## pConFullScreen ></div

AND THE REAL PROPERTY OF THE PROPERTY OF

to //www.dengine.co/te /mages/logo/og 220 ></e>

novi agentizione (a province) novi agentizione (a province) la formation (a province) la formation (a province) la formation (a province) la formation matrixes la formation matrixes no dans (annifere) matrixes no dans (annifere) matrixes matri

/a></div> oid(0);" class="searchBt">&mbsp:</a>

tengiue.cn/plus/search.php Tid="search\_news"> Tontflck="\$f"#search\_news")\_submit rchSubmitBr">&nbsp:</a>

mFullScreen ><//div

Thidden">

# IoT Red Team

Sala"

-selline light- threadland he

An one of the York part of the second s

Planters Constrained Conditioning States

will be of here a first second of the lengest of the

and Control Tax I go ...... I salaway diversing from some of the second second



Adithya Rao Alkankara



Ashton Sopher



Daniel Chong



Joseph Shenouda



Justin Wang



Rishika Sakhuja



Samuel Minkin



### Objective

To successfully attack the Blue Team's Internet of Things system.

There are three primary types of attacks we will be trying to conduct.

- Sniffing: reading data that is being sent.
- Jamming: preventing data from being sent (ex. interfering with signals).
- Spoofing: sending fake or edited data without Blue Team noticing.



### Methods and Technologies

#### Software:

- openHAB IoT framework
- GNU Radio

#### Sensors:

- TI Sensortag CC2650
- TI Sensortag CC2541
- Pip Sensor

### Other hardware:

- Ubertooth One
- WINLAB ORBIT
- USRP X310





### This Past Week



- Researched specific Bluetooth attack strategies
- Researched various IoT frameworks
- Acquired an Ubertooth one and set it up on our computers to detect nearby bluetooth traffic
- Got started with Wireshark and its various capabilities and functions





Features:

- Open source 2.4GHz device used for bluetooth experimentation
- Not only sends and receives 2.4GHz signals but can also work in monitor mode capturing bluetooth traffic in real time
- Ubertooth one software allows us to track all the bluetooth



### WIRESHARK

- Open-source application to sniff data back and forth off of ethernet, WiFi, BLE or a Raw USB traffic.
- Designed to understand structures (encapsulation) of different protocols.
- Equipped with bunch of filters to read specific data
- Mainly used to troubleshoot network issues and also to develop and test software.

Capturing from enp0s3         - + ×           File         Edit         View         Go         Capture         Analyze         Statistics         Telephony         Wireless         Tools         Help															×														
		R		۲	lf				×	6		٩			-		•	₹				Ð	Θ		⊒,	1			
Apply a display filter <ctrl-></ctrl->																						C		E>	pres	ssio	n	lle <b>t</b>	F.
No.		Tim	e			S	ouro	e					De	stin	natio	n		F	rotoco	l Le	ngth	Inf	0						-
Г	1	0.0	000	000	00	1	3.3	3.3	7.19	6			10	.0.	2.1	5		5	SSL	5	730	Co	ntin	uat	ion	Da	ta		
	2 3 4 5 6 7 8 9	0.0 0.0 0.1 0.1 0.1 0.1 0.1	000 128 128 500 504 506 629 629	292 296 597 582 410 235 377 549	72 81 38 31 04 98 27 48	1 1 1 1 1 1 1	0.0 3.3 0.0 0.0 0.0 0.0 92. 92.	.2.: 3.3 .2.: .2.: .2.: 168 168	15 7.19 15 15 15 .204 .204	6 .9 .9			13 10 13 19 19 19 10	.33 .0. .33 2.1 2.1 2.1 2.1 .0.	.37 2.1 .37 .68. .68. .68. 2.1 2.1	.196 5 204.9 204.9 204.9 5 5	) ) )		TCP SSL TCP DNS DNS DNS DNS DNS DNS	4	54 961 54 89 89 89 460 460	35 Col 35 St St St St	450 ntin 450 anda anda anda anda anda	→ 4 uat → 4 rd rd rd rd rd rd	43 [ ion 43 [ quer quer quer quer	ACI Da ACI Y Y Y	K] S ta K] S 0x97 0xb8 0xf3 resp resp	Seq Seq 7c0 383 3e1 Se1 Son	-
<ul> <li>Frame 1: 5730 bytes on wire (45840 bits), 5730 bytes captured (45840 bits) on interface 0</li> <li>Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_2e:08:e3 (08:00:27:2e:08:e3)</li> <li>Internet Protocol Version 4, Src: 13.33.37.196, Dst: 10.0.2.15</li> <li>Transmission Control Protocol, Src Port: 443, Dst Port: 35450, Seq: 1, Ack: 1, Len: 5676 Secure Sockets Layer</li> </ul>															)														
000 001 002 003 004 005 006 007 008 009	0 08 0 16 0 02 0 ff 0 d8 0 f7 0 27 0 0b 0 04 0 7f	00 54 0f ff f7 9e 01 18 66 4e	27 bf 01 55 d4 5c 4e ff 02 5e	2e f2 bb 3a a8 9d e2 71 83 71	08 00 8a 00 d4 8e b5 c1 11 6a	e3 00 7a 00 e6 e7 29 63 6d cd	52 40 20 f5 72 4e a9 92 bc 61	54 06 75 d7 c2 cb 30 8b de	00 65 72 db a9 7a 78 75 71 85	12 be ab 92 a5 a3 91 72 a6 7f	35 0d dd 76 46 2b b6 45 f8 b6	02 21 ca ee 71 57 12 e3 ae 7d	08 25 dd 4b b8 be 65 e9 de f3	00 c4 55 a0 92 da fa cf 7f b3	45 0a 50 b5 13 02 81 54 62 c5	00 00 18 d1 5f 79 5e 7d 9c 6f		RT @. .z u r. N. .c.0 .m j.a.	5 e!% r v.k Fq. z.+W. xe urE q }	.E. UP.  y  .T} 									
0	7 6	enpO	)s3:	<li></li>	ve c	apt	ure	in p	rogr	ess	>					Pad	kets: (	67 · I	Display	ed: 6	57 (1	100.	0%)	F	rofil	e: [	Defa	ult	



### This Coming Week

- Figure out how to use GNU Radio and Software-Defined Radios
- Read packets captured by Wireshark
- Learn about Z-wave attacks with EZ-wave

