RFID Hacking: Reconsidering Physical Security

April 29, 2015

Jackson Schultz
Security Consultant

Michael J. Kannan, CISSP, C|EH
Senior Security Consultant

GRAVOC ASSOCIATES
"Our Business is Your Success!"

GraVoc Associates, Inc.

- Founded in 1994
- Located in Peabody, MA
- Organized into 4 Practices
- Information Security Practice:
  1) Risk Management & Compliance
  2) IT Assurance
  3) IT Audit

GRAVOC ASSOCIATES

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?

GraVoc Associates

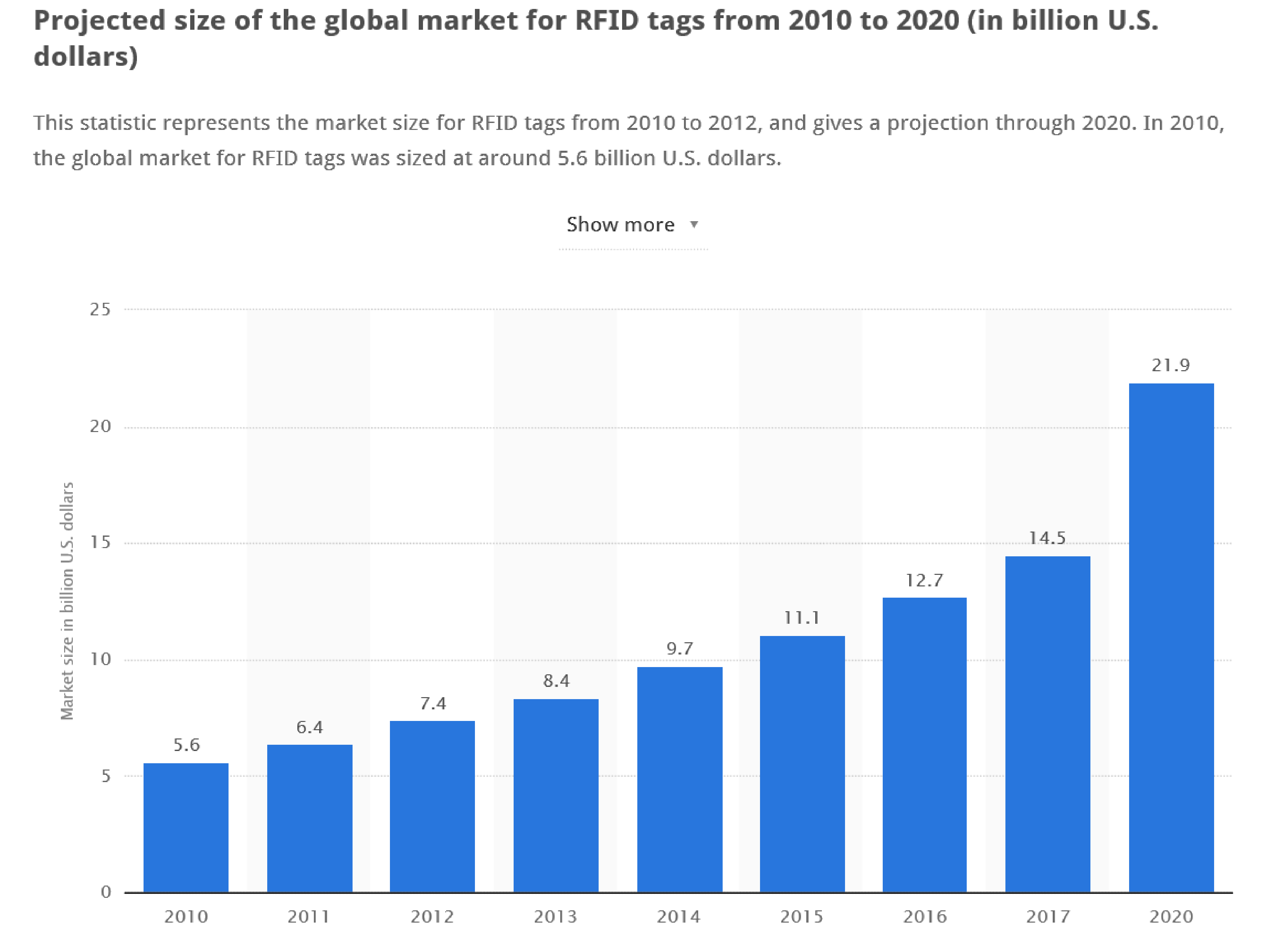
Show of Hands:
How many of you…

Have exterior doors protected by RFID?

GRAVOC ASSOCIATES

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.

GraVoc Associates

Introduction: RFID Basics

Not so fun fact: Low frequency RFID has been hacked and is insecure.

GRAVOC ASSOCIATES

Video Demonstration: Summary

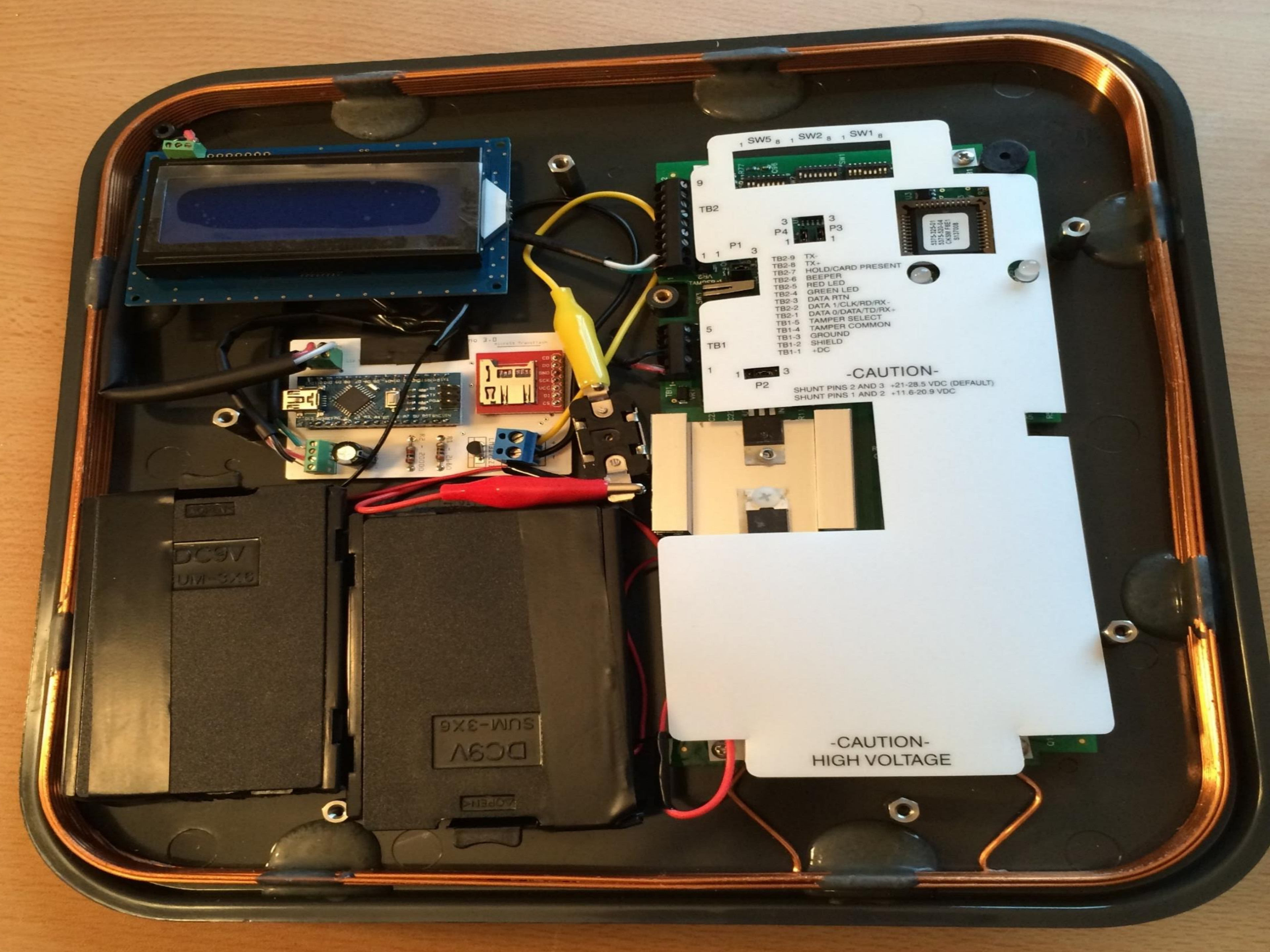
1. Passively steal RFID keycard data.
2. Create card with stolen data.
3. Gain entry and execute exploit.

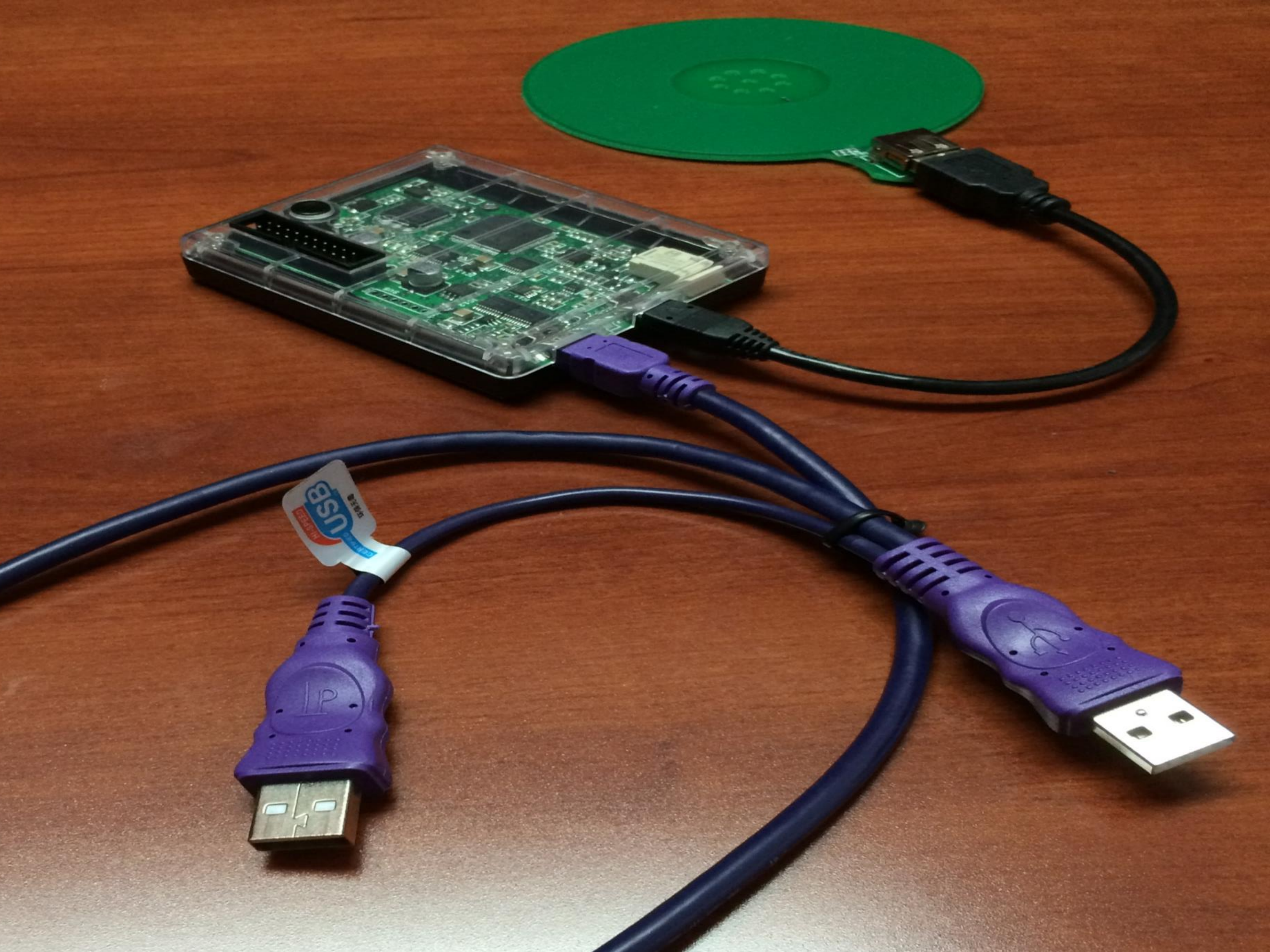
GraVoc Associates

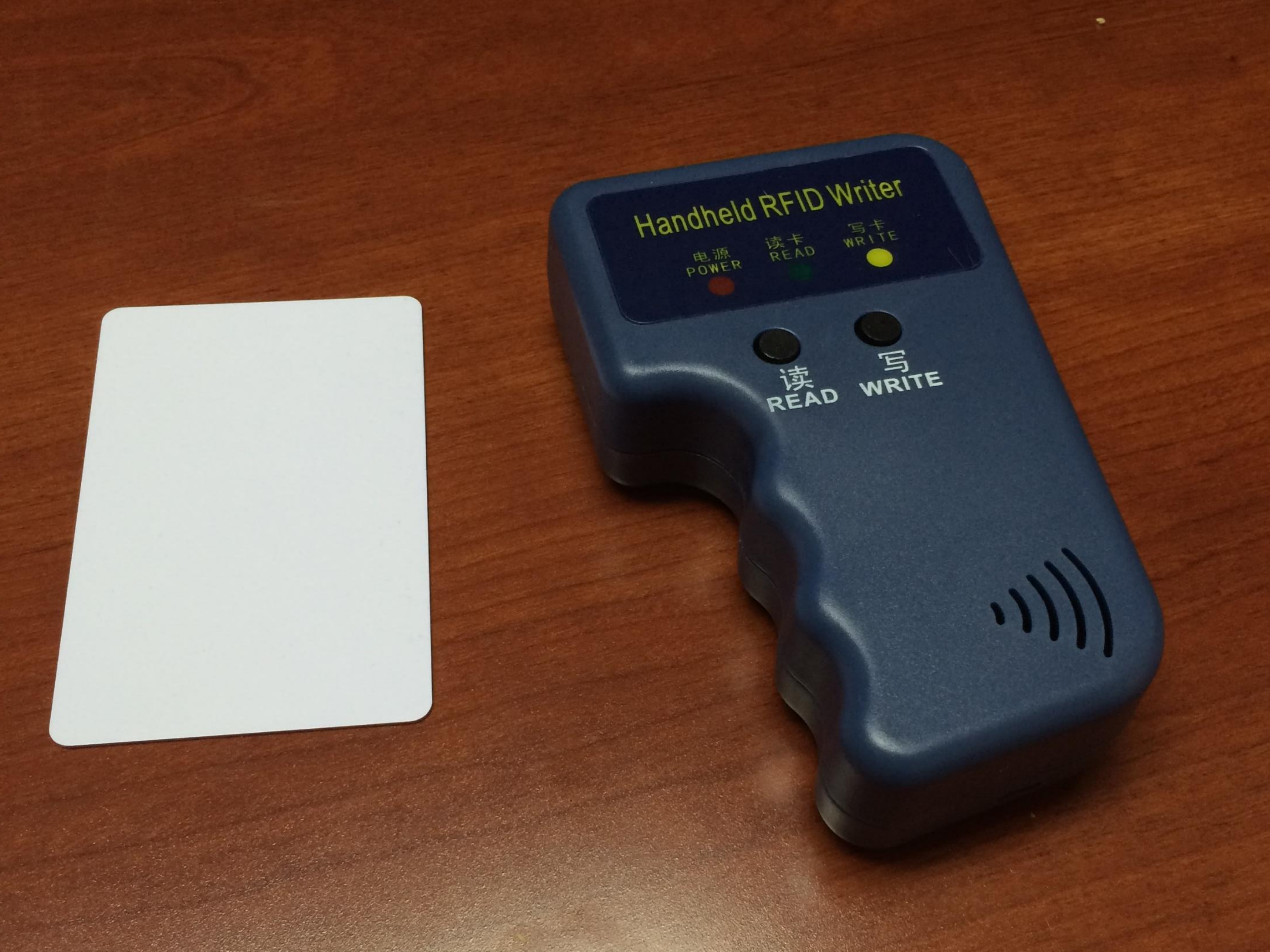
Video Demonstration: Tools

- **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

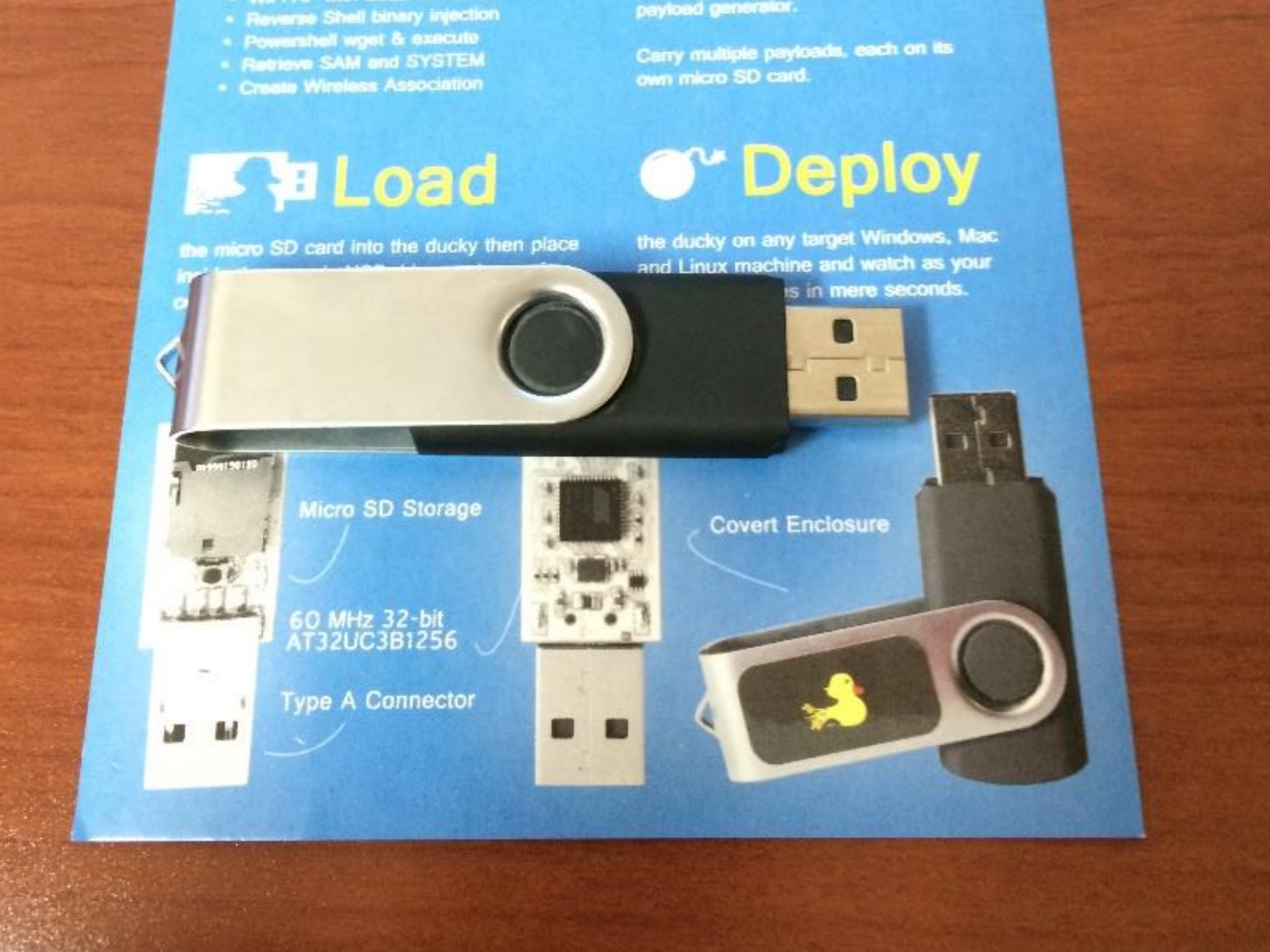
GRAVOC ASSOCIATES


SW5
SW2
SW1
TB2
P4
P3
P1
TB1
P2
TB2-9 TX-
TB2-8 TX+
TB2-7 HOLD/CARD PRESENT
TB2-6 BEEPER
TB2-5 RED LED
TB2-4 GREEN LED
TB2-3 DATA RTN
TB2-2 DATA 1/CLK/RD/RX-
TB2-1 DATA 0/DATA/TD/RX+
TB1-5 TAMPER SELECT
TB1-4 TAMPER COMMON
TB1-3 GROUND
TB1-2 SHIELD
TB1-1 +DC
-CAUTION-
SHUNT PINS 2 AND 3 +21-28.5 VDC (DEFAULT)
SHUNT PINS 1 AND 2 +11.6-20.9 VDC
-CAUTION-
HIGH VOLTAGE
DC9V
UM-3X6
DC9V
SUM-3X6
OPEN
CD
DO
GND
SCK
VCC
DI
CS


USB



Handheld RFID Writer
电源
POWER
读卡
READ
写卡
WRITE
读
READ
写
WRITE



- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

payload generator.

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

Load

the micro SD card into the ducky then place in

Deploy

the ducky on any target Windows, Mac and Linux machine and watch as your es 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

Next Steps (for an attacker)…

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)

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

GRAVOC ASSOCIATES

Recommendations

Disable USB ports and create a whitelist of approved devices

Monitor all log files

Closing Remarks

“**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

GraVoc
Associates

Closing Remarks

"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

GRAVOC
ASSOCIATES

Question & Answer

Credits

BISHOP FOX

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

http://www.statista.com/statistics/299966/size-of-the-global-rfid-market/

GraVoc Associates

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/

GRAVOC ASSOCIATES

Thank You!

Jackson Schultz

Security Consulatant – Information Security Practice

jschultz@gravoc.com

978-538-9055 ext. 131

Michael J. Kannan

Senior Security Consultant

mkannan@gravoc.com

978-538-9055 ext. 125

GRAVOC ASSOCIATES