How Hackers Won the Zombie Apocalypse

Dennis Brown
QuahogCon
July 2010

Introduction

- What is Quahogcon
  - New regional con in Rhode Island
  - Focusing on Infosec and Maker Culture
- Who am I?
  - Dennis Brown – Quahogcon Organizer
    - DC401 – Rhode Island Defcon Group
    - Day Job - Security Researcher for Tenable Network Security

Badge Hardware

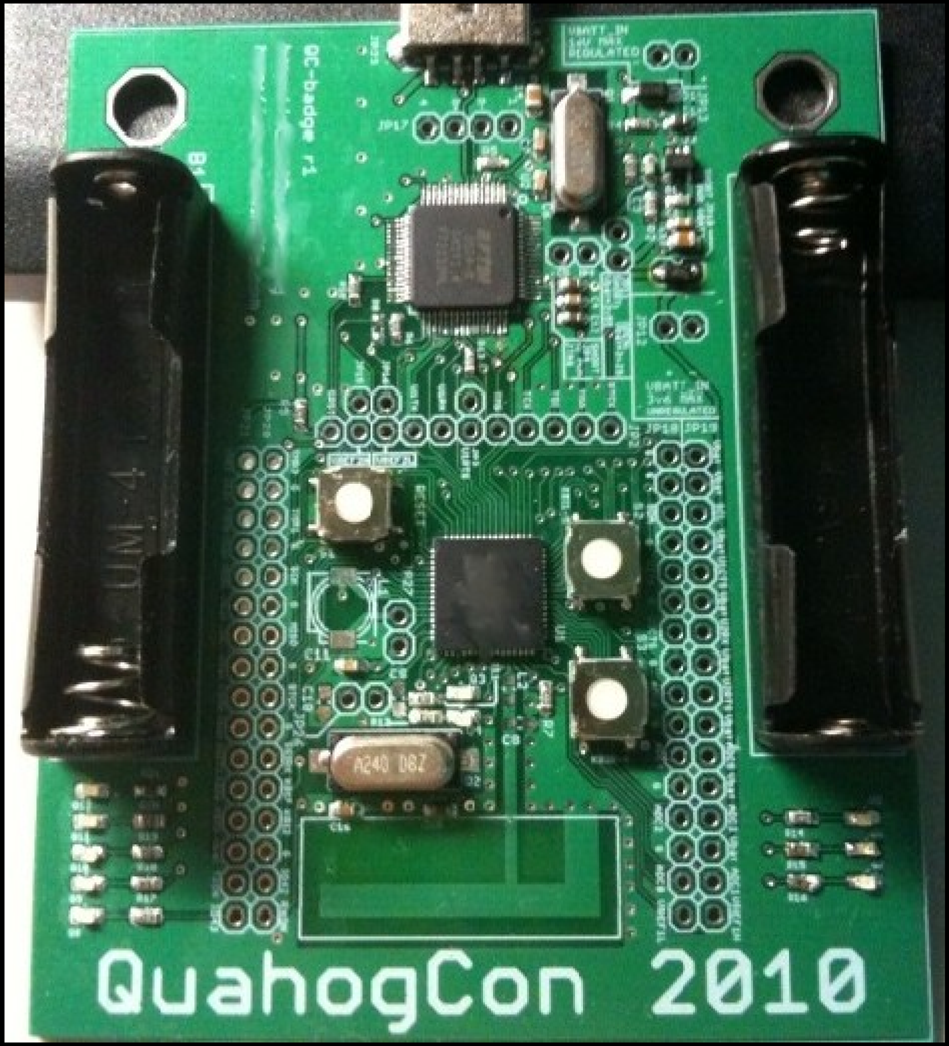
- Ultimate goal was to have a hackable badge
    - Functional and usable post-con
- Our desired result was to include
    - Wireless connectivity
    - A compelling “game” in the firmware
    - Open source development environment
    - Easy to write custom firmware for
        - We got 3 out of 4!

The Badge

- Based off of RedWire LLC's RedBee Econotag
  - Freescale MC13224v ARM7 Microcontroller
  - Zigbee!
  - 36 GPIO Headers
  - USB connector – easy to flash
- Added 2 AAA batteries and 7 LEDs
- Low cost (~$30 per badge)

End Product

- Interface Components
  - 2 Buttons + Reset
  - 5 Red LEDs on left
  - RGY LEDs on right



Badge Features

- Easy to code for
  - Sorta
- Custom firmware
  - Kismet client – Zigbee sniffer
  - Killerbee firmware – Zigbee packet injector
  - Contiki support – Full system environment

Con Firmware

- Wanted an interactive “game” for attendees
  - Ways to affect other attendees
  - Ways to hack other attendees badges
- Multiple design ideas
- Landed on a Zombies vs. Humans concept
  - Chosen 3 weeks before the con
  - Note: More time is a good idea!

Zombies versus Humans!

- Humans kill Zombies!
  - Multiple attack modes
- Zombies kill Humans!
  - Charge-up attacks
- Speakers and Vendors were Clerics!
  - Healed Humans, reclaimed Zombies
- Security “Mussel” could attack anyone
  - Not very powerful (so they'd get to work!)

How It Worked

- Live demo!
  - Attacks did 1-5 damage
  - Humans had 500 health, Zombies 300
  - Dead Humans became Zombies
  - Dead Zombies became incapacitted
    - Could come back to life
  - Clerics healed up to 20 health
      - Uh, oops!

How It Worked (2)

- God mode!
  - Only 2 badges flashed in this mode
  - Designed to be a “prize” for attendees
  - Allowed user to turn badges into any mode
    - Except God mode

Predictions

- “Encryption” would be cracked
  - Intentionally bad!
  - XOR, no checksum
- Packet replay attacks
- Hardware Hacks
  - Auto-attacks
- The Unknown!

The Invasion Begins!

- Badges distributed 5PM Apr. 23
  - 65% Human, 30% Zombie
- First wave: Predictable
  - Human dominance, not completely interested
  - Zombies attacked, tried to get a foothold
- Saturday Apr 24, everything changed!

Badge Hacks

- Some predicted, some not
- Unsuccessful Attacks
  - Hardware Hacks
    - 555 Timer to automate attacks
    - Predicted!
    - Stopped in firmware, rate limit on attacks
    - Still automated attacks, simplified gameplay

Moderately Successful Attacks

- Fuzzing
  - Not entirely predicted
  - Graph goes here
  - Modified code samples to create/replay packets
  - Successful at making badges “freak out”
  - More successful at Denial of Service
    - Overloaded badges, essentially halted the game
      - Very confusing!

Very Successful Attacks

- Packet Replay
  - No Checksum on packets
  - Could replay “known good” packets
  - No rate limiting
    - Successful autoattack!
  - God Mode was obtained this way, but not fully
    - More work was needed to crack it!

Very Successful Attacks

- Cracking Encryption
  - Very simple XOR “encryption” for Zigbee packets
    - XX XX XX XX XX XX XX
    - First byte = key
    - Second Byte = Packet Type (XORed by key)
    - Third Byte = Action “Strength” (XORed by key)
    - Other Bytes = Junk

Very Successful Attacks

- Brute Forcing
  - Post-encryption cracking
  - Discovering the protocol
    - Graph of valid commands
  - Obvious attempts
    - Examples – so close!
  - Grand Prize – Cracking God Mode!
    - Only a few people managed this

Spoiler Alert!

- Quahogcon 2011 Badge
  - Preliminary Design – Arduino based
  - More to come!

Lessons Learned

- Denial of Service Attacks Suck!
  - Game outages were no fun
  - Will need to take steps against fuzzing next year
- XOR Encryption was ALMOST good enough!
  - Remained uncracked for about 18 hours!
- More potential hardware hacks needed
  - No successful hardware hacks affected the game
    - People still had fun with the hardware regardless!

Conclusion

- Wireless Badges means Maximum Fun!
- Messing with other peoples badges is More Fun!
- Having great badges is affordable!

Special Thanks

- John 'Ducksauz' Duksta – Badge Hardware
- Dragorn – Firmware Concept and GPIO Code
- Redwire LLC – Econotag Design
- m33p – Playtesting
- Con Attendees – Making it all happen!

Q&A