From the Perspective of a Medical Device Manufacturer

Potential Benefits of a Scoring System Tailored to Medical Devices

- A methodology/tool to make vulnerability assessment/scoring for medical devices…
  - …easier
  - …more consistent between vulnerabilities
  - …more consistent between devices (scored by different teams)
  - …better reflect the actual severity of the vulnerability for the device in its operating environment
- More consistency across the industry
  - HDOs can rely on the consistency
  - HDOs can inspect the vector to understand better how the device is affected
- Extra credit for hints or correlates to patient safety

Potential Questions or Concerns

- Is it easier than the current process?
- What is the reproducibility (is there more precision than accuracy)?
- Does the amount of time it takes to use the tool overly burden current processes?
- Will it find its way into an FDA guidance document?

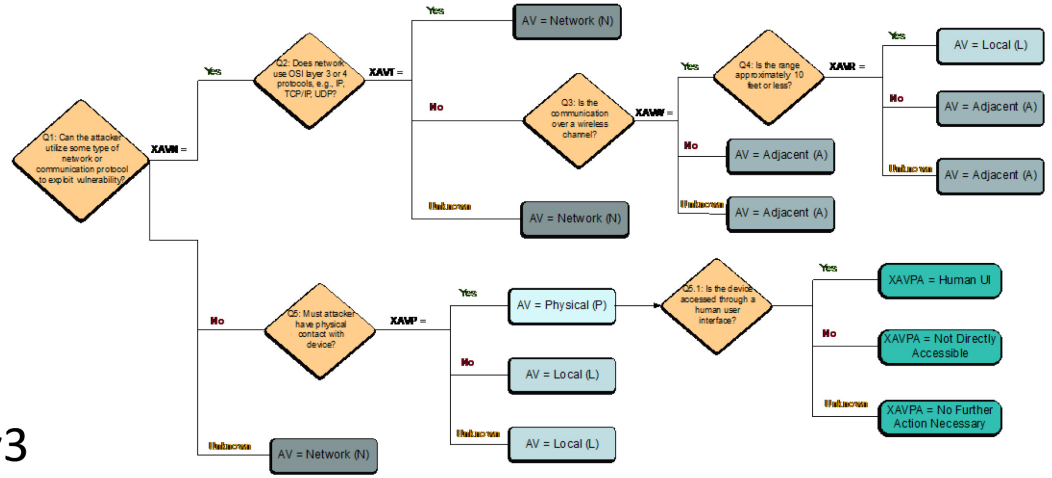
Risk Scoring System

- Focus on impact to patient safety
  - Functional/operational impact: *The So What…*
  - Vulnerability characterization: *Details and attributes…*
- Primary benefits
  - Standardizes vulnerability scoring for risk analysis
  - Provides understandable and common framework for evaluating identified vulnerabilities
  - Designed to help organizations gain understanding of risk associated with identified vulnerabilities related to delivery of patient therapy

www.RiskScoringSystem.com

CVSS Rubric and Extended Vector for Medical Devices

- Rubric is a series of questions at the decision points for each vector element, and includes
  - Customized, HDO-specific guidance that is not included in the original specification
  - Device-specific examples
  - Discussion of difficulties in (1) repeatability of the rubric and/or (2) conformance to the spirit of the original CVSS v3 specification
  - Consideration of many perspectives that would be relevant to a medical device manufacturer or an HDO, including (1) patient safety, (2) patient/clinician privacy, and (3) cybersecurity risk from an enterprise vulnerability-management perspective
- Extended vector records the decisions behind the CVSS vector element
- https://www.mitre.org/md-cvss-rubric



Question	Element	Values
Q1: Can the attacker utilize some type of network or communication protocol to exploit this vulnerability?	Extended Attack Vector Network (XAVN)	Yes (Y) No (N) Unknown (U)
Q2: Does the network use OSI layer 3 or 4 protocols, e.g. IP, TCP/IP, or UDP?	Extended Attack Vector TCP/IP or UDP (XAVT)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q3: Is the communication over a wireless channel?	Extended Attack Vector Wireless (XAVW)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q4: Is the range approximately 10 feet or less?	Extended Attack Vector Range (XAVR)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5: Must the attacker have physical contact with the device?	Extended Attack Vector Physical (XAVP)	Yes (Y) No (N) Unknown (U) Not Answered (NA)
Q5.1: Through an intended human UI?	Extended Attack Vector Physical Access Type (XAVPA)	Human UI Not Directly Accessible No Further Action Necessary

Approved for Public Release; Distribution Unlimited. Case Numbers 18-0914, 18-2208. © 2019 The MITRE Corporation. All rights reserved.

Key characteristics and use cases of vulnerability scores

Attributes to look for in a vulnerability scoring system

- Standardized scoring methodology
- Transparent scoring characteristics
- Widely used and industry accepted

Vulnerability Scores

- Typically represent ordinal scales
  - Provide rank
  - No way to provide 'distance' between ranks
  - Qualitative in nature

Vulnerability Score Use Cases

- Contextualizes the vulnerability to the organization
- Provides consistency in organizational processes
  - Unified vulnerability management policy;
  - Prioritization and;
  - Mitigation strategy

Examples of a data-type and scale

Nominal	Ordinal	Interval	Ratio
On/Off	High/Medium/Low	Degrees Celsius	Number with true zero
	Red/Yellow/Green	Letter Grade	
		Height	
		Vulnerability Score	

Operations for each data-type

Provides:	Nominal	Ordinal	Interval	Ratio
Count (frequency)	X	X	X	X
Has defined order or rank		X	X	X
Can Quantify Distance between values			X	X
Qualitative		X		
Quantitative			X	X
Can add or subtract values			X	X
Can multiply and divide values			X	X
Has true zero				X