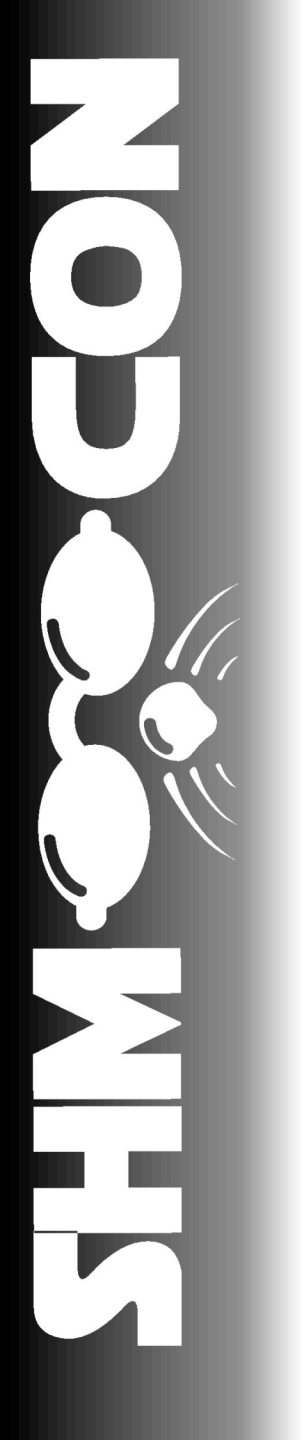


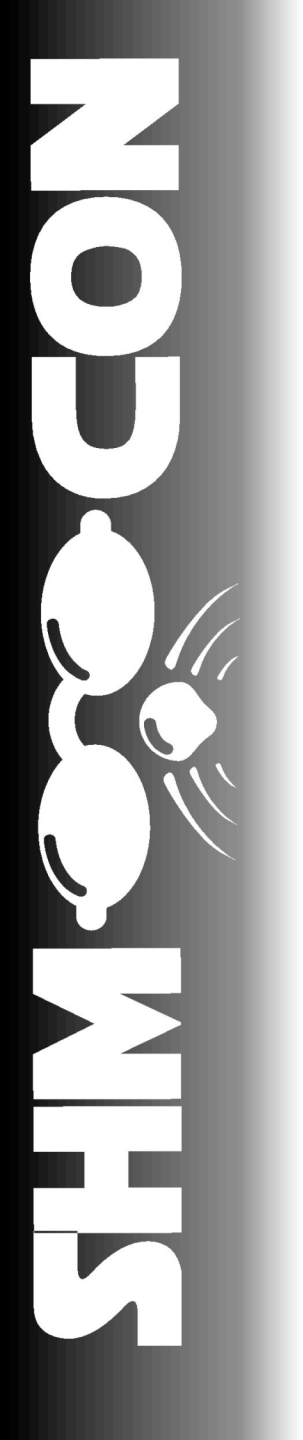

# Bluetooth Defense Kit

Bruce Potter

…with help from Will Davis

August, 2006

**BlackHat USA - Aug 2006**




# Don’t Believe Anything I Say

- "Do not believe in anything simply because you have heard it. Do not believe in anything simply because it is spoken and rumored by many. Do not believe in anything simply because it is found written in your religious books. Do not believe in anything merely on the authority of your teachers and elders. Do not believe in traditions because they have been handed down for many generations. But after observation and analysis, when you find that anything agrees with reason and is conducive to the good and benefit of one and all, then accept it and live up to it.” - Buddha
- By Day, Senior Associate for Booz Allen Hamilton
- By Night, Founder of The Shmoo Group and restorer of hopeless Swedish cars

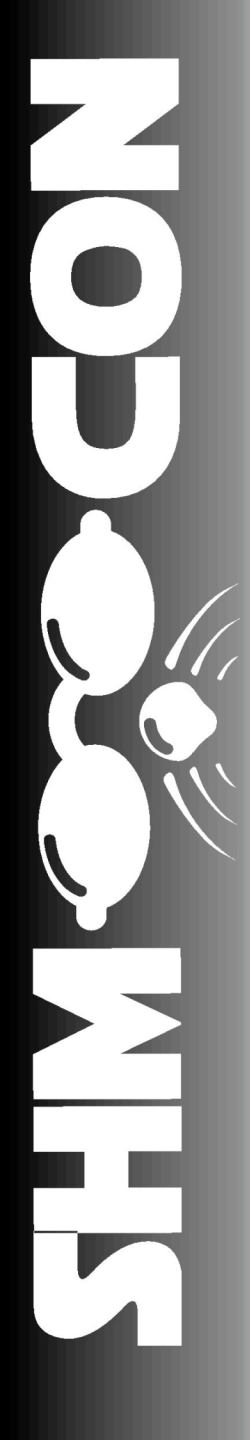
**BlackHat USA - Aug 2006**

# Bluetooth Crash Course

- 2.4 GHz, Frequency Hopping, Personal Area Network Technology
- NOT WiFi!
- Pairing - Mechanism for establishing long term trust between two BT devices
- RFCOMM - Wireless serial port emulation (basically)
- AT Commands - You remember these, right? Used to control some devices across an RFCOMM connection
- Discoverable mode - When a device wants to be found, it will respond to other devices sending inquires

# State of the Union

- Current version of Bluetooth Core Spec is 2.0
  - Enhanced Data Rate (EDR) now allows for up to 3Mb/s… with basically the same power consumption
  - Security is largely unchanged from 1.1 spec
- As of Nov 2005, 9.5 Million BT radios were being shipped each week
  - At that rate, that's one radio for every 8 people on the planet in a year
  - 9.5 million was up from 4.75 million just 4 months prior
  - Makes WiFi look pretty wimpy from a market penetration
- Profiles govern how like devices talk to each other
  - In the past, a confusing experience… now we have icons to clear things up

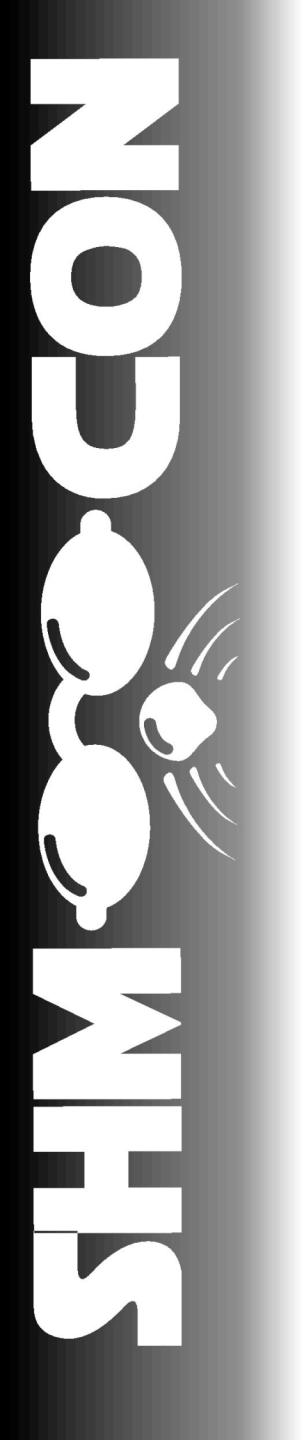



# Common Deployment Scenarios

- Unlike WiFi, Bluetooth has generally stayed where it was supposed to
- Mobility - Cell phones and ear buds, car hands free kits, network access
  - Every state that passes “no handheld cell use” laws impacts BT sales positively
- Cable replacement - mouse, keyboard, camera
- New uses - printers, mp3 players, etc..

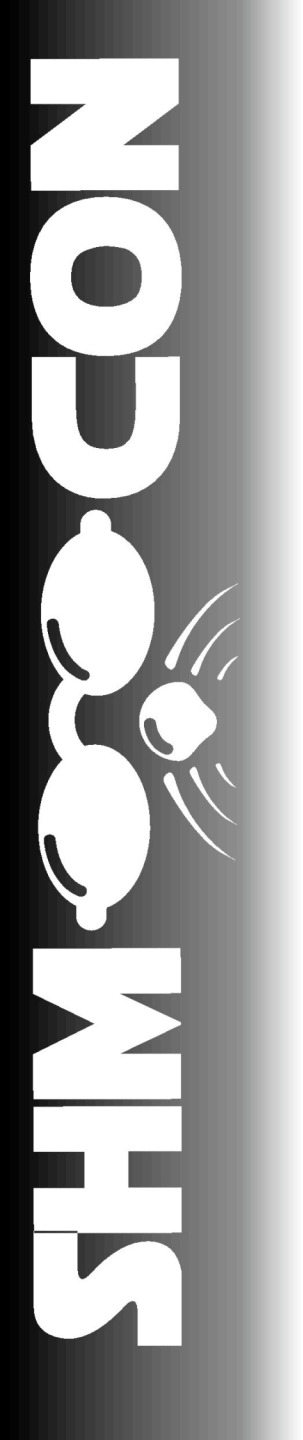
# The Industry Players (a subset)

- BT Stack Vendors
  - WIDCOMM
  - Toshiba
  - Microsoft
  - CSR
  - Extended Systems
  - Open Interface
- BT Chip Manufactures
  - CSR
  - Broadcom
  - TI
  - Infineon



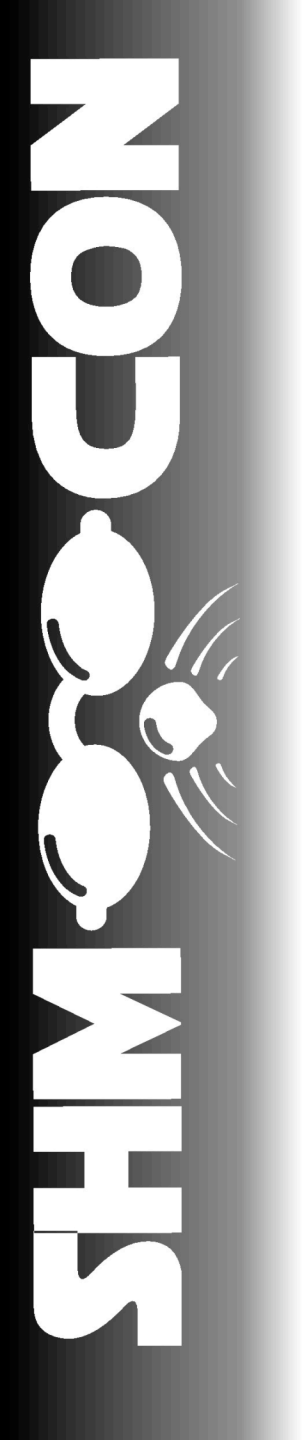

# Contemporary Bluetooth Attacks

- Trifinite.org has been leading the charge of publicly disclosed Bluetooth attacks
- Others such as @stake and TSG have tackled some BT security issues as well
- Most of what has been really damaging have been poor implementations
  - Rush to market leads to poor security
  - Super complicated protocol stack leads to poor security
  - Lack of security training for developers leads to power security
- Trifinite.org has lots of attack tools
  - Bluediving (bluediving.sourceforge.net) has Linux based impls of most of their tools




# Stupid Defaults

- Hard configured PINs - Only an issue at pairing time, but allows for attacks like Car Whisperer
- Profiles turned on by default - This is the same as keeping unneeded network services from running
  - If you don't need it, don't run it (don't expose it)
- No authentication - duh! Even for things like automatic vCard acceptance (Sony) this is sketchy at best

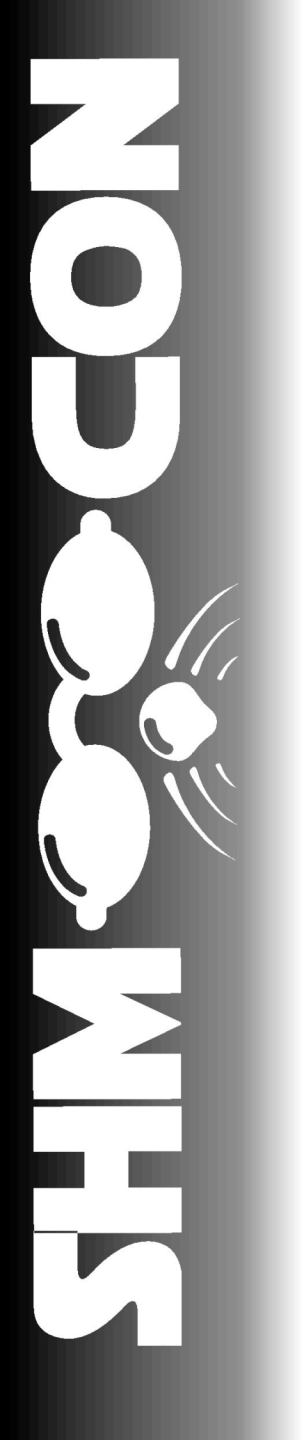



# More Stupid Defaults

- Poor per-profile default - Each profile is like an application… it can have bad defaults
  - Ie: I had a Belkin BT CF adapter that had the filesharing profile defaulted to world writeable and shared the entire filesystems
- Discoverable by default - Why make it that much easier for an attacker?
  - Anyone been attacked in non-discoverable mode by an unknown device?
  - Also, discoverable mode sucks down battery faster

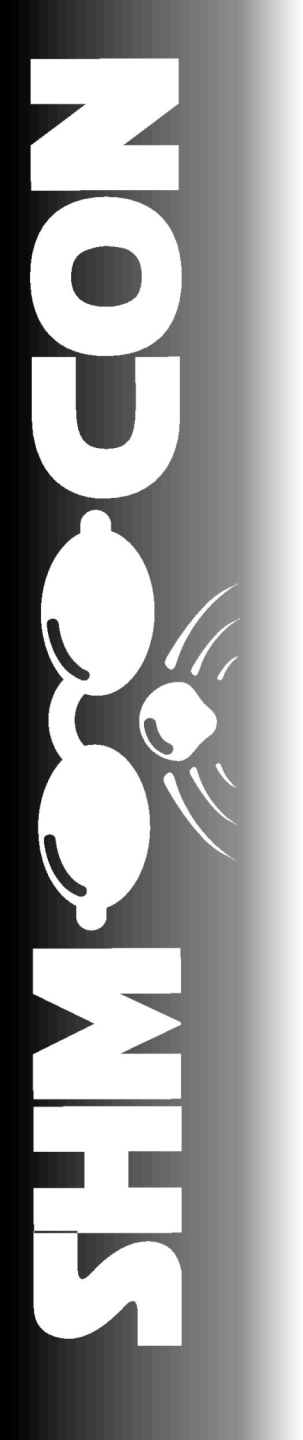
# Link-Level Attacks

- Resetting the link key - In Shaked and Wool's Paper (http://www.eng.tau.ac.il/~yash/Bluetooth/) they describe a way to force a device to lose it's link key and try and repair
  - Basically, fake the BDADDR and repeatedly fail to bring up a secure channel, and the device will assume you "lost" the link key
  - If a device has a default PIN, you can then automatically set up a trust relationship
- Cleartext data - Just like on the web, sometimes people forget to encrypt what they should encrypt
  - Usually need a protocol analyzer to make use of this
- Location Based - It's RF.. You can track people
  - http://braces.shmoo.com




# Bad Implementation

- Exposing functionality prior to authentication - This is the basis for the BlueSnarf attack
  - AT commands are sent to the phone that retrieve the address book
  - The phone for some reason assumes this is OK and gives you all the data
- Packet-o-death - Dear God… haven't we learned this problem yet?
  - Bluesmack sends a big l2ping packet to the device in an effort to kill it
  - Protocol fuzzing in general is a dandy way to knock over BT devices

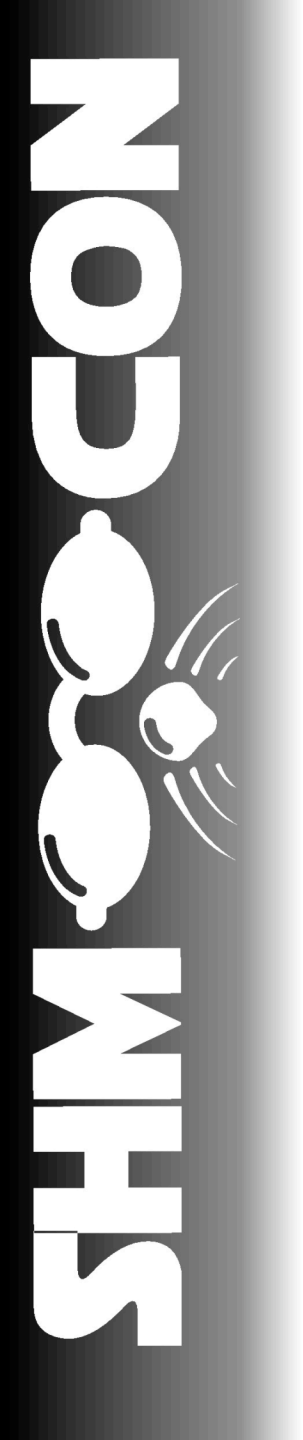



# Bluetooth Defense Techniques

- Great… now we need to figure out how to defend Bluetooth
- We haven't even figured out how to secure WiFi clients yet
  - HotSpot Defense Kit was a reasonable success (even if v2 never materialized)
  - Many host-based network security products now attempt rogue AP detection
- Bluetooth is more prevalent, and the deployment scenarios are far more varied
  - All the more reason to work to lock it down
  - User needs a way to protect themselves from bad implementations

# BT Defense - Some Advice

- Security products need to be usable
  - There's a corollary here that says "in complicated and emerging technologies, only users can recognize attacks"
  - Another corollary says that "products rushed to market don't have the best security"
- It turns out, like rogue access point defense, this is not rocket science… but yet it's not a readily available capability for the user




# User Notification and Authorization

- User should have the ability to be notified and authorize all connections and connection types
  - Inquiry scans (discovery), service discovery, RFCOMM connections, any particular profile that's being accessed
  - I can sit in a bar all day and search for discoverable devices without being detected.. That's just silly
  - Architecturally needs to be non-bypassable
- User should have the ability to whitelist based on MAC addr, device key, or other values

# Configuration Options

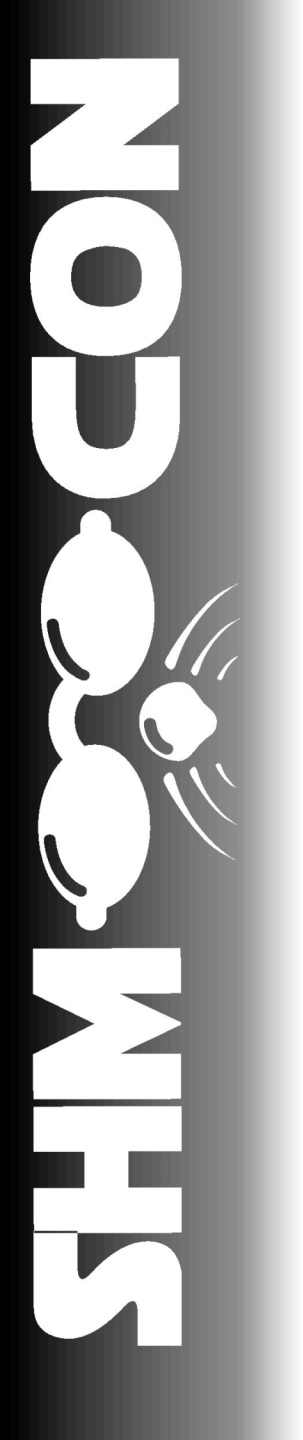
- Limiting access of trusted devices - Just because you've paired with a device doesn't mean it should be able to do _everything_
  - Per profile limits, connection limits, etc..
- Changing PINs
  - Even some of the PIN helpers are pretty lame.
  - Must have better PIN management
- Better protection of Link Keys
  - More secure storage of Link Keys (TPM?)
  - If a device suddenly "loses" it's Link Key, red alert should be sounded

# Profile Specific Guidance

- For all devices, if new profiles suddenly are offered, don't allow the connection
  - Ie: if your headset was just a headset yesterday, but now has OBEX and file transfer support, you may be under attack by a Linux box
- Handsfree/Headset - Whitelist AT commands that can be used (AT+RING, AT+CKPD, etc)
- Serial Port - Implement fuzzing detection
- OBEX - Require auth _always_
- File Access - Sanity checks for data leaving the device

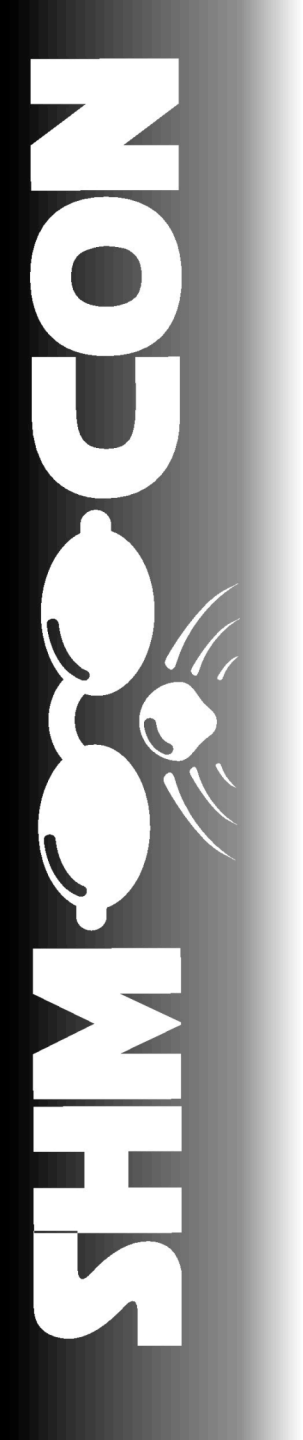
# Stack Changes Needed to Implement BT Defense

- Ability to whitelist BDADDRs
  - Sure they can be spoofed, but it's a start…
- Ability to scan connecting devices to verify the device is the type and specie of device you expect
  - This kind of "connect back" is much more socially acceptable in wireless PAN's
  - Allows for device profiling
- Notification hooks
  - At all sensitive points discussed before, provide hooks to audit actions and make decisions based on those actions




# Bluetooth Defense Kit - Demo

- http://bluetooth.shmoo.com/ for source code




# Summary/Questions?