Zero to Zero-Day

Who am I?

Shane Wilton

Grand Magistrate of Security

Palo Alto, California | Security and Investigations

Current Tinfoil Security

Top Skills

28 Sarcasm

TINFOIL SECURITY

TL;DR I Hack Shit

Q: What's the difference between a CTF and a hackathon?

A: I've never been arrested because of a hackathon.

TINFOIL SECURITY

Jeopardy Style CTF

- Multiple, discrete categories
  - Reverse Engineering
  - Cryptography
  - Binary Exploitation
  - Web Exploitation
  - Forensics
  - Programming

- 2 days to solve as many problems as possible
  - Basically a hackathon, with hacking!

TINFOIL SECURITY

Attack/Defense CTF

- Each team is given a server
- Each team is given vulnerable services
- Gain points by hacking the other teams
- Lose points by getting hacked
- The only rule is don’t get caught.

TINFOIL SECURITY

Why?

- You'll learn a little bit of absolutely everything
  - Decoding QR codes by hand? Check!
  - Cracking passwords with a fleet of super computers? You betcha!
  - Reverse engineering the bytecode for a distributed Erlang app? Absolutely.

- It'll make you a better engineer
  - **Only** legal way to get offensive security experience
  - You'll write more secure code, with fewer bugs

- It's fun!

TINFOIL SECURITY

Getting Started

- You're going to suck, and that's okay!
  - The sooner you realize this, the sooner you'll stop sucking
- Join your school's team
  - Better yet... start your school's team!
- Upcoming CTFs are listed on https://ctftime.org/
  - CSAW on September 18th (Students only. The BEST for beginners)
  - Hitcon on October 17th (My favourite)
- Read write-ups for EVERYTHING you don't solve

TINFOIL SECURITY

Getting Practice

- Exploit Development
  - MicroCorruption
  - pwnable.kr
  - Smash The Stack
- Cryptography
  - Crypto Pals (Matasano Crypto Challenges)
- Reverse Engineering
  - crackmes.de

TINFOIL SECURITY

Polyglot (Hitcon 2014)

- Write a program that outputs the contents of the file “flag”
- Must be a valid program in…
  - Python 2.7
  - Python 3.4
  - C
  - Ruby
  - Haskell

TINFOIL SECURITY

Homework

- Write a Ruby program that outputs “Hack the planet!”
- You’re only allowed to use letters, spaces, and newlines
- Bonus credit: write a program that reads in a Ruby program, and outputs an equivalent program that meets the above criteria
- Remember: there’s no such thing as cheating
- First 3 solutions get Tinfoil t-shirts!
  - Send them to mhacks@tinfoilsecurity.com

TINFOIL SECURITY

Pwnadventure 3

- A CTF that was a fully playable MMORPG

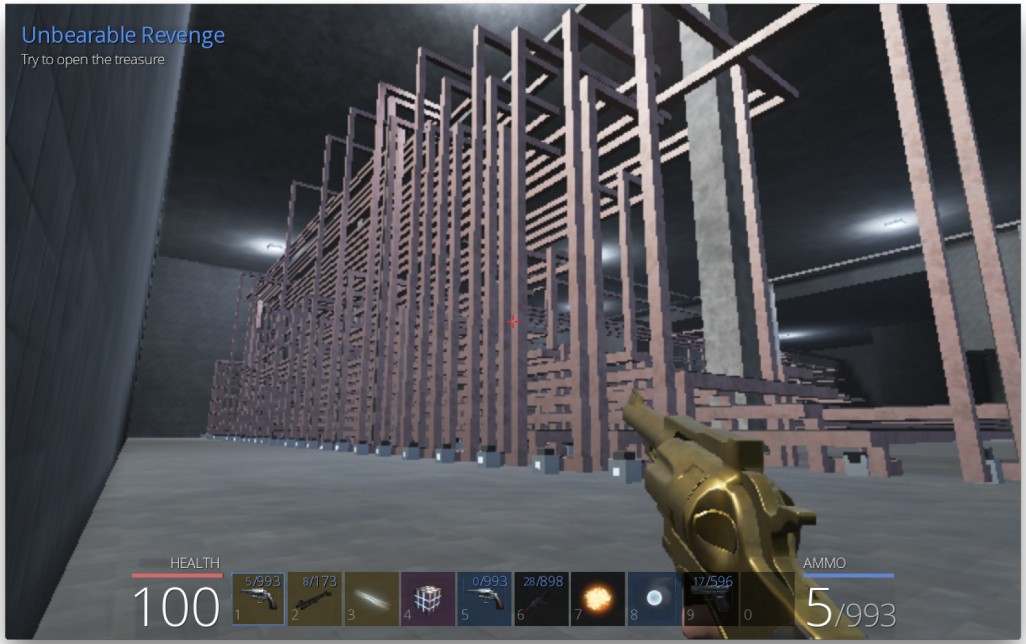
- Every quest required that you hack the game
  - Wallhacks to find secrets
  - Teleporting to escape bears with machine guns (Seriously.)
  - Maphacks to find the secret cow level (Again, seriously.)

- Most of my team had never hacked a game before
  - We tied for 1st
  - Not knowing how to do something isn't an excuse

Blocky’s Revenge

TINFOIL SECURITY

Blocky’s Revenge



TINFOIL SECURITY

	Switches		Row 1			Row 2			Row 3			Row 4			Row 5			Row 6			Row 7			Row 8			Row 9			Row 10			Row 11			Row 12		
	1	Off	1	Not	On	1	Not	On	1	Xor	Off	1	Or	On	1	Xor	On	1	Not	Off	1	Xor	On	1	Not	Off	1	Xor	On	1	Or	On	1	Xor	Off	1	Not	On
	2	Off	2	Not	On	2	And	On	2	Or	On	2	Or	On	2	And	Off	2	Or	On	2	Or	On	2	Or	On	2	Or	Off	2	Or	On	2	And	On	2	Or	On
	3	Off	3	Not	On	3	Xor	Off	3	And	Off										3	And	Off				3	And	Off								
	4	Off	4	Not	On	4	Xor	Off																														
	5	Off	5	Not	On	5	And	Off																														
	6	Off	6	Not	On	6	Xor	On	Row 13			Row 14			Row 15			Row 16			Row 17			Row 18			Row 19			Row 20			Row 21			Row 22		
	7	Off	7	Not	On	7	Xor	Off	1	Xor	On	1	Or	On	1	Xor	On	1	Not	Off	1	Xor	On	1	Or	On	1	Xor	On	1	Not	Off	1	Xor	Off	1	Not	On
	8	Off	8	Not	On	8	Xor	Off	2	Or	On	2	Or	On	2	And	Off	2	Or	On	2	Or	On	2	Or	Off	2	And	Off	2	Or	Off	2	Or	Off	2	Or	Off
	9	Off	9	And	Off	9	Xor	On	3	And	Off										3	And	Off									3	And	Off			
	10	Off	10	Not	On	10	Xor	Off																														
	11	**Off**	11	Xor	Off	11	Xor	Off	Row 23			Row 24			Row 25			Row 26			Row 27			Row 28			Row 29			Row 30			Row 31			Row 32		
	12	Off	12	Not	On	12	Xor	Off	1	Or	On	1	Or	Off	1	And	Off	1	Or	Off	1	And	Off	1	Or	Off	1	And	Off	1	Or	On	1	Xor	On	1	Not	Off
	13	**Off**	13	Not	On	13	Xor	Off	2	And	Off	2	Not	Off	2	Xor	Off	2	Not	On	2	Xor	Off	2	Or	On	2	Xor	Off	2	Not	On	2	Or	On	2	Or	On
	14	Off	14	Not	On	14	And	On	3	Xor	On										3	Or	On	3	Or	On											On
Entrance	15	Off	15	And	Off	15	And	On			On												On			Off											On
	16	Off	16	Not	On	16	And	On			Off												On			On											On
	17	Off	17	Not	On	17	And	On																		On											
	18	Off	18	Not	On	18	And	Off																														
	19	Off	19	And	Off	19	And	On	Row 33			Row 34			Row 35			Row 36			Row 37			Row 38			Row 39			Row 40								
	20	Off	20	Xor	Off	20	And	On	1	Or	Off	1	Or	On	1	Or	On	1	Or	On	1	Or	On	1	Or	On	1	Or	On	1	Not	Off						
	21	Off	21	Not	On	21	And	Off						On			On			On			On			On			On								
	22	Off	22	Xor	Off	22	Xor	On						Off			On			Off			On			On			Off								
	23	Off	23	Not	On									On			On			On			On			On			On								
	24	Off	24	Xor	Off																																
	25	Off	25	Xor	Off																																
	26	Off	26	Not	On																																
	27	Off	27	Not	On																																
	28	Off	28	Not	On																																
	29	Off	29	Not	On																																
	30	Off	30	Not	On																																
	31	Off	31	Not	On																																
	32	Off	32	Not	On																																
			33	Not	On																																
			34	Not	On																																
			35	Not	On																																
			36	Not	On																																
			37	Not	On																																
			38	Not	On																																
			39	And	Off																																
			40	Not	On																																
			41	And	Off																																
			42	Not	On																																

DOOR CLOSED

How do you solve this properly?

Ideas...

- We have a boolean equation
  - 1 => the door opens
  - 0 => the door closes

- How do we make it 1?

- This is a boolean satisfiability problem!

- Example: $a \vee b \wedge c = 1$
  - Solutions are (1, 0, 0), (1, 0, 1), (1, 1, 1), (0, 1, 1)

TINFOIL SECURITY

Enter Z3

- Theorem prover developed by Microsoft Research
- Uses a flavor of Lisp to encode theorems
- Produces either a proof, or a counter-example to those theorems
- Available online

```
1  (declare-const a Bool)
2  (declare-const b Bool)
3  (declare-const c Bool)
4
5  (define-fun f () Bool (or a (and b c)))
6
7  (assert f)
8
9  (check-sat)
10 (get-model)
```

```
sat
(model
  (define-fun a () Bool
    true)
  (define-fun c () Bool
    true)
  (define-fun b () Bool
    false)
)
```

TINFOIL SECURITY

Back to Blocky's Revenge...

```
(declare-const c2 Bool)
(declare-const c3 Bool)
(declare-const c4 Bool)
(declare-const c5 Bool)
(declare-const c6 Bool)
(declare-const c7 Bool)
(declare-const c8 Bool)
(declare-const c9 Bool)
(declare-const c10 Bool)
(declare-const c11 Bool)
(declare-const c12 Bool)
(declare-const c13 Bool)
(declare-const c14 Bool)
(declare-const c15 Bool)
(declare-const c16 Bool)
(declare-const c17 Bool)
(declare-const c18 Bool)
(declare-const c19 Bool)
(declare-const c20 Bool)
(declare-const c21 Bool)
(declare-const c22 Bool)
(declare-const c23 Bool)
(declare-const c24 Bool)
(declare-const c25 Bool)
(declare-const c26 Bool)
(declare-const c27 Bool)
(declare-const c28 Bool)
(declare-const c29 Bool)
(declare-const c30 Bool)
(declare-const c31 Bool)
(declare-const c32 Bool)
(declare-const c33 Bool)
```

```
(define-fun f2 () Bool (not c18))
(define-fun f3 () Bool (not c20))
(define-fun f4 () Bool (not c4))
(define-fun f5 () Bool (not c22))
(define-fun f6 () Bool (not c6))
(define-fun f7 () Bool (not c24))
(define-fun f8 () Bool (not c26))
(define-fun f9 () Bool (not c10))
(define-fun f10 () Bool (and c7 c26))
(define-fun f11 () Bool (not c28))
(define-fun f12 () Bool (xor c7 c27))
(define-fun f13 () Bool (not c8))
(define-fun f14 () Bool (not c27))
(define-fun f15 () Bool (not c30))
(define-fun f16 () Bool (and c10 c29))
(define-fun f17 () Bool (not c9))
(define-fun f18 () Bool (not c28))
(define-fun f19 () Bool (not c14))
(define-fun f20 () Bool (and c11 c30))
(define-fun f21 () Bool (xor c10 c29))
(define-fun f22 () Bool (not c32))
(define-fun f23 () Bool (xor c11 c30))
(define-fun f24 () Bool (not c16))
(define-fun f25 () Bool (xor c13 c32))
(define-fun f26 () Bool (xor c15 c18))
(define-fun f27 () Bool (not c6))
(define-fun f28 () Bool (not c25))
(define-fun f29 () Bool (not c5))
(define-fun f30 () Bool (not c24))
(define-fun f31 () Bool (not c4))
(define-fun f32 () Bool (not c23))
(define-fun f33 () Bool (not c3))
(define-fun f34 () Bool (not c22))
(define-fun f35 () Bool (not c2))
(define-fun f36 () Bool (not c17))
```

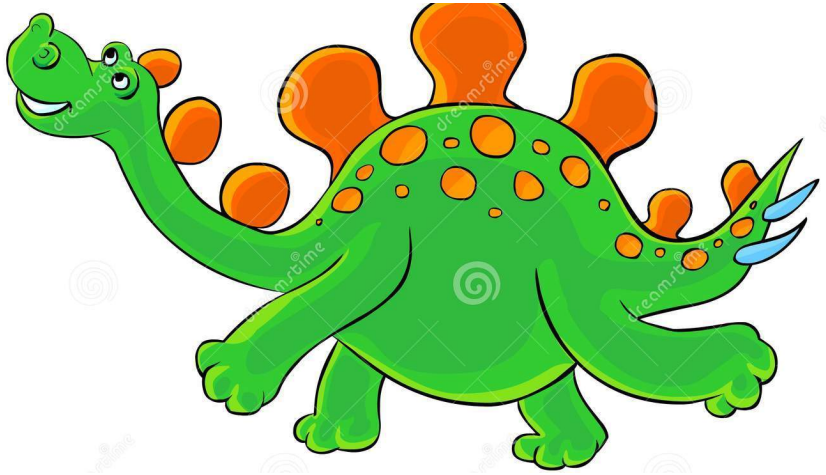
blah blah blah blah blah blah
blah blah blah blah blah blah
blah blah blah blah blah blah
blah blah blah blah blah blah
blah blah blah blah blah blah
blah blah blah blah blah blah

Full write-up online

TINFOIL SECURITY

Let’s do some steganography!

- Encryption is about restricting access to secret information
- Steganography is about hiding the presence of secret information
- Data hidden in…
  - images
  - sounds
  - PDFs
  - etc

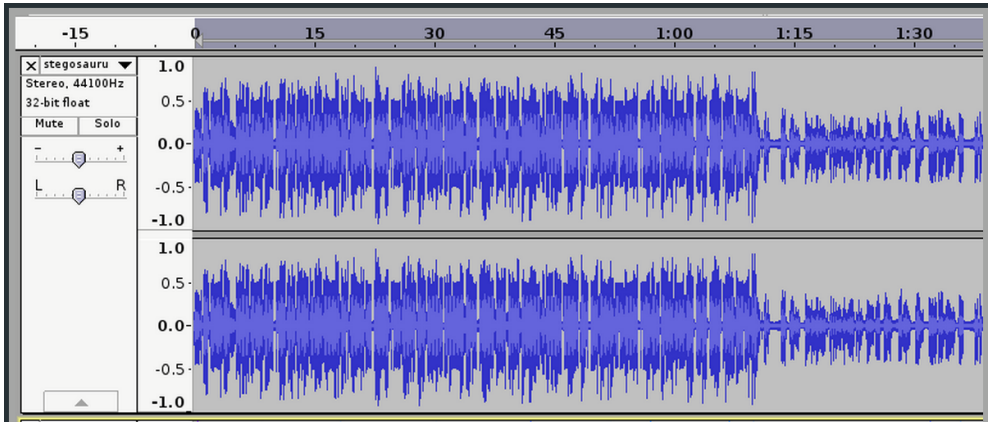


TINFOIL SECURITY

STEGOsaurus (NCN CTF 2014)

- 3 minute MP3
  - Just a recording of “The Hacker’s Manifesto”

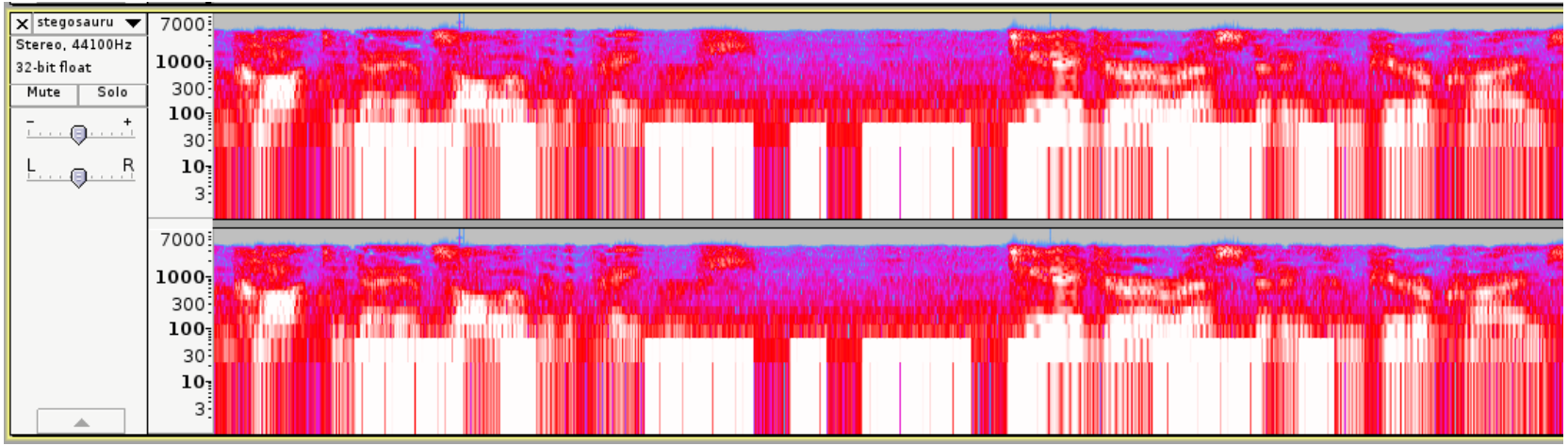
- Let’s open it in Audacity



TINFOIL SECURITY

STEGOsaurus (NCN CTF 2014)

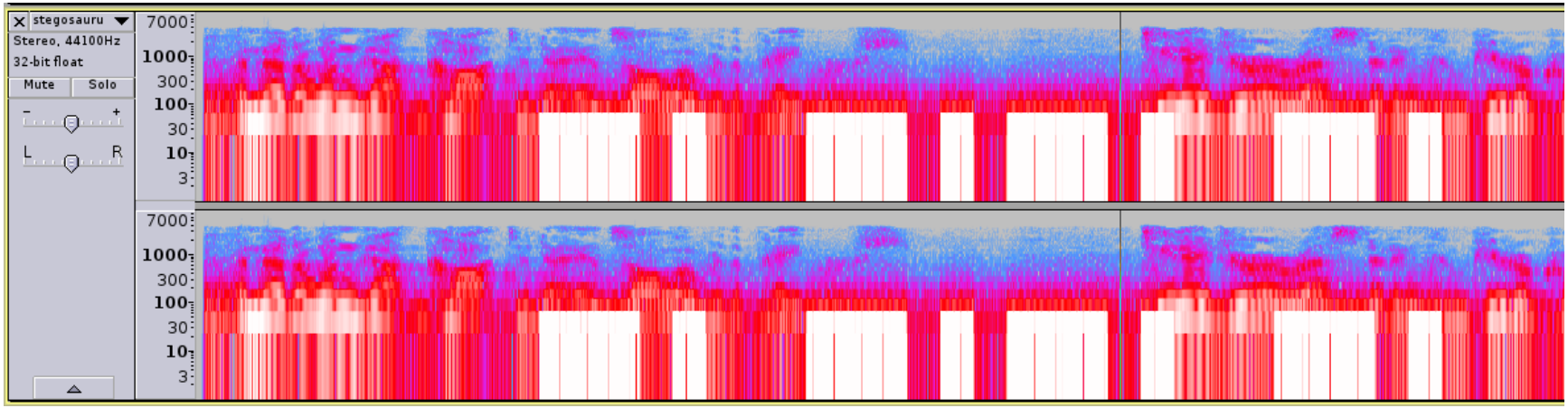
- Switching to spectrogram view...



TINFOIL SECURITY

STEGOsaurus (NCN CTF 2014)

- Run a low pass filter over it (at 100 Hz)



TINFOIL SECURITY

Notice anything?

STEGOsaurus (NCN CTF 2014)

- Morse code!
- Transcribe it to ascii
  - NCN3cbfdcc8d7a257d8062560e88dd7d7fd65dc647a
- You win.

TINFOIL SECURITY

Essential Tooling

- Wireshark
  - But watch out for 0days!
- IDA Pro
  - OllyDBG / Hopper are cheap alternatives
- Binjitsu / Pwntools
  - Python framework for exploit development

TINFOIL SECURITY

Meet Geohot

TINFOIL SECURITY

There's No Such Thing as Cheating

- NoNameYet (DEFCON Qualifiers 2014)
  - Part 1 - trivial web exploitation
  - Part 2 - complicated exploit in an image processing library

- The organizers left ~/.bash_aliases world writeable (accidentally!)
  - Geohot backdoored the service
  - Later, another team triggered his backdoor, and he won

- What other sports call cheating, CTF calls clever

TINFOIL SECURITY

Apple CTF

- Apple is hosting a CTF **right now** (until 11:30)
  - GG Brown 1571
  - Cool prizes, great practice.

- All web exploitation problems
  - SQL injection
  - XSS injection
  - CSRF (Cross-Site Request Forgery)
  - OWASP cheat sheet

TINFOIL SECURITY

Find the bug!

```
String sql = "SELECT id FROM users" +
  " WHERE username='" + request.getParameter("name") + "'" +
  "   AND password='" + request.getParameter("password") + "'" +
  " LIMIT 1";
```

TINFOIL SECURITY

Find the bug!

```
String sql = "SELECT id FROM users" +
  " WHERE username='Donald Trump'" +
  "   AND password='' OR id=1 --'" +
  " LIMIT 1";
```

TINFOIL SECURITY

Thanks!

- Contact us if you win the Apple CTF!
  - 6 months of free Tinfoil Security
  - mhacks@tinfoilsecurity.com

- I'm here all night
  - Happy to help audit your hackathon project
  - Wanna talk cryptography? I love cryptography.

- Reach out to me if you start playing CTF
  - shane@tinfoilsecurity.com
  - I love getting new players involved!

TINFOIL SECURITY

Happy Hacking!