



Badges? We Don't Need No Steenkin' Badges!

Making of the CCDC Badge and Access Control
System

About Me

- Manager for IS Security and Disaster Recovery at Care New England
- Penetration Tester and Chief Research Officer with PaulDotCom Enterprises
- Host of PaulDotCom Security Weekly, a weekly computer security podcast discussing recent trends, news and technical details.
- Author with Syngress publishing, including Ultimate WRT54G Hacking, Using Wireshark and Ethereal, and How to Cheat at Configuring Open Source Security



Current Interests

- Of course, penetration testing and hacking!
 - The only difference is permission...
- Recon!
 - From the complex to the mundane, how can we be better informed about a target? Metadata, SIM cards, Barcodes, etc.
 - How do attackers leverage the same information?
- Wireless of all varieties!
 - 802.11, Zigbee, RFID Public radio frequencies (900Mhz, pagers), video, and most recently HAM radio.
- Hardware Hacking!
 - If I own it, I open it. Data Sheets, Oscilloscopes, Multimeters and Soldering Irons are your friends!
 - Currently working on several projects, WRT54G, Arduino and RFID related. Looking to explore more on automated systems and DIY UAVs



About the Badge

- Laser cut acrylic
 - Red team == RED
 - Blue team == BLUE
 - Exercise Control == WHITE/CLEAR
 - Volunteers == BLACK
- In a form factor familiar to many for access control systems
- A big thanks to our local hacker/artist collective, AS220
- A word of advice, don't wait until the last minute to book time on the laser cutter!



Badge Electronics

- Very simple electronics:
 - Passive RFID tag
 - No battery needed!
- Each badge spits out a unique ID when accessed
- Only the Red and Blue teams are enabled
- Overall cost per badge ended up at \$6 each
- No, I won't tell you more...



WANT !

- Originally we wanted to provide each member of the Red and Blue teams with
 - Laser cut badge
 - RFID tag
 - RFID reader/writer
 - ACG Dual ISO OEM Module
 - http://www.therfidshop.com/images/ACG_Pass_Dual_ISO_OEM_V2_2_Datasheet_03.pdf



WANT MOAR!

- FTDI serial to USB converter
 - USB-RS232-PCB Converter
 - http://www.ftdichip.com/Documents/DataSheets/Modules/DS_USB-RS232_PCB_V130.pdf
- Badge cost rose to \$90!
 - I couldn't get any vendors to return my calls for sponsorship...
 - ACG reader hard to come by in the US, needed to be imported



MOAR!

Access Control Reader

- Based around some open, easy to use hardware:
 - Parallax RFID reader
 - Arduino Duemilanove Atmega328 with custom shield
 - Processing!
- Simple feedback to the user
 - No swinging gates, man traps or shotguns
 - Simple color output on TOP of system based on badge access permissions
 - Red when ready to read
 - Red flash, no access
 - Green light up with return to red, access granted
- When system fails, assume that it fails open!
- This is a learning exercise, so the “honor system” is at play



Recreate

- We wanted this system to be:
 - Inexpensive - student budgets
 - Easy to recreate - readily available parts
 - Have few dependencies - open development tools, no large infrastructure pieces
 - Easily transportable and stored - think shipping and dorm rooms, but not TSA :-)



Reanimate!

- We wanted to you, as Red AND Blue teams to be able to recreate this at a later date
 - The learning should not end on Saturday evening!
 - I won't release ALL of the details until Sunday morning
 - Check <http://www.pauldotcom.com> for more in the coming week



Some Rules

- If you want to gain access to the opposing space, the RFID reader has to give feedback for a “green light”
 - This will allow for physical access, but to keep things safe and sane, we’ll grant you layer 1 access behind the firewall.
 - If physical access is maintained onto day 2, we’ll give you walk on access:
 - No physical touching, throat punches, or using crutches as a weapon.
 - If asked to leave, please do so.



Some More Rules

- In the event that your badge “bricks”...
 - I have limited spares
 - The badge color will always allow you access to the correct space - think visual authentication, such as an armed guard, licenses, etc.
- Plz, no DoS thx.
 - If you break it, or goof up so that the readers do not function as initially installed, they will be “reset to installed defaults”



How Larry Can Help

- Think of me as your friendly neighborhood physical security integrator/installer.
- I do have some RFID gadgets
 - I'll "loan" them to you, with some limitations
 - May include the specific modules we wanted to implement but could not afford...
- Of course this is intended to give you some education, so I'm here to help - without giving away all of the secrets.
- I've got all sorts of bits and bobs that might help with some of your endeavors...



Wrapping Up

- I'll give you all the secrets in 5-10 minutes during closing, including a few things that you might not have thought of
- Don't hesitate to ask if an attack or defense mechanism is in scope; you might be surprised
 - Some will require some discussion by the organizers
 - Others may come with some penalties or additional rules.



Go HAX!



MARCH 11-13 2010
UNDERSTAND, DETECT AND DEFEND
5TH MID-ATLANTIC REGIONAL CCCD