



# **Wrestling With Reality — Integrating New Security Solutions into Existing Control Systems**

**David M. Nicol**

**Director, ITI**

**Professor of ECE**

**University of Illinois at Urbana-Champaign**

[www.iti.uiuc.edu](http://www.iti.uiuc.edu)



# Making the Industrial Connection....



## NetAPT --- Network Access Policy Tool

- Borne of experience with validation of large secure publisher-subscriber system for DARPA
  - How do you know what is accessible through systems with many many firewalls?
- Originally intended function --- validation of firewall implementation
  - Compare implementation against “Global Policy”
- Original sponsor ---
  - Institute for Information Infrastructure Protection (I3P)
    - Part of a team effort focused on security solutions for oil and gas industry
    - “Tech transfer” a serious objective



# Gratuitous NetAPT Graphic

APT - Access Policy Tool

Mode:  Configuration  Online  Offline

StaticLayout

Topology File: NetAPT\_demo.drw

End Traffic Analysis Log

Rulesets Global Policies

- Access Decision Path #139
- Access Decision Path #140
- Access Decision Path #141
- Access Decision Path #142
- Annotated Paths
- Likely Root Causes
  - [1] permit incoming any/ip
  - [3] permit incoming 23/tcp
  - [6] permit incoming 1433/tcp
  - [7] permit incoming 8541/tcp
  - [3] permit incoming 23/tcp
  - [1] permit incoming 1433/tcp
  - [4] permit incoming 00#

**Rule**

Rule Name: [1] permit incoming any/ip

Description: [1] permit incoming any/ip

Source IP: any

Source Mask: 0 . 0 . 0 . 0

Source Ports: any

Dest. IP: any

Dest. Mask: 0 . 0 . 0 . 0

Dest. Ports: any

IP Protocol: ip

Negated: false

Action: permit

TCP Connect: false

Direction: in

Enabled: true

Audit: false

Test Mode: false

Found 22 path(s) originating from node(s) [Wonderware HMIs (172.16.104.0/24)]

# Making Connections...Not so Easy



- The I3P project had
  - Industrial advisory Board
  - Industrial workshop / security training events in coordination with industry meetings
- Relatively few connections formed
  - Requires NDA, a “working advocate”, management has to be OK with it, access to potentially sensitive data
- We connected with someone at an electric utility responsible for audits



# Learning Expectations

- NetAPT needs topology
  - We naively supposed the user would provide network map
  - Our user figured the tool should figure it out, referenced ANTFARM
  - Topology discovery validation in fits and starts
    - Things our team initially ignored “for simplicity” were found to matter
- Tool needs to be OFF NETWORK
  - We thought automated configuration fetch would be helpful...
  - Scriptable interface (rather than GUI) would make it useable running over-night

# Learning What Mattered to the Customer



- Coordination increased dramatically when customer aimed for using NetAPT in an up-coming NEC CIP audit
- What he appreciated about the tool:
  - graphical display of network
  - full connectivity analysis
  - easy access to firewall rules
- Didn't seem to have an interest in global policy analysis!
- Had many suggestions on what NetAPT could do to help him
  - Support annotation of paths, export in spreadsheet form
  - Graphical highlighting of paths, constrain what is displayed
- NetAPT helped in the audit, impressed auditors, tech transfer continues



# Value Added

APT - Access Policy Tool

Mode:  Configuration  Online  Offline

Rulesets Global Policies End Traffic Analysis Log

StaticLayout Search Topology File: Ne

(Filtered 22/142)

Path #	Source Firewall	Source Node	Source	Sour...	Destina...	Destin...	Destin...	D...	N...
95	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
96	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
97	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
98	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
99	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	120...	80/tcp	n/a	
100	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	120...	80/tcp	n/a	
101	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	120...	80/tcp	n/a	
102	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	120...	80/tcp	gr...	
103	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
104	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
105	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
106	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
107	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
108	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
109	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
110	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	172...	80/tcp	gr...	
111	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	120...	5450/t...	gr...	
130	GenSite FW #1	172.16.104...	any/tcp	gro...	GenSit...	101...	80/tcp	n/a	
131	GenSite FW #1	172.16.104...	any/tcp	gro...	Bound...	101...	80/tcp	n/a	
139	GenSite FW #1	172.16.104...	any/tcp	gro...	Perime...	28.1...	80/tcp	n/a	
140	GenSite FW #1	172.16.104...	any/tcp	gro...	Bound...	101...	80/tcp	n/a	
142	GenSite FW #1	172.16.104...	any/tcp	gro...	Perime...	101...	80/tcp	n/a	

Found 22 path(s) originating from node(s) [Wonderware HMIs (172.16.104.0/24)]

# Reality Checks for Us



- Getting industry's attention can be tough, if they are needing to volunteer time and attention
- The value we see in our work may differ from the value industry sees
- Industry has constraints we may be un-aware of
  - Important to listen

# RBAC for Industrial Control Systems



Context: DoE funded project for developing RBAC solution for ICS, and impact Honeywell product line

RBAC is ....

Some (expected) constraints

- Minimize introduction of new software
  - implies trying to piggyback RBAC concepts on top of Windows Active Directory mechanisms
- Find solutions for legacy systems
  - Means placing “guard” devices that do RBAC policy enforcement in front of old stuff



# An Important Technical Constraint

Experion security model has a notion of “domain of responsibility”

- Controlled devices partitioned hierarchically
- Users get “responsibility” for (most) things within a sub-hierarchy
  - But this is not the same as permission!

RBAC policy *in this context* has to be expressed in terms of domains of responsibility, and permissions

The question is whether this can be shoe-horned into existing software ...

# Supporting Complex Policies



On the one hand

Microsoft has a version of RBAC

- supported in “Windows Authorization Manager”
- Concepts/constructions largely baked in, not very extensible, questionable it can support all aspects of policy needed

On the other hand

Microsoft includes “Management Console” which supports complex extensions of AD objects

- Role permissions can be described in terms of a relational database
- BUT that leaves still the problem of policy enforcement....

# A Surprising non-Technical Constraint



Discussions with IT manager at a chemical facility revealed a surprise

- Access checking is entirely physical
  - Personnel checked coming into control station
  - Control consoles open for use for anything, anytime, by anyone
- He asserts that any kind of logging in would be roundly rejected
- Can you guess who objects, and why?
- Creates challenge of crafting a technological solution that supports RBAC while respecting social constraint



# Conclusions

Developing new security solutions for industrial control system is

- Critical
- Challenging
  - Getting effective cooperation, data
- Industry has constraints that academics may find surprising

If we view them as customers, we need to view ourselves as vendors

But as with any set of constraints on technical solutions, it serves to create new technical challenges we can address