



SCADA Honeynets

Dale Peterson, Digital Bond

peterston@digitalbond.com

See our SCADA Security Blog

www.digitalbond.com/SCADA_Blog/SCADA_blog.htm



Digital Bond

- ◆ A Consulting and Research Security Practice
 - 80%+ of our work is in control system security
 - Assessments, architecture, policy
 - Active in SCADA security standards efforts
- ◆ Research Projects
 - SCADA IDS Signatures
 - Field Device Protection Profile
 - Nessus SCADA Plugins
 - Vulnerability Disclosure
 - SCADA Honeynet



Honeynets

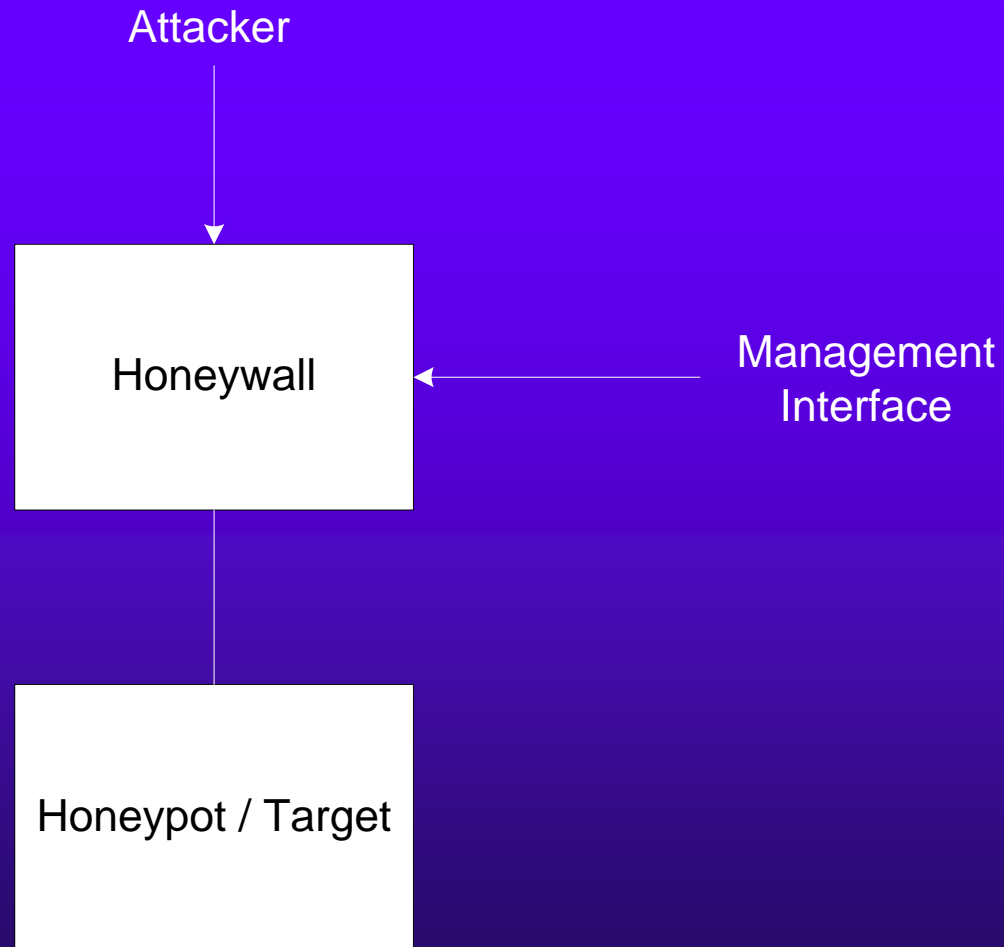
◆ Honeywall

- Capture attack data
- Control the attacker
- Manage the honeynet
- Not visible to an attacker

◆ Honeypot / Target

- Real or virtual (simulated)
- High interaction
- Provides responses to keep attacker going

Honeynets





Why Honeynets? Research

- ◆ Learn about the threat
 - Risk = Vulnerability * Threat * Consequence
 - We (the community) know consequence
 - We are understanding the vulnerabilities
 - Threat is the big unknown
 - What is the frequency (likelihood) of attack?
 - How will a control system be attacked?
 - How far will an attacker take the attack?



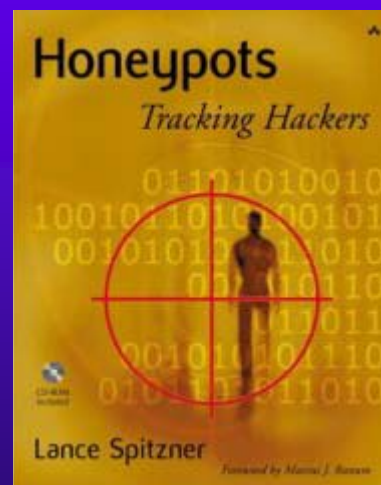
Why Honeynets? Production

- ◆ Early warning sensors for attacks
 - Honeynets in a production environment should never be attacked
 - Any activity on a production honeynet should be investigated



More on Generic Honeynets

- ◆ The Honeynet Project, www.honeynet.org
 - Gen III honeywall
 - Many tools available at this site





SCADA Honeynets

- ◆ Existing honeynets look like systems commonly found on the enterprise
- ◆ They do not look or act like SCADA systems
- ◆ How will attacks on SCADA systems be similar to IT attacks?
- ◆ How will attacks on SCADA systems differ from IT attacks?



Exposing SCADA Honeynets

Three models considered in project:

1. Internet exposed SCADA Honeynet
 - Low cost broadband wireless data services
2. Wireless LAN 802.11
 - A plant floor, substation, pumping plant
3. Honeynet on production SCADA system



SCADA Honeywall

- ◆ Minor changes and additions to a standard Roo deployment
 - Added Digital Bond's SCADA Snort rules
 - Iptables rules to restrict traffic to realistic protocols
 - Modified swatch scripts and added health check for enhanced alerting



Real Target

- ◆ Modicon Quantum PLC at BCIT
 - Running Modbus TCP Port 502
 - Management via http and ftp
 - Real, changing data
 - Measuring water height and temperature in a lab system

Verizon
Internet

Raven
Cellular
Modem

Honeywall PC
in Austin, TX

Open VPN PC
in Austin, TX

Internet

Modicon PLC
in Vancouver, BC

Open VPN PC
in Vancouver, BC



Interesting Design Findings

- ◆ A real target can support many honeywalls
 - We did not come close to reaching the limit
 - Very low traffic with occasional bursts
- ◆ Most realistic target and data
 - Do you have a spare PLC sitting around?
 - Could a vendor do this to test their system?
- ◆ Pinging was essential, every 5 minutes, to keep target responsive at all times



Interesting Design Findings

- ◆ Cost is the main drawback
- ◆ Two PC's at Honeywall site
 - One for Honeywall and one for OpenVPN
 - Complexity with internal bridging and IP tables in a single PC implementation
 - Is not an issue on co-located Honeynets or Honeynets on a private WAN



First Virtual SCADA Target

- ◆ Developed by Matt Franz and Venkat Pothamsetty in Cisco's CIAG
 - <http://scadahoneynet.sourceforge.net/>
- ◆ Why not use this?
 - Very limited support for a small number of Modbus function codes
 - Values were hard coded
 - Would need to write a Modbus simulator
 - Modbus simulators exist; why do it again?



Triangle MicroWorks Target

- ◆ Initial solution was Triangle MicroWorks (TMW) Protocol Test Harness
 - TMW provides the DNP3 stack used in most DNP3 implementations
 - Product exists and is easily customized
 - Sample devices and data exist in Test Harness
 - Example: SEL Protective Relay



TMW Findings

- ◆ Licensing
 - Runs on Windows; possible port to Linux
 - TMW licensing issues, USB key
- ◆ Did not work with VMware
 - Requires two PC's
- ◆ Runs under GUI, not as a service
- ◆ Unreliable with multiple connections



SCADA Virtual Honeynet Goals

- ◆ Single PC solution
- ◆ No license fee (s)
 - Ruled out Windows and some simulators
- ◆ High interaction
 - Realistic, varying responses to requests
 - Realistic management interfaces



Virtual SCADA Honeynet

- ◆ Uses all open source applications

Host Operating System: Linux

Modbus TCP Service: jamod

HTTP Service: fizmez

FTP Service: iftp

Honeywall: Roo Gen III

- ◆ No license fees



Virtual Target

- ◆ Appears to be a PLC running Modbus TCP
- ◆ Realistic data points
 - Points list and sample data provided by one of the ten largest electric utilities in the US
 - Data is from a real, deployed device
 - Data points that should change, do change



Virtual Target

- ◆ Modbus TCP support
 - Jamod simulator support a large number of function codes
 - Modbus scanners and simulators will communicate with the virtual target
 - Not all function codes supported, but this is very realistic



Virtual Target

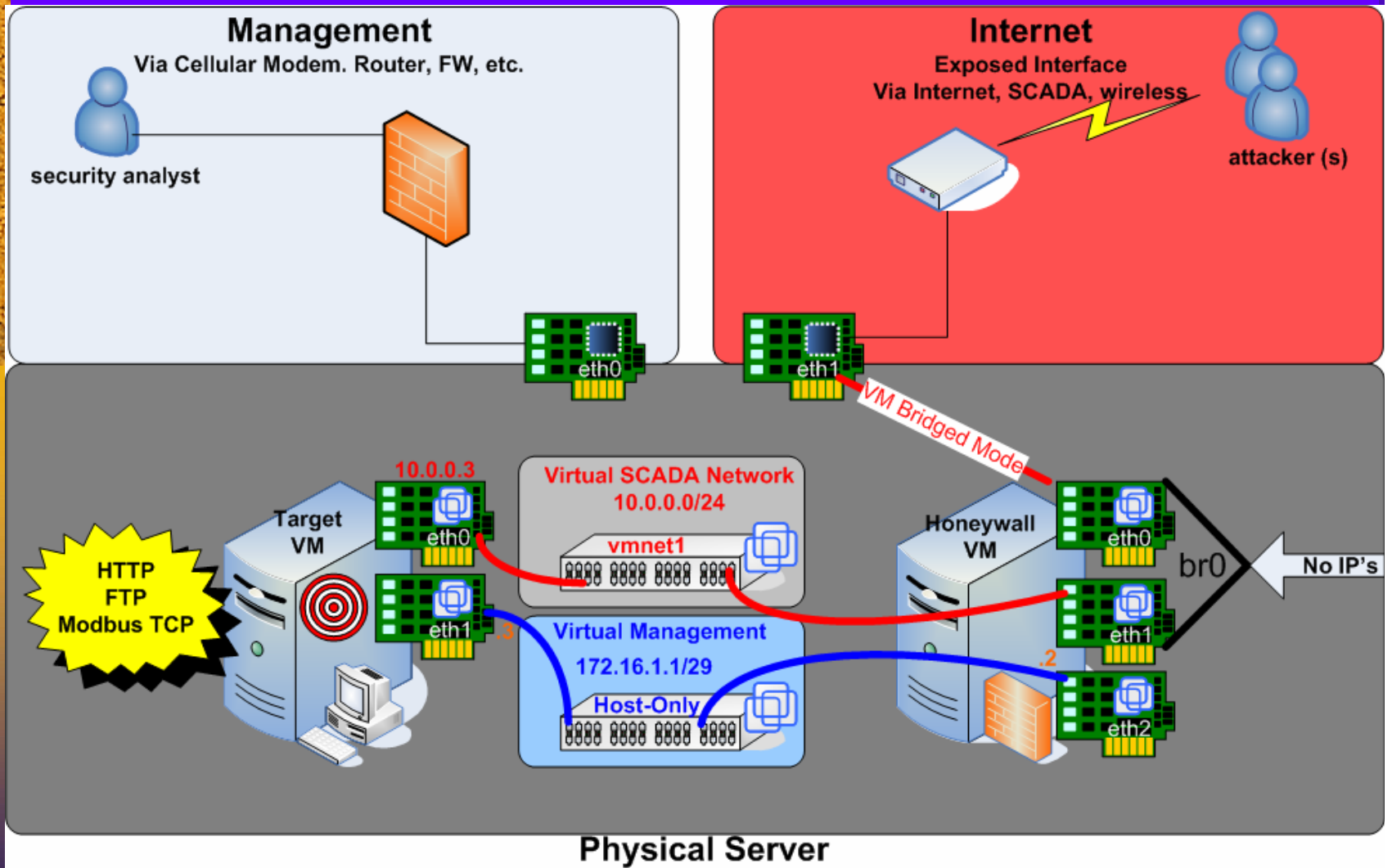
- ◆ Management interface is critical because this includes ports commonly attacked
 - http, ftp, telnet, ...
- ◆ Virtual target mimics a top-3 vendors PLC management interface
 - Deployed with default credentials
 - Responds to many management commands



Virtualization - VMWare

- ◆ Single PC solution requires two virtual PC's
 - Linux host operating system
 - One VM for Honeywall
 - One VM for target
- ◆ We (developer) buys VMware
- ◆ Develop VMware server images
- ◆ No license required to run VMware images

Architecture





Installation

- ◆ Install Linux
- ◆ Download two VMware server images
- ◆ Install the VMware console
- ◆ Configure the physical interfaces
- ◆ Start the VMware servers

SCADA Honeynet Is Running



Honeynet Results

- ◆ Caveat – limited time and limited honeynets deployed. Not statistically significant
- ◆ Honeynets were exposed to the Internet as well as in less exposed environments
- ◆ No activity on SCADA port
 - Modbus TCP port 502
 - Very important finding, dispels some FUD
 - Needs more data and bears watching



Honeynet Results

- ◆ Robust, automated attacks on http and ftp management ports
 - Rigorous password cracking attacks from lists
 - Web server and ftp server attacks
- ◆ Why do we say automated attacks?
 - Web & ftp management had default credentials
 - Attacker could simply Google the vendor / equipment and discover credentials
 - This never happened



Prediction

Control system default credentials
will be added to hacking tools
within two years!

Honeynets could help identify this important shift



Other SCADA Honeynets

- ◆ Stephan Lueders at CERN, Switzerland
 - Similar results on a production network
- ◆ George Mason University



Future SCADA Honeynet Work

Get many more SCADA Honeynets deployed

- ◆ Looking for two to three “beta” sites
- ◆ Available on Digital Bond subscriber site in September '06.



Future SCADA Honeynet Work

- ◆ Configurable points list file
 - Today, Honeynet looks like one realistic PLC
 - Provide capability for asset owners and researchers to easily configure with their own points list
- ◆ GUI
 - The next step after a configuration file would is a GUI interface making customization simple



Future SCADA Honeynet Work

- ◆ DNP3 simulator support
- ◆ DCS Honeynet
 - Appear as multiple PLC's
 - Add Windows HMI
 - Still on one PC
 - Planned for early '07 pending sponsor



Contact Information

Dale Peterson

peter@digitalbond.com

954-315-4633

Presentation available at:

www.digitalbond.com/SCADA_Blog/SCADA_blog.htm