Level 0x0d

Keeping Secrets

Topics

- CQ Recap
- Hacking History
- Bugs

Upcoming Events

LOCKHEED MARTIN CYBERQUEST® COMPETITION

- Lockheed Martin Cyber Quest
  - Saturday, March 23rd
  - 3 hours. Free Breakfast and Lunch
  - Teams are 3-5 students
    - 3 laptops per team
  - No team limit given
  - Registration Timeframe:
    - Wed Jan 03 2024 - Mon Feb 26 2024
- Pico CTF (Carnagie Mellon)
  - March 12-26
  - Online CTF

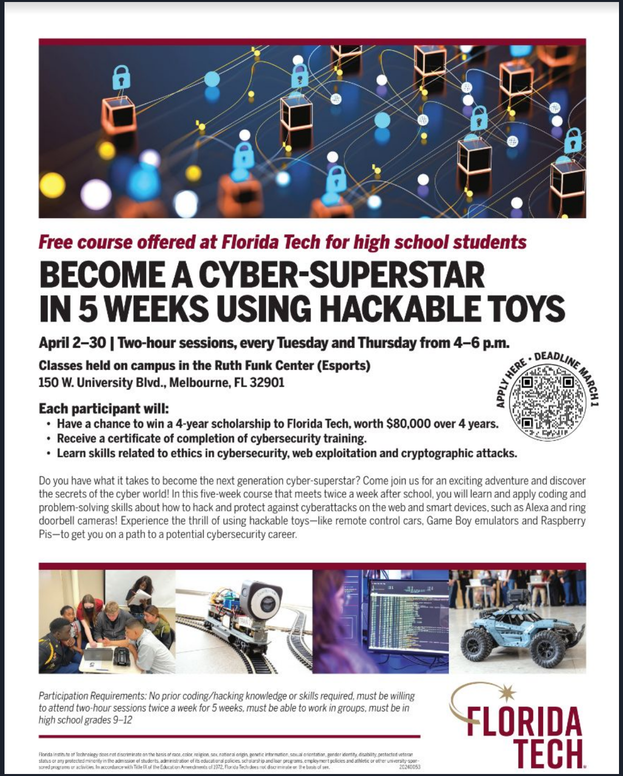
Wildcat Hackers 1	Wildcat Hackers 2
Dominick M Jay J Parker W Sam S Zachary W	Eshan V Saaketh K Shoaib A Dylan G Justin T

GenCyber Camp

- Cyber Security Summer Camp at Florida Tech
- 60 hours of instruction / labs
- June 10 - 14 - Register at https://event.fit.edu/gencyber
- 40 students, entering 9th - 12th grades
- Big Brother CTF - March 2nd 10AM - 4 PM
- Student selection is on Monday Feb 19th, so register before then!!
- Funded via NSA grant, no cost to students

Cyber Fundamentals Course

- The fall course gave out scholarship to winning student (4 years, $80K value)
- After school class for 5 weeks in April
- Tuesdays and Thursdays, 4-6PM
- April 2 - 30th
- **Deadline March 1**
- [Register Here]



Free course offered at Florida Tech for high school students

BECOME A CYBER-SUPERSTAR IN 5 WEEKS USING HACKABLE TOYS

April 2–30 | Two-hour sessions, every Tuesday and Thursday from 4–6 p.m.

Classes held on campus in the Ruth Funk Center (Esports)
150 W. University Blvd., Melbourne, FL 32901

APPLY HERE • DEADLINE MARCH 1

Each participant will:

- Have a chance to win a 4-year scholarship to Florida Tech, worth $80,000 over 4 years.
- Receive a certificate of completion of cybersecurity training.
- Learn skills related to ethics in cybersecurity, web exploitation and cryptographic attacks.

Do you have what it takes to become the next generation cyber-superstar? Come join us for an exciting adventure and discover the secrets of the cyber world! In this five-week course that meets twice a week after school, you will learn and apply coding and problem-solving skills about how to hack and protect against cyberattacks on the web and smart devices, such as Alexa and ring doorbell cameras! Experience the thrill of using hackable toys—like remote control cars, Game Boy emulators and Raspberry Pis—to get you on a path to a potential cybersecurity career.

Participation Requirements: No prior coding/hacking knowledge or skills required, must be willing to attend two-hour sessions twice a week for 5 weeks, must be able to work in groups, must be in high school grades 9–12

FLORIDA TECH

Florida Institute of Technology does not discriminate on the basis of race, color, religion, sex, national origin, genetic information, sexual orientation, gender identity, disability, protected veteran status or any protected minority in the admission of students, administration of its educational policies, scholarship and loan programs, employment policies and athletic or other university-sponsored programs or activities. In accordance with Title IX of the Education Amendments of 1972, Florida Tech does not discriminate on the basis of sex. 20240053

Code Quest Lessons Learned

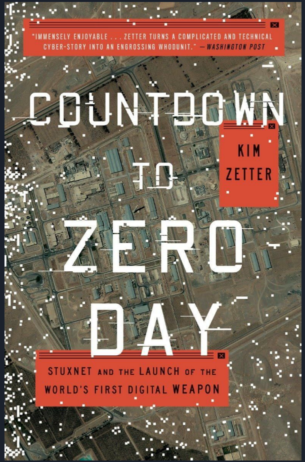
- Managing the workload / picking problems
- Scaling problems? Integer sizes ? Algorithm speed?
- Floating Point Numbers
- Languages?
- Code template / input and output

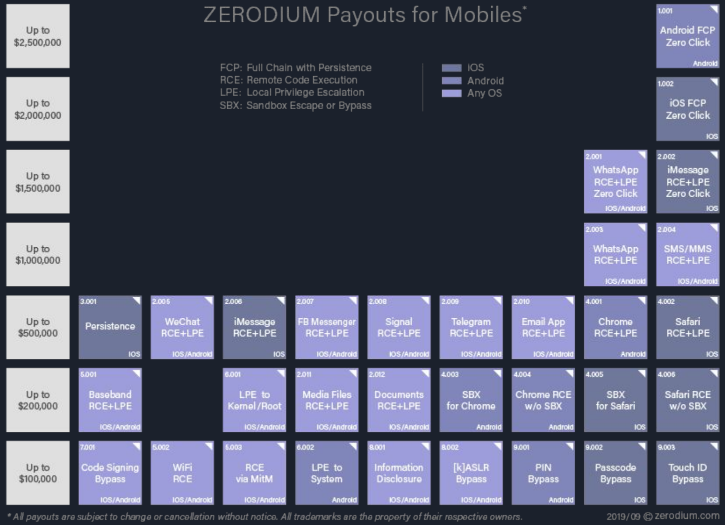
Stuxnet aka
Operation Olympic Games

- Worm created jointly by Israel and USA
- The first Cyber Weapon
- Named Stuxnet by Symantec security analysts in 2010
- Worm spread between Windows PCs, mostly in Iran
    - 4 zero-day exploits
- Infected Windows and Siemens Step 7 PLC controllers
- Targeted gas centrifuges that were refining nuclear materials
    - Malware was looking for 807Hz and 1210 Hz motors
    - Would command different frequencies, but report normal operation
- Destroyed 1,000 centrifuges (of 4,700 for Iran)

Zero-Day

- A vulnerability in a computer system that is completely unknown to users and developers of software
  - The vendor has 0 days to fix the problem
- Countdown to Zero Day ($14.99 Paperback)
  - Book by Kim Zetter
  - About Stuxnet and the security researchers that discovered and analyzed it
- Zero Day Vendors
  - Researchers can sell 0-day exploits


"IMMENSELY ENJOYABLE . . . ZETTER TURNS A COMPLICATED AND TECHNICAL CYBER-STORY INTO AN ENGROSSING WHODUNIT." —WASHINGTON POST
COUNTDOWN TO ZERO DAY
KIM ZETTER
STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

▨ iOS
▨ Android
▨ Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Stored Secrets

- Storing a secret key in your software
- Stored keys can be discovered by reverse engineering
- Xing DVD Player Software for Windows
  - Stored the DVD CSS decryption key without obfuscation

XingDVD Player

00:00:00 REMAINING

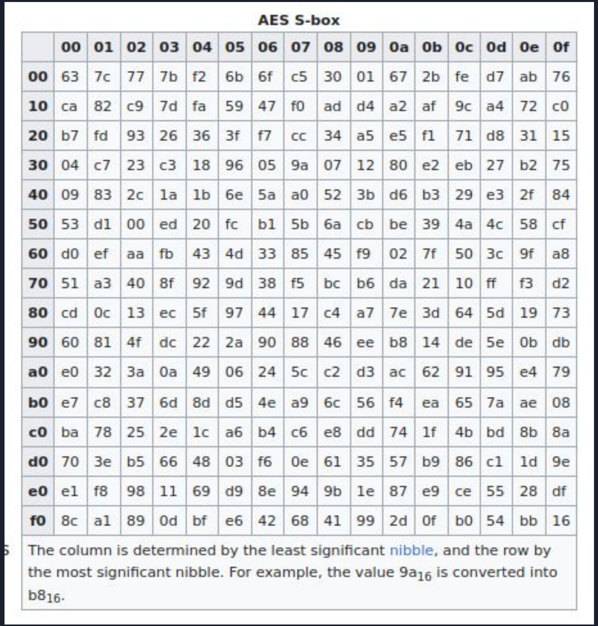
DEFAULT AUDIO

NO SUBTITLES

2.0X

Obfuscation / White-box encryption

- Avoid storing secrets in your source
- Obfuscate secrets so they can't easily be found
- AES White Box Encryption
  - Change the S-Box default constants
  - Embeds a key that can't easily be recovered
- Attacker can sometimes just wrap the whitebox
  - Use algorithm as-is as your own decryption library
  - Still preserves the key
  - The attacker will still want the key so they can do their own decryption implementations typically



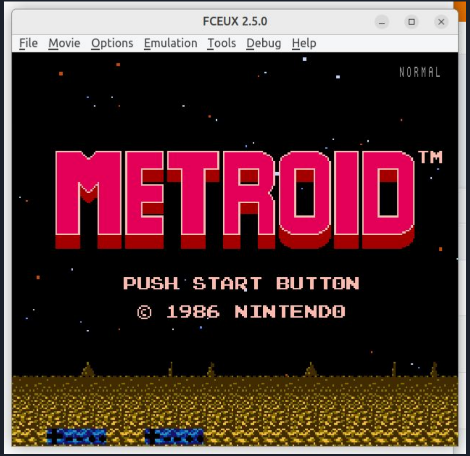
AES S-box

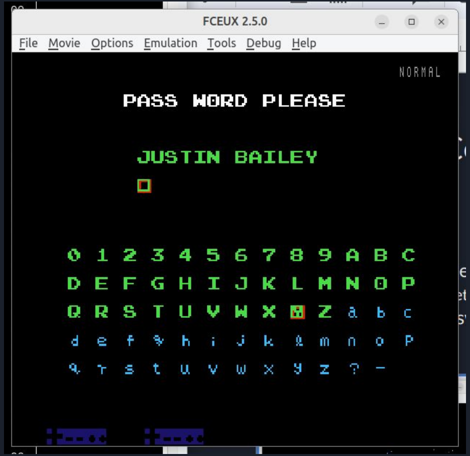
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

The column is determined by the least significant nibble, and the row by the most significant nibble. For example, the value $9a_{16}$ is converted into $b8_{16}$.

Secret Codes

- Video game codes / key sequences
  - Sometimes were just there for debugging game
- Secret passwords / account names
- Forgotten developer credentials

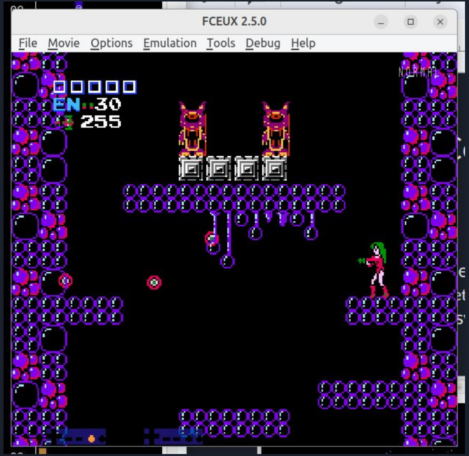




PASS WORD PLEASE

JUSTIN BAILEY

```
0 1 2 3 4 5 6 7 8 9 A B C
D E F G H I J K L M N O P
Q R S T U V W X Y Z a b c
d e f g h i j k l m n o p
q r s t u v w x y z ? -
```



Code Quest Follow Opportunities

- Code Quest Internships - APPLY HERE
  - 16+ years old
  - Rising HS Junior or Senior
  - US Citizen
  - Code Quest participant
- Lockheed Apprenticeships
  - Rotary and Mission Systems (RMS) is hiring high school graduates
  - To look for opportunities, visit www.lockheedmartinjobs.com
    - search for keyword “Engineering Aide”
    - set location as “Orlando”
    - filter by business area “Rotary and Mission Systems”
- Lockheed Scholarship - Info Here

Links

- https://event.fit.edu/gencyber/
- https://admissions.fit.edu/register/?id=9a859888-aa49-49cb-8c03-0ad00052a395
- https://en.wikipedia.org/wiki/Stuxnet
- https://zerodium.com/program.html
- https://www.penguinrandomhouse.com/books/219931/countdown-to-zero-day-by-kim-zetter/
-