

# Late-Breaking Computer Attack Vectors



---

**PaulDotCom Enterprises, LLC**

July 2008

Paul Asadoorian

PaulDotCom Enterprises, LLC

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

# Introduction

---

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



# Outline

---

- What you need to know about the DNS bug
- Tips for securing Mac OS X
- Hacked before you know it (without wires)
- Who has the key to your city?
- Nmap: The Book
- Insecurity Moment Of The Month

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

- pdp, gnucitizen.org

# What you need to know about the "DNS Bug"

---

- By sending requests to vulnerable servers, cached entries can be changed
- This means that [www.google.com](http://www.google.com) can become an attacker's web server
- This is a noisy attack, requires lots of packets
- Tip: 16 bits does not provide enough randomness
- Reports that ISPs DNS servers are poisoned

# What you need to know about the "DNS Bug"

---

- Be certain that you patch your resolvers
- Check your ISP and make sure they patched ([www.doxpara.com](http://www.doxpara.com))
  - If not, use OpenDNS ([www.opendns.com](http://www.opendns.com))
- Update your IDS/IPS to catch it
- DJBDNS was "secure by design", some people have switched

# Tips For Securing Mac OS X

---

- Good tips for any operating system really
- Encrypt Your Data
  - OS X can create encrypted volumes
- Use Strong User Authentication
  - Two factor authentication would be nice
  - If you have fingerprint reader, use it

# Tips For Securing Mac OS X

---

- Don't Run With Administrative Privileges
  - Good for some malware
- Enable The Firewall
  - Still not futile
- Keep Your Software Up-To-Date
  - What if this goes wrong?

# Enter "Evilgrade"

---

- Subverts your computers connection to update servers
- Many do not sign/verify updates
- Supports many packages, including:
  - Java
  - iTunes
  - Winzip



<http://www.infobyte.com.ar/developments.html>

# Its About The Data

---

- “There are no viruses for OS X” - So what?
- OS X users still login to web sites (so do Windows and Linux users)
- All operating systems have updaters
- iTunes and Java are cross platform
- Attackers like to steal credentials (coreflood)
  - [http://www.darkreading.com/document.asp?doc\\_id=159874](http://www.darkreading.com/document.asp?doc_id=159874)

# Why Aren't We Signing Apps?

---

- Example from Joanna Rutkowska, DailyDave list:

```
# find /Applications -name "*.app" -exec codesign -v {} \;  
  
/Applications/iWork '08/Keynote.app: code object is not signed  
/Applications/iWork '08/Numbers.app: code object is not signed  
/Applications/iWork '08/Pages.app: code object is not signed  
/Applications/Microsoft Office 2008/Microsoft Entourage.app: code object is not signed  
/Applications/Microsoft Office 2008/Microsoft Excel.app: code object is not signed
```

- Sign your apps, use SSL, validate your updates! (<- for the vendors)

# Hacked Before You Know It (Without Wires)

---

- KARMA is a fantastic attack tool (become all SSIDs)
- Metasploit is a great exploit framework, especially for development



**Can I  
have an order of  
Metasploit with a  
dash of Karma?**

# Hacked Before You Know It (Without Wires)

---

- Karmetasploit!
- Lure clients to a captive portal login page
- Page loads top 500 web sites into your browser
- Collects all your cookies, even fakes FTP/IMAP/POP servers
- Windows XP, iPhones, OS X - Vulnerable

# Hacked Before You Know It (Without Wires)

---

- Don't automatically join networks
- Apply Windows XP patch
- Disable Wifi when not in use
- Use cellular Internet
- Always use encrypted protocols, pay attention to bogus certificates
- KARMA is easy to detect...

Would you use the wireless network here?



*“the free wi fi is also great considering that it is near the college and makes it helpful for studying”*

# Who has the key to your city?

---

- Terry Childs, a network administrator, had the keys to the entire city network

*Terry Childs, the network administrator accused of hijacking the city of San Francisco's computer network, has surrendered the access passwords he created that locked users out of the system. Childs had refused to give up the passwords, but a visit from San Francisco Mayor Gavin Newsom convinced him to reveal them.*

- Don't rely on the mayor to enforce your security policy

# Protecting Your City

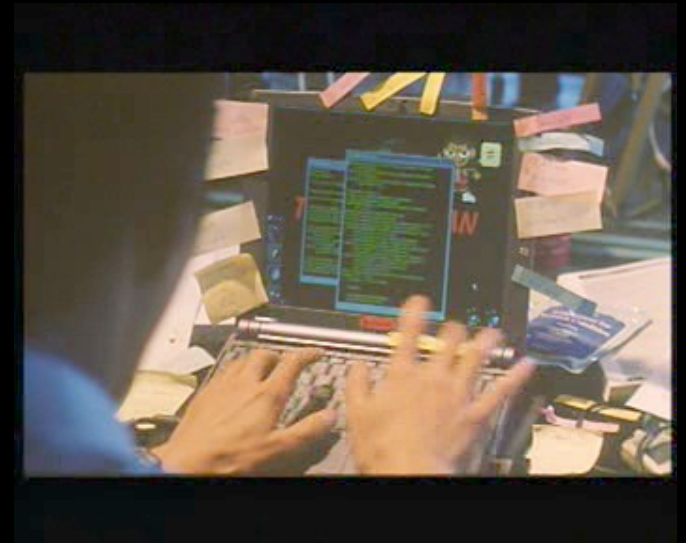
---

- Have more than one set of keys
- Log all access to your network gear
- Be certain that console access is available, require it in your policy
- Monitor changes to your configuration
  - Note if someone is locking everyone else out of the network

# Nmap: The Book

---

- <http://nmap.org/book/toc.html>
- Nmap: The Movie?
- Practical usage examples:
  - Detect open proxies
  - Find vulnerable services
  - Detect “evil” devices
  - Use the information for social engineering!

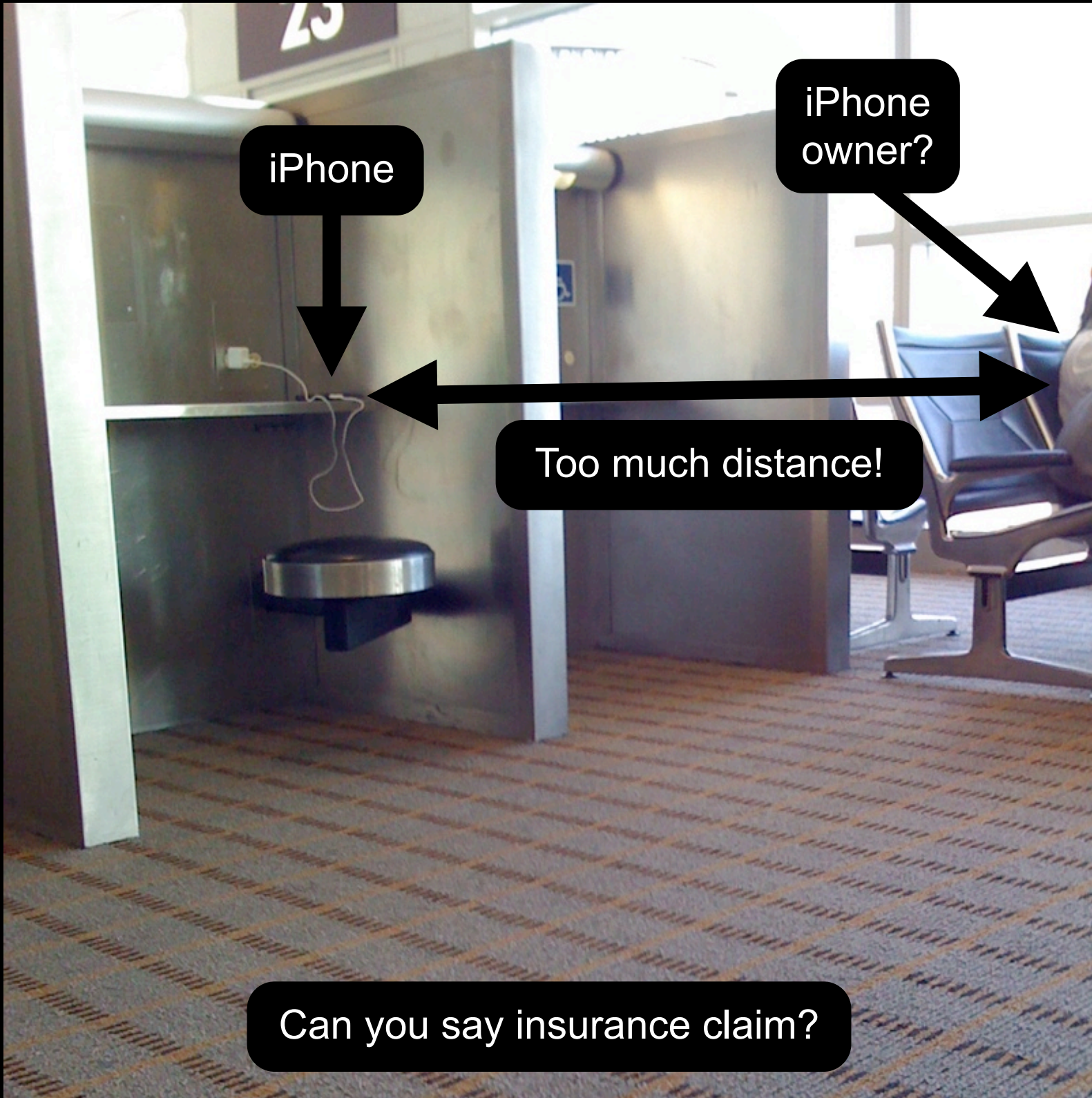


iPhone

iPhone  
owner?

Too much distance!

Can you say insurance claim?





# Epic Fail

I find your lack of win disturbing.  
May the fail be with you.

**/\* End \*/**

---

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



PaulDotCom Enterprises, LLC

