

# Isolating and Protecting Goofball Devices

A database-driven methodology

Tom Zeller July 2008



# Purpose

- Automatic
- Detect special categories of devices
- Apply appropriate policies to them
- Examples:
  - SCADA => SCADA vlan
  - Printer => port ACL with few ports open
  - Stolen laptop – notify police



# Assumptions

802.1x on all (most) wired and wireless ports

Switch proxies for non-802.1x

using MAC address as username and pw

RADIUS server customizable to recognize MAC addresses, look up and apply policy



# Define Device Categories

- Categories should be EASILY created
- RoboDog Lives!



# Define Policy Action for Each Category

- VLAN ID
- Port ACL
- Access Denied
- Alert someone (e.g. stolen laptops)
- Allow only if in a particular building
- Allow only if network type matches



# MAC Table Input

- Web application with granular access to register devices
  - e.g. Only physical plant admins can add cameras
- API for IDS, scanners, etc to add devices on fly
- Include date for annual refresh
- Force building restriction for most categories
  - e.g. printers
- Restrict to wired only or wireless only ?



# RADIUS Logic

- Detect username=MAC address
- Is device registered? No=DENIED
- Yes => is location and network ok?
- Yes => send policy as RADIUS attributes
  - (or other action)



# One Issue

- Translating policy (e.g. SCADA) to correct VLAN ID



## Transparency: The Solution to Complexity

- Develop web application to allow support personnel to enter MAC address and see what SHOULD have happened (category, building, VLAN, ACL) and/or what ACTUALLY happened (from log file)
- Never mind, we'll do that later when we write the documentation



# Need to investigate

- Trusted Computing Group – Trusted Connect Group
  - New IF-MAP standard for NW database
  - Input from multiple sources
  - Info subscribed by network device
- Consider intersection between device and user, if any



# Isolating and Protecting Goofball Devices

A database-driven methodology

Tom Zeller July 2008

