**FUNTENNA**

Noun:

1: Software payload that intentionally causes its host hardware to act as an improvised RF transmitter using existing hardware, which are typically not designed for electromagnetic emanation.

2: Software which intentionally causes compromising emanation.

---

Ang Cui, PhD
a@redballoonsecurity.com

8/10/15
Blackhat USA 2015
About me,

Columbia University
About me,

Columbia University

Red Balloon Security
1. Research presented in this talk not funded by any government sources or Columbia University.
Disclaimer

1. Research presented in this talk not funded by any government sources or Columbia University.

Disclaimer

1. Research presented in this talk not funded by any government sources or Columbia University.


3. I only pretend to know how electricity works.
You are doing real science when you are using...
You are doing **real science** when you are using...
You are doing **real science** when you are using...
You are doing **real science** when you are using...

Homemade dog whistle **detector** (in a cup)
You are doing **real science** when you are using...

**Anti-Radiation Shield Women Maternity Briefs Panties Protection Medium**

8900651M

Be the first to review this item

List Price: $99.98
Price: **$75.98** ✔Prime & Free Returns. Details
You Save: $24.00 (24%)

**Only 1 left in stock.**
Sold by OurSure and Fulfilled by Amazon. Gift-wrap available.

Want it Tuesday, Aug. 4? Order within **28 hrs 58 mins** and choose **One-Day Shipping** at checkout. Details

- 100% Silver-Nylon Blend
- 100% silver blend fabric provides super RF radiation shield efficiency up to 80 dB in the frequency range from 10 MHz to 3 GHz and beyond, let you take advantage to prevent your baby from RF radiation
- Silky feel, light stretch, comfort woman briefs offer full front and back coverage following the natural leg curve
- Breathable and comfortable

Roll over image to zoom in
Noun:
Noun:

1: Malware that intentionally causes compromising emanation.
Noun:

1: Malware that intentionally causes compromising emanation.

2: Software payload that intentionally causes its host hardware to act as an improvised RF transmitter using existing hardware, which are typically not designed for electromagnetic emanation.
xyz

thing

Laptop, Server,
Laptop, Server, Phone.
xyz

thing

laptop, server, phone, router, printer
Laptop, server, phone, router, printer, TV, car, building, etc
? + Fun tenta payload

xyz
thing
xyz thing + Funtenna payload (tiny malware)
xyz thing

all your secret info

☠ Hacker
Monitored
Transmission mediums

Receiver

Attacker

xyz

Thing

 LTE

 WiFi

 Bluetooth

?
Monitored
Transmission mediums

Attacker

xyz thing

8/10/15
Transmission medium of the attacker's choosing

xyz

Thing

Attacker

receiver
Transmission medium of the attacker's choosing

Where you *don't monitor*

xyz

thing

Attacker

receiver
Sub-acoustic

xyz
thing

8/10/15
Blackhat USA 2015
why?
Too Obvious =(

Super Secret Fort!
Super Secret Fort!
Anti-Super Secret Fort Technology
Anti-Super Secret Fort Technology

Amazing Ninja Tech
Anti-Super Secret Fort Technology

Intern
Anti: Super Secret Fort Technology

Amazing Ninja Tech

Intern

(Retro Reflector)

Implant
Anti-Super Secret Fort Technology

Intern + Implant

(Retro Reflector) + (Radar Illuminator)
Step 1: Intern sneaks into secret fort
Step 1: Intern sneaks into secret fort
Step 1: Intern sneaks into secret fort

Step 2: Intern physically implants target thing with retro-reflector
Step 1: Intern sneaks into secret fort

Step 2: Intern physically implants target thing with retro-reflector

Step 3: Continuous RF Illumination (CTX4k, etc) into secret fort
Step 1: Intern sneaks into secret fort

Step 2: Intern physically implants target thing with retro-reflector

Step 3: Continuous RF Illumination (CTX4k, etc) into secret fort, secret data comes out
Step 1: Intern sneaks into secret fort

Step 2: Intern physically implants target thing with retro-reflector

Step 3: Continuous RF Illumination (CTX4k, etc) into secret fort, secret data comes out
Good idea if...
Good idea if...

1: Infinite Interns
Good idea if...

1: Infinite Interns
2: Not worried about leaving evidence behind (see #1)
Retroreflector Technology
Retroreflector Technology

In Historical Context...
Retroreflector
In Historical Context...

Way back when...
Retroreflector

In Historical Context...

Phone

Designed for this
Retroreflector
In Historical Context...

Deployed in the age of this
Retroreflector
In Historical Context...

Designed for this
Retroreflector
In Historical Context...

Deployed in the age of this
The Difference?
The Difference?

~ 50 Million Transistors
The Difference?

~ 50 Million Transistors
~ 1 Million Lines of Code
The Difference?

~ 50 Million Transistors
~ 1 Million Lines of Code

All-purpose computing hardware
Inside special-purpose packaging
Leverage This Difference

~ 50 Million Transistors
~ 1 Million Lines of Code

All-purpose computing hardware
Inside special-purpose packaging

And...
"Emanate like a
Scrub
Boss!"
Leverage This Difference

And...

1. Exfilrate using only software
Leverage This Difference

And...

1. Exfiltrate using only software
2. Exfiltrate using all the things
Leverage This Difference

And...

1. Exfiltrate using only software
2. Exfiltrate using all the things
3. Exfiltrate using arbitrary frequency range
Leverage This Difference

1. Exfiltrate using only software
2. Exfiltrate using all the things
3. Exfiltrate using arbitrary frequency range

4. Evaporate when done
Part I

Compromising Emanations!
Part I

Compromising Emanations!

Part II

Firmware Shenanigans
PRIOR ART

Electromagnetic Eavesdropping Risks of Flat-Panel Displays

Markus G. Kuhn

University of Cambridge, Computer Laboratory,
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
http://www.cl.cam.ac.uk/~mgk25/
Fig. 4. Original and intercepted data signal at 7 m and 98 MHz (FM band).

The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables

Peter Smulders
Example: Acoustic Crypto-Analysis
Genkin, Shamir, Tromer

Figure 7: Acoustic measurement frequency spectrogram of a recording of different CPU operations using the Brüel&Kjær 4939 microphone capsule. The horizontal axis is frequency (0–310 kHz), the vertical axis is time (3.7 sec), and intensity is proportional to the instantaneous energy in that frequency band.

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis

Daniel Genkin
Technion and Tel Aviv University
danielg@cs.technion.ac.il

Adi Shamir
Weizmann Institute of Science
adi.shamir@weizmann.ac.il

Eran Tromer
Tel Aviv University
tromer@cs.tau.ac.il

8/10/15
Blackhat USA 2015
Example: Acoustic Crypto-Analysis
Genkin, Shamir, Tromer

4 Meters!

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*

Daniel Genkin
Technion and Tel Aviv University
danielg@cs.technion.ac.il

Adi Shamir
Weizmann Institute of Science
adi.shamir@weizmann.ac.il

Eran Tromer
Tel Aviv University
tromer@cs.tau.ac.il

December 18, 2013
Majority of Compromising Emanations Research
Majority of Compromising Emanations Research

Faint, accidentally Leaked signal
Majority of Compromising Emanations Research

Faint, accidentally
Leaked signal

Big powerful receiver
What if...

Faint, accidentally
Leaked signal

Big powerful receiver
What if...

Loud, intentionally generated compromising emanation

Big powerful receiver

8/10/15
Blackhat USA 2015
DEMO 1: Acoustic Funtenna Emanation

Sub 1kHz emanation
No, not like Alive humans
DEMO 1.5: Ultrasonic Funtenna Emanation

8/10/15  Blackhat USA 2015
DEMO 1.5: Ultrasonic Funtenna Emanation

~27 Khz

~42 Khz
Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

Markus G. Kuhn* and Ross J. Anderson

University of Cambridge, Computer Laboratory, New Museums Site, Pembroke Street, Cambridge CB2 3QG, United Kingdom
{mgk25,rja14}@cl.cam.ac.uk

Fig. 1. Example screen contents that cause the authors’ computer monitor to broadcast an $f_t = 300$ Hz (left) and $1200$ Hz tone (right) on an $f_c = 2.0$ MHz carrier in amplitude modulation.
Soft Tempest: Hidden Data Transmission
Using Electromagnetic Emanations

Markus G. Kuhn and Ross J. Anderson
Computer Laboratory

Conclusions

→ Interesting field of study, mostly unexplored in the open literature
Probably not a new idea

But not discussed "in the open"
A decade later...
BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations

Guri, Monitz, Mirski, Elovici

Distance: 40cm
Data Rate: 1-8 bits per hour

On Covert Acoustical Mesh Networks In Air
Hanspach & Goetz

Distance: 19.7 M
Data Rate: 20 bits per second

AirHopper: Bridging the Air-Gap Between Isolated Networks and Mobile Phones Using Radio Frequencies

Guri, Kedma, Kachlon, Elovici

Distance: 7 M
Data Rate: 60 bits per second
The next steps
The next steps

1. Generalize and Unify Methodology
The next steps

1. Generalize and Unify Methodology
2. Minimize hardware dependencies
Funtenna 101

XYZ

Thing
Funtenna 101

XYZ
Thing

P_{out}
Funtenna 101

\[ P_{out} : 010101010101 \]
Funtenna 101

P_{out}

XYZ Thing

???

→ Win!

(rf signal)

P_{out}: 0 1 0 1 0 1 0 1 0 1 0 1

...
E-lec-tron
\[ \nabla \times E = \frac{\partial B}{\partial t} \]
\[ \nabla \times H = \frac{\partial D}{\partial t} \]
\[ \nabla \cdot D = \rho \]
\[ \nabla \cdot B = 0 \]

Maxwell's Equations
Common Output Pins

- PWM (Pulse Width Modulation)
- GPIO (General Purpose Input Output)
- UART (Universal Asynchronous Receive Transmit)
Science!
Science!

For each

- PWM
- GPIO
- UART
Science!

For each

- PWM
- GPIO
- UART
Science!

For each

1. Possible values for $f$
2. Optimal values for $f$

- PWM
- GPIO
- UART
Science!

For each
- PWM
- GPIO
- UART

1. Possible values for $f$
2. Optimal values for $f$

For each radiator length
- 0cm
- 15cm
- 30cm
Experimental Setup

- "Faraday" Cage
- Buspirate (transmitter)
- USRP2 & BasicRX Board (receiver)
For example, 30cm radiator, \( f = 500\text{kHz} \), harmonic signal @ 2.5\text{mhz}
Full raw dataset available at www.funtenna.org
Data Analysis...

Possible values for $f$

Optimal values for $f$

Optimal length of radiator
Data Analysis...

Optimal length of radiator

Anything $> 0$, longer better...
Data Analysis...

Possible values for $f$

- **PWM**: 10kHz - 4MHz
- **GPIO**: 10kHz - 5MHz
- **UART**: 10kHz - 4MHz
Data Analysis...

Possible values for $f$

- **PWM**: 10kHz – 4MHz
- **GPIO**: 10kHz – 5MHz
- **UART**: 10kHz – 4MHz

Optimal values for $f$

- **120MHz – 205MHz**
Figure 2. Diagram of Building 12500 at the A-15A Site on Elgin Air Force Base.
Measurement of RF Propagation into Concrete Structures 
over the Frequency Range 100 MHZ to 3 GHz

by

Clayborne D. Taylor
Samuel J. Gutierrez
Steven L. Langdon
Kenneth L. Murphy
William A. Walton, III

Phillips Laboratory/WSM
3550 Aberdeen Ave. SE
Kirtland AFB, NM 87117-5776

ISBN 9781461378617
Say you wanted to Funtenna out of a 2-ft reinforced concrete structure
Say you wanted to Funtenna out of a 2-ft reinforced concrete structure.

structures. For two-feet thick concrete walls, the measured attenuation above 200 MHz appears to increase with an increase in frequency. And for frequencies near and below 100 MHz, rebar attenuation becomes significant and seems to affect the magnetic field more than the electric field penetration. In the frequency range between 120 and 205 MHz the attenuation is often less than 20 dB. For four-inch and eight-inch thick walls the attenuation is much less (see Table 3).

\[
\begin{align*}
F \leq 100\text{MHz}, & \text{ bad for magnetic field penetration} \\
F \geq 200\text{MHz}, & \text{ bad for electric field penetration}
\end{align*}
\]

Figure 4. The internal magnetic field \((B)\) at measurement point B relative to the incident magnetic field for illumination source point X.

Figure 5. The internal electric field \((E)\) at measurement point B relative to the incident electric field for illuminating source point X.
Generalized Funtenna Algorithm
Generalized Funtenna Algorithm

\[ P_{out} \]

\[ P_{out} \rightarrow 1 \]
\[ \text{Delay (\( \Delta t \))} \]
\[ P_{out} \rightarrow \% \]
\[ \text{Delay (\( \Delta t \))} \]
Generalized Funtenna Algorithm

\[ P_{out} \rightarrow 1 \]
\[ \text{Delay}(\Delta t) \]
\[ P_{out} \rightarrow 0 \]
\[ \text{Delay}(\Delta t) \]

\( P_{out} \)
Generalized Funtenna Algorithm

\[ P_{out} \rightarrow 1 \]
\[ \text{Delay}(d_1) \]
\[ P_{out} \rightarrow 2 \]
\[ \text{Delay}(d_2) \]

\[ f = X \]
Generalized Funtenna Algorithm

\[
\text{Do } \text{Symbol Times}
\]

\[
P_{\text{out}} \rightarrow 1 \\
\text{Delay}(d_1)
\]

\[
P_{\text{out}} \rightarrow 0 \\
\text{Delay}(d_2)
\]

\[f = x\]
Generalized Funtenna Algorithm

- ASK (Amplitude Shift Keying)
- FSK (Frequency Shift Keying)
- OOK (On-Off Keying)
Generalized Funtenna Algorithm
Amplitude-Shift Keying
Generalized Funtenna Algorithm
Amplitude-Shift Keying
Generalized Funtenna Algorithm
Amplitude-Shift Keying
Generalized Funtenna Algorithm
Frequency-Shift Keying (sort of)
Generalized Funtenna Algorithm
Frequency-Shift Keying (sort of)
Generalized Funtenna Algorithm
On-Off Keying
Generalized Funtenna Algorithm
On-Off Keying
Generalized Funtenna Algorithm
On-Off Keying
Funtenna In Practice
### Funtenna In Practice

![Pantum P2502W Wireless Monochrome Laser Printer](image)

<table>
<thead>
<tr>
<th>Store</th>
<th>Price Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Newegg.com</td>
<td>Free shipping, no tax</td>
<td>$39.99</td>
</tr>
<tr>
<td>eBay</td>
<td>Free shipping, no tax</td>
<td>$53.00</td>
</tr>
</tbody>
</table>

View all stores and prices »
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

1. Cheap
2. Typical ARM SoC
3. GPIO (lots)
4. PWM
5. UART
6. JTAG
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

The Controller Board
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

The SoC

Marvell 88PA6110
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

Hardware Triage
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

Hardware Triage
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

Hardware Triage
Funtenna In Practice (PWM)

Pantum P2502W Wireless Monochrome Laser Printer

13Khz PWM
Funtenna In Practice (PWM)

Pantum P2502W Wireless Monochrome Laser Printer

13Khz PWM

No love -(
Funtenna In Practice (GPIO)

4 GPIO Banks, 121 pins in all
Funtenna In Practice (GPIO)

Input pins: Buttons, few sensors, switches
Funtenna In Practice (GPIO)

Output pins: LEDs, Engine Control, Power Control, Fuser Control, Toner Control and lots more!
Funtenna In Practice (GPIO)

Which pin to flip?
"Emanate like a
Scrub
Boss!"
Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!
Funtenna In Practice (GPIO)

Which pin to flip? **Every pin, at the same time!**

<table>
<thead>
<tr>
<th>Pin</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x20</td>
<td>Pin OFF</td>
</tr>
<tr>
<td>0x24</td>
<td>Pin ON</td>
</tr>
</tbody>
</table>

GPIO Bank A – Memory Mapped Control Registers
Funtenna In Practice (GPIO)

```assembly
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020

.loopy:
  LDR  R5, =all_p1mp
  LDR  R1, =gpio_bank_a_off_addr
  LDR  R2, =gpio_bank_b_off_addr
  LDR  R3, =gpio_bank_c_off_addr
  LDR  R4, =gpio_bank_d_off_addr
```
Funtenna In Practice (GPIO)

All Pins on
Funtenna In Practice (GPIO)

```assembly
.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020

.loopy:
    LDR   R5, =all_p1mp
    LDR   R1, =gpio_bank_a_off_addr
    LDR   R2, =gpio_bank_b_off_addr
    LDR   R3, =gpio_bank_c_off_addr
    LDR   R4, =gpio_bank_d_off_addr

    STR   R5, [R1, #0x4]
    STR   R5, [R2, #0x4]
    STR   R5, [R3, #0x4]
    STR   R5, [R4, #0x4]
```

All Pins off
Funtenna In Practice (GPIO)

.equ all_p1mp, 0xffffffff
.equ gpio_bank_a_off_addr, 0xFD040020
.equ gpio_bank_b_off_addr, 0xF8040020
.equ gpio_bank_c_off_addr, 0xF8041020
.equ gpio_bank_d_off_addr, 0xF8042020

.loopy:
    LDR   R5, =all_p1mp
    LDR   R1, =gpio_bank_a_off_addr
    LDR   R2, =gpio_bank_b_off_addr
    LDR   R3, =gpio_bank_c_off_addr
    LDR   R4, =gpio_bank_d_off_addr

    STR   R5, [R1, #0x4]
    STR   R5, [R2, #0x4]
    STR   R5, [R3, #0x4]
    STR   R5, [R4, #0x4]

    All Pins on
Funtenna In Practice (GPIO)

All Pins on

F = Approx 5MHz
Funtenna In Practice (GPIO)

\[ F = \text{Approx } 5\text{mhz} \]

And things get really interesting
Funtenna In Practice

Funtenna Demo 2: ALL GPIO Funtenna - On Off Keying
Funtenna Demo 2: ALL GPIO Funtenna - On Off Keying

on_off_recording.ogv
Funtenna In Practice

Funtenna Demo 2: ALL GPIO Funtenna - Freq Shift Keying (sort of)
Funtenna Demo 2: ALL GPIO Funtenna – Freq Shift Keying (sort of)
Funtenna In Practice

Pantum P2502W Wireless Monochrome Laser Printer

UART Funtenna
UART Funtenna 460800 baud

“UUUUUUUUUUUUUUU”
UART Funtenna 460800 baud

```
172.17.0.61 # stty -F /dev/ttyAMA1 460800
172.17.0.61 # perl /home/craft/yakyak.pl > /dev/ttyAMA1
```

Frequency Spectrum Analysis

- **Vertical Scale**
  - Linear
  - Set Max Scale
  - Logarithmic

- **FFT Source**
  - Channel A
  - Channel B

- **FFT Window**
  - Rectangular
  - Hamming
  - Hann
  - Triangular

**Sampling Rate**
- 5.0 MS/s

**Number of Samples**
- 1024.0

8/10/15 Blackhat USA 2015
Funtenna In Practice

Let's be more sneaky...
Funtenna In Practice

```
LDR R3, =asc_1121944 ; "/home/lihaixiong/source/common/devices/"
BL sub_49F668
MOV R3, R0
MOV R2, R3
LDR R3, =dword_EC63
STR R2, [R3]
```

```
asc_1121944 DCB "/home/lihaixiong/source/common/dev"
DCB "ices/uart/dwapb/src/dw_apb_uart.c", 0
```

dw_apb_uart.c
Funtenna In Practice

DesignWare DW_apb_uart Databook

DesignWare Synthesizable Components for AMBA 2
  DW_apb_uart

8/10/15  Blackhat USA 2015
**Funtenna In Practice**

[Diagram of Funtenna In Practice]

**FLIP sout pin**
Step 1: UART Break-Ctrl Bit → 1

**LCR**
- Name: Line Control Register
- Size: 32 bits
- Address Offset: 0x0C
- Read/write access: read/write

<table>
<thead>
<tr>
<th></th>
<th>Break (or BC)</th>
<th>R/W</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Break (or BC)</td>
<td>R/W</td>
<td>Break Control Bit. This is used to cause a break condition to be transmitted to the receiving device. If set to one the serial output is forced to the spacing (logic 0) state. When not in Loopback Mode, as determined by MCR[4], the serial output is forced low until the Break bit is cleared. If SIR_MODE is enabled and active (MCR[6] set to one) the sir_out_n line is continuously pulsed. When in Loopback Mode, the break condition is internally looped back to the receiver and the sir_out_n line is forced low.</td>
</tr>
</tbody>
</table>

**FLIP sout pin**
Step 2: UART Loopback bit -> 1

### MCR
- **Name**: Modem Control Register
- **Size**: 32 bits
- **Address Offset**: 0x10
- **Read/write access**: read/write

<table>
<thead>
<tr>
<th></th>
<th>LoopBack (or LB)</th>
<th>R/W</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>LoopBack</td>
<td>R/W</td>
<td>LoopBack Bit. This is used to put the UART into a diagnostic mode for test purposes. If operating in UART mode (SIR_MODE != Enabled or not active, MCR[6] set to zero), data on the <strong>sout</strong> line is held high, while serial data output is looped back to the <strong>sin</strong> line, internally. In this mode all the interrupts are fully functional. Also, in loopback mode, the modem control inputs (dsr_n, cis_n, ri_n, dcd_n) are disconnected and the modem control outputs (dtr_n, rts_n, out1_n, out2_n) are looped back to the inputs, internally. If operating in infrared mode (SIR_MODE == Enabled AND active, MCR[6] set to one), data on the <strong>sir_out</strong> line is held low, while serial data output is inverted and looped back to the <strong>sir_in</strong> line. <strong>Reset Value</strong>: 0x0</td>
</tr>
</tbody>
</table>

**FLIP sout pin**
Step 3: UART Loopback bit -> 0

MCR
- Name: Modem Control Register
- Size: 32 bits
- Address Offset: 0x10
- Read/write access: read/write

<table>
<thead>
<tr>
<th>LoopBack (or LB)</th>
<th>R/W</th>
<th>LoopBack Bit. This is used to put the UART into a diagnostic mode for test purposes. If operating in UART mode (SIR_MODE != Enabled or not active, MCR[6] set to zero), data on the sout line is held high, while serial data output is looped back to the sin line, internally. In this mode all the interrupts are fully functional. Also, in loopback mode, the modem control inputs (dsr_n, cts_n, ri_n, dcd_n) are disconnected and the modem control outputs (dtr_n, rts_n, out1_n, out2_n) are looped back to the inputs, internally. If operating in infrared mode (SIR_MODE == Enabled AND active, MCR[6] set to one), data on the sir_out_n line is held low, while serial data output is inverted and looped back to the sir_in line. Reset Value: 0x0</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Funteenna In Practice (UART)

```assembly
.equ uart_conf_reg, 0xFD060000

@ set BREAK bit to force SOUT to low
MOV   R1, #0x43
LDR   R2, =uart_conf_reg
STR   R1, [R2, #0xc]
MOV   R1, #0x23
MOV   R3, #0x33

STR   R1, [R2, #0x10]

Uart_sout -> 1
```
Funtenna In Practice (UART)

```asm
.equ uart_conf_reg, 0xFD060000

@ set BREAK bit to force SOUT to low
MOV   R1, #0x43
LDR   R2, =uart_conf_reg
STR   R1, [R2, #0xc]
MOV   R1, #0x23
MOV   R3, #0x33
```

Uart_sout -> 1

Uart_sout -> 0
Funenna In Practice (UART)

equ uart_conf_reg, 0xFD060000

@ set BREAK bit to force SOUT to low
MOV R1, #0x43
LDR R2, =uart_conf_reg
STR R1, [R2, #0xc]
MOV R1, #0x23
MOV R3, #0x33

Uart_sout -> 1
Uart_sout -> 0
Funtenna In Practice (UART)

```
equ uart_conf_reg, 0xFD060000
@ set BREAK bit to force SOUT to low
MOV R1, #0x43
LDR R2, =uart_conf_reg
STR R1, [R2, #0xc]
MOV R1, #0x23
MOV R3, #0x33
```

\[ F = \text{Approx} \ 500\text{kHz} \]

Uart_sout -> 1

Uart_sout -> 0

8/10/15

Blackhat USA 2015
Funtenna In Practice

Funtenna Demo 2: UART, On Off Keying

UART Pin, 10 feet of console cable
Funtenna Demo 2: UART FUNTENNA DEMOD
Take Away

• Funtenna works

• Network IDS is no substitute for host-based defense

• Host-based embedded defense important!
Big Thanks!

Chris Evans
Big Thanks!

Joseph Pantoga
Big Thanks!

Kang-Wei Chang

8/10/15  Blackhat USA 2015
Ang Cui, PhD
a@redballoonsecurity.com
Backup slides
Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Memory Mapped Registers

0x1600D58 <- Contains GPIO Bank & Register List

GPIO bank A - 0x1600DA8 MEMREG 0xFD040000
GPIO bank B - 0x16011B8 MEMREG 0xF8040000
GPIO bank C - 0x16015C8 MEMREG 0xF8041000
GPIO bank D - 0x16019D8 MEMREG 0xF8042000
Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Memory Mapped Registers

0x1600D58 <- Contains GPIO Bank & Register List

GPIO bank A - 0x1600DA8 MEMREG 0xFD040000
GPIO bank B - 0x16011B8 MEMREG 0xF8040000
GPIO bank C - 0x16015C8 MEMREG 0xF8041000
GPIO bank D - 0x16019D8 MEMREG 0xF8042000
Funtenna In Practice (GPIO)

Which pin to flip? Every pin, at the same time!

Memory Mapped Registers

0x1600D58 <- Contains GPIO Bank & Register List

GPIO bank A - 0x1600DA8 MEMREG 0xFD040000
GPIO bank B - 0x16011B8 MEMREG 0xF8040000
GPIO bank C - 0x16015C8 MEMREG 0xF8041000
GPIO bank D - 0x16019D8 MEMREG 0xF8042000

GPIO Bank A