Founded in 1994

Located in Peabody, MA

Organized into 4 Practices

Information Security Practice:
1) Risk Management & Compliance
2) IT Assurance
3) IT Audit
Today’s Agenda

- Introduction
- Demonstration/Show & Tell
- Recommendations
- Question/Answer & Closing Remarks
Show of Hands:
How many of you...

Have back office and other sensitive areas protected by RFID?
Show of Hands:
How many of you...

Have exterior doors protected by RFID?
Show of Hands:
How many of you...

Have your server room protected by RFID?
Projected size of the global market for RFID tags from 2010 to 2020 (in billion U.S. dollars)

This statistic represents the market size for RFID tags from 2010 to 2012, and gives a projection through 2020. In 2010, the global market for RFID tags was sized at around 5.6 billion U.S. dollars.
Introduction: RFID Basics

Frequencies:

1. Low (LF)
2. High (HF)
3. Ultra-High (UHF)

Fun fact: Between 70-80% of all physical access RFID devices in US use low frequency.
Not so fun fact: Low frequency RFID has been hacked and is insecure.
1. Passively steal RFID keycard data.
2. Create card with stolen data.
3. Gain entry and execute exploit.
Video Demonstration: Tools

- **Tastic RFID Thief**
  Sniff card data and store to SD card

- **Proxmark3**
  Copy RFID card

- **Rubber Ducky**
  USB to bypass antivirus and gather credentials

- **Mimikatz**
  Software that extracts Windows passwords
Load

Deploy

the micro SD card into the ducky then place inside the covert USB enclosure.

 MICRO SD STORAGE

60 MHz 32-bit
AT32UC3B1256

TYPE A CONNECTOR

COVERT ENCLOSURE

Carry multiple payloads, each on its own micro SD card.

the ducky on any target Windows, Mac and Linux machine and watch as your code executes in mere seconds.
Video Demonstration: RFIDecoder

Disclaimer: This video was created for educational purposes only. No illegal entry or data compromise occurred during the making of this video.
GraVoc Associates Presents...

View on YouTube: http://youtu.be/ODJyjL4gjBc
1. Introduce a USB device that automatically dumps Windows passwords (Rubber Ducky)
2. Bypass antivirus using procmon (developed by Microsoft) to gather system memory and later extract Windows passwords in cleartext (Mimikatz)
3. Plant malicious device/backdoor to extract data to remote location (Raspberry Pi)

Next Steps (for an attacker)…
Recommendations

Use RFID shield wallet cards

Do not wear RFID card in plain view (if your ID card is an RFID card, consider using two separate cards)
Recommendations

Monitor access with cameras

Use a two-factor authentication (RFID + keypad, lock/key, etc.)
Recommendations

Upgrade RFID systems to use more secure protocols (i.e. higher frequency)

Enhance testing methodologies to incorporate physical security with vulnerability assessments and social engineering
Recommendations

Disable USB ports and create a whitelist of approved devices

Monitor all log files
“Don’t forget physical security. Not all data thefts happen online. Criminals will tamper with computers or payment terminals or steal boxes of printouts.”

Executive Summary to 2014 Data Breach Investigations Report
Verizon
“To be sure, RFID is still widely used in retail and shipping today. It’s even at the heart of near field communication — the technology that powers Apple Pay and other contact-less payment systems.”

Before Apple Pay, There Was That Thing Called RFID
WIRED Magazine
Credits

Francis Brown, Partner
Bishop Fox
Live Free or RFID Hard, August 2013
BlackHat 2013 & DEF CON 21
Resources

Bishop Fox
Presentations surrounding RFID security
http://www.bishopfox.com/resources/tools/rfid-hacking/presentation-slides/

Proxmark
RFID cloning hardware
http://www.proxmark.org
Resources

SecurityTube
Instructional Videos
http://www.securitytube.net

Statista.com
RFID Market Statistics
Resources

Verizon 2014 Data Breach Investigations Report
2014 Breach Statistics by Type and Industry
http://www.verizonenterprise.com/DBIR/2014/

WIRED Magazine
2014 Breach Statistics by Type and Industry
http://www.verizonenterprise.com/DBIR/2014/
Thank You!

Nathaniel C. Gravel  
Director – Information Security Practice  
ngravel@gravoc.com  
978-538-9055 ext. 129

Michael J. Kannan  
Senior Security Consultant  
mkannan@gravoc.com  
978-538-9055 ext. 125