# “How can I pwn thee? Let me count the ways”



**RenderMan**

**RenderLab.net & Church of Wifi**

**Render@Renderlab.Net**

# How can I pwn thee?

- Born out of conversations at SECTOR
- Workforce is increasingly mobile and wireless
- Mobile users are away from your watchful BOFH eye (and punishment)
- How do you educate them, protect your company, protect yourself
- By no means and exhaustive list
- Full Disclosure

# Meet Bob



- Bob works for widgets international
- Bob sells widgets
- Bob travels to customer sites
- Bob is your worst nightmare

# Bob

- Bob likes to think himself tech savvy
- Bob really just knows enough to get access to pr0n
- Bob is widgets internationals worst enemy
- Bob is also the worst case scenario



# Let me count the ways

- Let's pwn Bob
- We won't touch Bob, just abuse wireless communication
- I.E. Bored hackers on long trips to a conference through international airports coming from another international conference in, say, Norway...



# WiFi Threats

- Bob has a laptop with tons of private company info
- Bob likes to connect to hotspots at airports, train stations, hotels
- Bob connects to anything – Linksys Global Network



# WiFi Threats

- Hotspots generally do not encrypt
- Cleartext = Clear to read = Clear to inject
  - Images, Scripts, DNS, etc
- No VPN = certain pwn'age
- No firewall + browsable shares = pillage!
- MiTM attacks, password snarf
- Defcon 15 Hotel net
- Attacker is on the local net
- Driver Vulns

# Norway experiment

- Airpwn inject 'alternate' images
- See if other continents were observant
- First image, not so much...

# First Image



# Norway Experiment

- Not many noticed
- A few scratched heads
- Lets up the ante
- Second image...

# Second Image

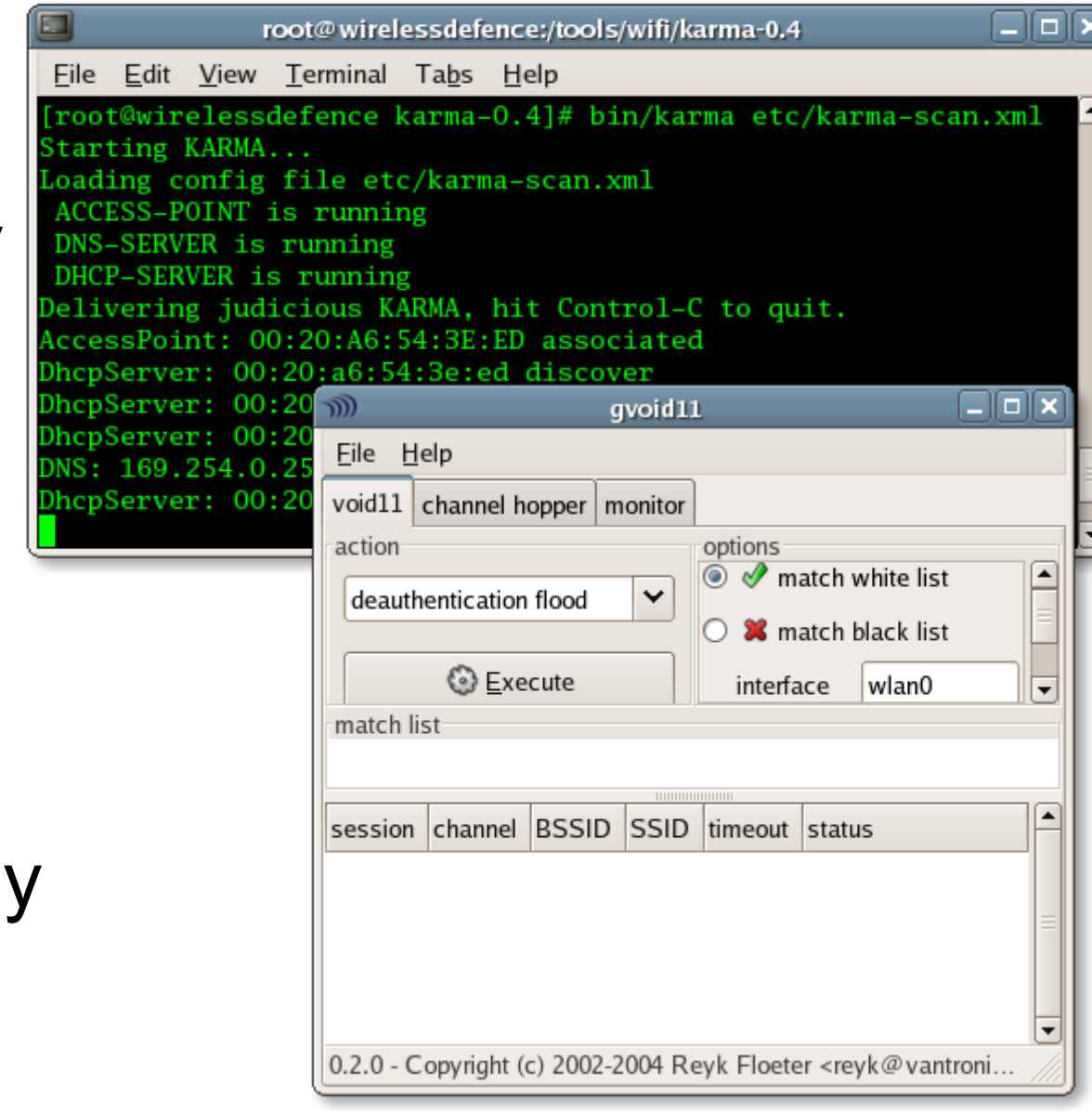


# They got the hint

I didn't get punched in the face (yay!)

# WiFi Threats

- Karma, Hotspotter, Metasploit
- Hacking the friendly skies
- Cafe Latte exploit, recover company WEP keys
- De-auth headaches
- If it's on, it's probably pwn'able



# Stopping WiFi Threats

- Disable Wifi when not in use
- Connect to network but use VPN for everything
- Assume your being attacked
- Don't trust customer nets either
- Turn on Firewall
- Be cautious
- TOR solves a fair number of problems in a pinch

# Bob's Phone



- Bob lives on his cell phone
- Bob loves his Bluetooth headset
- Uses cell phone for SMS One Time Pads
- Keeps the companies private directory in his phone book

# Bluetooth Threats

- If Bob's phone is on discoverable with default PIN, anyone can connect
- Paired devices get access to whole device
- Read/Write SMS, Phonebook, notes, images
- Remote AT commands on some models
- Premium rate calls
- Bob has to explain 9 hour call to Madame whipsalot's fun time party line on the company phone

# Bluetooth Threats



Apologies to Major Malfunction

# Bluetooth Threats

- Bob's headset uses default PIN
- Bluebump and re-pair
- Listen to conversations
- Inject audio (car whisperer)
- Boardroom bug
- Make Bob think he's crazy

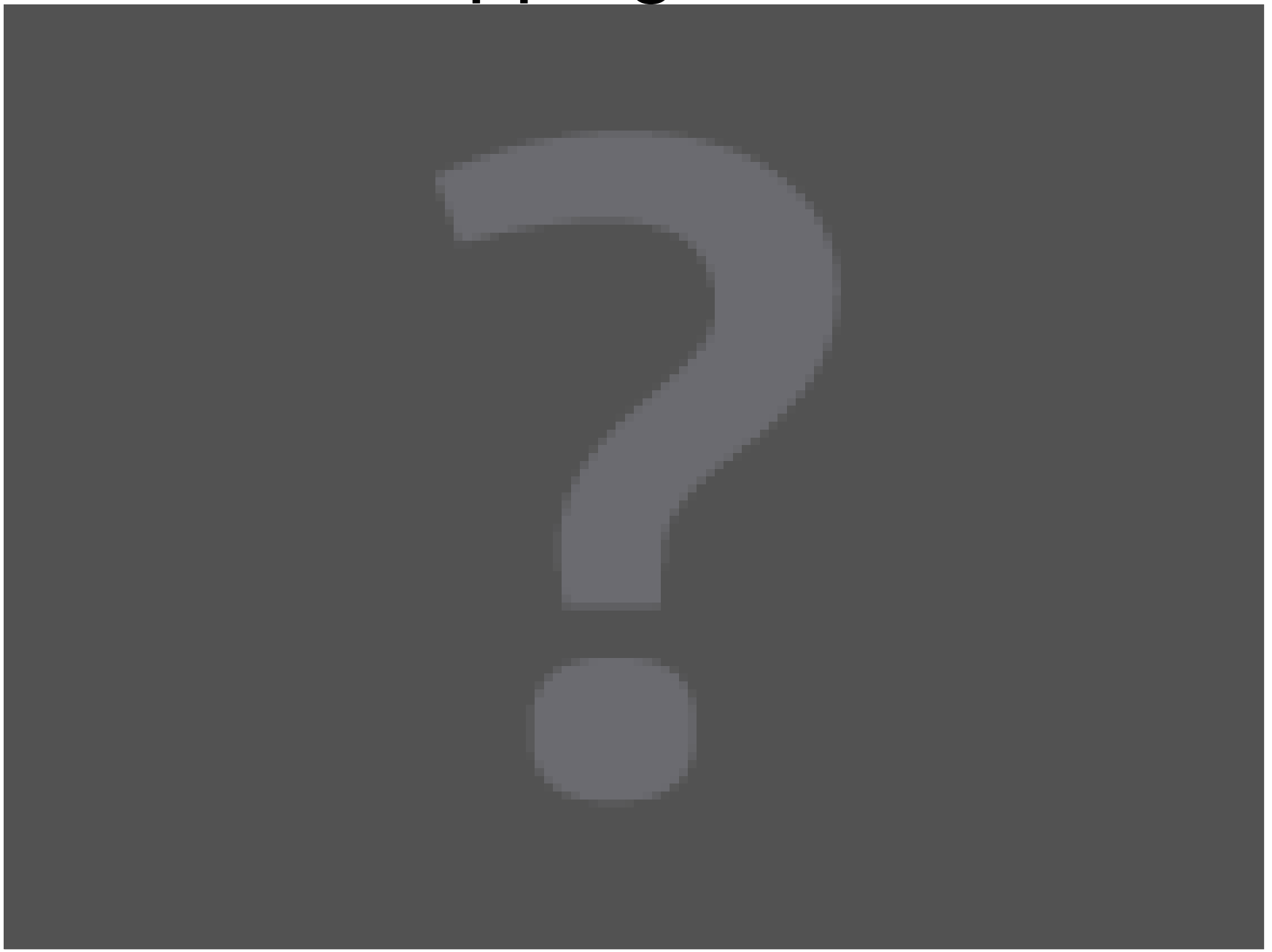
# It is god!



# I Hate Headsets



# Eavesdropping on Headsets



# Pwn'ing Bobs Wife

- While rummaging through Bob's phone, we make a discovery
- Some things should not be wirelessly enabled
- 'Special' SMS messages on Bobs phone, start sending on his behalf to his wife
- It's not discoverable but...
- Who thought this was a good idea?

# 'The Toy'


Imagine...
a shared naughty secret...
tease...please...excite...control...
from anywhere in the world with a simple text message...

# 'The Toy'

- Bluetooth enabled vibrator, 'reacts' to special SMS messages when paired to a compatible phone
- Each character has it's own reaction
- thetoy.co.uk



# Get the Innuendo out of the way

- 'Penetration Test'
- 'Rooting the Box without a trojan'
- 'Reach out and touch someone'
- 'Can you hear me now?'
- I can't wait to find one on a site survey.....

# 'The Toy'

- Teledildonics really needs some lessons in security
- An extreme example of a generally bad idea
- Serious implications here
- If Bob is not sending the messages, is it rape?
- Could non-printable characters cause potentially dangerous actions of the device?
- Seems funny, but is quite serious

# Stopping Bluetooth threats

- Turn off Bluetooth or just discoverability
- Change default PIN
- If possible, limit access to paired devices
- Prompt for pairing
- Turn off headsets when not in use
- Consider the security implications of your devices



# Bob's Keys

- Bob has a proximity card key for the office
- Card is on a lanyard with his ID badge
- Wears it all the time
- See Johnny Long's 'No Tech Hacking' talk

# Keying Bob

- Most common prox cards are not encrypted
- cq.cx  - DIY prox card cloner
- Copy the key for later use





# Keying Bob

- Traditional keys vulnerable too
- Photo can reveal bitting, keyway
- Diebold web store for spare keys
- Common office furniture key, copied from photo



# Keying Bob



# Bob's Passport





# Bob's Passport

- New RFID passports can be easily read
- Encryption not very strong
- Even US “Tin Foil Hat” doesn't work well



# Bob's Passport



# Bob's other Duties

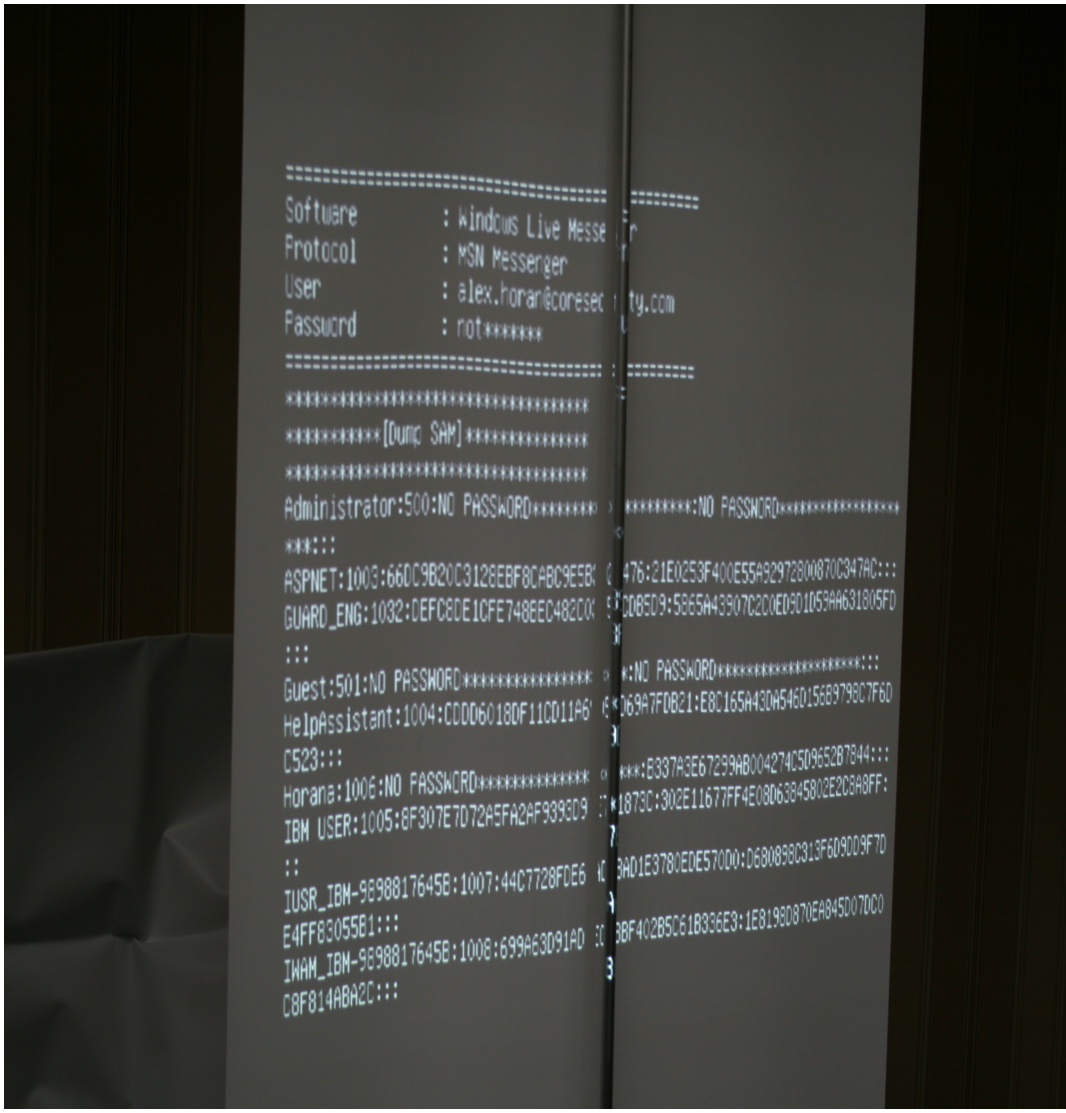
- Bob occasionally works trade shows
- Bob's sales depend on demo widgets being operational
- What happens when you have widgets that accept unauthenticated commands?
- Don't try this at home.....

# Gizmodo at CES 2008



# Bob's other Duties

- USB Switchblade, pwn the demo laptop
- Shmoocon 2007, unnamed vendor laptop
  - Was a marketing laptop, no company passwords
  - Right place, right time, Right Tool
  - I'm dangerous when bored



# Bob's pwn'd

- Pwn'd his laptop
- Pwn'd his data
- Pwn'd his cellphone
- Pwn'd his wife!
- Pwn'd his keys
- Pwn'd his demo's
- Pwn'd his ability to work

# Bob is Pwn'd

- Suggestions of your own?
- Mobile workforce education
- What are you doing to help them help themselves?



# Have you got any suggestions?

- Blackberry a different beast but worth exploring
- Wireless presentation mics?
- Wideband jamming?

# Game Over

Questions, comments, accusations?

render@renderlab.net

Huge, gargantuan, mega thanks to Rob T Firefly for the Bob illustrations