RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-R05

The Air Up There: Wireless Beyond Wi-Fi, IoT from DC to 10GHz

Balint Seeber
@spenchdotnet

Director, Vulnerability Research

Bastille

#RSAC

"Technological progress is a blessing, but also a curse, and the biggest curse is that the **Internet of Things** is making everything vulnerable."

Benjamin Netanyahu – January 2016

THE PROBLEM

By 2020

50 BILLION DEVICES

NO SECURITY

EARLY DAYS
Finding Our Way

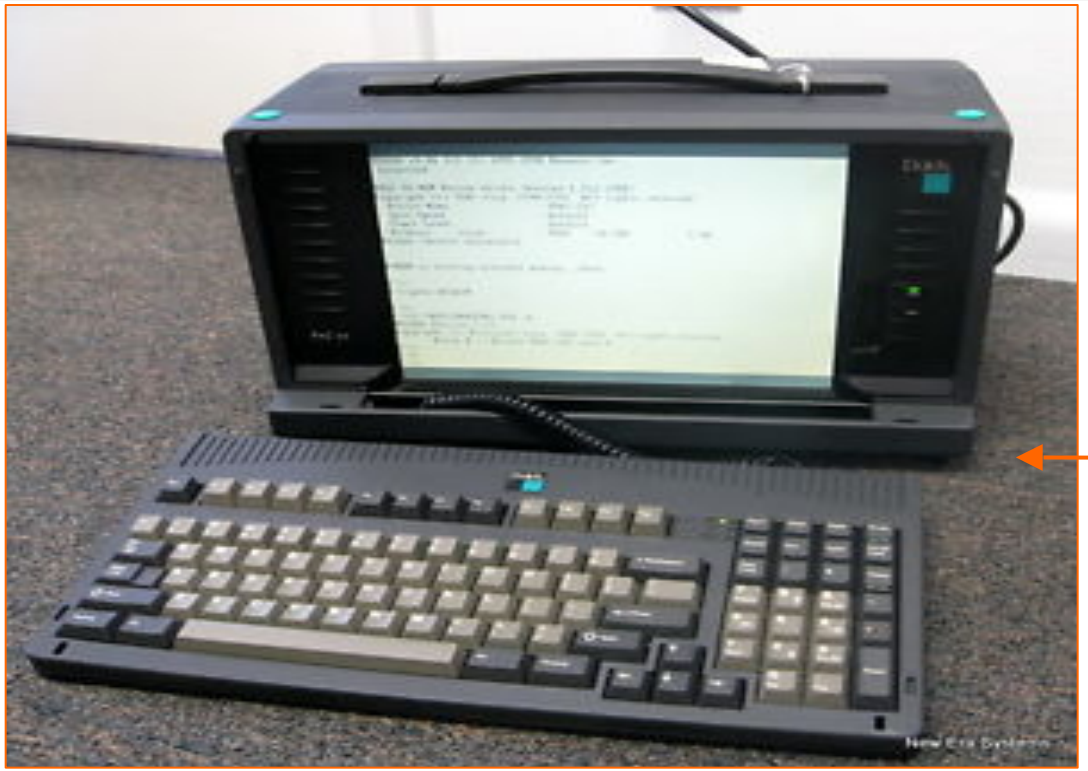
MOSAIC

Sun microsystems

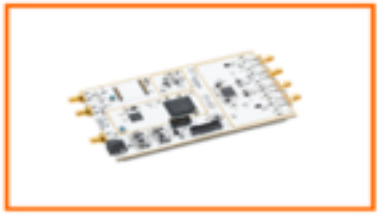
TCP/IP

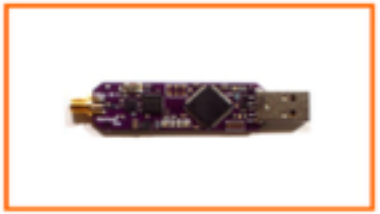
MICROSOFT. WINDOWSNT.
Version 3.1

Novell.



Network General Packet Sniffer ($25k)





IoT and Software Defined Radio

$20 - $1000

60 MHz to 6 GHz

INNOVATION
Still a mess

HACKING CELLULAR

Rogue WiFi of the decade

- Showing up in the wild
- Cost went from $500K to $500
- World now depends on cellular 2-auth

SAMSUNG FRIDGE
Google Login Theft

- Connection to Google calendars
- No SSL cert validation
- Login details accessible to anyone that could access WiFi

GLOBALSTAR NETWORK

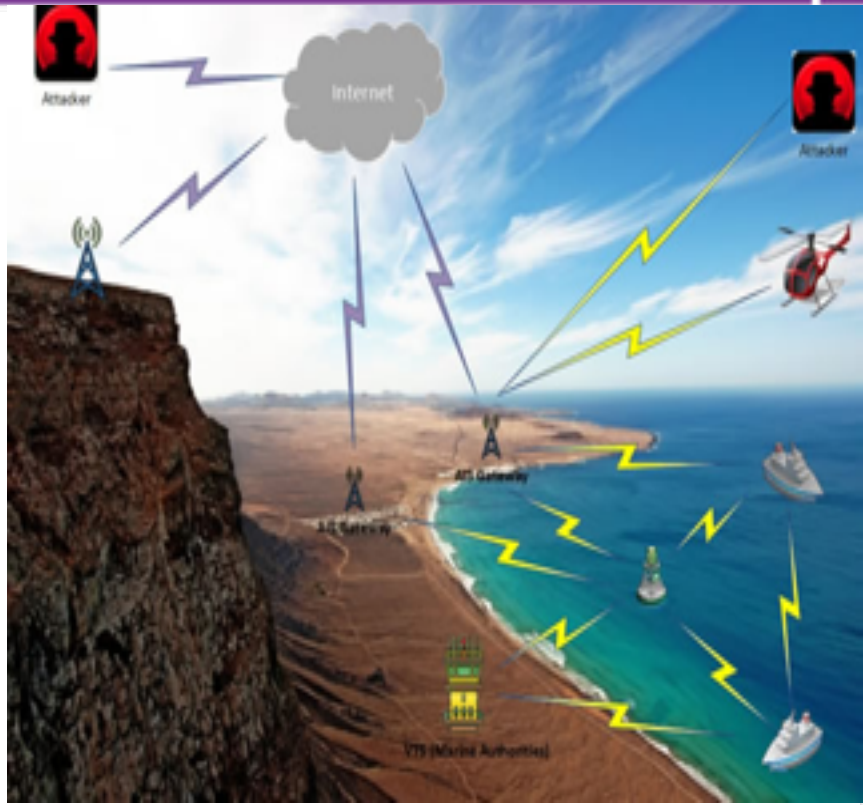
Space is the new frontier

- Simplex Data Network
- Spoof and Jam
- HTTP not HTTPs

SHIP TRACKING SYSTEMS

Automated Identification System

- Fire man-overboard
- Override auto-pilot
- Insecure, running VHF



PCWorld

Researchers hack GSM mobile calls using $9 handsets *January, 2011*

WIRED

Researchers Hack Air-Gapped Computer With Simple Cell Phone *July, 2015*

engadget

Some SIM cards can be hacked in about 2 minutes with a pair of text messages *July, 2015*

ZDNet

Android smartwatches vulnerable to snooping
December, 2014

SANS

Bluetooth and its Inherent Security Issues
March, 2015

The Register®

Bluetooth privacy is mostly ignored, so you're beaming yourself to the world *July, 2014*

9F 55 95 F1 02 57 C8 A4 69 CB F4 2B C9 3F EE 31

engadget

Researchers find major security flaw with ZigBee smart home devices *August, 2015*

GIZMODO

Philips Hue Light Bulbs Are Highly Hackable
August, 2013

NETWORKWORLD

Researchers exploit ZigBee security flaws that compromise security of smart homes *July, 2014*

SHMOOCON

SHMOOCON 2016: Z-WAVE PROTOCOL HACKED WITH SDR *January, 2016*

Forbes

How Your Security System Could Be Hacked To Spy On You *July, 2014*

black hat

Honey I'm Home - Hacking Z-Wave Home Automation Systems *November, 2013*

ars technica

Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords *July, 2014*

CNNMoney

'Bash' bug could let hackers attack through a light bulb *September, 2014*

engadget

Philips Hue susceptible to hack, vulnerable to blackouts *August, 2013*

CNBC

Biggest hacking threat to business? Wearables.
March, 2015

c|net

Fitness tracking goes under the security spotlight
July, 2014

WT VOX

Simple Hacking And Data Stealing In Wearables That Can Be Used Against You *September, 2014*

Forbes

How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home *March 2015*

COMPUTERWORLD

Black Hat: Nest thermostat turned into a smart spy in 15 seconds *August, 2014*

VentureBeat

I control your thermostat. Google's Nest gets hacked *August, 2014*

INTERNATIONAL BUSINESS TIMES

'Extremely chatty' Samsung smart TVs pose major security risk to government, healthcare and energy companies *March 2015*

black hat

Hacking, Surveilling, and Deceiving Victims on Smart TV *August, 2014*

SC MAGAZINE

Alarm bells ring for Internet of Things after smart TV hack *June, 2014*

The New York Times

The August Smart Lock Shows Why You Should Stick With Dumb Keys *October 2014*

WIRED

Millions of Kwikset Smartkey Locks Vulnerable to Hacking *August, 2013*

tom's GUIDE

This 'Smart' Lock May Have Dangerously Dumb Security *March, 2015*

InformationWeek DARKReading

Five Ways To (Physically) Hack A Data Center
May 2010

SECURITYWEEK

Recent Bank Cyber Attacks Originated From Hacked Data Centers, Not Large Botnet *October, 2012*

COMPUTERWORLD

Hackers exploit SCADA holes to take full control of critical infrastructure *January, 2014*

NETWORKWORLD

Hacks to turn your wireless IP surveillance cameras against you *April, 2013*

GIZMODO

A Creepy Website Is Streaming From 73,000 Private Security Cameras *November, 2014*

WIRED

Popular Surveillance Cameras Open to Hackers, Researchers Say *May, 2012*

The Register

DECT wireless eavesdropping made easy
December, 2013

HELP NET SECURITY

Is Your Cordless Phone Being Hacked?
March, 2014

NETWORKWORLD

DECT phones and POS terminals are vulnerable
January, 2009

InformationWeek DARKReading

Smart Meter Hack Shuts Off The Lights
September, 2014

KrebsonSecurity
In-depth security news and investigation

Target Hackers Broke in Via HVAC Company
February 2014

black hat

Energy fraud and Orchestrated blackouts: Issues with wireless metering *July 214*

ZDNet

Tesla electric cars vulnerable to remote unlocking hack, researchers say *April, 2014*

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It. *July, 2015*

The Washington Post

'Car hacking' just got real: In experiment, hackers disable SUV on busy highway *July, 2015*

CSO

Rogue cell towers discovered in Washington, D.C
April, 2014

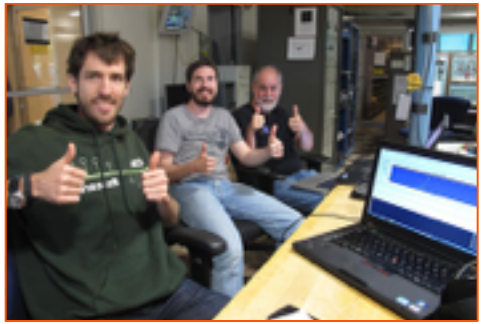
Forbes

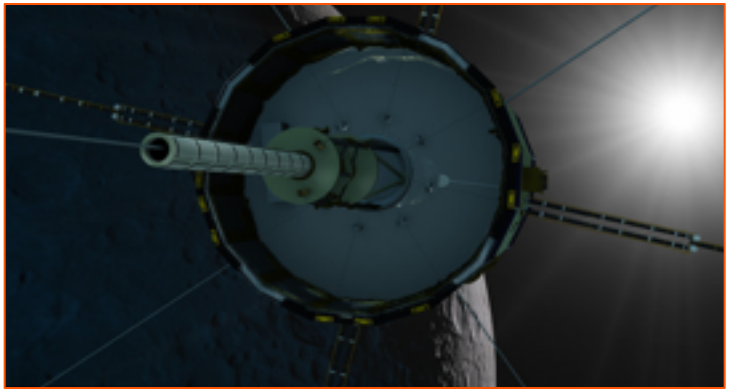
Rogue Cell Towers Could Be Intercepting Your Call
September, 2014

BLACK BAG

Rogue "Interceptor" Cell Phone Towers Discovered Near U.S. Army Bases *September 2014*

Hacking Satellites (ISEE-3)





WHAT COULD GO WRONG - PRIVACY

IoT Enabling Big Brother

- Impact insurance premiums
- Allow for discrimination

- Allow for off hours monitoring
- Track productivity

Apply What You Have Learned Today

- Next week you should:
  - Check your Information Security policies for IoT specific risks around:
    - Sensors
    - IoT applications and how they collect/store data
  - Audit your current IoT footprint
    - Interview stakeholders in HR, Facilities, IT, etc.

Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Educate peers, users and partners on IoT Adoption/Usage and Policy
  - Ensure your existing MDM and Wireless Security suppliers have a plan to help counter IoT threats
  - Perform a full spectrum wireless assessment in critical areas

Apply What You Have Learned Today

- Within six months you should:
  - Identify/Deploy tools to inventory IoT devices and networks in corporate airspace
    - Deploy full-spectrum IDS in critical areas
      - Data Centers
      - BackOffice
      - Call Centers
  - Continue to educate users on personal/corporate IoT device crossover.

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-R05

The Air Up There: Wireless Beyond Wi-Fi, IoT from DC to 10GHz

Balint Seeber
@spenchdotnet

Director, Vulnerability Research

Bastille

#RSAC