PROCESS CONTROL SYSTEMS FORUM

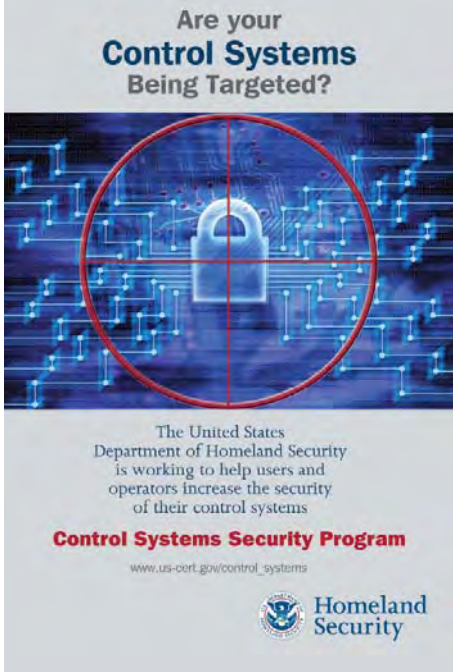
Security Ideals and Baseline set of Technical Metrics

Wayne Boyer & Miles McQueen
Idaho National Laboratory
PCSF March 6, 2007

DHS Control Systems Security Program

- The sponsor for this effort is the Department of Homeland Security (DHS) Control Systems Security Program (CSSP)
- The goal of the CSSP is to

  "Reduce Cyber Risk to Critical Infrastructure Control Systems by providing guidance and building partnerships"



Outline

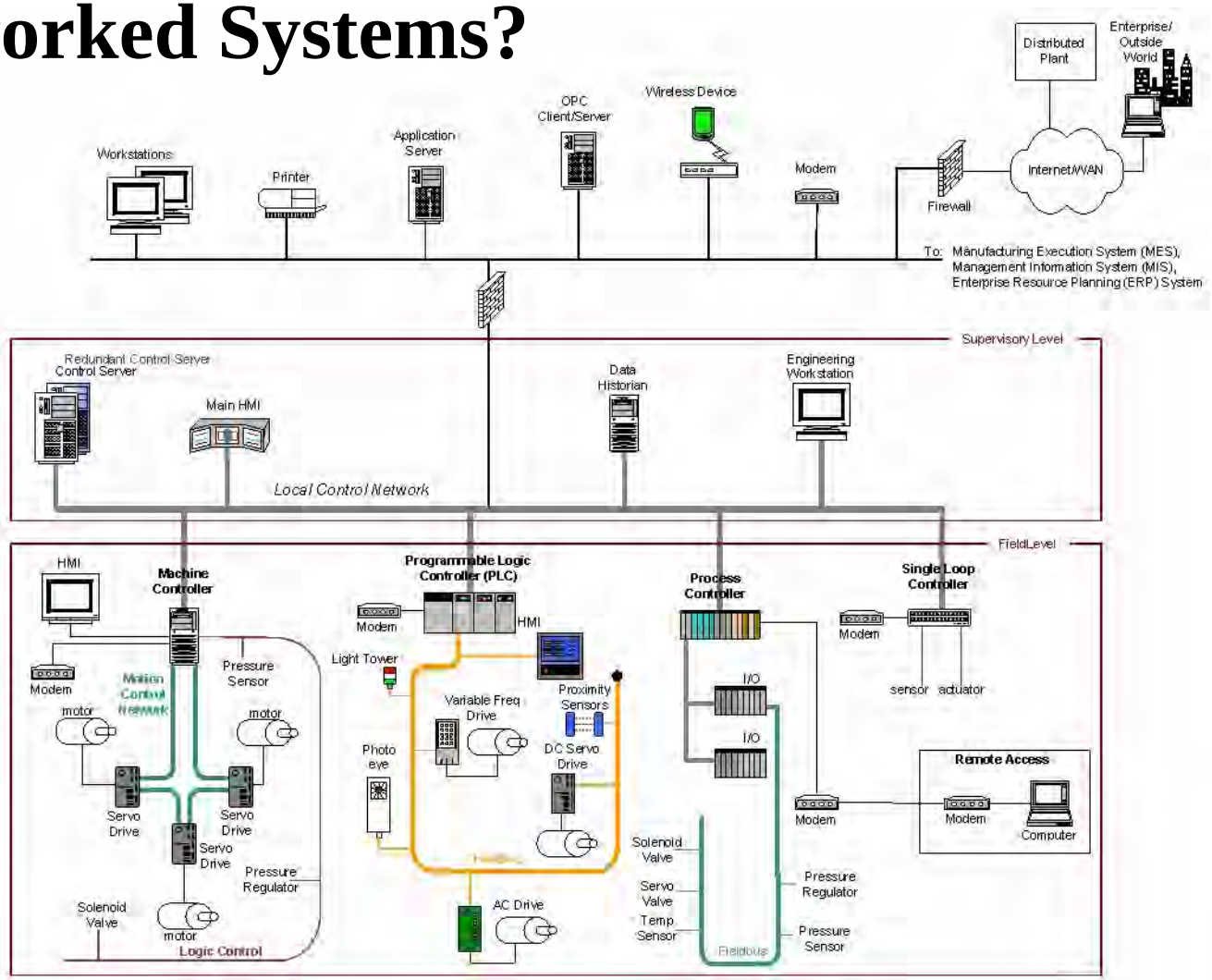
- Goal
- Background
- Seven Ideals
- Proposed Metrics
- Summary and Future

Goal

Identify a Set of Technical Security Metrics that Owners/Operators Can Use to Manage Control System Cyber Security

- A Technical Security Metric is the security relevant output from an explicit mathematical model that makes use of objective measurements
  of a technical object.
- Good metrics lead to good products (good decisions)

Objective Security Measures for Networked Systems?



PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Background

- **INL's recent work in cyber security measures & models**
  - Time-to-compromise estimation model – 1st ACM Quality of Protection Workshop, Sept 2005
  - Risk reduction estimation case study- HICCS conference, Jan 2006
  - Attack graph analysis – ACM conference CCS'06, Nov 2006
  - Attack surface analysis – 2nd ACM Quality of Protection Workshop, Nov 2006
- **Cyber Security Metrics, INL Report to DHS, Dec. 2006**
- **The measurement of cyber security risk is a grand challenge. What is feasible now?**

Existing Metrics

Standards & Guides Searched for Technical Metrics

30 Technical Metrics Identified

Industry Metrics Sampled

Standards & Guides Do Not Recommend Specific Metrics

Identified Metrics Have Serious Weaknesses

How to Choose a Good Set of Metrics?

- Small in number (< 20)
- Easy to understand
- Measurable and objective
- Related directly to security goals
- Represent the most important measurable security attributes
- Avoid averaging items of unequal weights

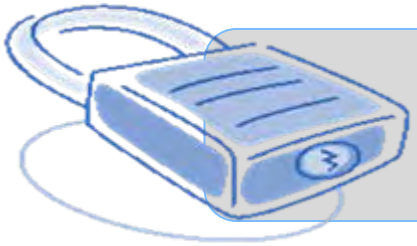
Proposed Metrics

Based on 7 security ideals
(abstract dimensions of security)

7

1 or more …for each ideal

For Each Ideal: What can be measured that is
a good representation of the security dimension?



The security principles from the literature
were mapped to the 7 ideals

Seven Ideals 7

Security Dimension	Ideal
1. Security Group (SG) knowledge	1. SG knows current system perfectly.
2. Attack Group (AG) knowledge	2. AG knows nothing about the system.
3. Access	3. System is inaccessible to AGs
4. Vulnerabilities	4. The system has no vulnerabilities
5. Damage potential	5. The system can’t be damaged
6. Detection	6. SG detects any compromise instantly.
7. Recovery	7. SG can restore system integrity instantly.

Proposed Metrics

Security Ideal	Metric
1. Security Group (SG) knows current system perfectly	Rogue change days
	Component test count
2. Attack Group (AG) knows nothing about the system	Minimum password strength
3. System is inaccessible to AGs	Reachability count
4. The system has no vulnerabilities	Vulnerability exposure
5. The system can't be damaged	Worst case loss
6. SG detects any compromise instantly	Detection mechanism count
7. SG can restore system integrity instantly	Restoration time

Proposed Metrics (Extended)

Security Ideal	Metric
1. Security Group (SG) knows current system perfectly.	Rogue change days
	Component test count
2. Attack Group (AG) knows nothing about the system.	Minimum password strength
	Data transmission exposure rate
3. System is inaccessible to AGs	Reachability count
	Root privilege count
	Defense depth
4. The system has no vulnerabilities	Vulnerability exposure
	Attack surface
5. The system can't be damaged	Worst case loss
6. SG detects any compromise instantly.	Detection mechanism count
	Detection Performance
7. SG can restore system integrity instantly.	Restoration time

Proposed Metrics Descriptions

- **Rogue Change Days:** The number of rogue changes multiplied by number of days the changes were unknown to the Security Group (SG). A Rogue change is any change to the system configuration without prior notification to the SG
- **Component Test Count:** The number of control system software components that have not undergone independent security testing
- **Minimum Password Strength:** Minimum time needed to crack a single password for any account on the system
- **Reachability Count:** Number of access points (relative to a specific point of origin such as the Internet)

Proposed Metrics Descriptions (2)

- **Vulnerability Exposure:** Number of known vulnerabilities multiplied by exposure time interval
- **Worst Case Loss:** The maximum dollar value of the damage/loss that could be inflicted by malicious personnel via a compromised control system
- **Detection Mechanism Count:** Number of devices that are externally accessible and without compromise detection mechanisms
- **Restoration Time:** Worst case elapsed time to restore the system to a known uncorrupted version

Metrics Template

- Name
- Brief Description
- Associated ideal
- Associated principle
- Key assertion
- Units
- Range of metric
- Strengths
- Weaknesses
- What data is collected
- How data is collected (Example of data collection process)
- Mathematical models and/or formulas
- Tools that may be used
- Frequency of data collection
- Discussion

Metric Name	Rogue change days
Brief Description	The number of rouge changes multiplied by number of days the changes were unknown to the Security Group (SG). A Rogue change is any change to the system configuration without prior notification to the SG.
Associated ideal	Security Group (SG) knows current system perfectly.
Associated principle	1C. The system configuration should not be changed without the security group's knowledge.
Key assertion	The security risk from changes to the system without notification to the security group is, on average, worse than for changes which are announced in a well managed system.
Units	RCD (RogueChangeDays)
Range of metric	integer, 0 to infinity (best to worst)
Strengths	A valid worst case measure of the quantity of potentially security impacting changes.
Weaknesses	The metric does not include any measure of the actual security impact of changes. (We stipulate competency of the SG.)
What data is collected.	The set of objects under change control must first be established and a version identifier must be saved for each object to establish a baseline. Periodically the current version identifier is scanned and compared to the previously saved identifier. Examples of objects under configuration management are: critical computer files, network devices attached to the local network, etc.
How data is collected	Each type of configured object must have an associated mechanism for self identification that produces an identifier that an audit program can obtain from the object. For example, computer files may use a hash function on the file content to calculate an identifier that can be used to determine when the file has changed. Network devices have MAC addresses associated with them, etc.
Mathematical models and/or formulas.	S_T == An ordered set of version identifiers for all configured objects, measured at time T. S_{T+k} == An ordered set of version identifiers for all configured objects, measured at time T + k. Note: there may be missing or new objects of any object type that is under change management. TSC_{T+k} == Number of mismatches between sets S_T and S_{T+k} CC_{T+k} == Changes introduced into the system only after notification of the security group, RC_{T+k} == TSC_{T+k} - CC_{T+k} is the number of Rogue Changes between the current measurement of the system and the previous measurement of the system. RCD == $RC_{T+k} * k$
Tools	Tripwire [TW06] is an example of a tool that supports change auditing.
Data collection Frequency	Since the data collection time interval is included in the calculation of the metric, there is built in incentive to measure often.
Discussion	RCD is somewhat conservative since the metric assumes the rogue change was introduced immediately after the previous measurement. Only when one has a clear understanding of all the devices, components, processes, and topology of a system is it possible to discuss effective security management. Since some system components are more critical than others (for example, some components are accessible directly from external networks), the system manager may choose to categorize the system components and calculate the metric for each category.

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Summary

Seven Security Ideals

Proposed metrics based on ideals

Proposed metrics encourage increased security

What's Next?

Feedback from Participants, Owners/Operators

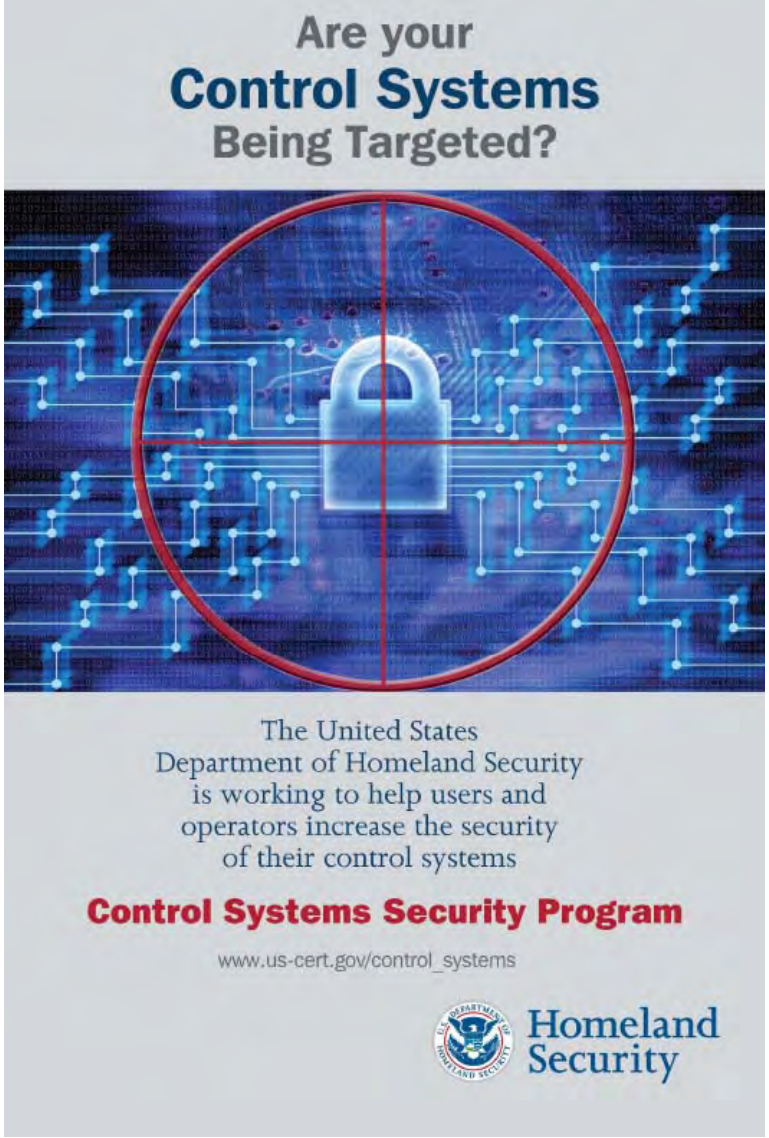
↓

Field Trial Metrics with Industry Partners

↓

Refine Metrics

Questions?



For additional information on the Control Systems Security Program

www.us-cert.gov/control_systems

Or email us at cssp@dhs.gov