Process Control Systems
Industry Conference

Technical Metrics for Control System Cyber Security

Wayne Boyer
Miles McQueen

Analysis Team

- Rob Hoffman
- Bob Huber
- Sean McBride

Outline

- Introduction & Framework
- 10 core metrics
- Case studies and assessments
- Primer and support tool
- Measurement exercise

Introduction to Metrics

- General definition – a standard of measurement

- “Measure what is measurable, and make measurable what is not so.”

Galileo Galilei (1564-1642)

- "If you can not measure it, you can not improve it."

Lord Kelvin (1824–1907)

- “You cannot control what you cannot measure.”

DeMarco, 1982

- “…Even when it is not clear how we might measure an attribute, the act of proposing such measures will open a debate that leads to greater understanding.”

Fenton and Pfleeger, 1997

Goal of this Effort

- **Develop a security metrics framework that allows owner/operators to assess their security improvements, guide their security thinking, and aid in risk assessment for their control system environments**

- **Notes**
  - Security is not directly measurable
  - For self-comparison over time
  - Evolving technology
  - Framework – not a detailed answer

Technical Metrics

- Types of metrics
  - Organizational
  - Operational
  - Technical
- Cyber security technical metric – **the security-relevant output from an explicit mathematical model that makes use of objective measurements of a technical object**

Levels of measurement

- **Nominal scale**

  (classification) ex. Software, hardware, firmware

- **Ordinal scale**

  (ordering) ex. 5 People ordered by height, 1= shortest, 5= tallest

- **Interval scale**

  (differences) ex. Fred is 2 inches taller than John...

- **Ratio scale**

  (absolute) ex. Kelvin temperature

What is wrong with this metric?

"Percent of machines patched to current level"

- **Implies an absolute scale. (At 50% we are half way to something)**
- **Implies an ordinal relationship to security that does not exist. (Is 60% more secure than 50% ?)**

A Good Set of Technical Metrics

- Small in number (About 10)
- Easily understood
- Measurable
- Objective
- **Measure** most important security attributes **of a system**

Framework- 7 dimensions of security

1. Security Group Knowledge

2. Attack Group Knowledge

3. Access

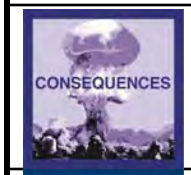
4. Vulnerabilities

5. Damage Potential

6. Detection

7. Recovery

Recommended 10 Core Metrics

	Rogue Change Days
	Security Evaluation Deficiency Count
	Data Transmission Exposure
	Reachability Count
	Attack Path Depth
	Known Vulnerability Days
	Password Crack Time
	Worst Case Loss
	Detection Mechanism Deficiency Count
	Restoration Time

Why not combine 10 metrics into one score?

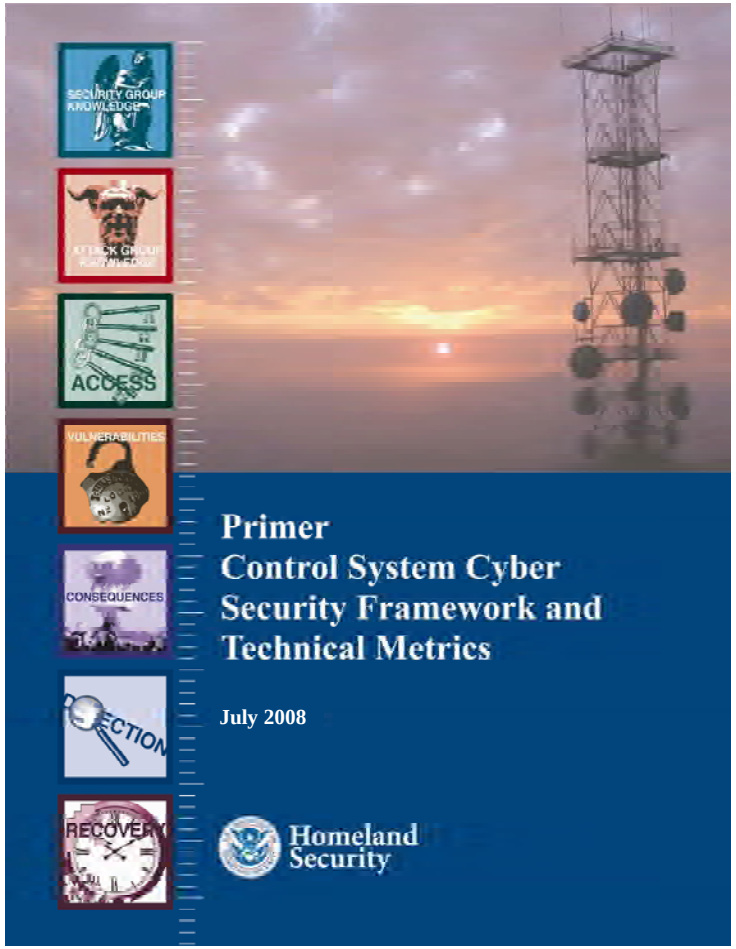
- These metrics are on an ordinal scale (absolute and interval math not applicable)
- Even if the 10 metrics were on a ratio scale (absolute) the relative weights are unknown.

Case studies and assessments

- **Two case studies- metrics validated/refined**
- **Security Assessment findings mapped**
  - 7 assessments, 225 findings
  - 100% of findings map to 7 security dimensions
  - 87% of findings map to 10 core metrics

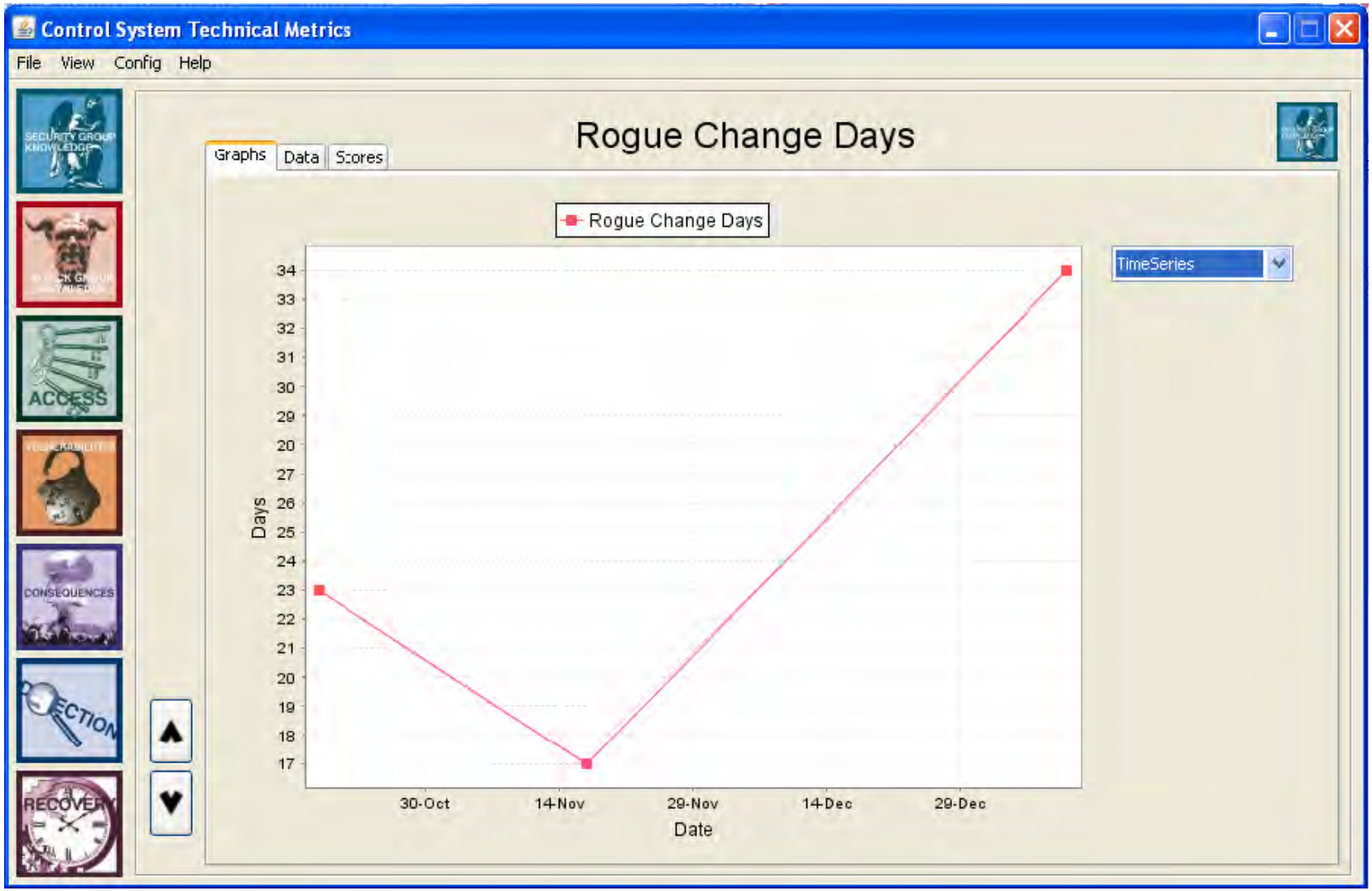
Primer

- A guide to help get your metrics program started.

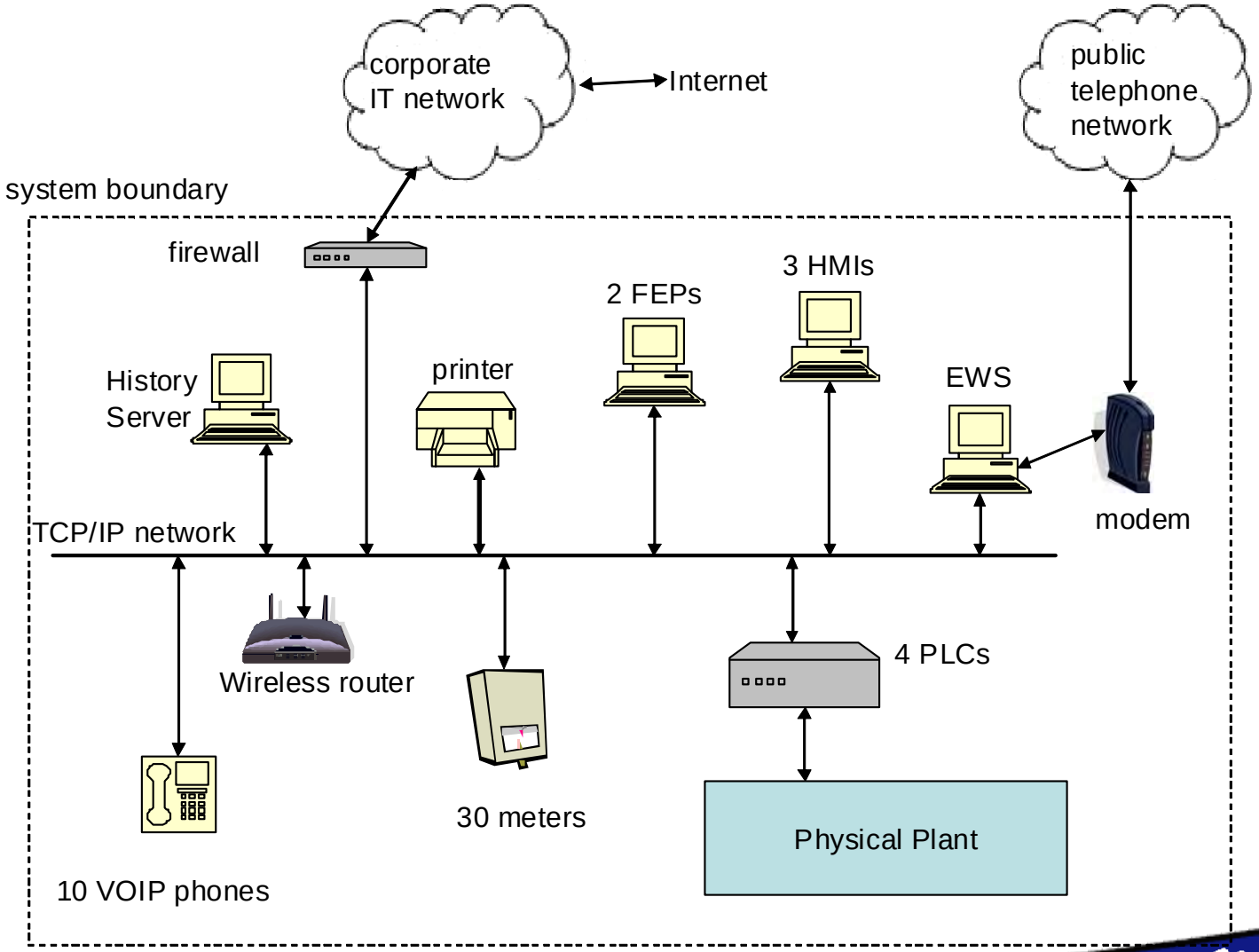


Metrics Support Tool

- A Companion to the primer
- Tracks 10 core metrics
- GUI for data entry and display
- Prototype now. Release planned for October.


Control System Technical Metrics
File View Config Help
Rogue Change Days
Graphs Data Scores
Rogue Change Days
TimeSeries
Days
34
33
32
31
30
29
20
27
26
25
24
23
22
21
20
19
18
17
30-Oct
14-Nov
29-Nov
14-Dec
29-Dec
Date
ACCESS
CONSEQUENCES
RECOVERY

Measurement exercise – System XYZ



Rogue Change Days

- (Number of Rogue changes) * (days since previous audit)
- Value for System XYZ:

  3 * (60 days) = 180 days

- Target Value =

  0 (effective configuration management)

Security Evaluation Deficiency Count

- Number of network devices that have not undergone a security evaluation.
- Value for system XYZ:

  1 (new printer)

- Target Value:

  0 (reasonable goal)

Data Transmission Exposure

- **Number of unencrypted channels used by control system devices**

Clear text protocol	Machines that use protocol	# of machine
HTTP	EWS, printer	**2**
FTP	History Server	**1**
TELNET	HMI-1, HMI-2, HMI-3	**3**
V.34 28.8 kbps (modem)	EWS	**1**
total		**7**

- **Value for system XYZ = 7**
- **Target Value = 0**

Reachability Count

- **Number of Access points (data channels)**

	Ns (services)	No (outgoing)	Np (physical)	Total
Through IT firewall	*97*	*52*	-	*149*
Through wireless	*15*	*0*	-	*15*
Through modem	*1*	*1*	-	*2*
Physical access	-	-	*4*	*4*
total	*113*	*53*	*4*	*170*

- **Value for system XYZ = 170**
- **Target value = 1**

Attack Path Depth

- Minimum number of exploits for successful attack
- Value for system XYZ = 1
- Target value = 2

Known Vulnerability Days

- **Sum of known vulnerabilities each multiplied by its exposure time**

Vulnerability	Disclosure Date	Days since disclosure	Machine types affected	# machines affected	Vulnerability days
CVE-200X-0001	7/29/2008	30	FEP(2), HMI(3)	**5**	**150**
CVE-200X-0002	7/29/2008	30	FEP(2), EWS(1), printer	**4**	**120**
CVE-200X-0003	8/18/2008	10	EWS(1), VOIP(10)	**11**	**110**
PCSF-001	5/20/2008	100	HS(1)	**1**	**100**
total					**480**

- **Value for system XYZ = 480**
- **Target value = 0**

Password Crack Time

- Minimum time to crack at least one password
- Value for system XYZ = 0 days
- Target value = 90 days

Worst Case Loss

- Maximum dollar value of damage caused by a compromised control system
- Value for system XYZ = $100M
- Target value = $10M

Detection Mechanism Deficiency Count

- Number of externally accessible devices without any detection mechanism
- Value for system XYZ = 52
- Target value = 0

Restoration Time

- Worst case elapsed time to restore control system to an uncompromised state
- Value for system XYZ = 3 days
- Target value = 4 hours

Summary

- Seven dimensions provide a good framework for metrics
- Do regular and consistent measurement
- Use the 10 core metrics