Endpoint Security

Hidden Threats and a Proposed Solution to the Problem

ISACA Fall Conference Sept 18th, 2007

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Better Knowledge
Better Decisions
Better Security
The Security Consortium

Who Am I?

- Mark S. Kadrich, CISSP
  - CEO of TSC
    - I have an axe to grind so use appropriate filters
  - 25 years of security experience
    - Practitioner, Customer, Vendor
    - Electrical Engineer (this becomes relevant later)
  - Author Endpoint Security
    - Published by Addison-Wesley
    - ISBN 0-321-43695-4
  - Calls, complaints, compliments
    - markkadrich@thesecurityconsortium.net
    - 408-313-6263

Agenda

- Problem Statement
- Some History
- Differences?
- Conclusions
- Present State of EPS
- Signs of Good EPS

Agenda

- Bad News
- A Proposed Solution
- Closed Loop Process Control Defined
- Endpoints Discussed
- Some Vendors
- Some Questions for Vendors

Our Talk….

- There are systems on your network that you don't control. When did the vending machines become a vector for a network attack? Why can't I trust my printer? Besides the standard Windows, Mac, and Linux systems, I will discuss the security issues of various types of systems ranging from handhelds to embedded control systems. Virtually everything is getting a network connect these days and sometimes, many times, that's a bad thing. We will discuss what type of controls are available and how a process control model can be used to ensure system trust - and how some systems just can't be trusted. I will discuss how the endpoint and the network must work together to ensure compliance and security because by themselves they are not capable of making an accurate determination.

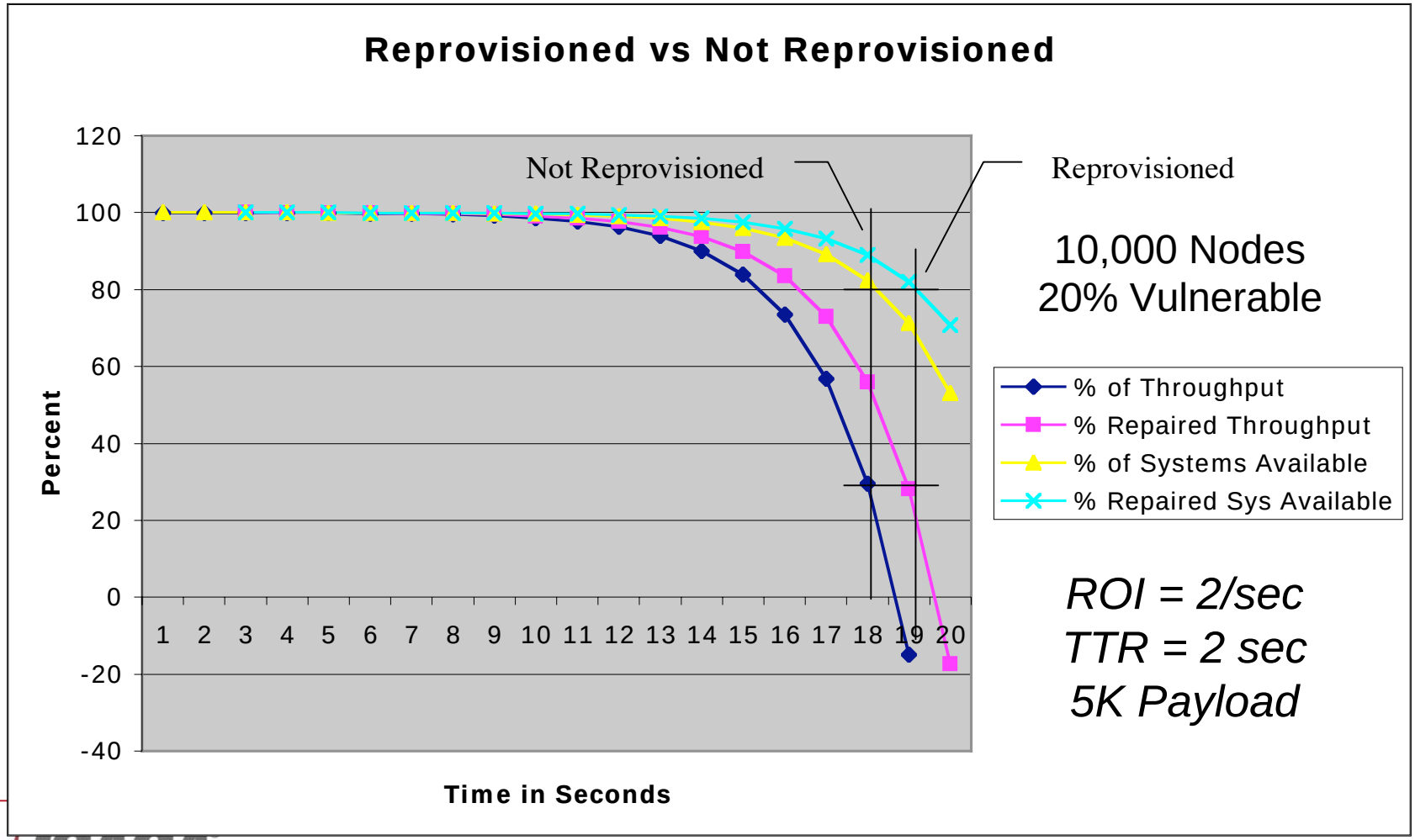
Problem Statement

- Controlled network growth difficult
  - Wireless helping here!
- Regulatory environment hostile
  - Lots of regulations
  - Lots of different interpretations
- Business processes drive architecture
  - (except for Microsoft)

Problem Statement (more)

- Attacks are automated
  - Botnets are centrally managed
  - Smart malware tests multiple vectors
- Rootkits have “how to” books
  - You don’t have to be smart
  - Population of attackers increases
- Things happen really fast

Dead Man's Curve



Audit 101

- Must have a policy to audit against
- Process must produce repeatable results
- Secure endpoints are:
  - Managed
  - Auditable
  - Trustworthy

Some History

- <fud>
- Feds say things are getting better!
  - Never hear that in the media!
  - FBI/CSI report
- Anecdotal evidence says otherwise
- High profile failures
- Scary $$ Numbers
- </fud>

Why the Difference?

- Regulatory pressure
  - Changes reporting pressure
  - Must report some things now
- Reporting requirements makes more things public
  - More things reported means that more action can be taken
  - More actions means improvement!
- Fiduciary responsibility
  - Forces legal group to manage survey responses
  - CSI/FBI had fewer details on financial loss

Conclusions

- Security continues to fail
  - That's why we have numbers
  - That's why they measure losses
- So…
  - Original hypothesis is incorrect?
  - Method for gathering information is incorrect?

- How about both?

Present State of EPS

- Independent products for:
  - Firewall
  - Antivirus
  - Antispyware
  - Software updates
  - Vulnerability management
  - Intrusion detection
  - Intrusion prevention
  - User provisioning
  - Policy management
  - Authentication
  - Authorization

Present State of EPS

- That's Okay, it's only 11 or so consoles to manage
  - Piece of cake, right?
- For the most part
  - None of them talk to each other
  - Configurations must be independently managed
- Vendors continue to
  - Generate new products
  - Provide no proof that they have secure products

Present State of EPS

- Vendors worried about vulnerabilities
  - Eliminate all vulnerabilities and you're secure!
  - Most VM solutions are Windows only
- Market Driven
  - Legislation (and thus audit) du jure
  - Lot's of templates
    - They're easy
    - Allow for OS hook
- Lots of Places that Leak
  - Printers
  - Embedded systems (More later)

Present State of EPS

- Risk Management
  - Systems measured by state of patches
  - Also measured by vulnerability profile
    - What apps are running
    - Exchange, IIS, Apache are all vulnerabilities with some nice features
- Instead of Risk, use Trust
  - Does system represent risk? (tough question)
  - But do you trust it enough to allow access?
    - This is really the question you're asking!

Signs of Good EPS

- Centralized management
  - Good build, release, test, and update process
  - All systems comply with process
  - A way to track this exists
- Good policy
  - Covers all contingencies (like a good contract)
  - Doesn't have to be worked around
- Trust based architecture
  - Decisions made regarding compliance
  - Do I trust this system enough to be on my network?

More Signs of good EPS

- Basic blocking and tackling
  - Antivirus
  - HIDS
  - Host based firewalls
  - Anti-spyware
  - Anti-spam
  - User training
- Network Security Too!
  - Firewalls
  - NIDS/NIPS
  - NAC

The Bad News

- Worse thing about the present state of EPS
  - It only focuses on things that you see or make the news
    - Desktops
    - Notebooks
    - Servers
    - Handhelds
- Hidden things still out there
  - Embedded systems
  - Access Points
  - Printers (where are all your printers?)

What Can Be Done?

- Need a better answer
  - Acknowledge lack of integrated engineering
    - Driven by marketing
    - Treading water
  - Integrate network and endpoints
    - Both have strengths and weaknesses
    - Overlap can be used to our advantage
- Identify the applicable processes
  - Many processes (human and technological)
  - Many disciplines (business and engineering)
  - Must be identified and accounted for

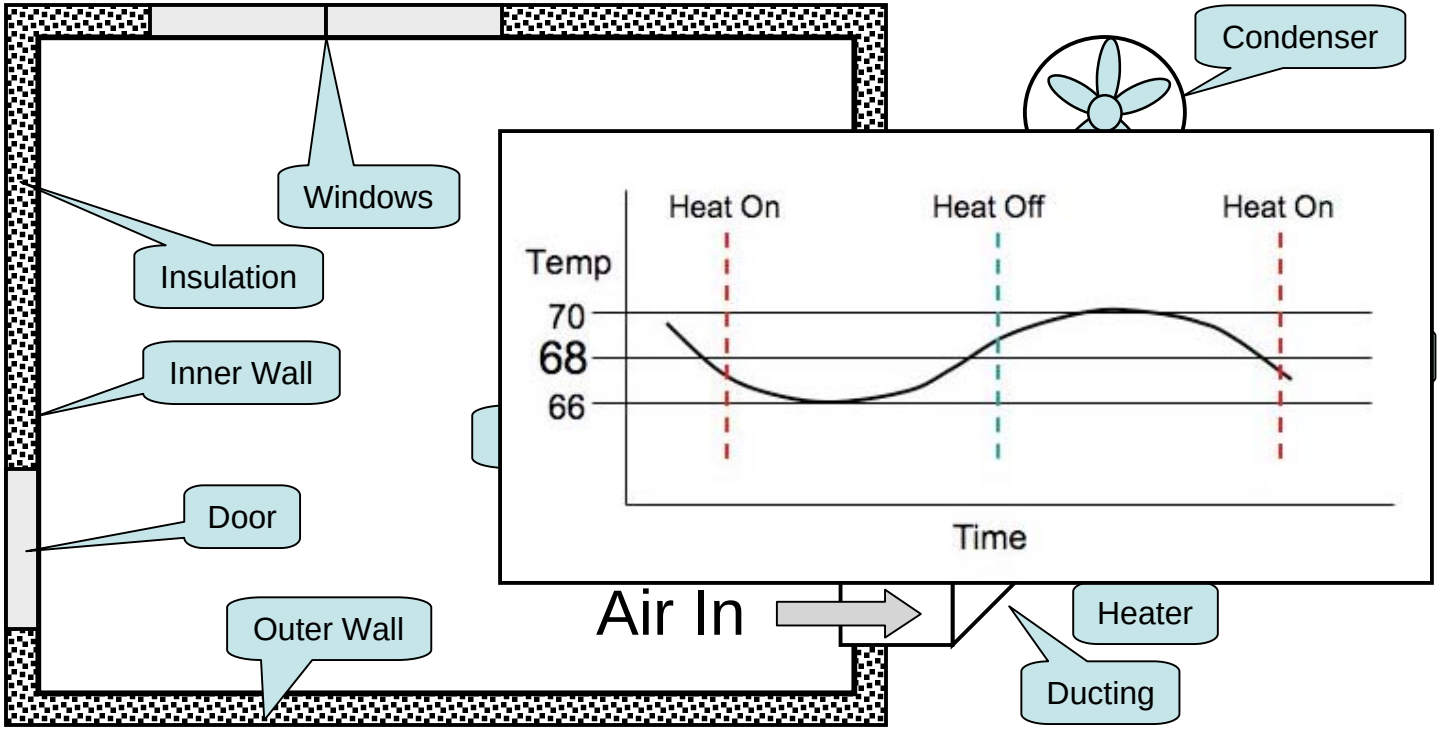
A Different Approach

- What is CLPC?
  - Closed Loop Process Control
  - A method of applying feedback such that a system (or process) becomes self regulating
- Why CLPC?
  - Needed to describe the science
  - Things happen too fast for humans to deal with
  - Things happen too slow for our unconnected technology to address
- Why CLPC applied to Networks
  - I was curious about our failures and our successes
  - Analyzed security technology from the perspective of a process control engineer.

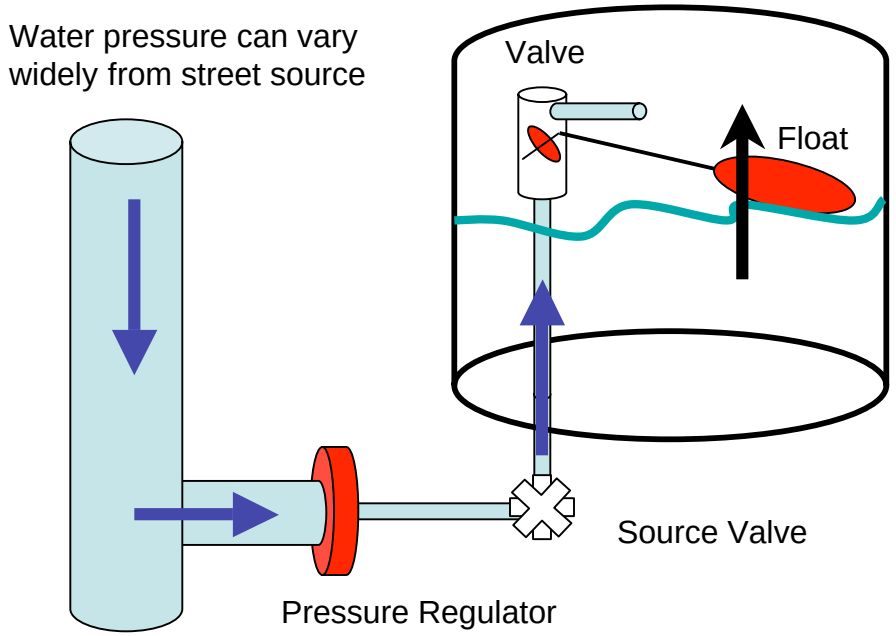
How Does CLPC Work?

- Manages to a Set Point
  - Like the temperature in the house
  - In our case, a level of trust (compliance)
- Uses a proportional control as the foundation
  - Basic function that coarsely maintains setpoint
  - We'll need to combine some things to make this work
- Uses Integral and Derivative controls to "home in" on set point
  - Integration sums errors (ex: failed logins)
  - Derivative monitors rate of change (ex: attack rate)
- All network devices must play

CLPC Example



CLPC Example



1. Success Criteria well understood
2. Failure modes are well understood
3. Operates to same level every time
4. Self regulating

Analysis

- Devices categorized by their ability to address proportional, derivative or integral control modes
- Some controls are “bang-bang”
  - Bimodal controls are either on or off
  - Function like thermostat
- There was not one proportional control!
  - Nothing that controlled the introduction of risk into the network!
  - All endpoints treated with the same level of trust
  - Authorizations done strictly at user level

Analysis Results

Toilets have a better proportional control than our networks do.

What's Missing?

A Basic proportional control that we can hang the rest of our control solutions upon.

How Does CLPC Work For Us?

- Setpoint is Minimum Compliance Level for network you want access to
- Uses the network *and* the endpoint
  - Trust client on endpoint measures compliance, gathers authentication information
  - Trust client talks with NAC enabled architecture to control access to network
  - Although user may be trusted, untrusted systems aren't given a chance to attack network

CLPC Isn't Just for Endpoints

- Governs all processes, for example
  - Device provisioning
  - Incident Response
- Some feedback, feed forward, and feed through paths are human based
  - Very low frequency
  - Very unreliable
  - Must be identified within the model

Endpoints Defined

- Windows
- Linux
- Mac
- Handhelds
  - PDAs and Phones
  - iPods (yep!)
- Embedded Systems
  - Printers
  - Vending machines
  - Control systems (PLCs)
  - Ipods (here too!)
  - VoIP handsets

Systems We Know

- Windows
  - Lots of security software for them
  - CLPC capable
  - Trust client available
- Require RFC-3580 compliant Devices
  - VLAN assignment capable
  - Can be broken
- Or, DHCP based solution
  - Not very strong

Systems We Know

- Mac
  - Enterprise manageable
  - Basic security tools available
  - CLPC capable (limited)
  - Again with the DHCP enforcement
- Linux
  - Lots of options (open vs commercial)
  - Basic security tools available
  - Not CLPC capable

More Systems

- Embedded devices
  - Hidden from view
  - Printers and APs
  - Medical equipment
  - SCADA (PLC controllers)
  - Commercial systems (dispensers)
  - Transaction systems
  - NO UPDATE PROCESSES!

Some Vendors

- Cisco, ConSentry, Elemental, Entarasys, Extreme, ForeScout, InfoExpress, Juniper, Lockdown, McAfee, Microsoft, Mirage, Nevis, StillSecure, Symantec, Vernier
  - However, complex and “feature rich”
  - Difficult to implement today
  - Some (many?) not designed (or tested) by security people
  - Interoperability is not a consideration for most

Questions

- What kind of independent testing have you done?
- What type of SDLC do you employ?
- Do you have a documented process?
- What software security testing tools do you use?
- How do you do flaw analysis?
- How are flaws incorporated back into the product?
- How many security engineers do you have working on the product?
- What industry certifications do your security engineers possess?
- What industry certifications does the product have?

Thanks!

Questions?

Send them to:
markkadrich@thesecurityconsortium.net

Or call: 408-313-6263