



\$30, 30 Minutes, 30 Networks

Project Cowbird

Jonathan Squire, CISSP



Agenda

- Always popular disclaimer
- Project cowbird background
- Hardware
- Demo
- Why this works
- Future research



Important Disclaimer

(Pay Attention)

- This project is my own personal research and is not sponsored by anyone but me.
- If you break something you get to keep the pieces.
- If you'd like to contribute, please see me after the talk.



What Is a Cowbird?

- A cowbird is a brood parasite which lays its eggs within another bird's nest in order to have its offspring nurtured.
- These parasite eggs do not look much different than a normal egg, but when hatched the birds grow quickly due to their voracious appetites.
- If starving does not kill the natural offspring, the larger bird pushing them out of the nest will definitely help them on their way.



What Is a Cowbird?

- Nice little birdie.



Background

- Project Cowbird is part of a larger research project "The Ecology of Information Security" which equates different attack and defense techniques to creatures participating in an ecological system.
- Various forms of predator and prey are proposed and in some cases implemented using off the shelf hardware.
- "The Ecology of Information Security" is slated for release this time next year.



Project Cowbird

- Project Cowbird is an implementation of a parasitic predator using a standard off the shelf wireless media adapter, originally designed to display photos and play music on your TV.
- This device, which can be acquired for \$30-70, has been re-purposed to run kismet.



Project Cowbird Hardware

- Linksys WMA11b
 - Prism2 wifi card
 - 10/100 Ethernet
 - JTAG
 - TV Out!
 - IR Remote Control
 - 16 MB of ram
 - 2 MB of flash



Other Nice “Features”

- WMA11b already boots from the network
 - Uses UPnP to boot
- Device happily tells you it's on the network
- GPL code for the device available (though distribution has some problems)



Demonstration

PROTECT
Cowbird



Why Can We Do This?

- Boot “.img” files are just cramfs images
- No verification of image authenticity
- No control over who can boot the device
- Config file for boot server is just xml with a filesize and image file



Is This Bad?

- Who else is looking at your photos?
 - Cowbird makes it obvious it's not the original software
 - Will everyone else?
- This is not the only consumer device to boot insecurely off the network
- The hardware is cheap enough to throw-away yet provides a lot of hardware for the price
- No physical access to the device is needed



What Can Be Done?

- Sign boot images
- Authenticate devices to the network
- Private media networks
- Demand secure consumer devices



Future Research

- Cowbird Research
 - CHIRP
 - Cowbird Hypertext Inner Roost Protocol
 - FLOCK
 - Formal Loosely Organized Cowbird Kingdom
 - NEST
 - Cowbird booting other cowbirds
 - PEACOCK
 - Eye candy on the TV (still for \$30)
 - BIRD BRAIN
 - New boot loader / flash image



Future Research

- The Ecology of Information Security
 - Project Hawk
 - Predator for Cowbirds and other wireless pests
 - Potential to reuse same cheap hardware
 - Project Homing Pigeon
 - Self organizing mesh networks that find a way home
 - Will build on Cowbird/Hawk research



Questions?

Jonathan Squire, CISSP
project.cowbird<at>gmail<dot>com



References

- Cowbird updates and other research
 - <http://www.bigbrainlabs.com/>
- WMA11b information page
 - <http://www-jcsu.jesus.cam.ac.uk/~acw43/projects/wma11b/>
- Kismet
 - <http://www.kismetwireless.net/>

