CMS ALLIANCE TO MODERNIZE HEALTHCARE

May 18, 2017

Using CVSS in Medical Device Security Risk Assessment

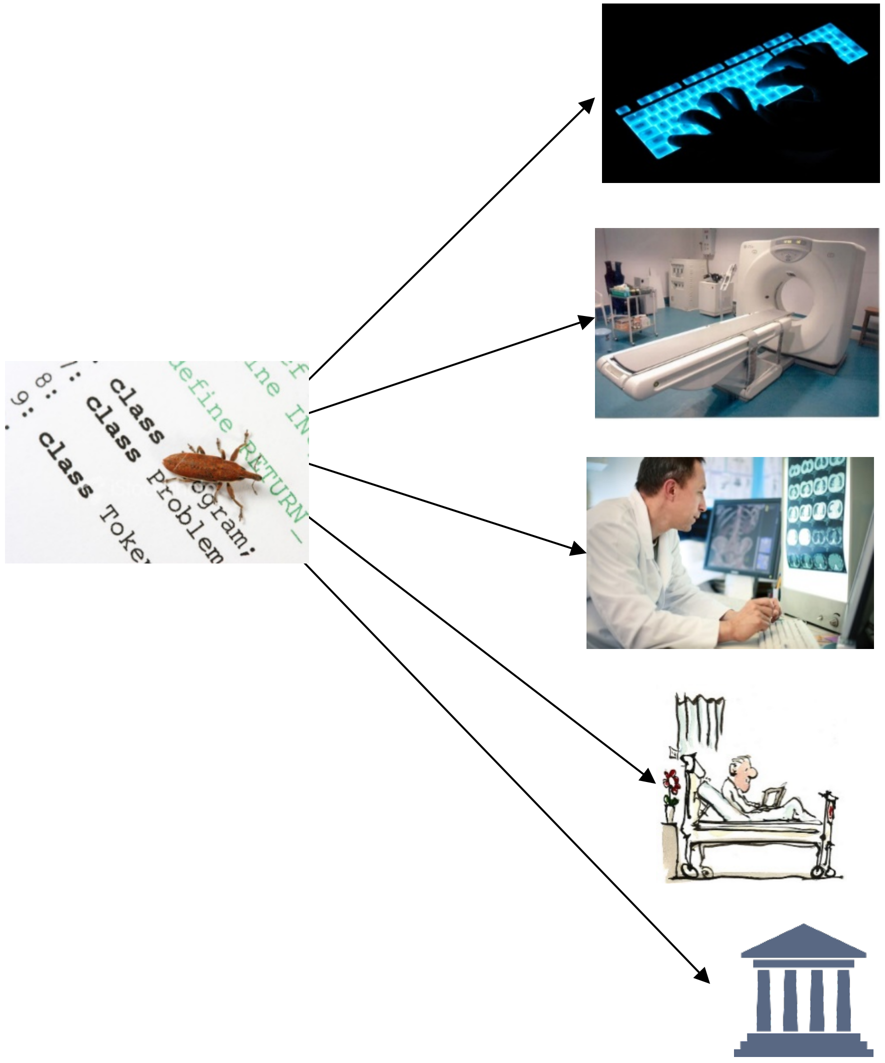
Penny Chase, The MITRE Corporation

Steve Christey Coley, The MITRE Corporation

Using CVSS in Medical Device Security Risk Assessment

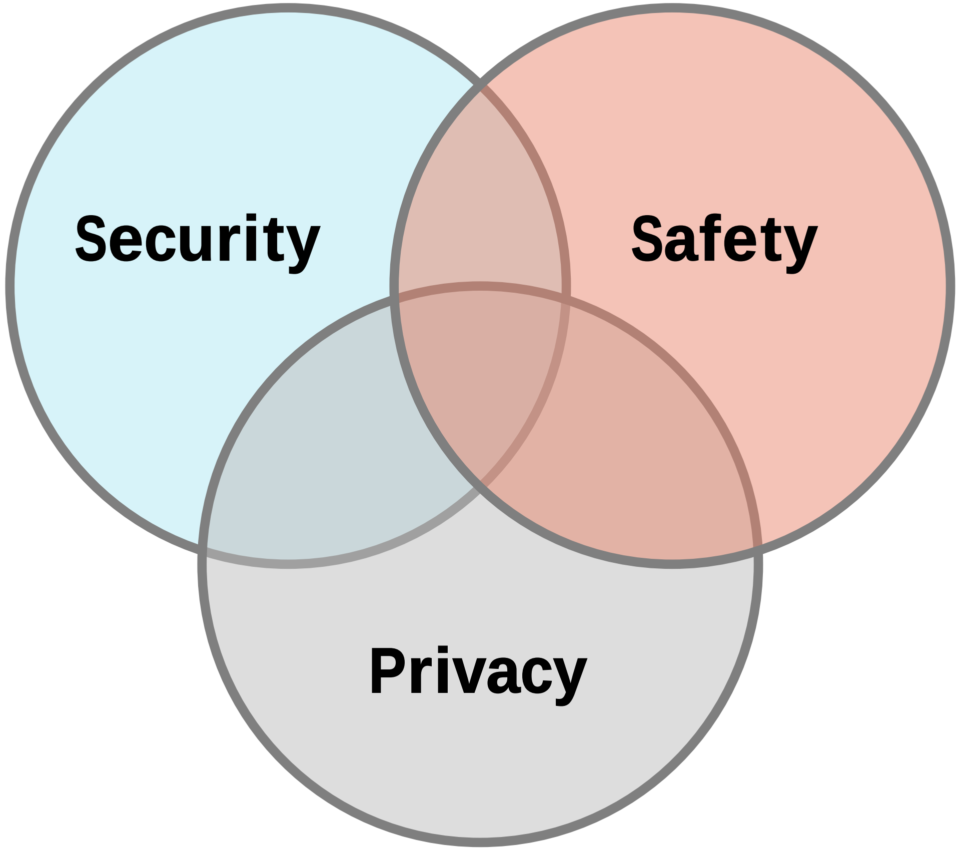
This work was performed by the Centers for Medicare & Medicaid Services (CMS) Alliance to Modernize Healthcare (CAMH) federally funded research and development center (FFRDC), operated by The MITRE Corporation (MITRE) in support of the Food and Drug Administration (FDA)

Problem: Different Perspectives of Vulnerabilities and Their Severity



- **Vulnerability Researcher**
  - This is bad and you have to fix it!
- **Device Manufacturer**
  - Do I need to patch it now or can I wait for the next upgrade?
- **Healthcare Provider**
  - Are there compensating controls or do I have to unplug it from the net?
- **Patient**
  - Should I refuse treatment with this device?
- **FDA**
  - Do we need to take action?

The Delicate Balance of Safety, Security, and Privacy



- "Everything is a priority"
- Varying risks to patient, device, clinical environment
- Different regulatory requirements
- Different prioritization depending on context of risk assessment
- Each can interfere with the other
  - – Don't want anti-virus to fire during surgery
  - – Security can erode privacy
- Our focus: safety and security

Real-World Vulnerabilities and Scoring Challenges

- Can be difficult to determine safety impact of a technical finding
  - Safety regulations already require separation and indirect defense-in-depth
  - Fail-safe operations
- Vulnerable applications might not directly interact with physical actions
  - Depends on the functionality and work/data flow
- Traditional information technology (IT) often prioritizes integrity and confidentiality over availability
- For patient safety, availability is often extremely important
  - "You can't reboot a patient"
- The clinical environment varies widely

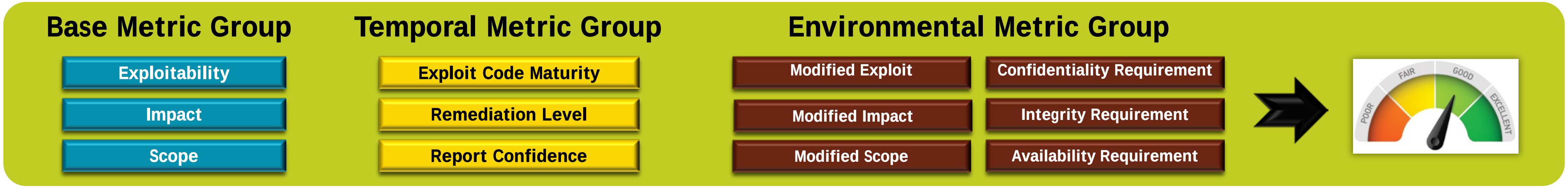
Example: Hospira LifeCare PCA3 and PCA5 Infusion Pump

- Technical vulnerability(ies)
  - Remote telnet root access without password
  - CVSSv2: 10.0 (ICS-CERT)
- Healthcare impact
  - Change drug libraries, including min/max allowed dosage
  - (unproven?) change actual dosage delivered
- Defense-in-depth:
  - Human still needs to manually confirm dosage change
- Environmental considerations
  - Pump may be on separate, “trusted” network
  - The vulnerable interface might not even be in use
- Scoring implications
  - In a hospital performing due diligence, risk may be minimal
- References
  - ICS-CERT Advisory: https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B
  - FDA Safety Communication: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm

Desired Features of a Health Care Scoring Method

- Minimal complexity
- Usable by practitioners
- Accepted by diverse stakeholders
  - Manufacturers, hospital, security researchers, patients, regulators
- Flexible for different clinical environments
- Flexible for different device classes
- Repeatable (different people come up with same score)
- Validated
- Provide common “language” for centering discussion and keeping disagreements focused

Common Vulnerability Scoring System (CVSS)



Base Metric Group

- Exploitability
- Impact
- Scope

Temporal Metric Group

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metric Group

- Modified Exploit
- Modified Impact
- Modified Scope
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

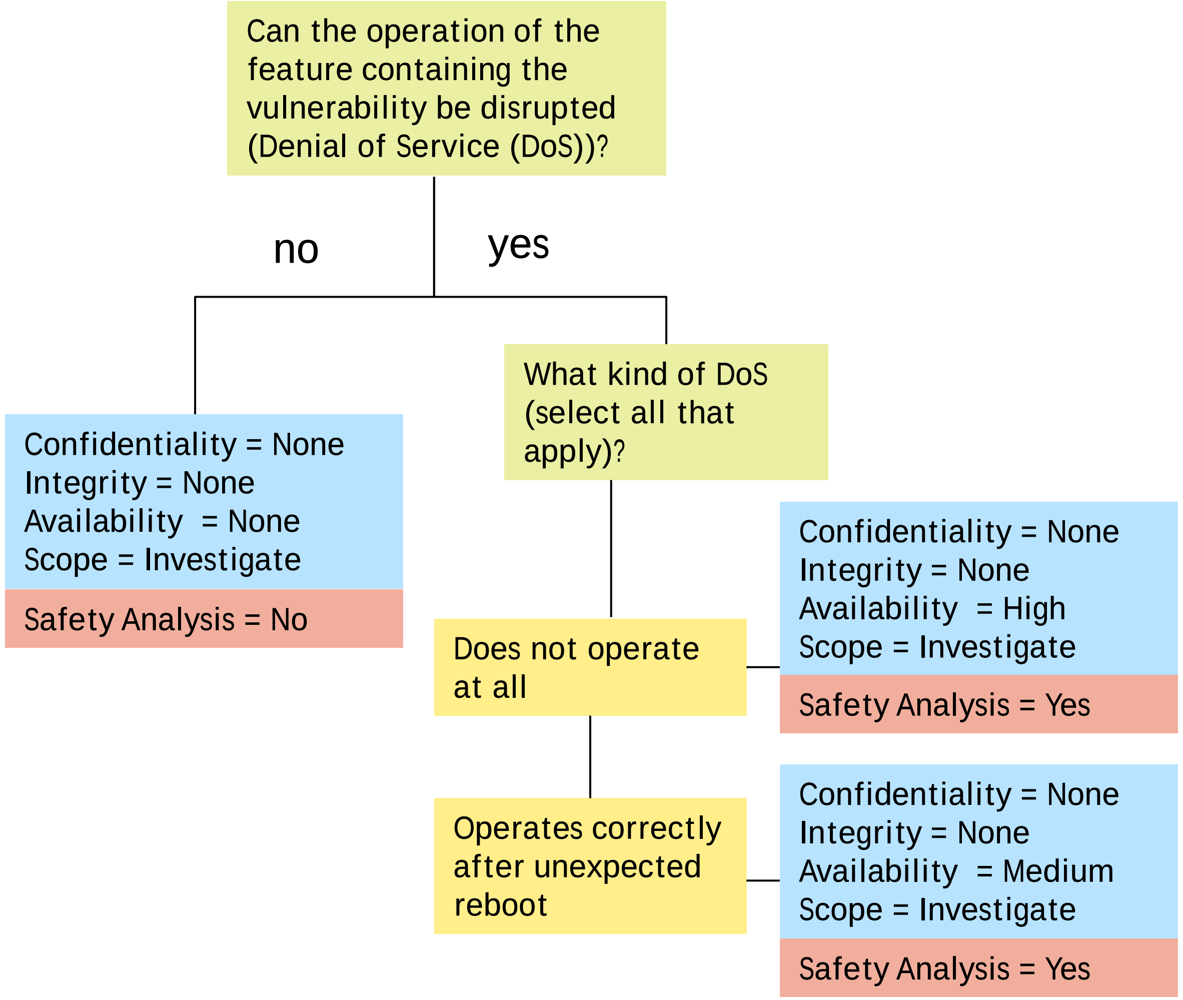
- **CVSS is an open framework developed by the Forum of Incident Response and Security Teams (FIRST) for communicating the characteristics and severity of software vulnerabilities**
  - The Base metric group represents the intrinsic qualities of a vulnerability
  - The Temporal metric group reflects the characteristics of a vulnerability that change over time
  - The Environmental metric group represents the characteristics of a vulnerability that are unique to a user's environment.
- **Each vector element is assigned a value and a single score is computed as a weighted sum of those values**

CVSS Version 3.0

Base Metric Group	Exploitability	Attack Vector	Network, Adjacent, Local Physical
		Attack Complexity	Low, High
		Privileges Required	None, Low, High
		User Interaction	None, Required
	Impact	Confidentiality	High, Low, None
		Integrity	High, Low, None
		Availability	High, Low, None
	Scope		Changed, Unchanged
Temporal Metric Group	Temporal	Exploit Code Maturity	Unproven, Proof of Concept, Functional, High
		Remediation Level	Official Fix, Temp Fix, Workaround, Unavailable
		Report Confidence	Unknown, Reasonable, Confirmed
Environmental Metric Group	Environmental	Confidentiality Req	Low, Medium, High
		Integrity Req	Low, Medium, High
		Availability Req	Low, Medium, High
		Modified Base	Same as Base values

Develop a Scoring Rubric for Medical Device Vulnerabilities

- A rubric provides guidance on assigning the vector values
  - Similar to a decision tree
  - CVSS provides a rubric, but the examples are very generic information technology
- Develop a rubric that provides relevant examples from healthcare (e.g., what is the appropriate vector value for a standalone imaging system + controlling workstation?)
  - In order to account for intrinsic (manufacturer) controls and extrinsic controls (that a hospital could put in place), we need to provide rubrics for both base and environmental score
  - We may also want to provide separate scores for exploitability and impact, so exploitability isn't overwhelmed by the impact (since exploitability alone can be used as a proxy for likelihood)
- Validate rubric – consistency, repeatability, granularity, etc.



Can the operation of the feature containing the vulnerability be disrupted (Denial of Service (DoS))?

no

Confidentiality = None
Integrity = None
Availability = None
Scope = Investigate

Safety Analysis = No

yes

What kind of DoS (select all that apply)?

Does not operate at all

Confidentiality = None
Integrity = None
Availability = High
Scope = Investigate

Safety Analysis = Yes

Operates correctly after unexpected reboot

Confidentiality = None
Integrity = None
Availability = Medium
Scope = Investigate

Safety Analysis = Yes

Approach

- Set up a cross-stakeholder working group
  - Medical device manufacturers
  - Health care delivery organizations
  - Cybersecurity researchers
  - FIRST CVSS SIG
- Interact via telecons, listserv, collaboration group
- Reviewed how some manufacturers and healthcare delivery organizations currently use CVSS
- Came to consensus on approach
  - Provide scoring guidance in form of a rubric and examples of use
  - Recognize that there are multiple use cases
- Next steps
  - Form subgroups to work on rubric for base and environmental groups
  - Get feedback from broader stakeholder community
  - Develop Medical Device Development Tool qualification package