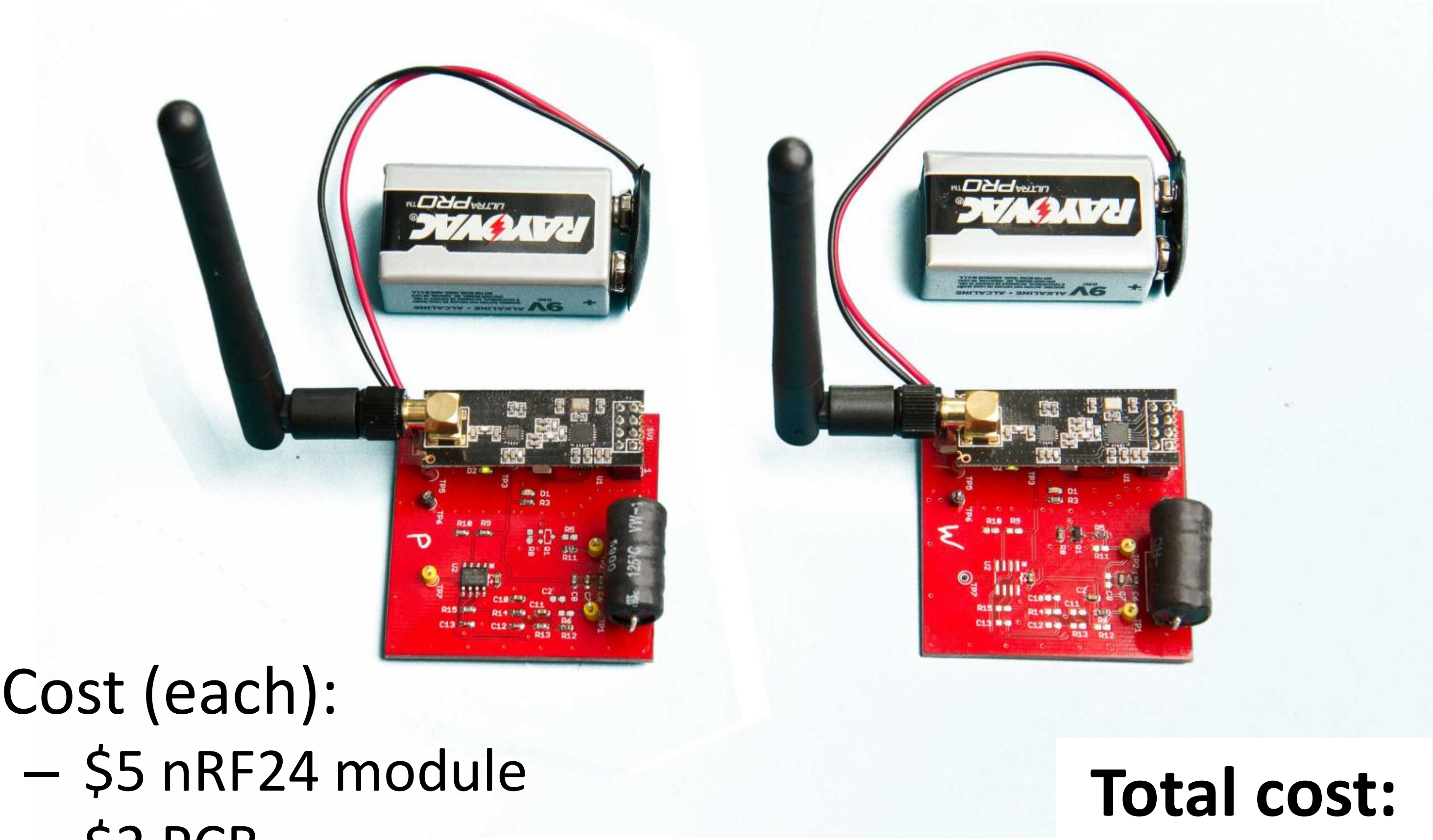
PIC16F MCU

Coil driver

5.35 kHz
BPF & amp

5.35 kHz
tuned coil

Relay devices (custom hardware)



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

Total cost: $20

(Demo of proximity-defeat)

Defense

- This is a difficult problem
  - Applicable to many products/industries
- Enforce very tight timing requirements
- Don’t use RF/NFC at all for proximity

Prevent authorized firing

DENIAL OF SERVICE

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

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

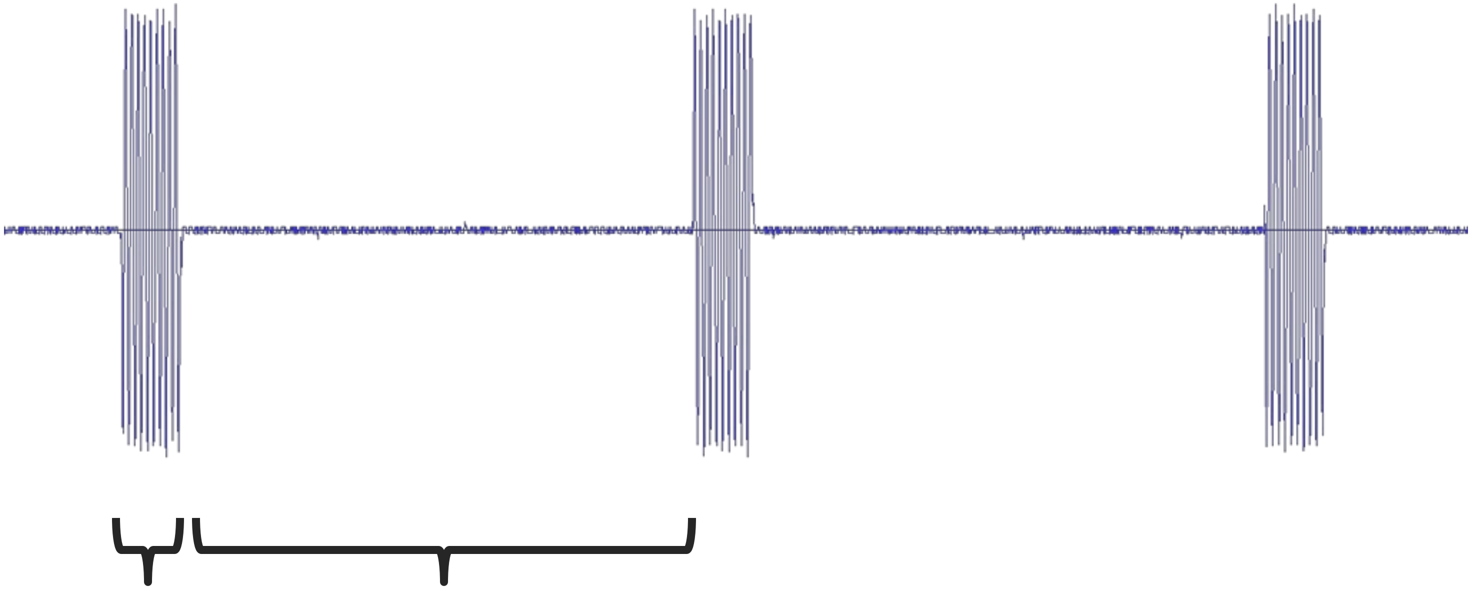
916.5 MHz RF

- 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

Not just intentional

- 900 MHz ISM band used by many products
  - Cordless phones
  - Baby monitors
  - Digital links
- Imagine your gun won’t fire because somebody’s grandmother is blabbing on a cordless phone

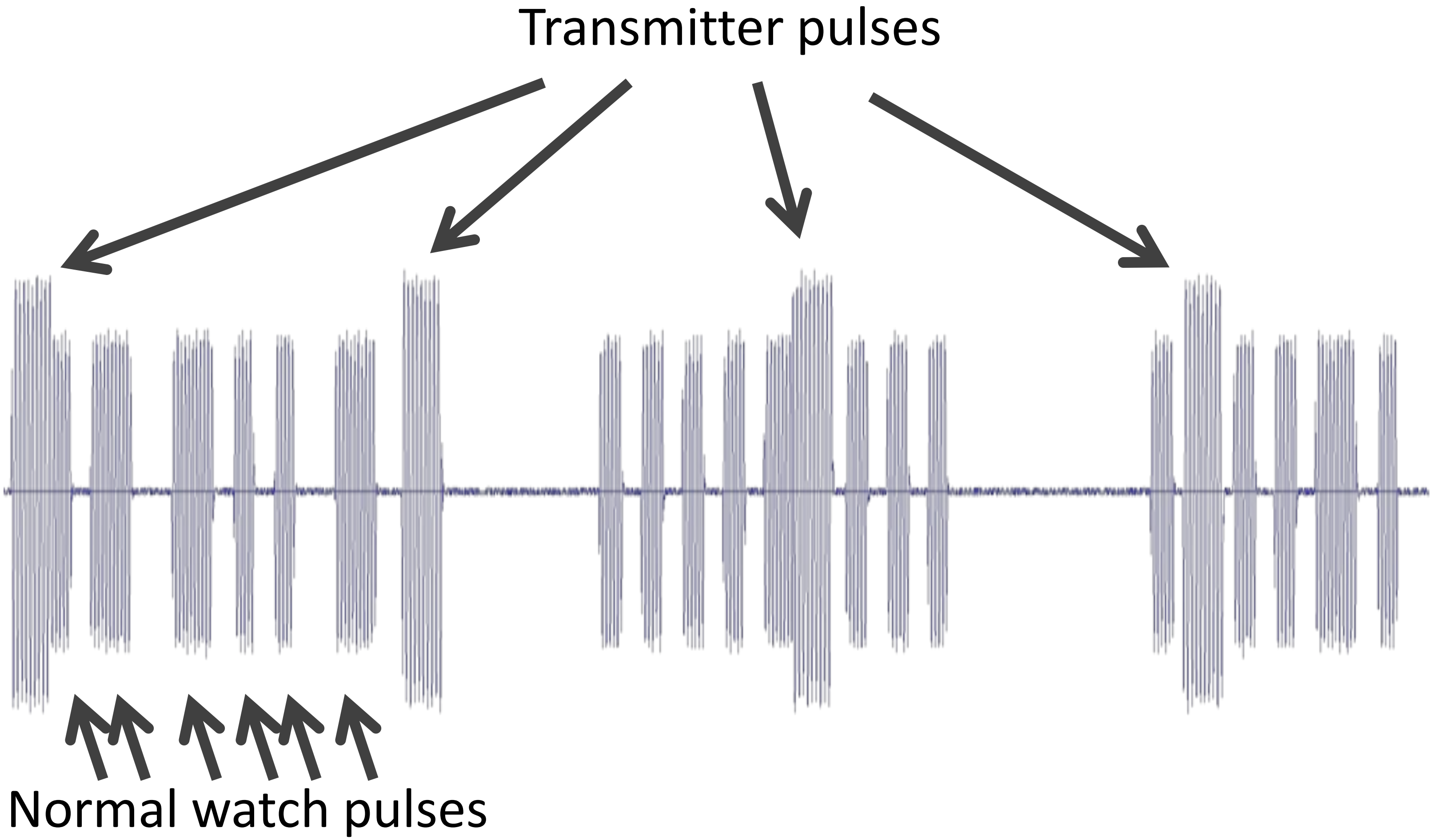
Test transmitter modulation



33 us active

300 us inactive

Transmitter stepping on watch signal

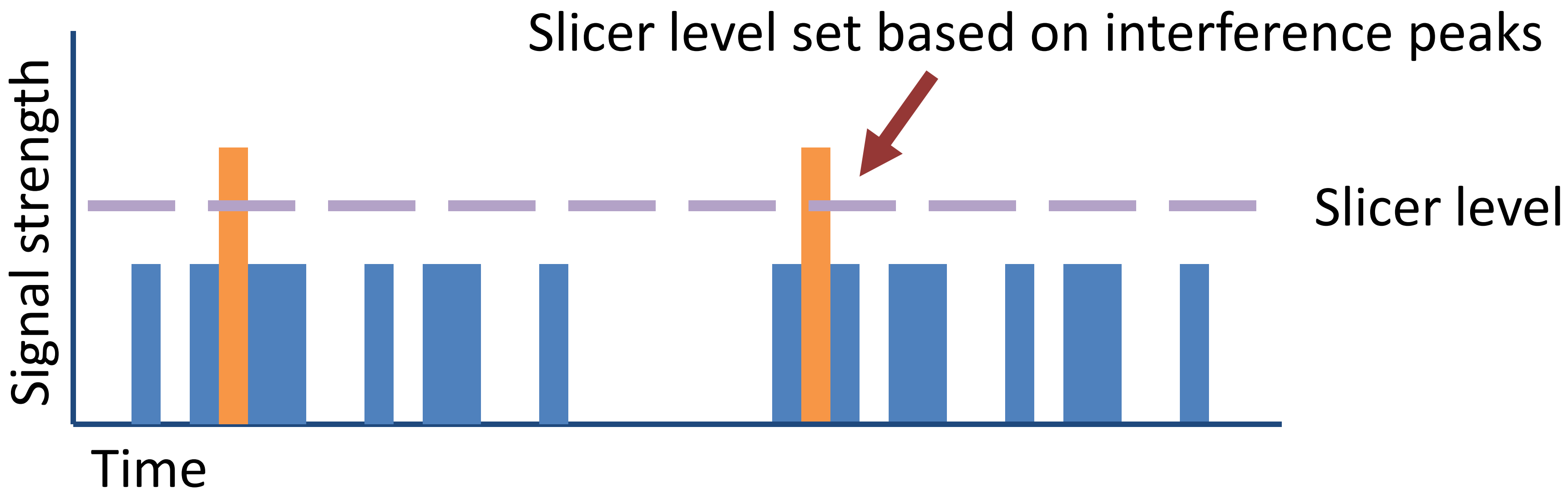


Transmitter pulses

Normal watch pulses

PRELIMINARY SLIDES
FINAL DECK AVAILABLE AFTER DEF CON

Scenario 1: Interference >> Signal



Slicer level set based on interference peaks

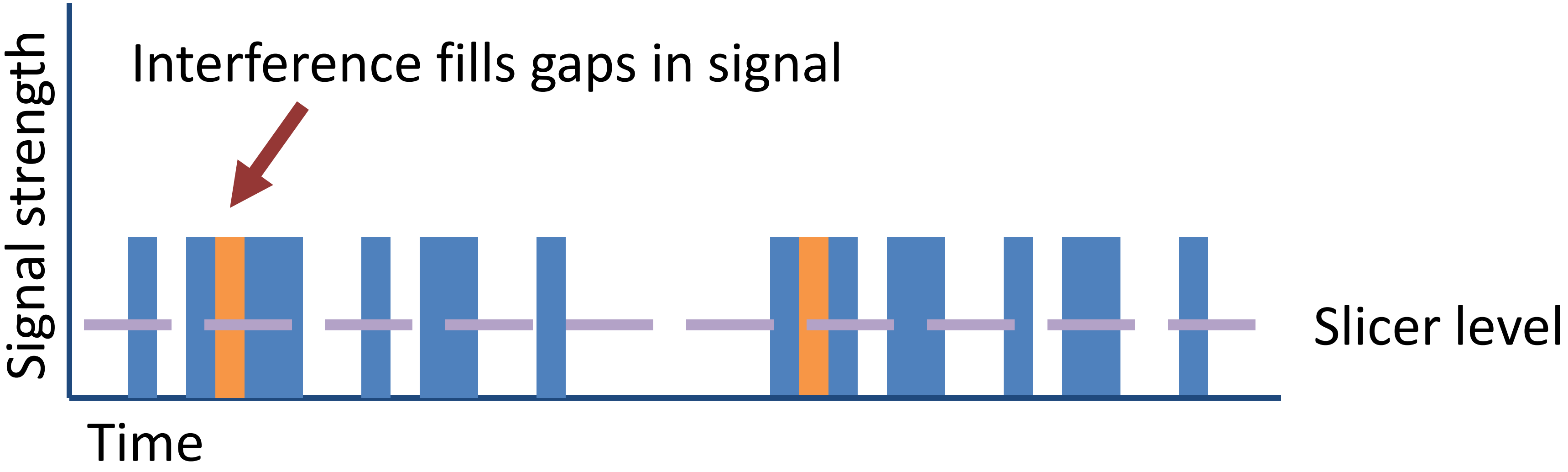
∴ Slicer level too high

∴ No signal bits recovered

🟧 = interfering signal

🟦 = watch signal

Scenario 2: Interference ≈ Signal



Interference fills gaps in signal

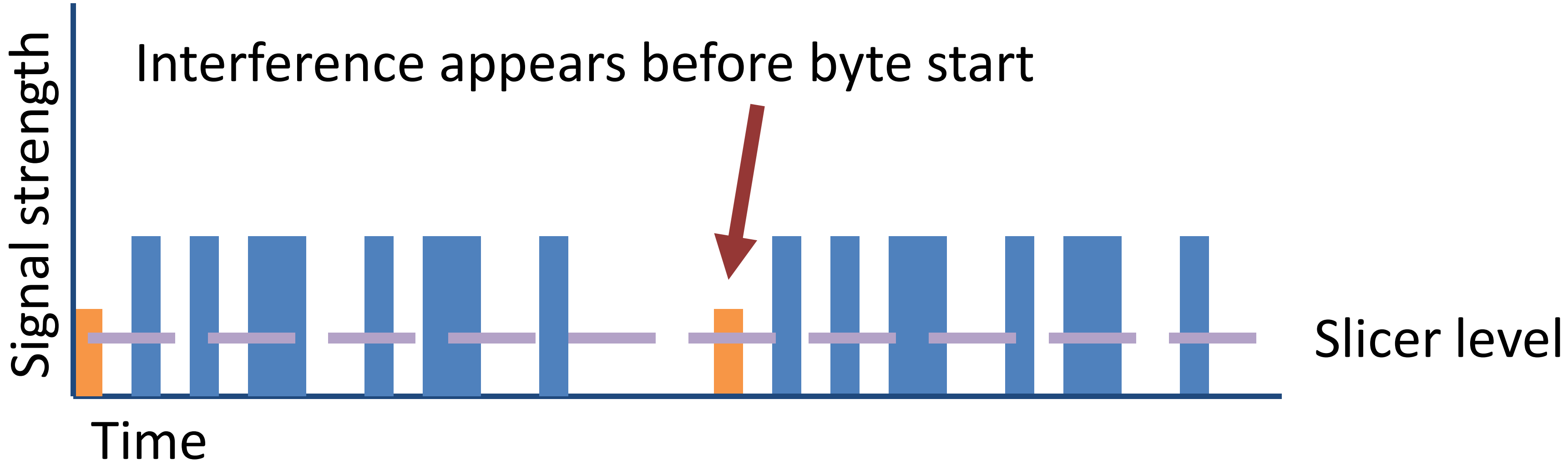
∴ No edges where there should be edges

∴ Manchester decoding fails

🟧 = interfering signal

🟦 = watch signal

Scenario 3: Interference < Signal



Interference appears before byte start

🟧 = interfering signal

🟦 = watch signal

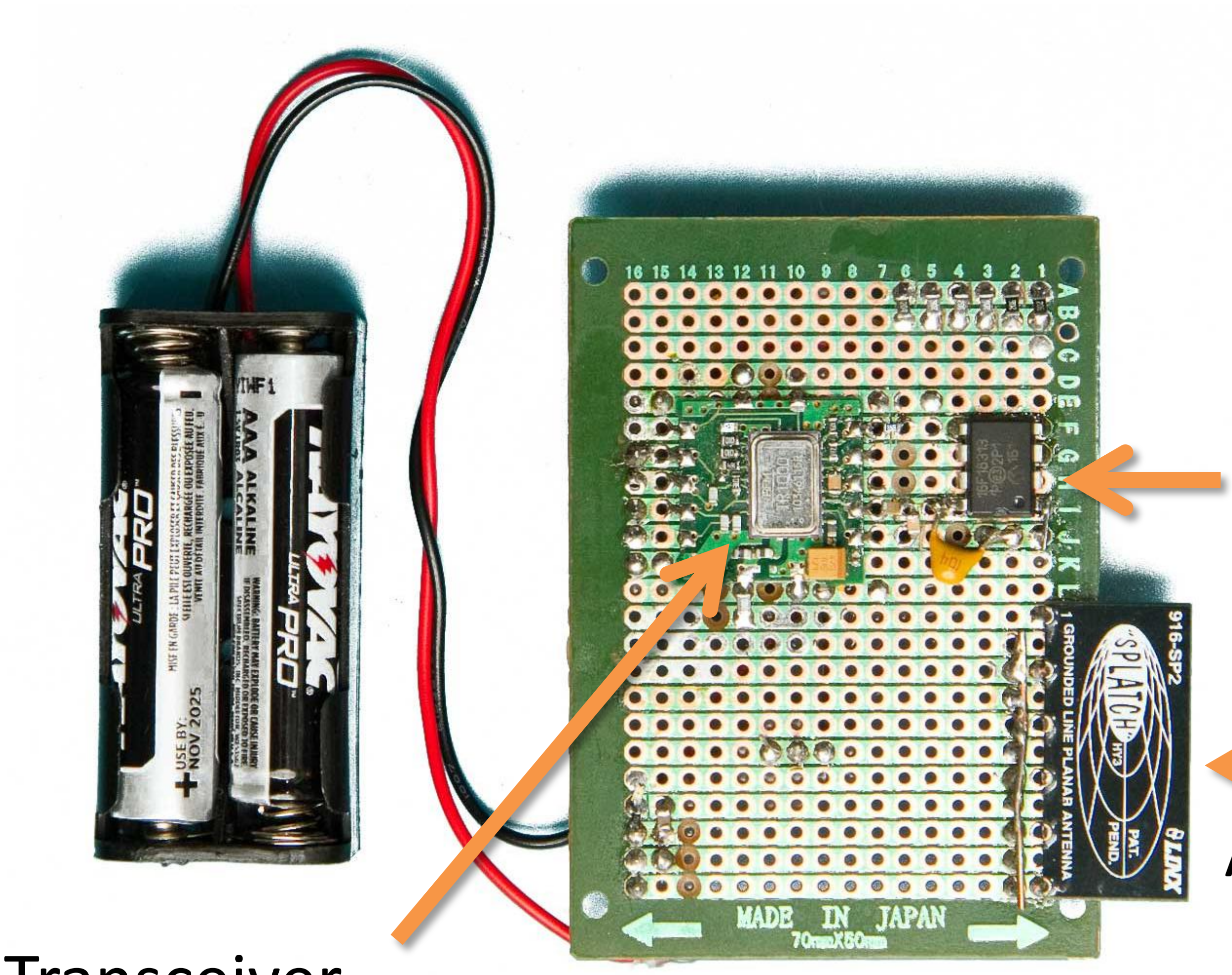
∴ Byte sync incorrect

∴ Byte decode fails

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)

Custom test transmitter



MCU

Antenna

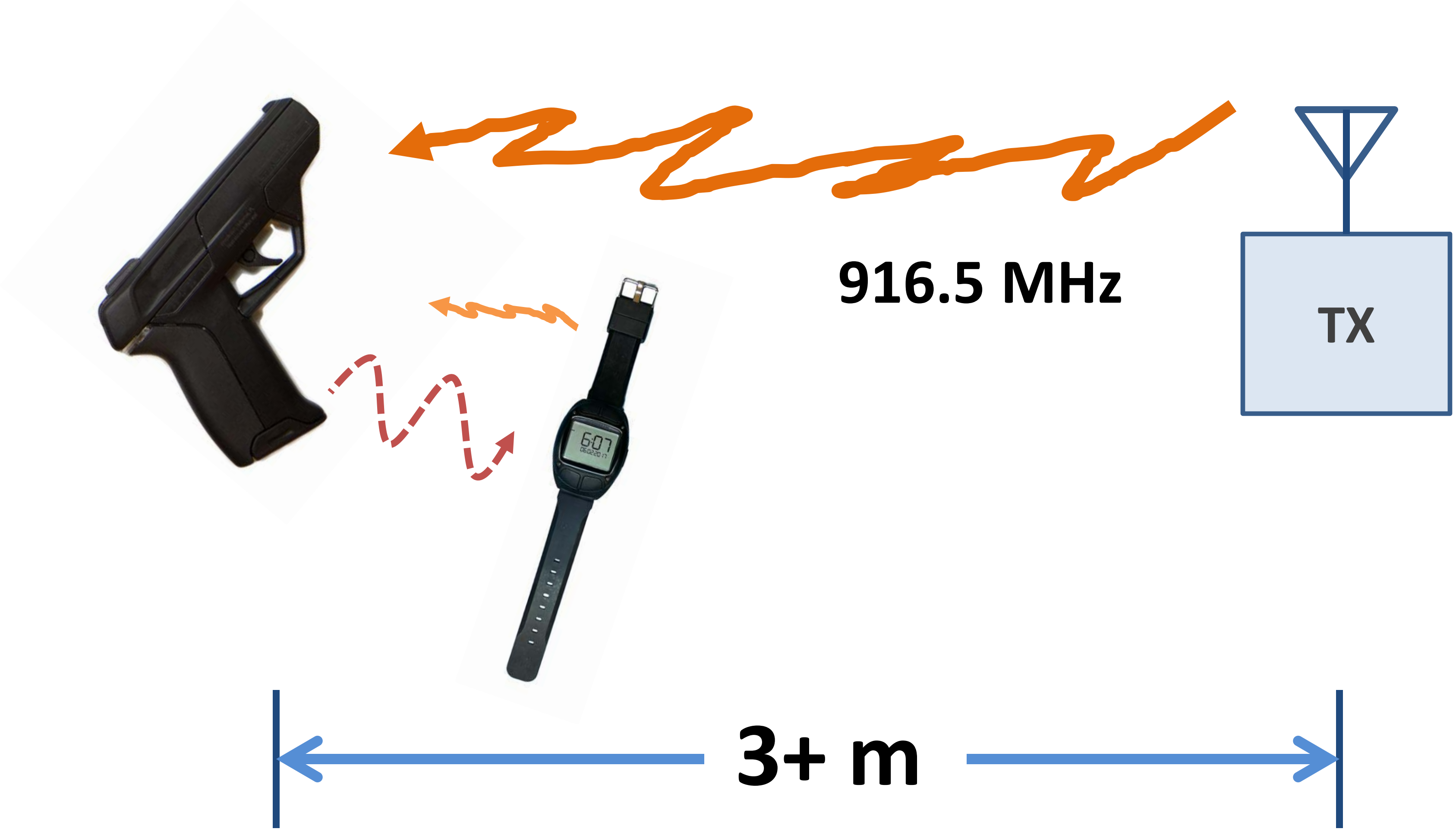
Transceiver

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

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)

Effective range



916.5 MHz

TX

3+ m

(Demo of denial of service)

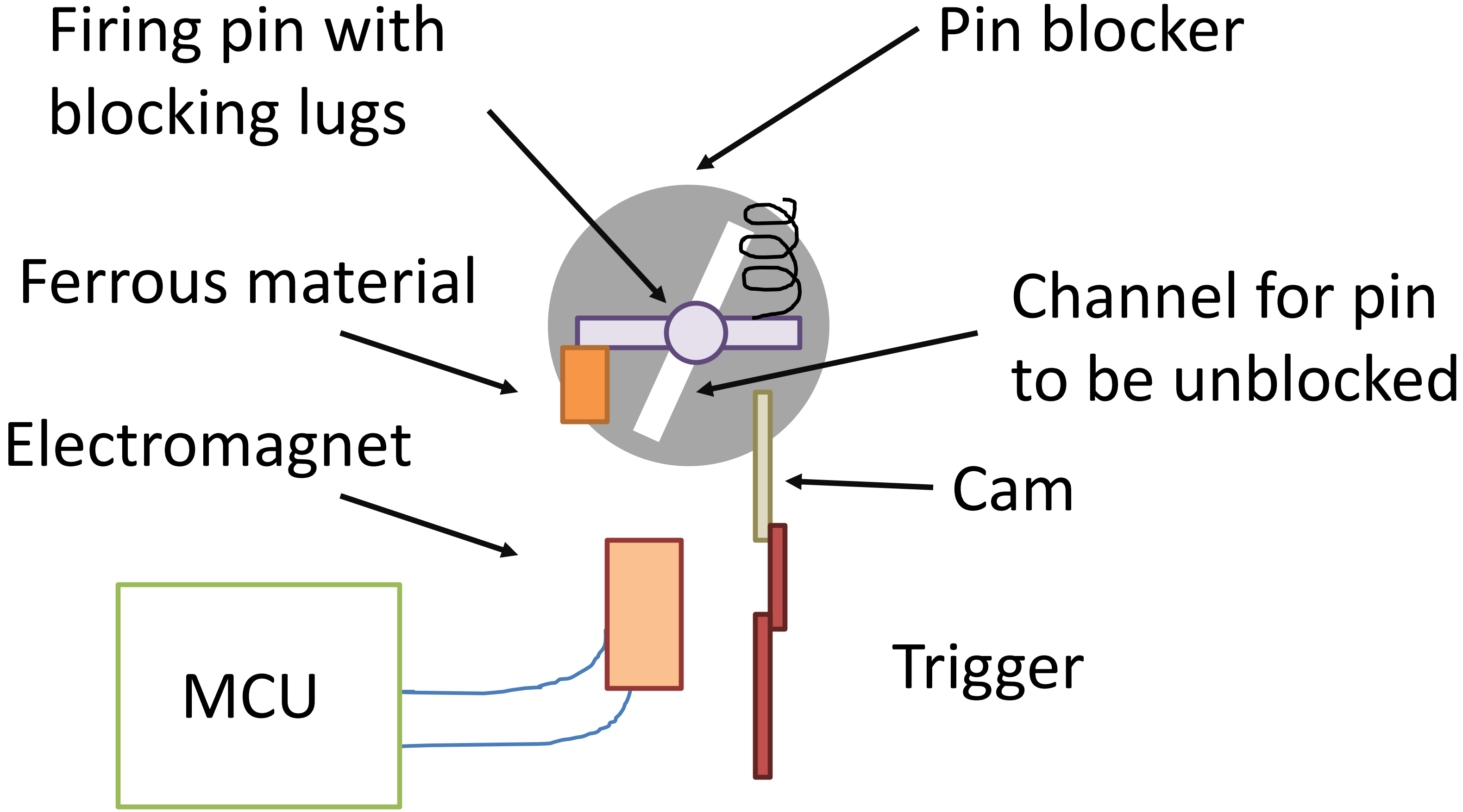
Defense

- Use more transmitter power
- Use error-correcting code
- Use more-robust modulation

Why have a smart gun in the first place?

FIRE WITHOUT AUTHORIZATION

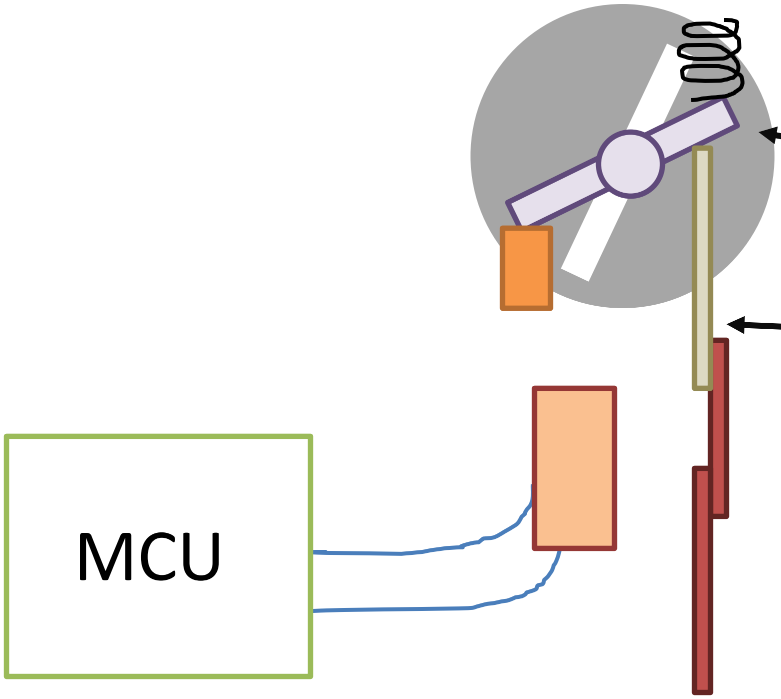
Unlocking mechanism



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

(Looking longitudinally)

Trigger partially pulled



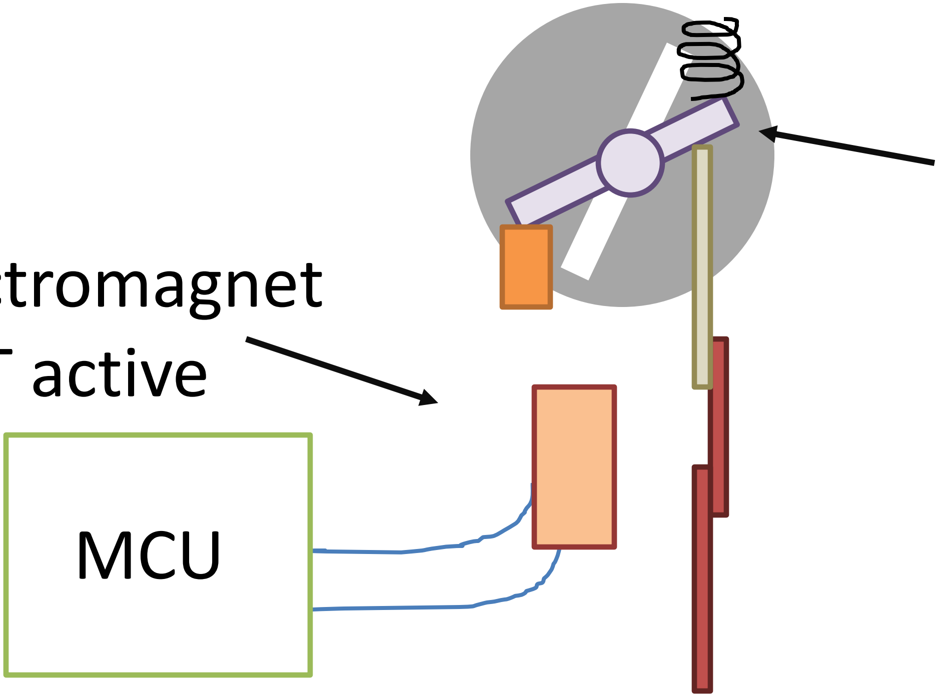
Firing pin closer to being unblocked

Cam moves up

Trigger partially pulled, presses on cam

(Looking longitudinally)

Scenario 1: Firing NOT authorized

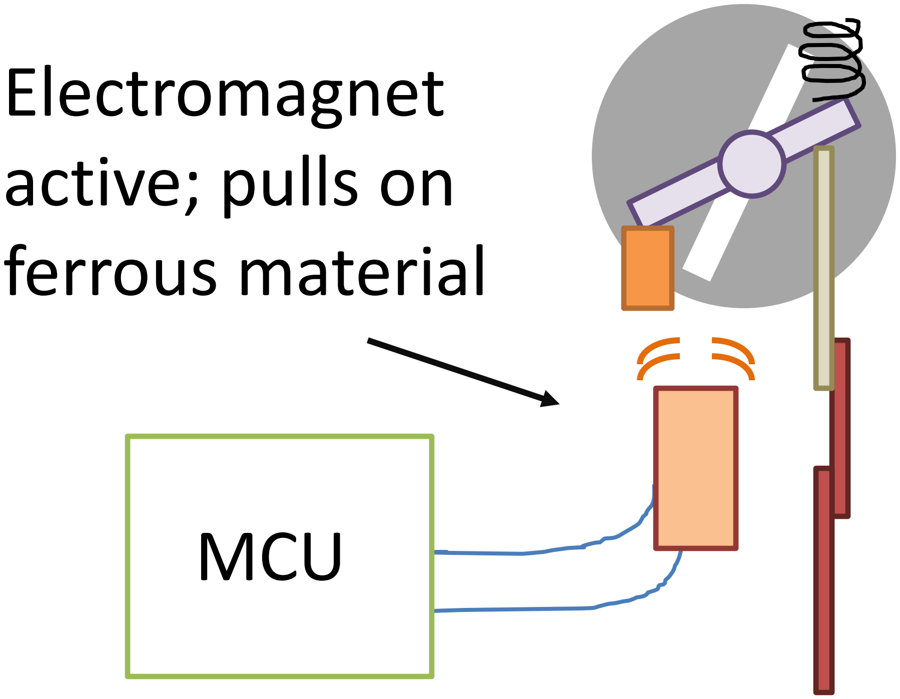


Electromagnet NOT active

Firing pin remains blocked;
Gun cannot fire

(Looking longitudinally)

Scenario 2: Firing IS authorized

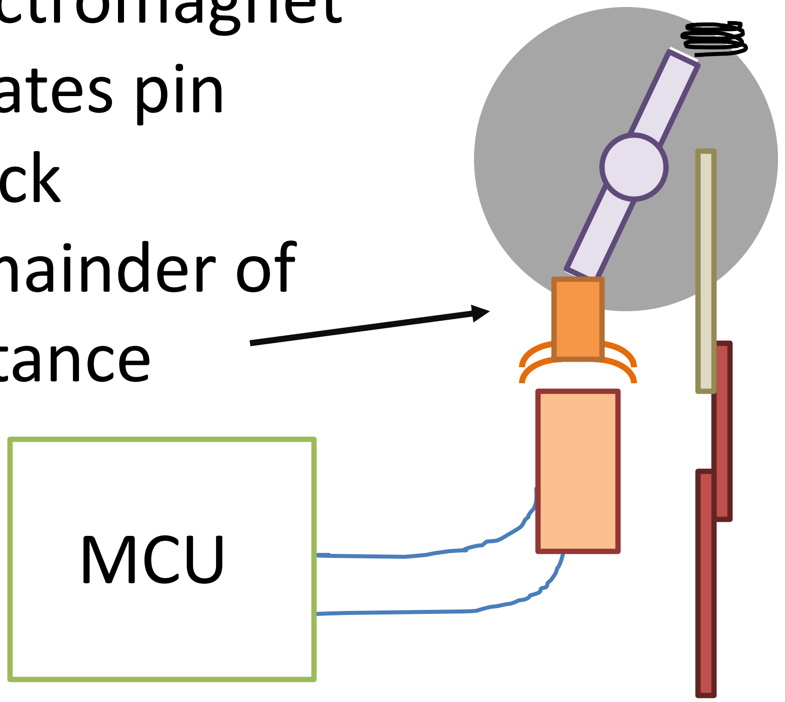


Electromagnet active; pulls on ferrous material

(Looking longitudinally)

Scenario 2, cont.: Gun can fire

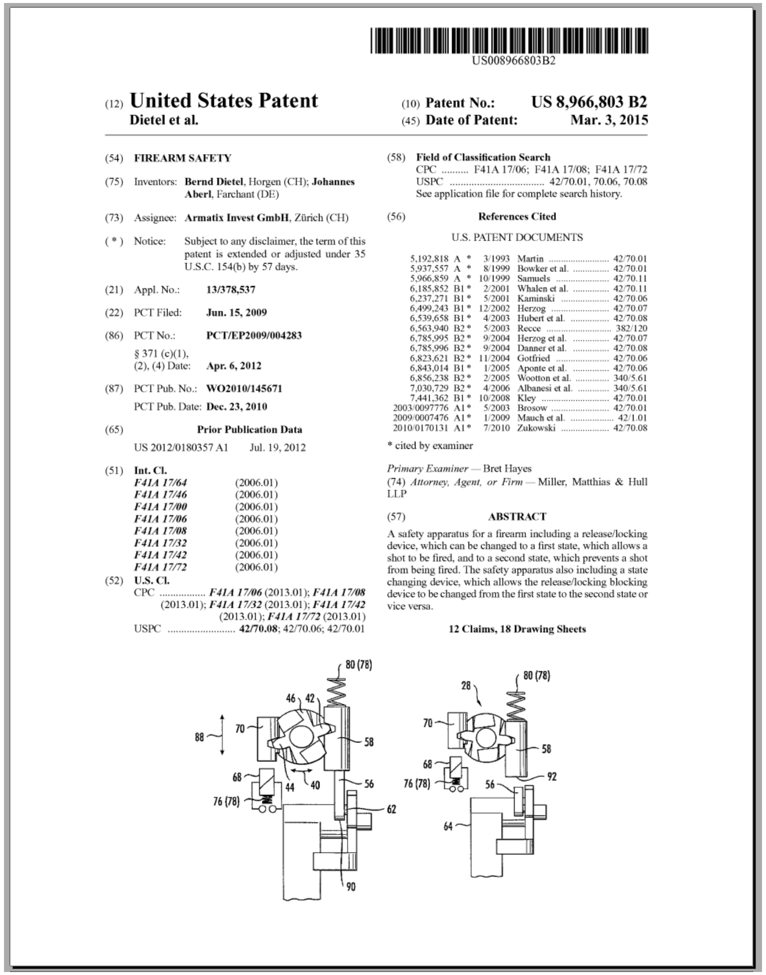
Electromagnet rotates pin block remainder of distance



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

(Looking longitudinally)

US patent 8,966,803



US008966803B2

(12) **United States Patent**
Dietel et al.

(10) **Patent No.: US 8,966,803 B2**
(45) **Date of Patent: Mar. 3, 2015**

(54) **FIREARM SAFETY**

(75) Inventors: **Bernd Dietel**, Horgen (CH); **Johannes Aberl**, Farchant (DE)

(73) Assignee: **Armatix Invest GmbH**, Zürich (CH)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 57 days.

(21) Appl. No.: **13/378,537**

(22) PCT Filed: **Jun. 15, 2009**

(86) PCT No.: **PCT/EP2009/004283**
§ 371 (c)(1),
(2), (4) Date: **Apr. 6, 2012**

(87) PCT Pub. No.: **WO2010/145671**
PCT Pub. Date: **Dec. 23, 2010**

(65) **Prior Publication Data**

US 2012/0180357 A1 Jul. 19, 2012

(51) **Int. Cl.**

F41A 17/64	(2006.01)
F41A 17/46	(2006.01)
F41A 17/00	(2006.01)
F41A 17/06	(2006.01)
F41A 17/08	(2006.01)
F41A 17/32	(2006.01)
F41A 17/42	(2006.01)
F41A 17/72	(2006.01)

(52) **U.S. Cl.**
CPC ***F41A 17/06*** (2013.01); ***F41A 17/08*** (2013.01); ***F41A 17/32*** (2013.01); ***F41A 17/42*** (2013.01); ***F41A 17/72*** (2013.01)
USPC **42/70.08**; 42/70.06; 42/70.01

(58) **Field of Classification Search**
CPC F41A 17/06; F41A 17/08; F41A 17/72
USPC 42/70.01, 70.06, 70.08
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,192,818	A *	3/1993	Martin	42/70.01
5,937,557	A *	8/1999	Bowker et al.	42/70.01
5,966,859	A *	10/1999	Samuels	42/70.11
6,185,852	B1 *	2/2001	Whalen et al.	42/70.11
6,237,271	B1 *	5/2001	Kaminski	42/70.06
6,499,243	B1 *	12/2002	Herzog	42/70.07
6,539,658	B1 *	4/2003	Hubert et al.	42/70.08
6,563,940	B2 *	5/2003	Recce	382/120
6,785,995	B2 *	9/2004	Herzog et al.	42/70.07
6,785,996	B2 *	9/2004	Danner et al.	42/70.08
6,823,621	B2 *	11/2004	Gotfried	42/70.06
6,843,014	B1 *	1/2005	Aponte et al.	42/70.06
6,856,238	B2 *	2/2005	Wootton et al.	340/5.61
7,030,729	B2 *	4/2006	Albanesi et al.	340/5.61
7,441,362	B1 *	10/2008	Kley	42/70.01
2003/0097776	A1 *	5/2003	Brosow	42/70.01
2009/0007476	A1 *	1/2009	Mauch et al.	42/1.01
2010/0170131	A1 *	7/2010	Zukowski	42/70.08

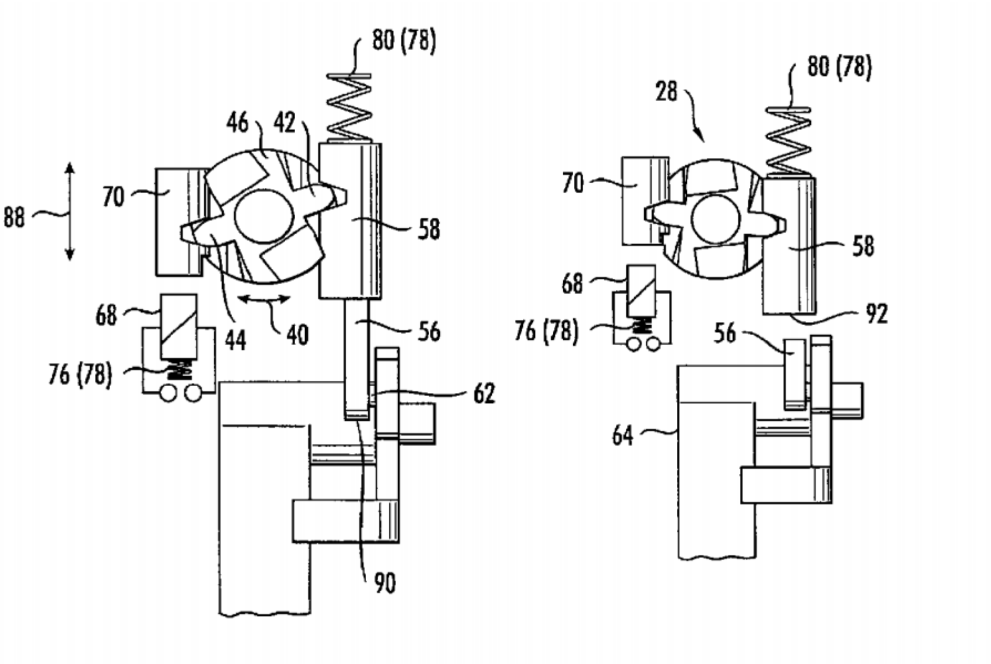
* cited by examiner

Primary Examiner — Bret Hayes
(74) *Attorney, Agent, or Firm* — Miller, Matthias & Hull LLP

(57) **ABSTRACT**

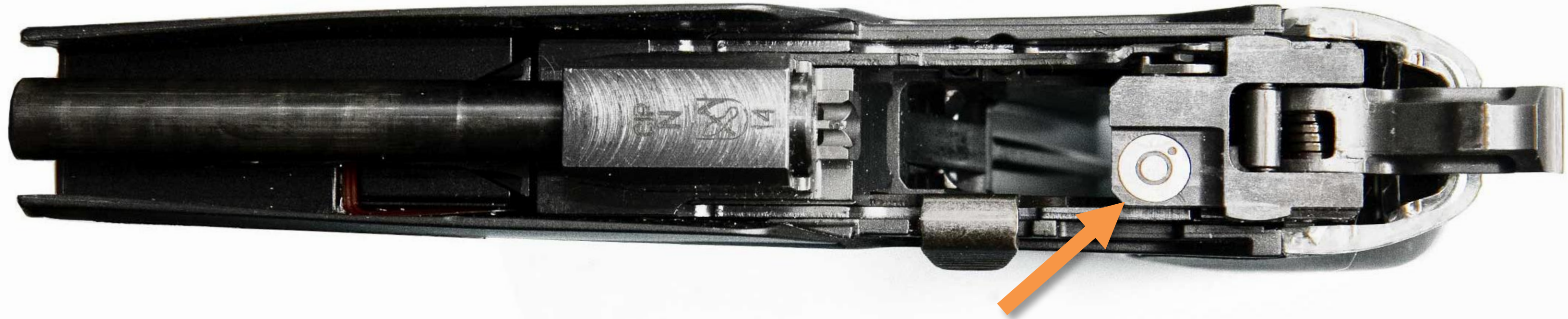
A safety apparatus for a firearm including a release/locking device, which can be changed to a first state, which allows a shot to be fired, and to a second state, which prevents a shot from being fired. The safety apparatus also including a state changing device, which allows the release/locking blocking device to be changed from the first state to the second state or vice versa.

12 Claims, 18 Drawing Sheets



Actual weapon

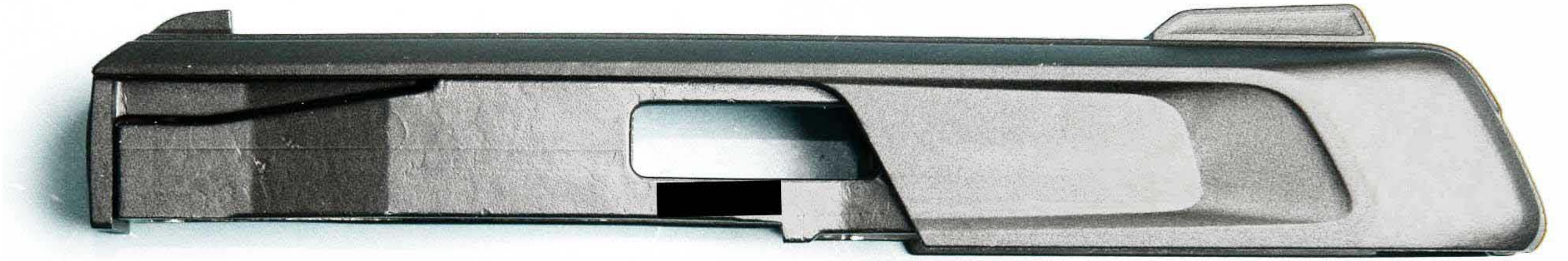
Top view of receiver



Electromagnet

Mechanism in slide

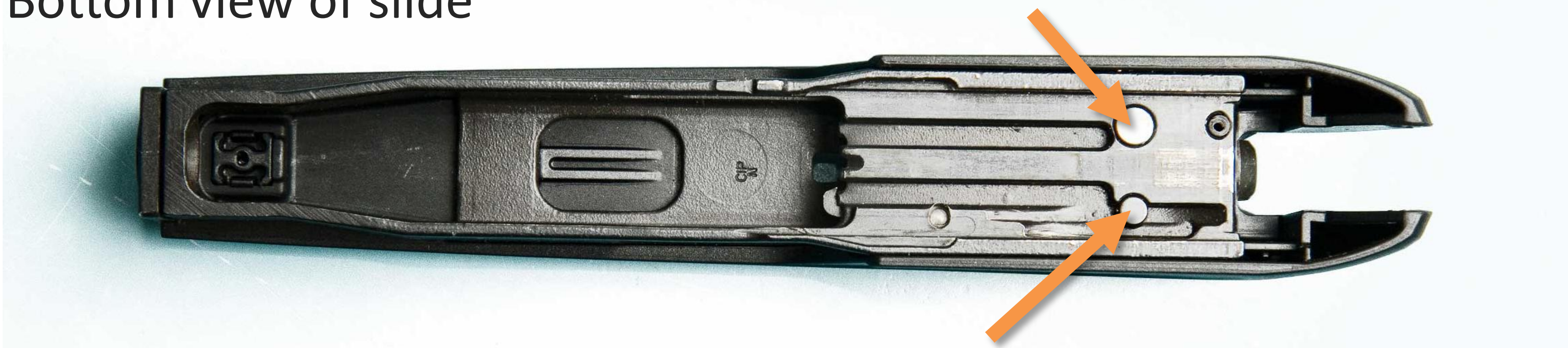
Profile view of slide



[redacted]

Bottom view of slide

Ferrous material

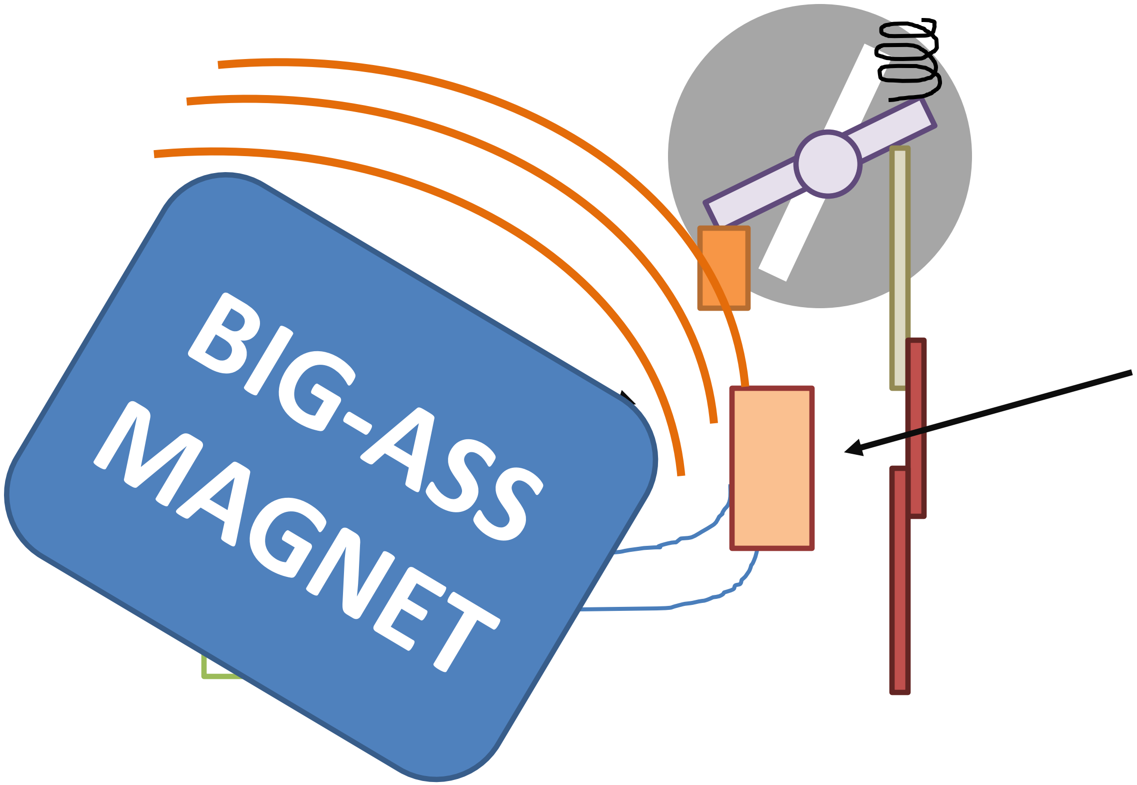


Cam presses here

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

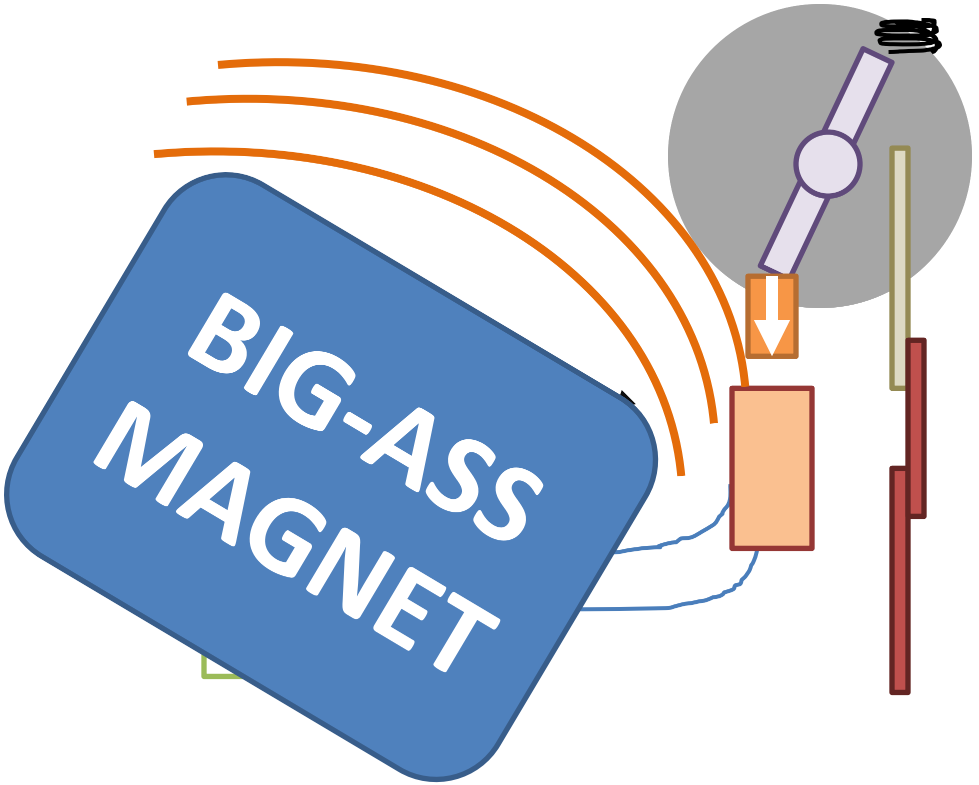
Magnet attack



Electromagnet not active

(Looking longitudinally)

Magnet attack



External magnet pulls ferrous material;

Pin unblocked;

Gun can fire

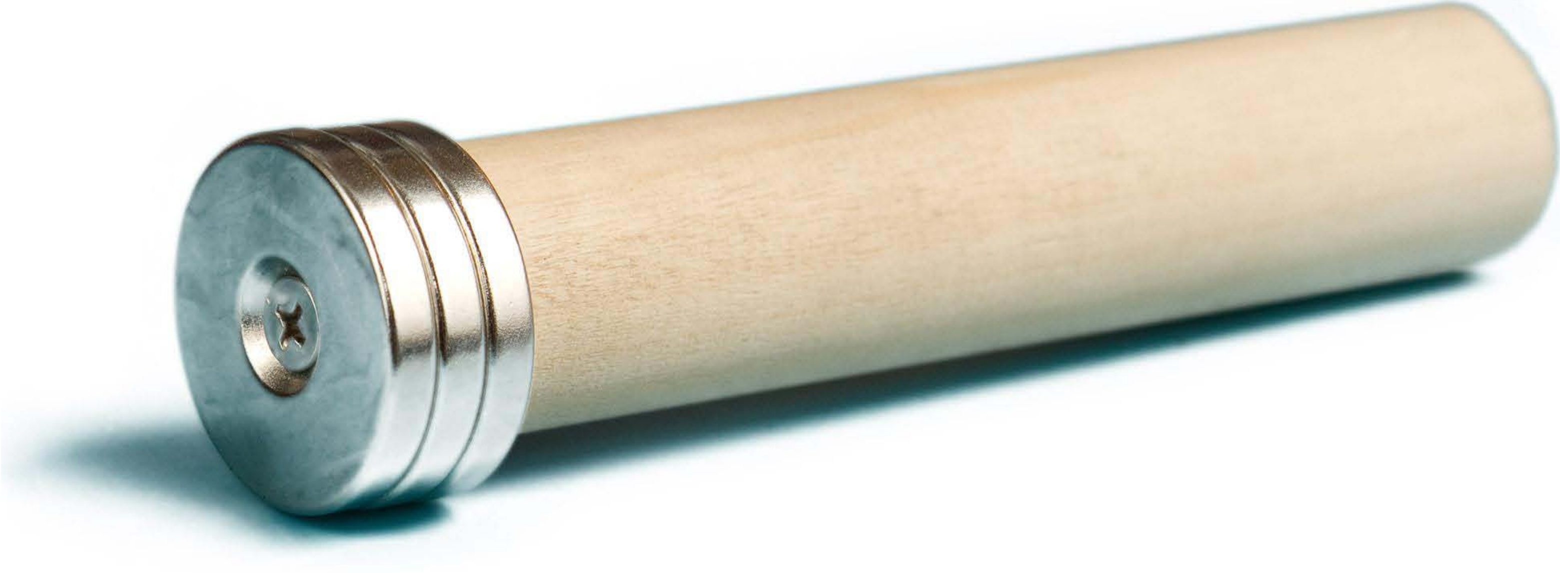
(Looking longitudinally)

Magnets

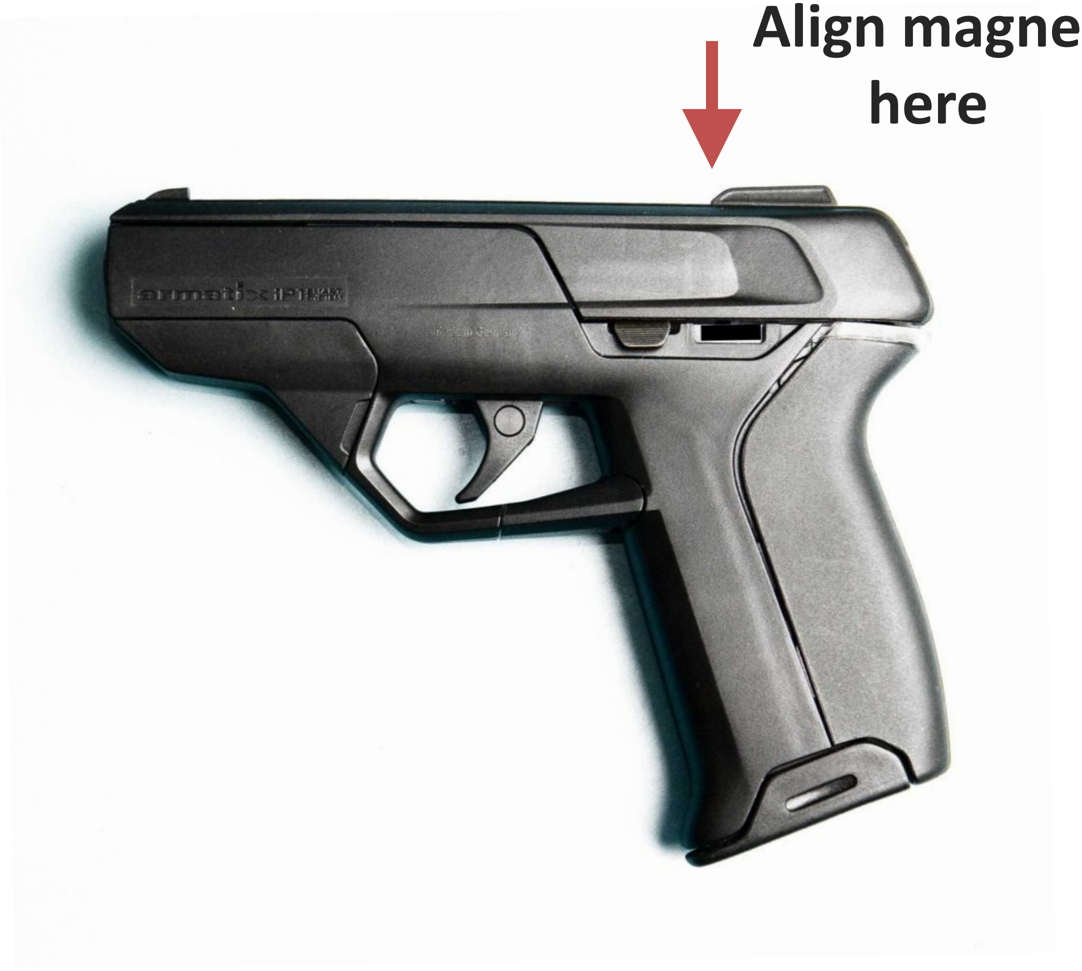
TAQTON
SCIENTIFIC SUPPLIES
MAGNETS ARE BRITTLE HANDLE WITH CARE
WEAR PROTECTIVE EYEWEAR AND GEAR
THESE MAGNETS ARE STRONG. ALWAYS USE RESPONSIBLY.
KEEP OUT OF REACH OF CHILDREN. USE AT OWN RISK.

- N52 neodymium magnets
- 32 mm × 5 mm
- $19 on Amazon for a four-pack (only three are required)
- Cost
  - $14.75 magnets
  - $0.20 scrap dowel
  - $0.05 stainless screw
  - Total: $15

Completed magnet tool

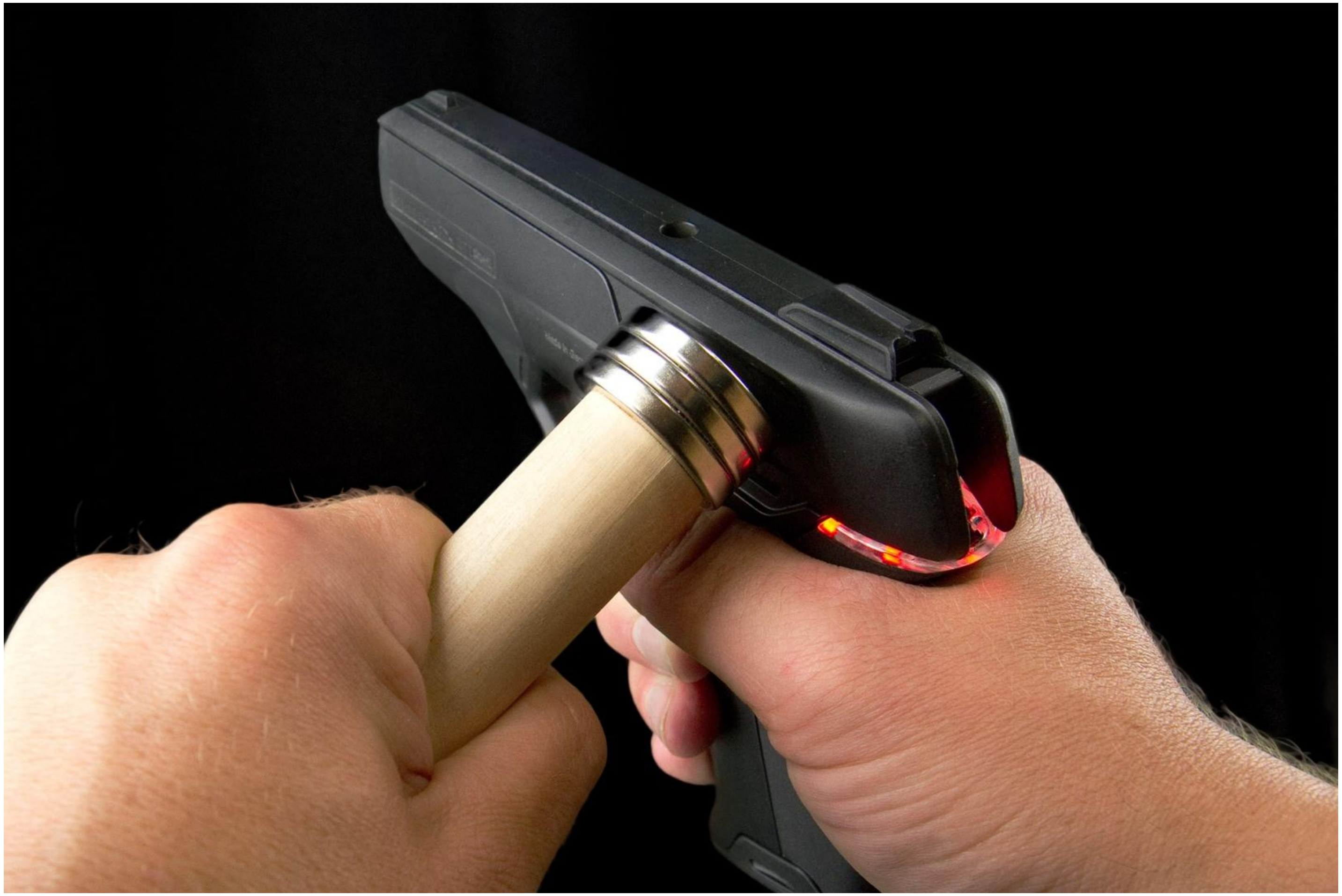


Magnet alignment



Align magnet here

Magnets on pistol



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

(Demo of magnet attack)

Defense

- Don’t use magnets, solenoids, etc.
  - Nothing involving a DC magnetic field
  - Consider motor-driven mechanism
- Detect external field and activate secondary lock
  - Kind of like a relocker in a safe

Lessons for future guns

- Lock is only as good as its weakest link
- Robust, secure electronics don't matter if they can be defeated with a magnet
  - The "Sentry Safe" lesson
- More secure unlocking mechanisms are contemplated in the Armatix patents
  - Why didn't they use them?

THANKS!

plore@tuta.io

@_plore

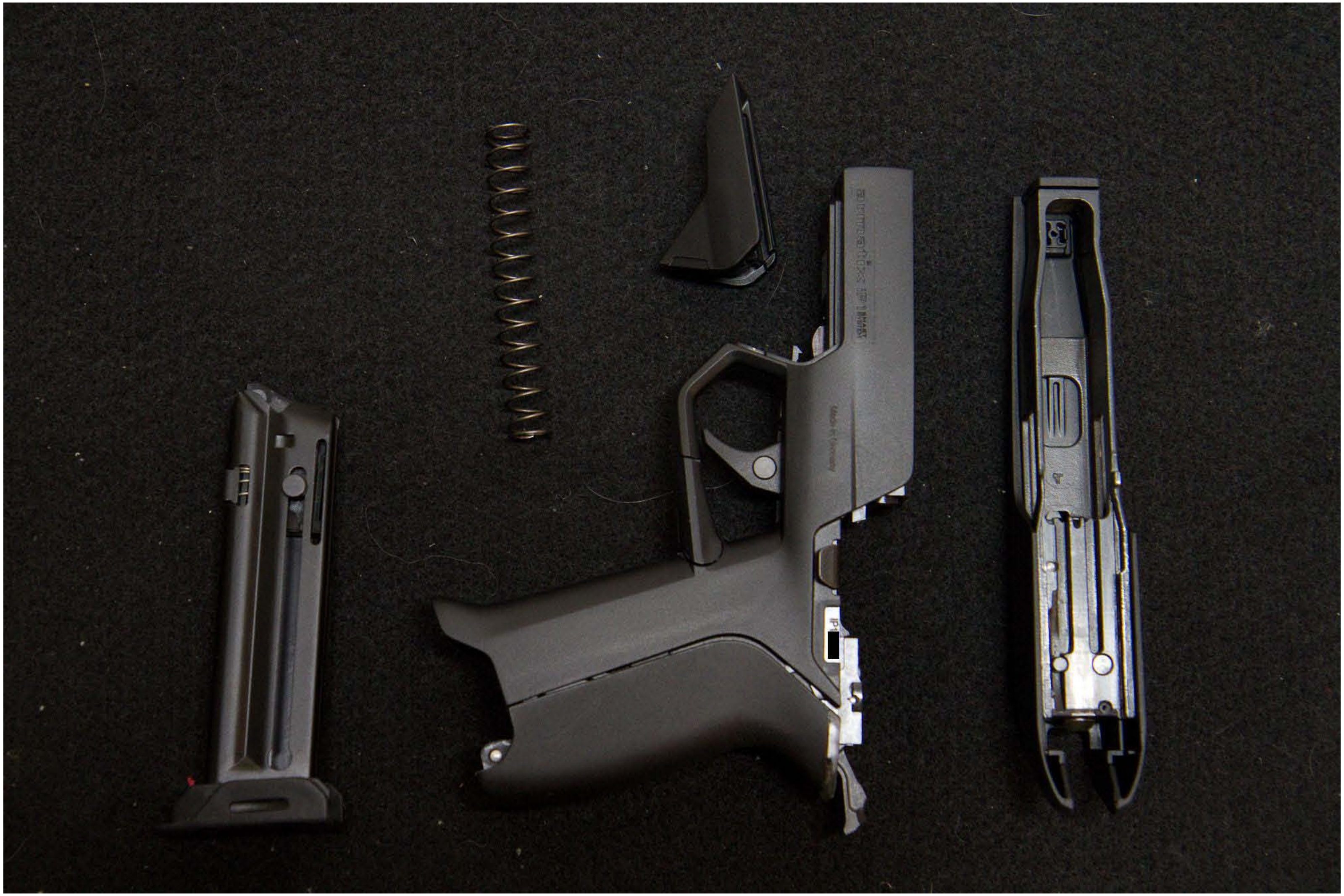
Updated slides will be available on DEF CON web site within a few weeks

BACKUP SLIDES

Armatix iP1

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

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

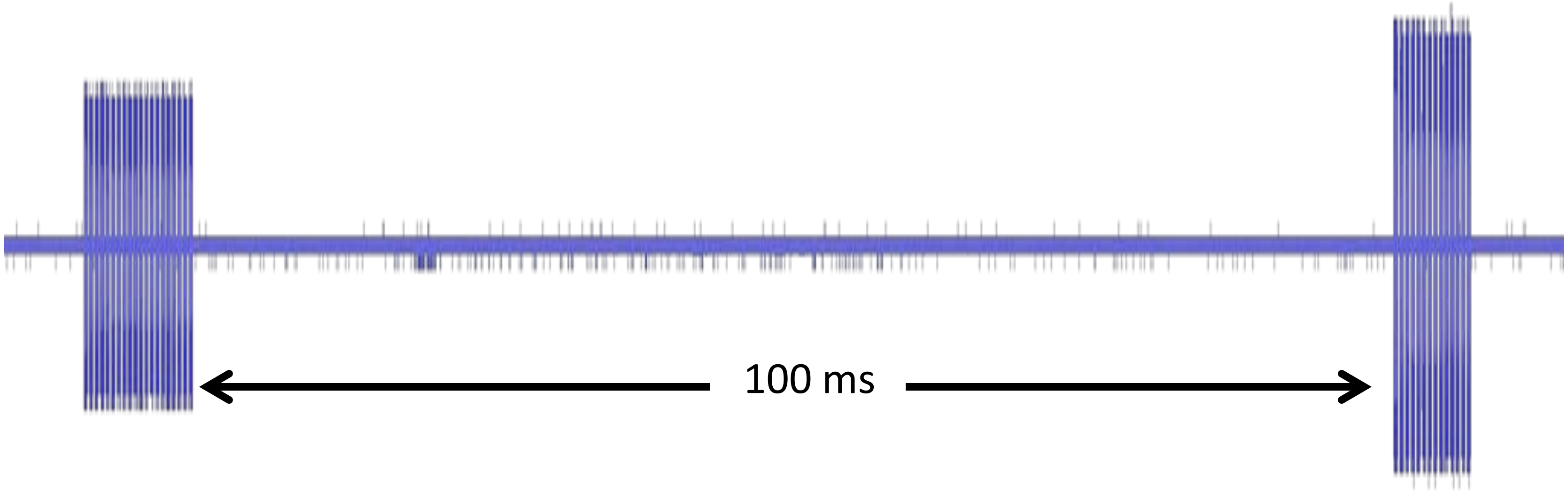
Operation overview

- 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



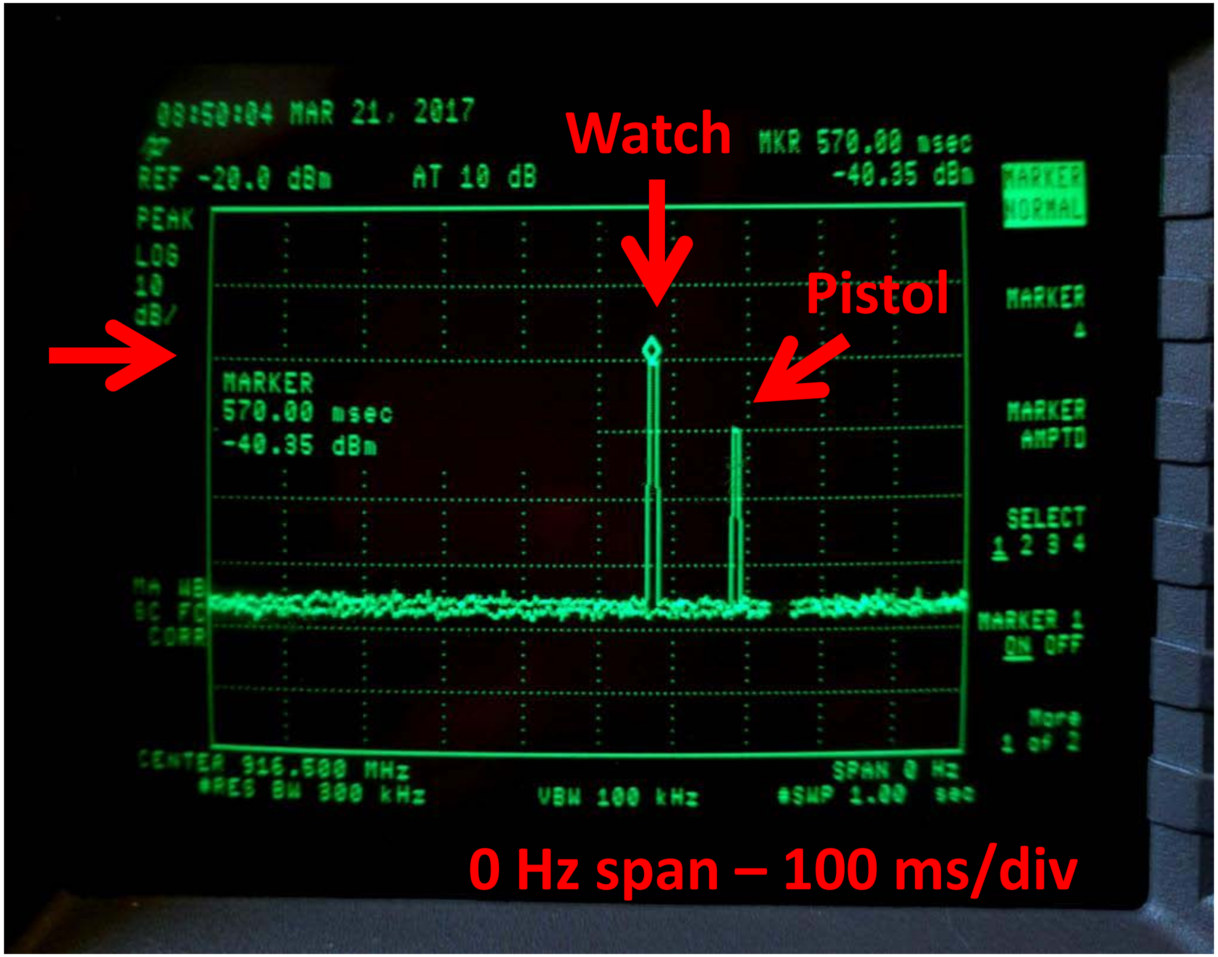
100 ms

Watch
sends token

Pistol ACKs
token

Watch and pistol on spectrum analyzer

-40 dBm



08:50:04 MAR 21, 2017

MKR 570.00 msec
-40.35 dBm

REF -20.0 dBm AT 10 dB

PEAK
LOG
10
dB/

MARKER
570.00 msec
-40.35 dBm

CENTER 916.500 MHz
#RES BW 300 kHz VBW 100 kHz SPAN 0 Hz
#SWP 1.00 sec

Watch

Pistol

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

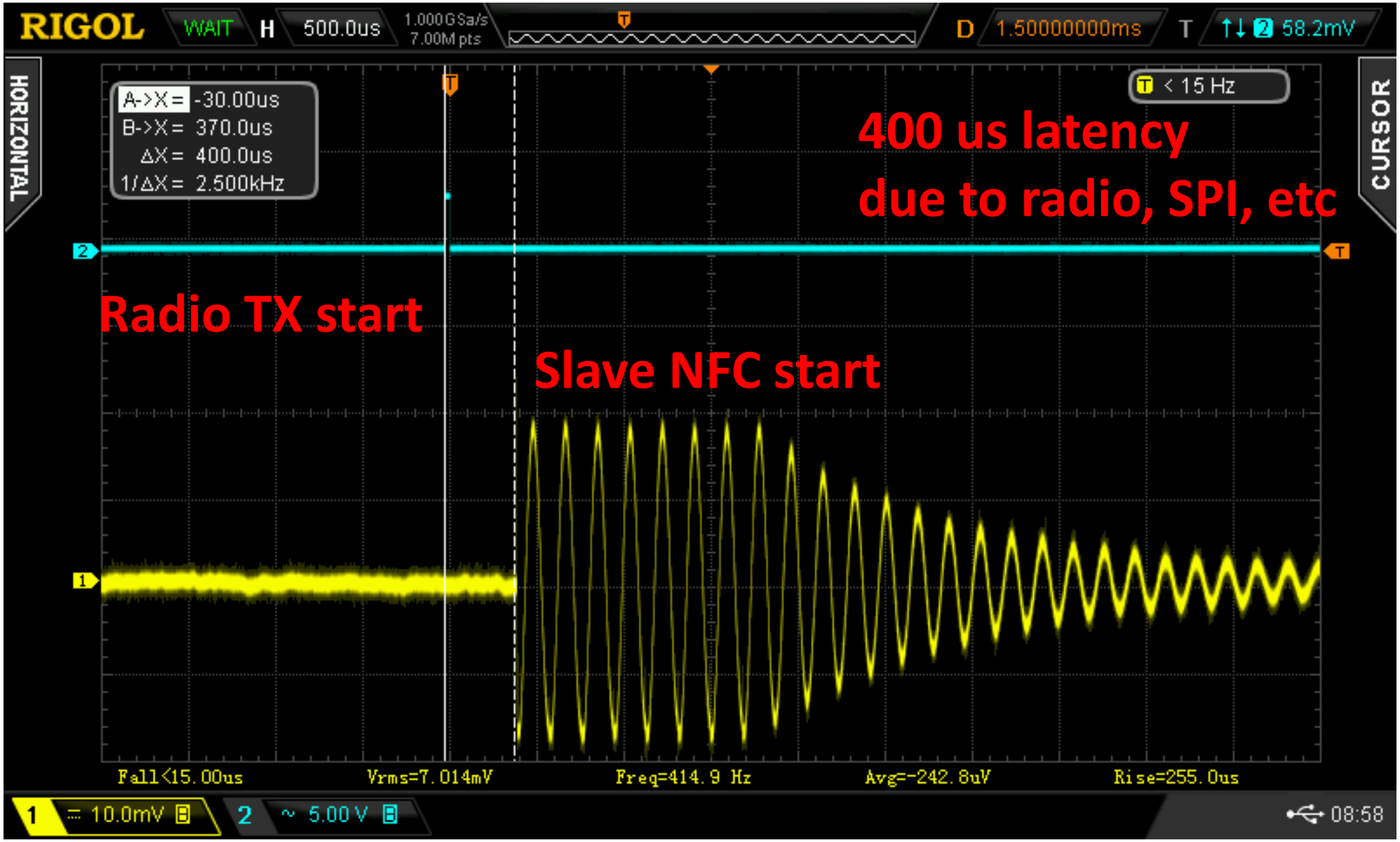
Proximity-defeat results

- 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



```
A->X= -30.00us
B->X=  370.0us
  ΔX=  400.0us
1/ΔX=  2.500kHz
```

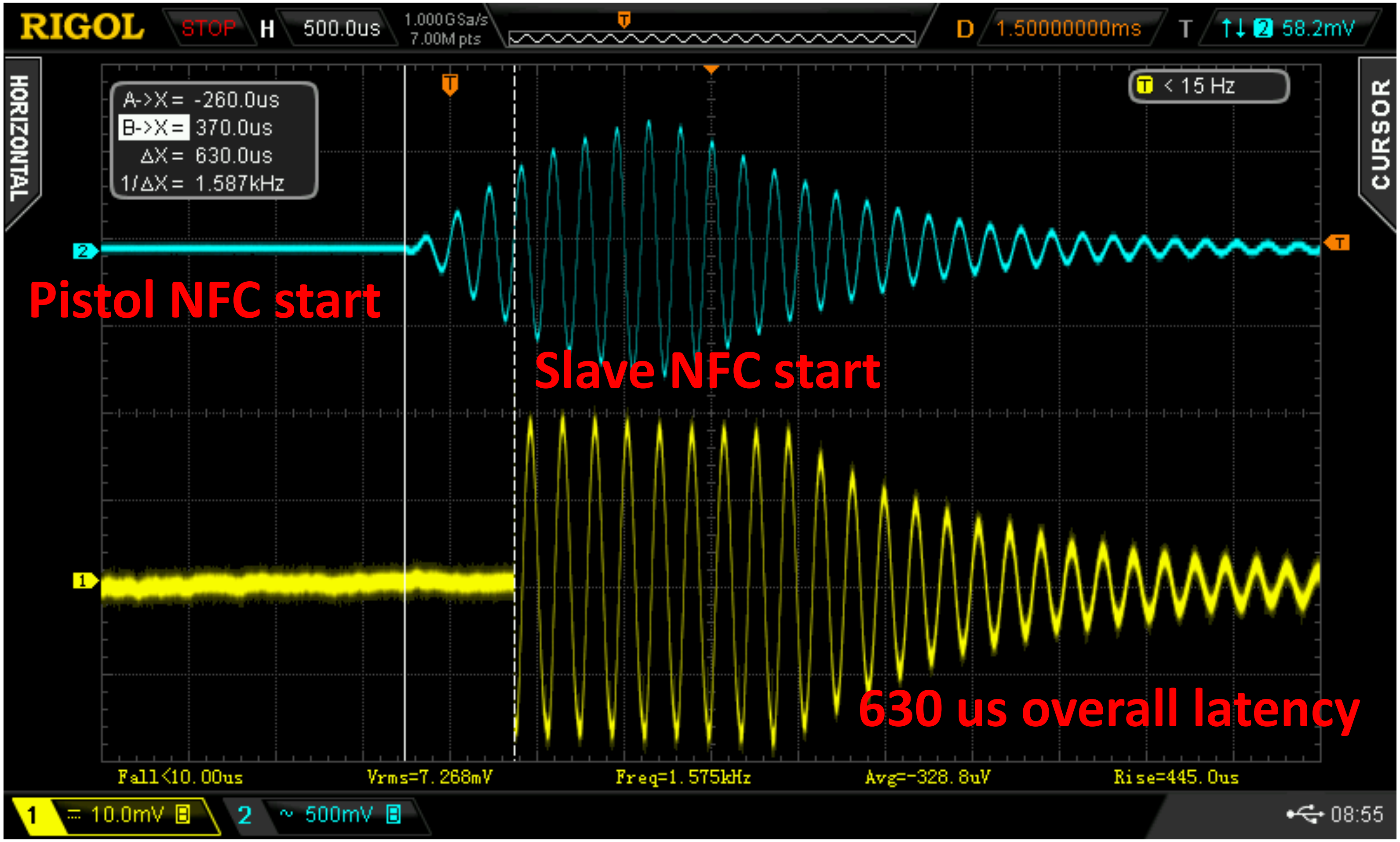
```
Fall<15.00us     Vrms=7.014mV     Freq=414.9 Hz     Avg=-242.8uV     Rise=255.0us
```

400 us latency
due to radio, SPI, etc

Radio TX start

Slave NFC start

Latency of relay



A->X= -260.0us
B->X= 370.0us
ΔX= 630.0us
1/ΔX= 1.587kHz

Fall<10.00us Vrms=7.268mV Freq=1.575kHz Avg=-328.8uV Rise=445.0us

Pistol NFC start

Slave NFC start

630 us overall latency

PRELIMINARY SLIDES
FINAL DECK AVAILABLE AFTER DEF CON

How sensitive to interference?

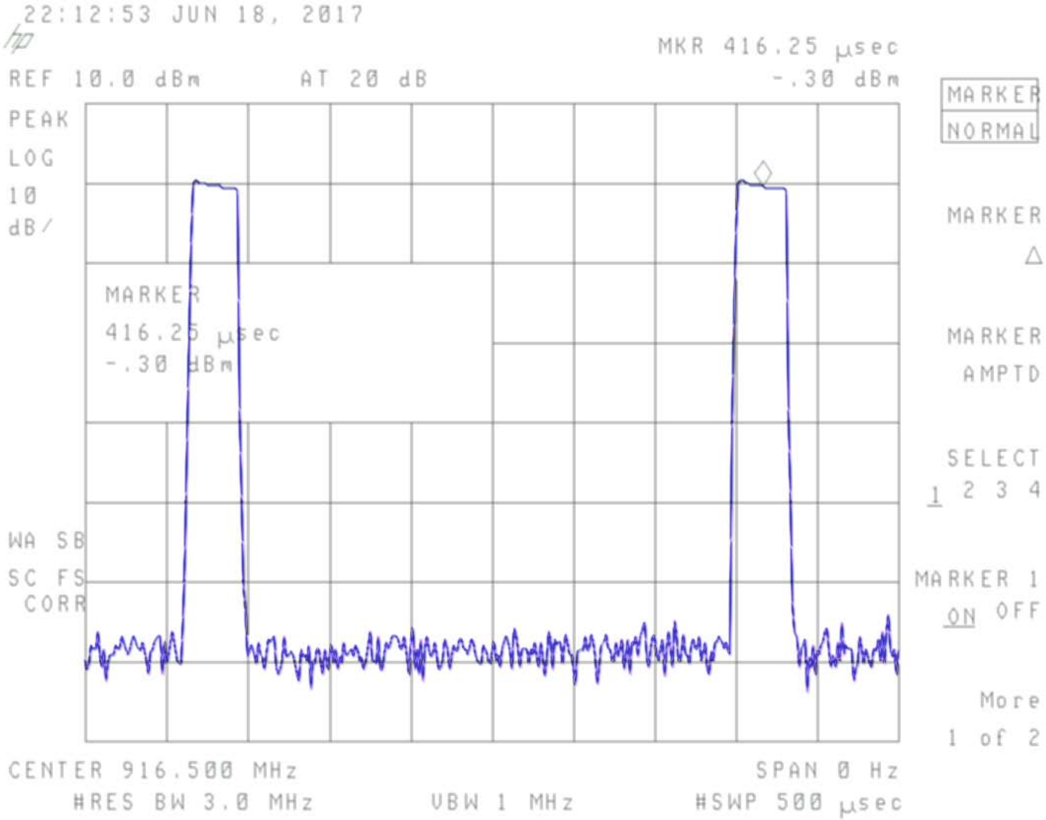
- OOK modulation is highly susceptible to interference
  - 916.5 MHz module datasheet used in iP1 warns that slicer will be “blinded” by strong noise pulses[1]
  - Slicer will also be fooled by lone pulses in bit timeslot that are less than 6 dB down from the normal bit peaks
- Signal from watch measured 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

[1] http://wireless.murata.com/media/products/apnotes/ook.pdf

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

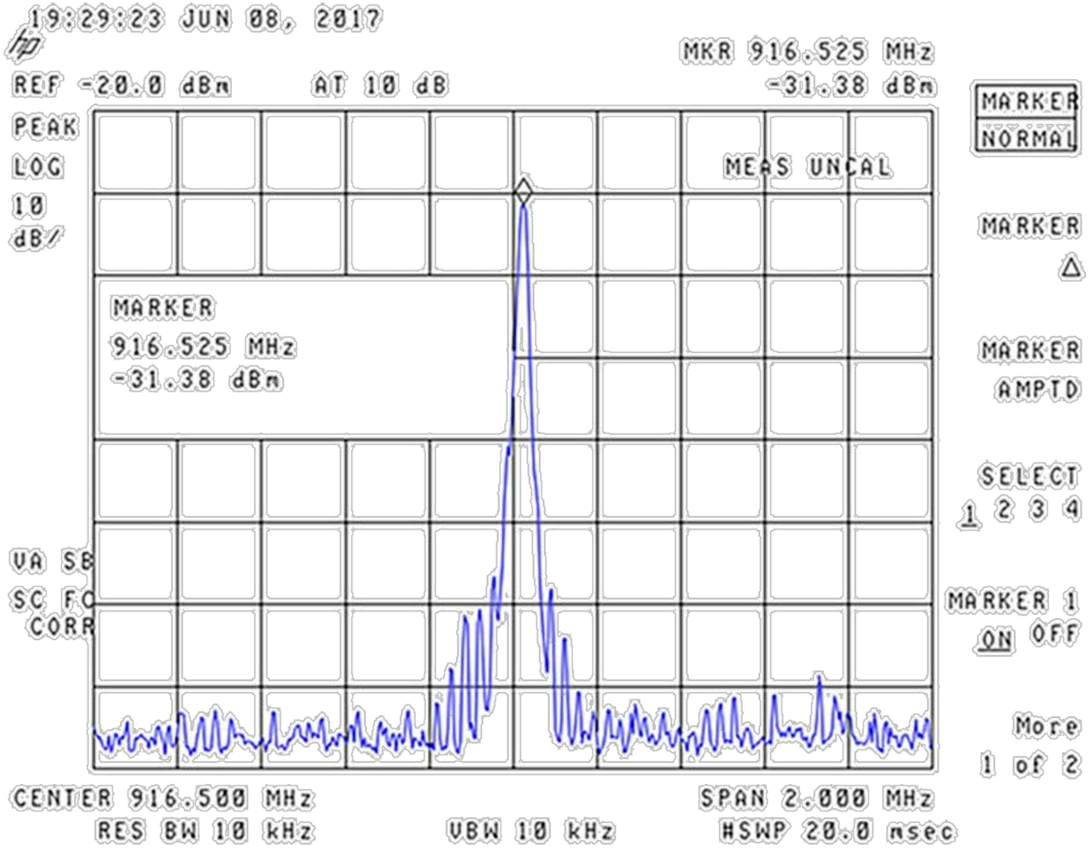
Transmitter output



```
22:12:53 JUN 18, 2017
                                                MKR 416.25 µsec
REF 10.0 dBm        AT 20 dB                        -.30 dBm
PEAK
LOG
10
dB/
        MARKER
        416.25 µsec
        -.30 dBm
WA SB
SC FS
 CORR
CENTER 916.500 MHz                               SPAN 0 Hz
   #RES BW 3.0 MHz        VBW 1 MHz         #SWP 500 µsec
```

PRELIMINARY SLIDES
FINAL DECK AVAILABLE AFTER DEF CON

Unmodulated carrier spectrum



19:29:23 JUN 08, 2017

hp

MKR 916.525 MHz
-31.38 dBm

REF -20.0 dBm   AT 10 dB

PEAK
LOG
10
dB/

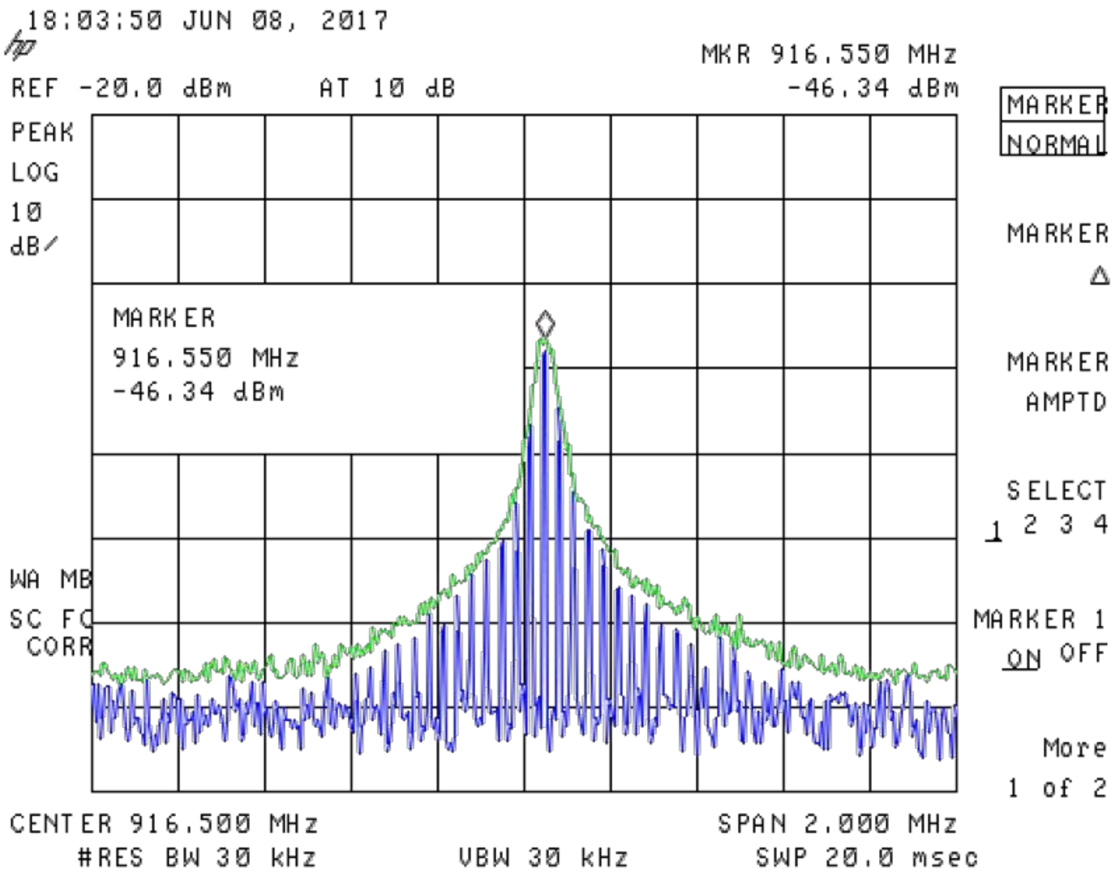
MEAS UNCAL

MARKER
916.525 MHz
-31.38 dBm

VA SB
SC FC
CORR

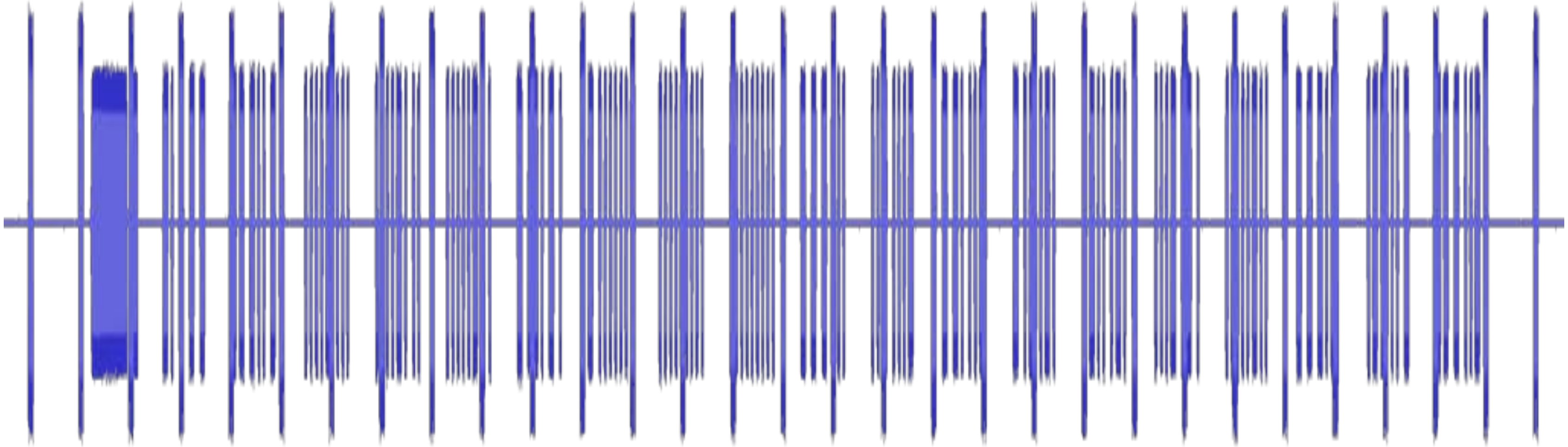
CENTER 916.500 MHz   SPAN 2.000 MHz
RES BW 10 kHz   VBW 10 kHz   #SWP 20.0 msec

Modulated transmitter spectrum



```
18:03:50 JUN 08, 2017
                                          MKR 916.550 MHz
REF -20.0 dBm      AT 10 dB                   -46.34 dBm
PEAK
LOG
10
dB/
        MARKER
        916.550 MHz
        -46.34 dBm
WA MB
SC FC
 CORR
CENTER 916.500 MHz                        SPAN 2.000 MHz
    #RES BW 30 kHz        VBW 30 kHz        SWP 20.0 msec
```

Transmitter over watch signal

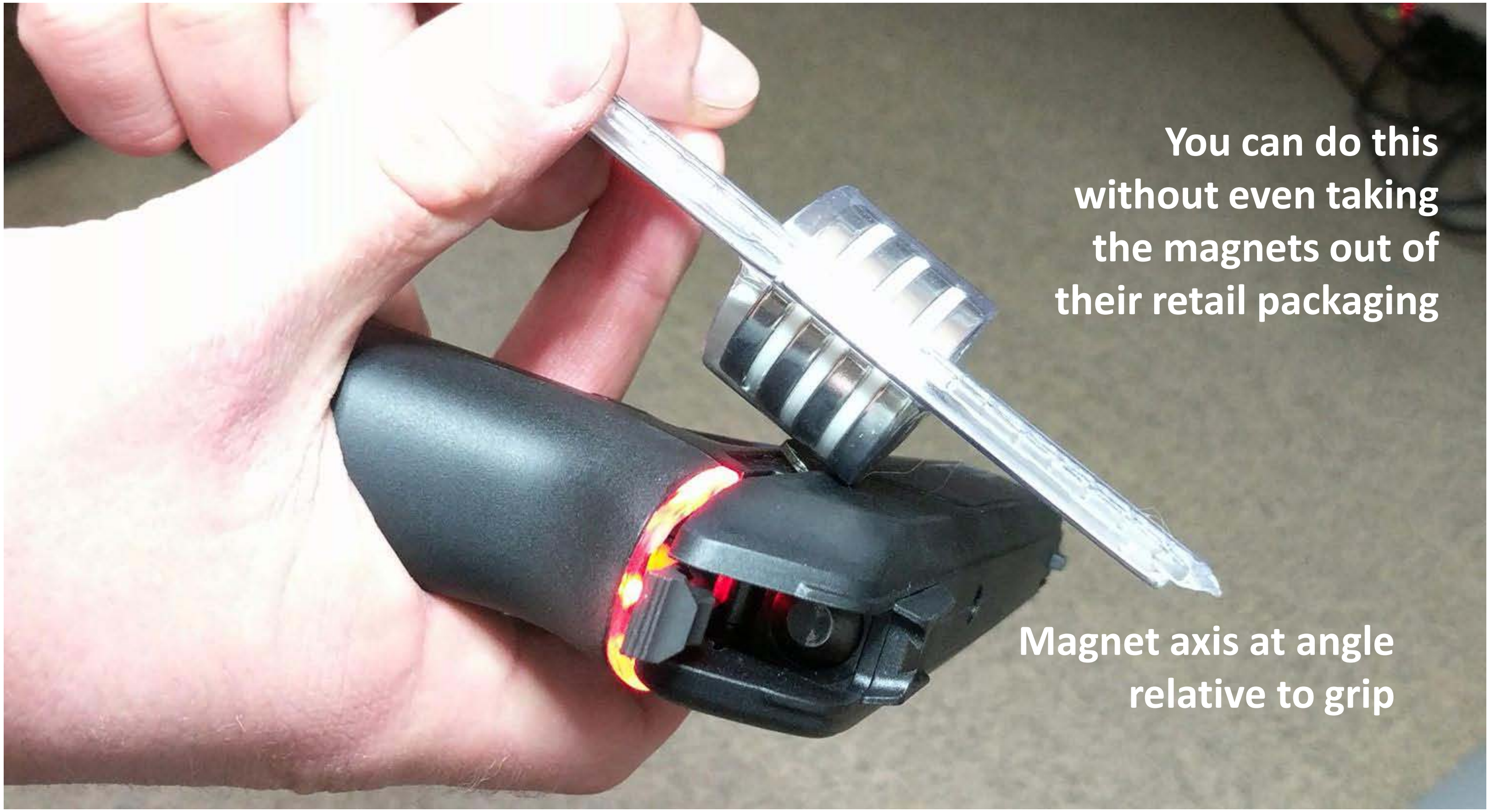


Electronic attack

- Impersonate watch?
- Replay attack?
  - Perhaps including forcing pistol/watch time to specific moment
- Some other exploit?
- Investigated, but then…

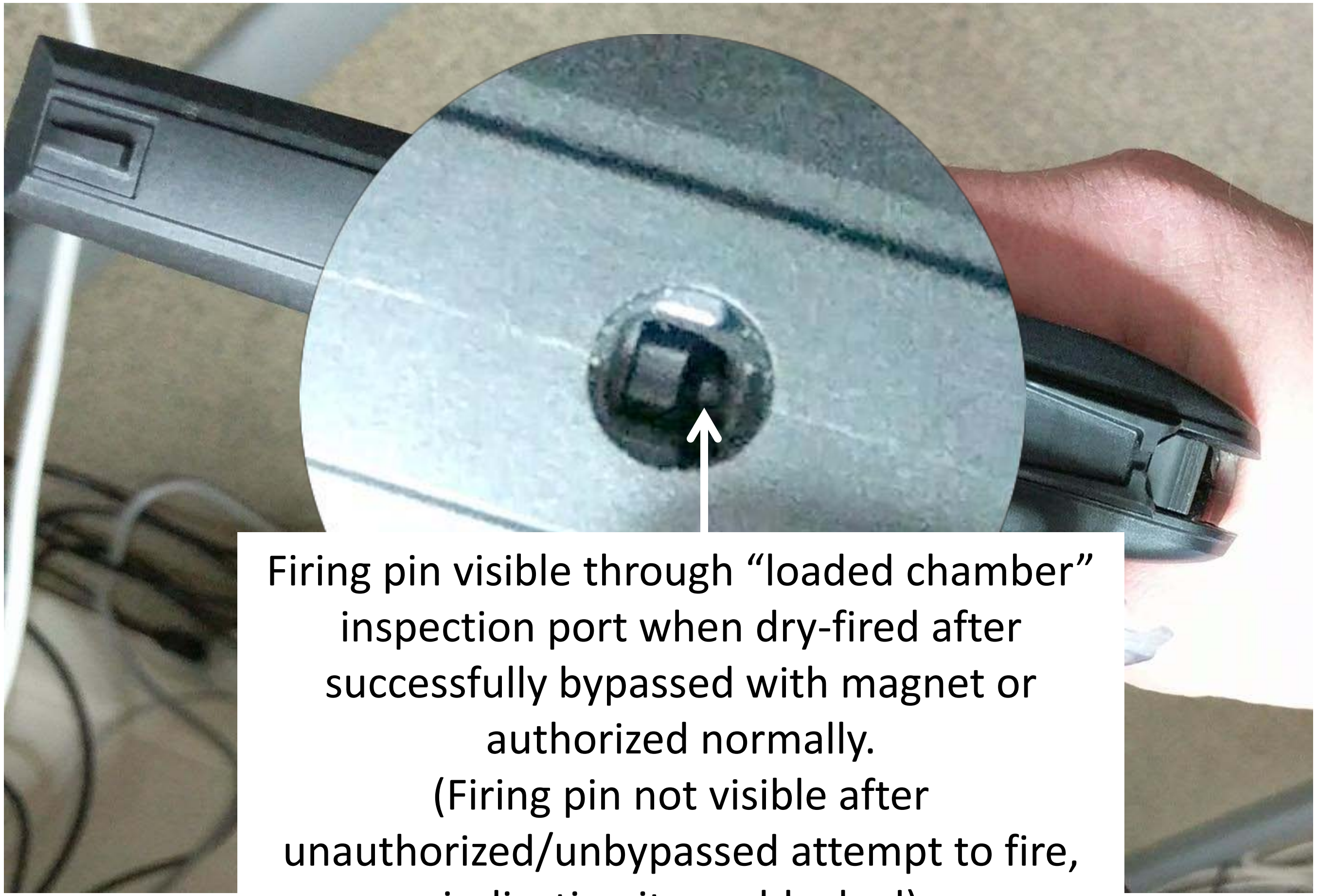
Mechanical operation

- 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



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

Magnet axis at angle relative to grip



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)

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