

Late-Breaking Computer Attack Vectors



PaulDotCom Enterprises, LLC

February 2008
Paul Asadoorian
PaulDotCom Enterprises, LLC
paul@pauldotcom.com

Outline

- Introduction
- Vendors shipping you vulnerabilities
- Latest social engineering techniques
- Managing the security process

Introduction

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



You Just Bought...A Vulnerability!

- Philips Skype Phone Vulnerabilities - Default username and password for “support”
- Asus Eee PC - Remote root vulnerability in default installation
- Embedded systems are notorious for this



I <3
r00t!

* Philips Skype Phone Vulnerabilities - [PaulDotCom] - Its really amazing to see vendors using default usernames and passwords in this day and age on embedded devices. This one is worse, the username is the same as the password (service/service). What were they thinking, or were they? Companies producing consumer and industry products need to step up their game when it comes to security. Oh wait, there's more, the directory traversal vulnerability discloses your Skype credentials. Sweet! I wonder, how many vendors would let a vulnerability like this slip by in a web application exposed to the Internet? Maybe some, but my point it, whats the difference?

* Asus Eee PC Root-Out-Of-The-Box - [PaulDotCom] - This is just silliness, why do vendors ship products with known vulnerable software? An exploit for Samba Version 3.0.24 was published early last year!!! I am putting the responsibility for fixing these flaws solely on the vendor. I will again go back to this episode's tech segment and say that its easy and important to scan devices and look for flaws.

DEFENSE: Scan everything that plugs into your network with a vulnerability scanner, review the results, make configuration changes and follow up with the vendor on any unpatched vulnerabilities.

Defense: Internal Vulnerability Scans

- Scan everything that plugs into your network with a vulnerability scanner
- Run regular internal vulnerability scans on a schedule
- Have a process in place for remediating!
- Follow up with the vendor for unpatched vulnerabilities

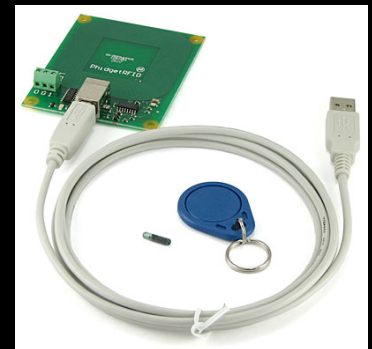
The Latest In Social Engineering

- Wireless headsets are an attack vector
- Use the information for social engineering
- RFID is an attack vector too
- Become the insider...



We took a position across the street from the facility and started up the scanner. Within seconds of turning on the device we were able to listen to conversations that appeared to be coming from our client's employees. Several of these conversations discussed the business in detail, as well as very sensitive topics.

http://www.darkreading.com/document.asp?doc_id=143779



The Latest In Social Engineering

- Caller-id spoofing aids in social engineering
- Several other VoIP attacks help too:
 - Call re-direction (e.g. help desk)
 - Eavesdropping
 - *“But no one can get on my VoIP network”*
 - Check out voiphopper
 - <http://voiphopper.sourceforge.net/>

Defense: User Awareness

- Defending against social engineering is difficult, some tips:
 - Don't give up on user awareness
 - Have a process for credentials and identification
 - Follow that process
 - Audit that process

Defense: VoIP Security

- Authenticate INVITE and REGISTER commands
- Use TCP for SIP handshakes and signaling traffic (prevents spoofing)
- Never trust caller-id
- Encrypt voice communications with SRTP

Manage The Security Process

- You have 127 web applications
- You bought a shiny new (expensive) web application testing tool
- You have 1 employee to manage the process
- You are doomed for...



* [<http://jeremiahgrossman.blogspot.com/2008/01/technology-helps-but-people-matter-most.html>] "Scanning" is more than identifying vulnerabilities, you have to fix them] - [PaulDotCom] - This is a great article from Jeremiah Grossman and it underscores a very important point. You can have all the fancy wizbang tools you want, however you need people to manage them and the results. This means following up on recommendations, and re-testing to be certain that recommendations are followed and that they fixes actually work. Otherwise, these tools are going to sit around, and when they are used they are going to be a waste of time

* [<http://www.securethoughts.net/2008/01/osxcrypt-alpha-beta-release.html>] OSXCrypt] - [Larry] - a follow on to our comments about the lack of affordable whole disc encryption. [securethoughts] - OSXCrypt is an open-source TrueCrypt-compatible port for OSX. Larry mentioned he didn't know of any cheap whole-disk encryption solutions for PCs or his Mac. TrueCrypt 5.0 (coming in Feb 2008) will support bootable Windows volumes. OSXCrypt has just released a pre-beta of their software, and should hopefully be including whole-disk encryption for Intel Macs soon.

DEFENSE: Properly staff your security folks to effectively manage risk.

Defense: Security Process

- Properly staff your security team to identify risk and make improvements
- Build application security into the development process
 - Source code analysis tools
 - Developer training

Manage The Security Process

- Laptop encryption is great to protect your data if its stolen
- Whole disk encryption presents recovery problems (imaging, lost password)
- It does not protect you from getting hacked (e.g. A keystroke logger will grab your password)
- <http://citp.princeton.edu/memory/>



**Hard To
Encrypt
Memory!**

Defense: Security Process

- Encrypted volumes or folders may be a better choice (password could still be grabbed)
- Store sensitive data encrypted on a server (harder to steal)
- Sensitive data is leaked on backups too, encrypt them and be careful who has your backup tapes
- Don't leave "Backups" lying around



/* End */

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



PaulDotCom Enterprises, LLC

