

# Late-Breaking Computer Attack Vectors



---

**PaulDotCom Enterprises, LLC**

March 2008

Paul Asadoorian

PaulDotCom Enterprises, LLC

[paul@pauldotcom.com](mailto:paul@pauldotcom.com)

# Outline

---

- Introduction
- Reasons For A Penetration Test
- When social networks attack
- Certified Pre-Owned
- RFID hacking for \$8
- Why vendor patch cycles don't work

*“...hacking is the action of outsmarting the others and as such it may take any form”*

- pdp, gnu citizen.org

# Introduction

---

- (Paul Asadoorian \* Geek) = PaulDotCom
- Weekly Security Podcast
- Penetration Testing, Security Consulting, Device Testing
- WRT54G Hacking course and book



# Reasons For A Penetration Test

- Understand threats to develop better defense
- Determine risk to make informed decisions
- Test defenses (Firewalls, IDS) and incident handling procedures
- TSA is a good example
  - They have a blog! ([www.tsa.gov/blog](http://www.tsa.gov/blog))



# When Social Networks Attack

---

- Social network “Evil Twin” attack more successful than we thought
  - Just ask “Twitchy”
- Beware of the grouping feature
- Taking over a social network profile is powerful
- Social networks can potentially distribute attacks



# When Social Networks Attack

---

- Twitter allows you to make short blog posts
  - Jabber, SMS, various clients
  - What if you send a malicious link?
- Exploit clients, browsers, and phones with one posting!
- Twitter + SMS + Caller ID Spoofing = Very Bad



# Social Networking Defense

---

- Register your identity on popular social networking sites, using fake info
  - Using real info and friends/family find you!
- Don't install user-written applications
- Keep your client software up-to-date
- Raise awareness for SMS attacks

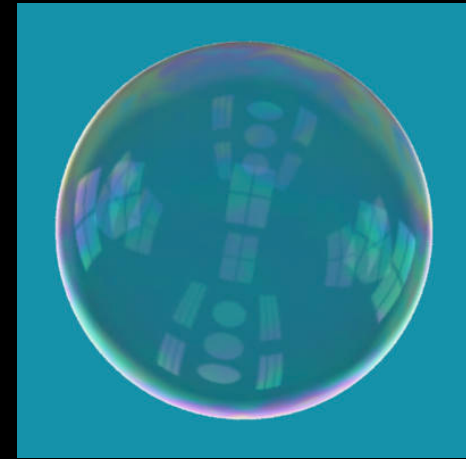


- [http://blog.washingtonpost.com/securityfix/2008/03/the\\_anatomy\\_of\\_a\\_vishing\\_scam\\_1.html](http://blog.washingtonpost.com/securityfix/2008/03/the_anatomy_of_a_vishing_scam_1.html)

# Certified Pre-Owned

---

- There is no perimeter, and this is one good reason why
- Devices can carry malware installed at the manufacturing plant
- Digital picture frames, USB thumb drives, SD cards, GPS devices
- Going back to the sneakernet
  - Check out USB wristband
  - <http://pauldotcommunity.blogspot.com/>



# Sneakernet Defense

---

- Don't allow code to run off of your removable devices
  - Hard with DMA
- Fill all USB ports with epoxy
- Disable USB ports with group policy and/or in BIOS
- Hard to balance security with usability
  - “Hi, Can you print this for me?”

# RFID Hacking For \$8

---

- Video shows how to skim for \$8
  - <http://tv.boingboing.net/2008/03/19/how-to-hack-an-rfide.html>
- Mifare RFID cards have been cracked
  - Used as national payment system in Netherlands
  - *“The MIFARE® classic family is the pioneer and front runner in contactless smart card ICs operating in the 13.56 MHz frequency range with read/write capability”*

# RFID Hacking For \$8

---

- Why is this important?
- When costs come down, we need to worry
- The Tao Of Information Security Says:

*“Enterprises stay dirty because we can not stop intruders, but we can make their lives more difficult. I've heard of some organizations trying to raise the \$ per MB that the adversary must spend in order to exfiltrate/degrade/deny information.”*

# RFID Defense

- RFID shielding wallet
  - <http://www.difrwear.com/products.shtml>
- Do you REALLY need RFID to pay for goods at the store? Is it too hard to swipe the card?
- Use RFID as one layer, and use other methods of authentication and encryption to protect it



Phidgets Reader  
\$99



Omnikey  
Cardman 5321  
\$130

# Why Vendor Patch Cycles Don't Work

---

- Why should your vendor make a risk decision for you?
  - Cisco (Including Linksys) - 6 Months
  - Microsoft - Monthly
  - Oracle - Quarterly
  - Apple - When they feel like it (bundled)
- Attackers don't wait for you to install the patch

# Why Vendor Patch Cycles Don't Work

---

- What can you do:
  - If there is an early release program, sign up for it
  - Evaluate the criticality of your systems and tailor your process accordingly
  - Consider vendor approved workarounds
  - Implement other measures to buy time

**/\* End \*/**

---

- Web: <http://pauldotcom.com/>
- Wiki: <http://pauldotcom.com/wiki/> - Show notes for each episode
- Email: [paul@pauldotcom.com](mailto:paul@pauldotcom.com)



PaulDotCom Enterprises, LLC



**WHITEHATWORLD.COM**