Black Hat/Defcon 2014 Debrief

Richard Peters
@rfhacker

September 18, 2014

BH/DC

BERKELEY RESEARCH GROUP

black hat USA 2014

Black Hat 2014

BERKELEY RESEARCH GROUP

- 17th Year
- Mandalay Bay now instead of Caesar's Palace
- ~9,000 attendees
- 180 speakers, 113 sessions, 10 roundtables
- 147 companies with booths
- ~66 two to four day training classes

Black Hat Training

BERKELEY RESEARCH GROUP

August 2-3

SOLD OUT

RADIO EXPLOITATION

PRESENTED BY:
HotWAN

Updated: 6/12/14

Participants will learn how to transmit, receive, and analyze radio signals by attacking smartphones and embedded devices wirelessly. This class will encompass:

- Android Over-the-Air Attacks (Cellular, GPS)
- GNU Radio
- Wireless SCADA Armageddon
- Advanced Software Defined Radio Hacking

August 2-3

87%

August 4-5

SOLD OUT

SOFTWARE DEFINED RADIO

PRESENTED BY:
Michael Ossmann

An introduction to digital signal processing, software radio, and the powerful tools that enable the growing array of SDR projects within the hacker community, this course takes a unique "software radio for hackers" approach, building on the participants' knowledge of computer programming and introducing them to the forefront of digital radio technology. Participants will learn how to transmit, receive, and analyze radio signals and will be prepared to use this knowledge in the research of wireless communication security. Each student will receive a HackRF One software defined radio transceiver, a $300 value.

Black Hat 2014

BERKELEY RESEARCH GROUP

- Internet of things – Nest thermostat hack in 15 seconds
- Default passwords in TSA scanning machines
- Stealing passwords with Google Glass, Smart Watches, Smartphones, and Camcorders
- RF Hacking
- One swipe credit card reader hacking

Defcon 2014

BERKELEY RESEARCH GROUP

- Defcon 22
- Rio hotel, three full days
- ~16,000 attendees
- 180 speakers, 121 sessions + village talks
- Hardware hacking, social engineer, wireless, lockpick, tamper evident, crypto and privacy, and **ICS** villages
- Contests, Events, Music, Kids hacking conference, charities, Movies
- $220

The DC 22 Badge Line

The DC 22 Badge Line

BERKELEY RESEARCH GROUP

DC 22 Badges

Nixie Tube Badge Hack

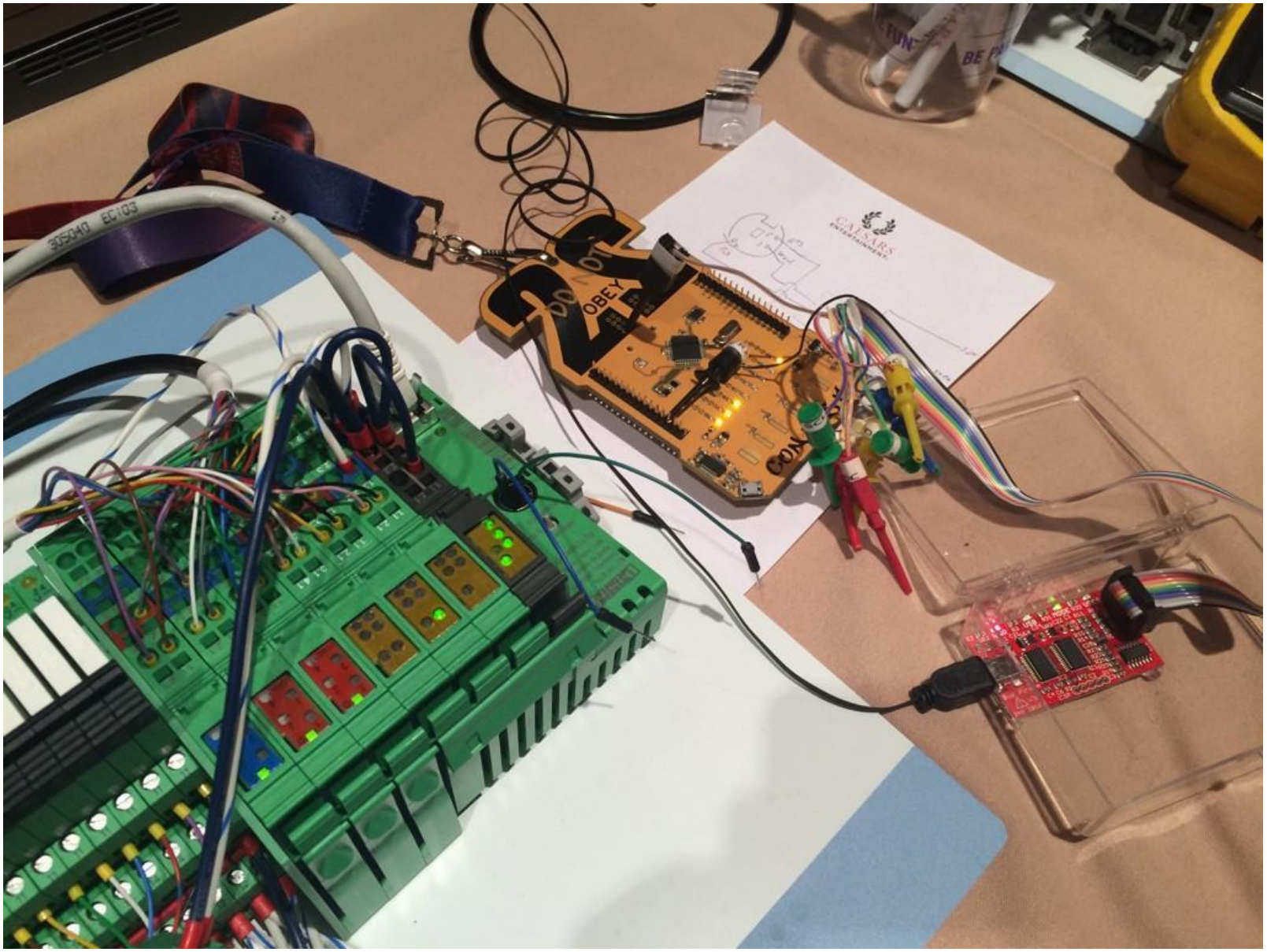
BERKELEY RESEARCH GROUP

DC 22 ICS Village

BERKELEY RESEARCH GROUP

DC 22 ICS Village

BERKELEY RESEARCH GROUP



DC 22 ICS Village

BERKELEY RESEARCH GROUP

Tamper Evident Village

BERKELEY RESEARCH GROUP

Tamper Evident Tools

BERKELEY RESEARCH GROUP

Wall of Sheep

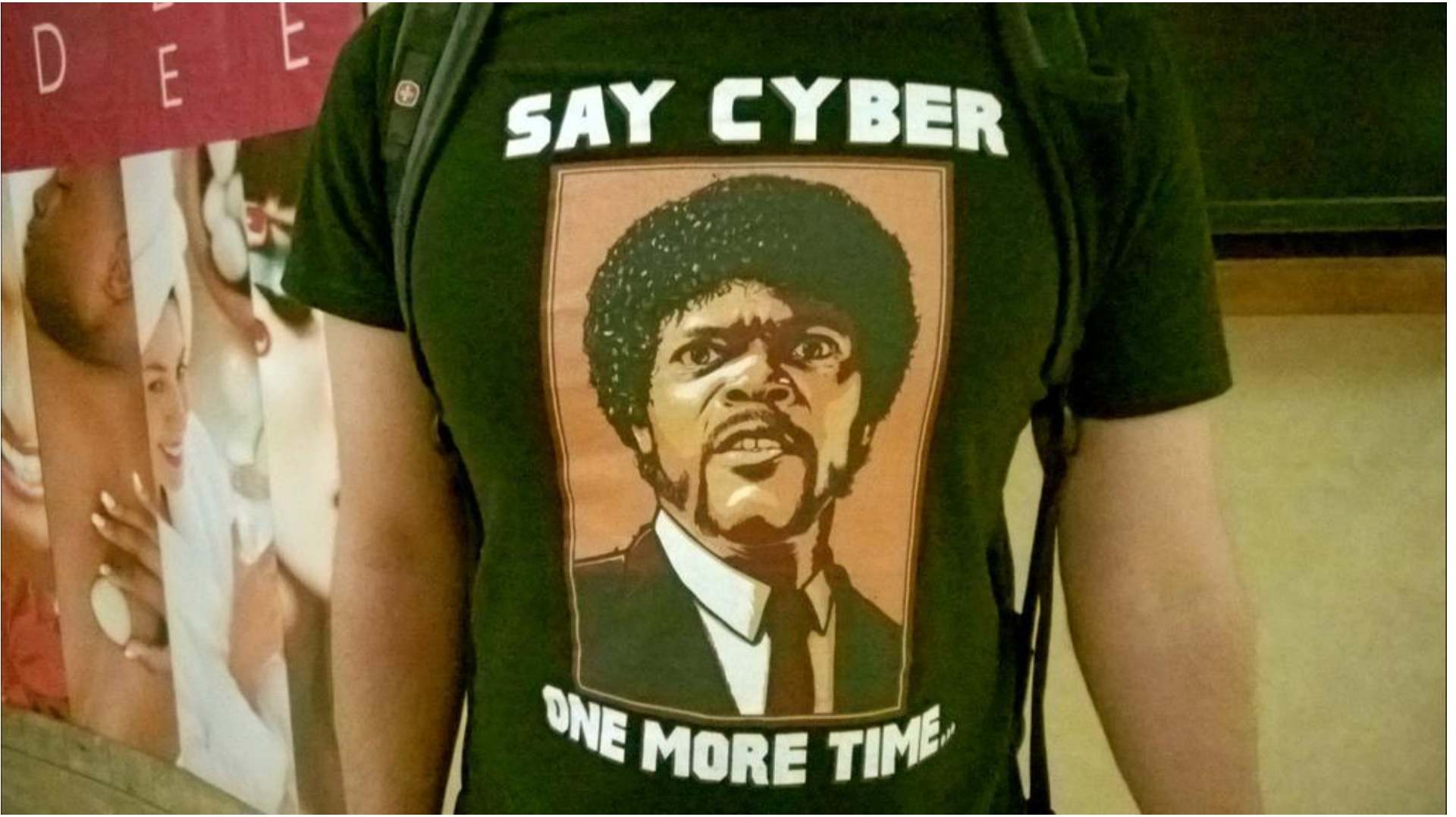
Mohawk Con

Lockpick Village

BERKELEY RESEARCH GROUP

Crack Me if You Can / Tesla

BERKELEY RESEARCH GROUP


SAY CYBER
ONE MORE TIME...

DC 22 – Internet of Things

BERKELEY RESEARCH GROUP

- **“Just What the Doctor Ordered”**
- **“Hack all the things: 20 devices in 45 minutes”**
- “Home Insecurity: No alarms, False alarms, and SIGINT”
- “NinjaTV – Increasing Your Smart TV’s IQ without Bricking it”
- “Attacking the Internet of Things using Time”
- **“Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment”**
- **“The Internet of Fails: Where IoT has gone wrong and how we’re making it right”**

Takeaways

Learning is awesome, but this presentation is about the

- You get a root!
- You get a root!
- You get a root!
- Everybody gets a root!

DC 22 – Internet of Things

BERKELEY RESEARCH GROUP

- **“Just What the Doctor Ordered”**
- **“Hack all the things: 20 devices in 45 minutes”**
- “Home Insecurity: No alarms, False alarms, and SIGINT”
- “NinjaTV – Increasing Your Smart TV’s IQ without Bricking it”
- “Attacking the Internet of Things using Time”
- **“Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment”**
- **“The Internet of Fails: Where IoT has gone wrong and how we’re making it right”**

BERKELEY RESEARCH GROUP

KNX/IP security

This slide is intentionally left blank

DC 22 – Internet of Things

BERKELEY RESEARCH GROUP

- **“Just What the Doctor Ordered”**
- **“Hack all the things: 20 devices in 45 minutes”**
- “Home Insecurity: No alarms, False alarms, and SIGINT”
- “NinjaTV – Increasing Your Smart TV’s IQ without Bricking it”
- “Attacking the Internet of Things using Time”
- **“Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment”**
- **“The Internet of Fails: Where IoT has gone wrong and how we’re making it right” (BuildItSecure.ly)**

DC 22 – RF Hacking

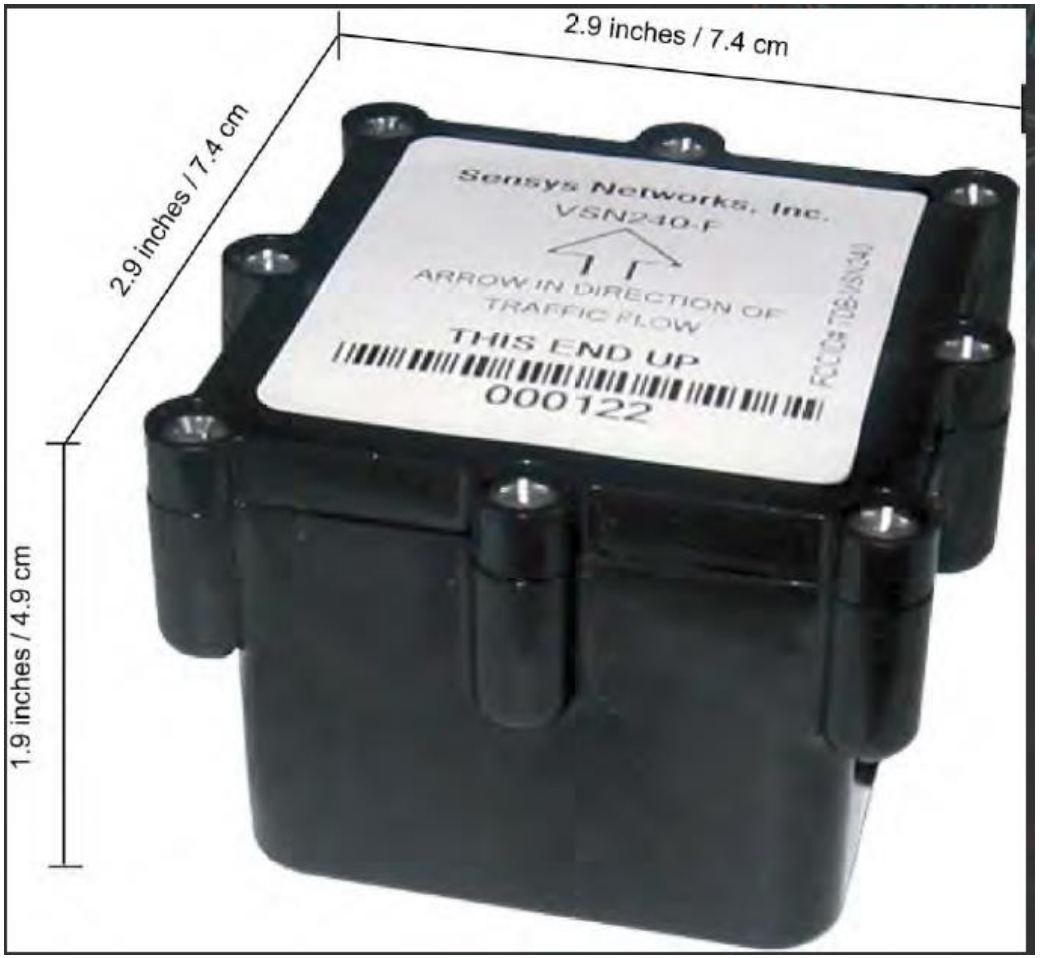
BERKELEY RESEARCH GROUP

- “RFIDler: SDR.RFID.FTW” – detect, sniff, decode & emulate RFID/NFC Kickstarter Project
- “RF Penetration Testing, Your Air Stinks”
- “Paging SDR…Why should the NSA have all the fun?” – remember pagers? (POCSAG/Flex decoding)
- “NSA Playset: GSM Sniffing”
- “The NSA Playset: RF Retroreflectors” – “*Surlyspawn* from NSA ANT Catalog”

DC 22 – RF Hacking

BERKELEY RESEARCH GROUP

- “Practical Foxhunting 101”
- **“Hacking US (and UK, Australia, France, etc.) traffic control systems”**
- “Steganography in Commonly Used HF Radio Protocols”
- Wireless Village - ~33 talks
- ICS Village - ~a few
- Ham Radio Exam World Record – 205 people, 181 passed (172 new/upgraded, 25 VE’s)


2.9 inches / 7.4 cm
2.9 inches / 7.4 cm
1.9 inches / 4.9 cm
Sensys Networks, Inc.
VSN240-F
ARROW IN DIRECTION OF
TRAFFIC FLOW
THIS END UP
000122


IOActive

BERKELEY RESEARCH GROUP

DC 22 – RF Hacking

BERKELEY RESEARCH GROUP

- “Practical Foxhunting 101”
- **“Hacking US (and UK, Australia, France, etc.) traffic control systems”**
- “Steganography in Commonly Used HF Radio Protocols”
- Wireless Village - ~33 talks
- ICS Village - ~a few
- Ham Radio Exam World Record – 205 people, 181 passed (172 new/upgraded, 25 VE’s)

DC 22 – Other

BERKELEY RESEARCH GROUP

- “Protecting SCADA from the Ground Up”
- “What the watchers see: Eavesdropping on Municipal Mesh Cameras for Giggles (or Pure Evil)”
- “Oracle Data Redaction is Broken”
- “Veil-Pillage: Post-exploitation 2.0” (veil-framework.com)
- “A Journey to Protect Points-of-sale”
- “Practical Aerial Hacking & Surveillance”
- “From root to SPECIAL: Pwning IBM Mainframes”

DC 22 - Other

BERKELEY RESEARCH GROUP

- “Detecting Bluetooth Surveillance Systems”
- “Hacking 911: Adventures in Disruption, Destruction, and Death”
- “Mass Scanning the Internet: Tips, Tricks, Results”
- “VOIP Wars: Attack of the Cisco Phones” (viproy.com)
- “Manna from Heaven: Improving the state of wireless rogue AP attacks”
- “Elevator Hacking – From the Pit to the Penthouse”
- “Burner Phone DDOS 2 dollars a day: 70 Calls a Minute”

Thank You!

Richard Peters | Principal

Berkeley Research Group, LLC

700 Louisiana Street, Ste. 2600 | Houston, TX 77002

D 713.493.2545 | O 713.481.9410 |

M 713.412.4105 | F 713.236.8596

@rfhacker

rpeters@brg-expert.com | www.brg-expert.com