UNIVERSITY OF SKÖVDE

An Approach to Discover and Assess Vulnerability Severity Automatically in Cyber-Physical Systems

November 4th

SINCONF20, Online Conference

Yuning Jiang, *Yacine Atif*

School of Informatics, University of Skövde, Sweden

Contact: yuning.jiang@his.se

OUTLINE

UNIVERSITY OF SKÖVDE

- Introduction
- Background
- Related Works
- Methodology
- Results
- Case Study
- Conclusion

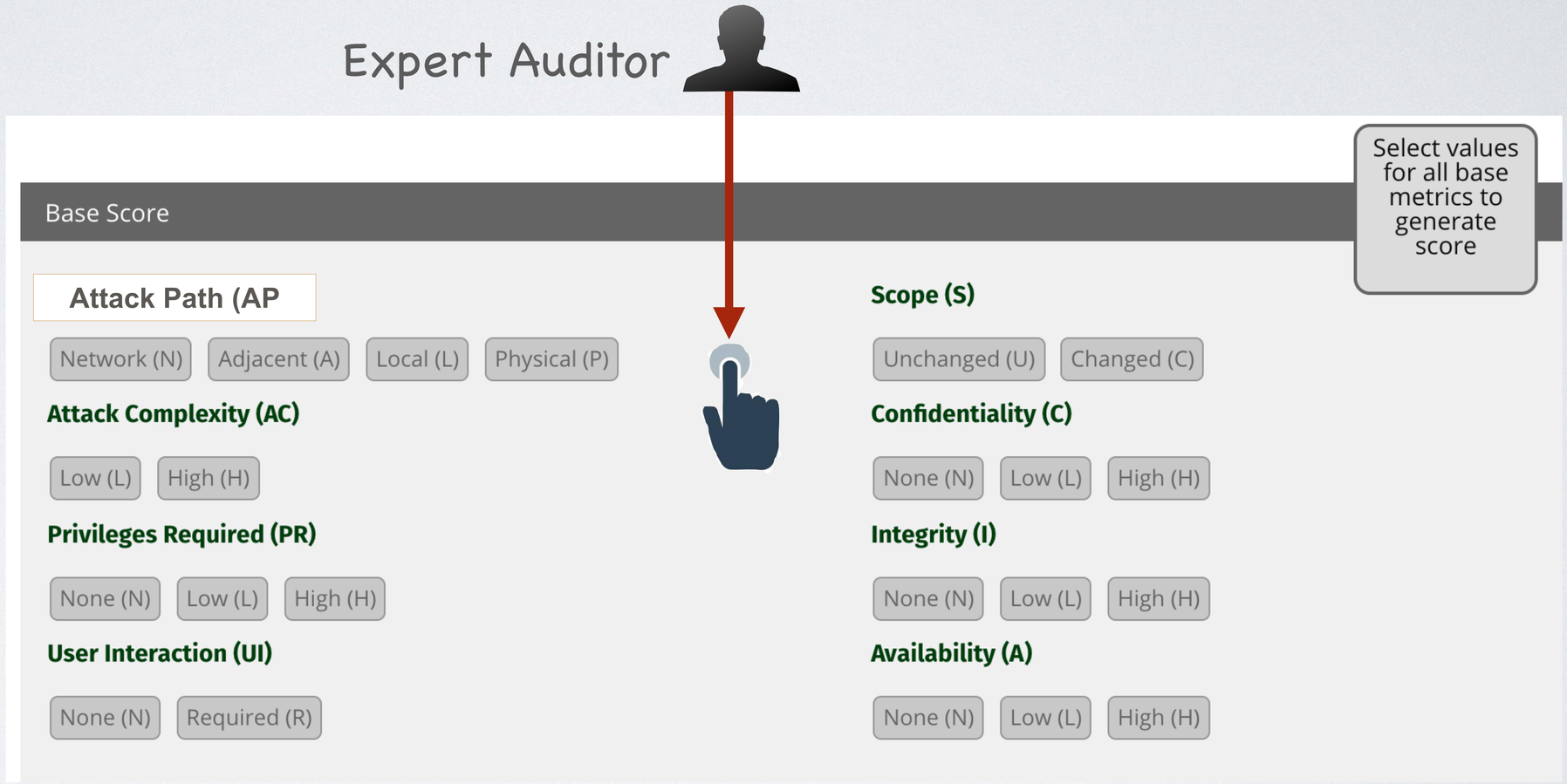
Challenges in Vulnerability Assessment:

(a) Subjective and Manual Audits.

(b) Diverse reporting sources with inconsistent scores.

Challenges in Vulnerability Assessment:

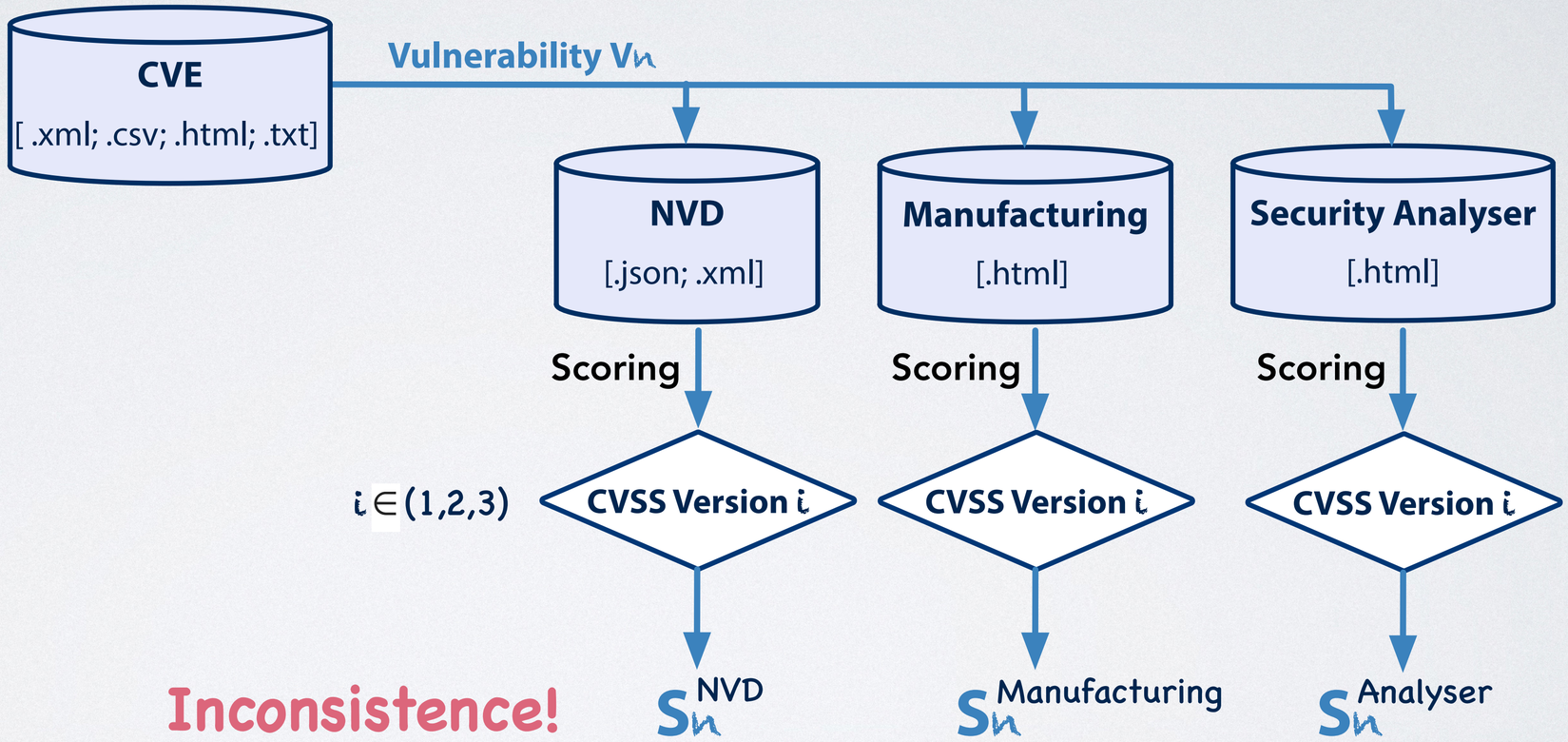
(a) Subjective and Manual Audits



(Common Vulnerability Scoring System (CVSS) V3 Calculator: https://www.first.org/cvss/calculator/3.0)

Challenges in Vulnerability Assessment:

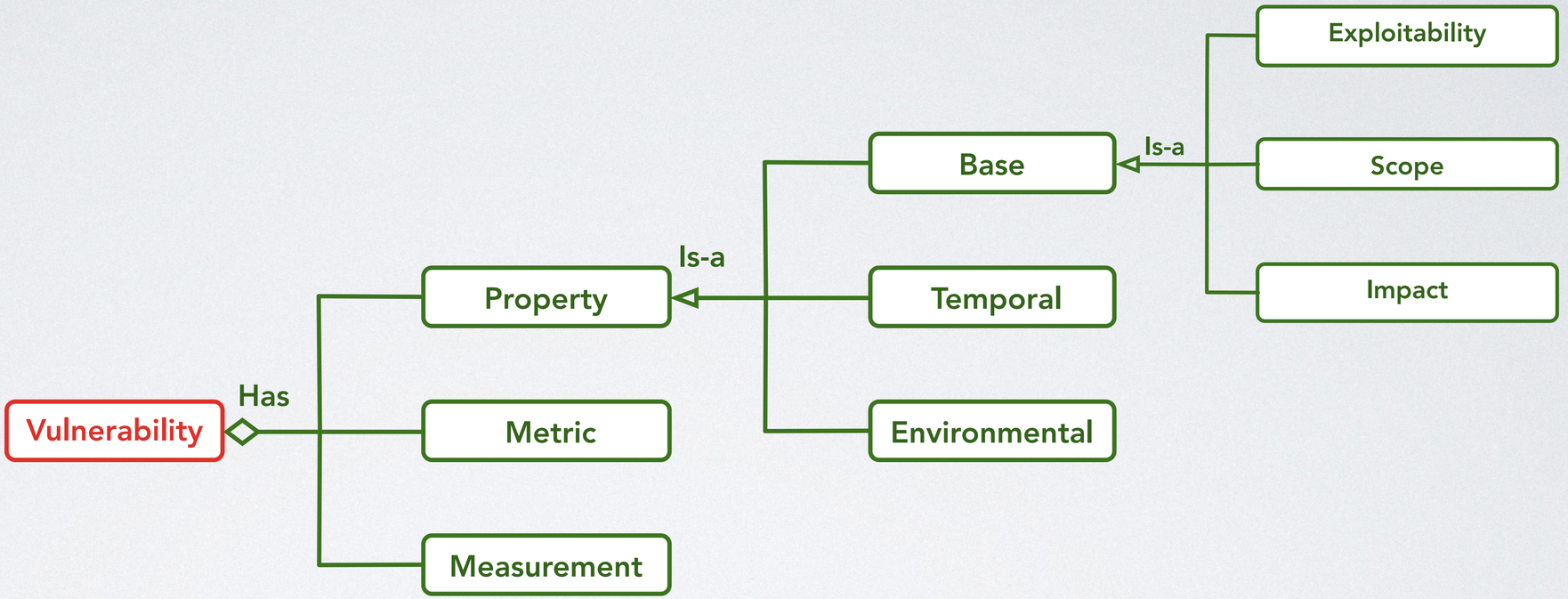
(b) Diverse reporting sources with inconsistent scores



Motivation: To Discover and Assess Vulnerability Severity Automatically

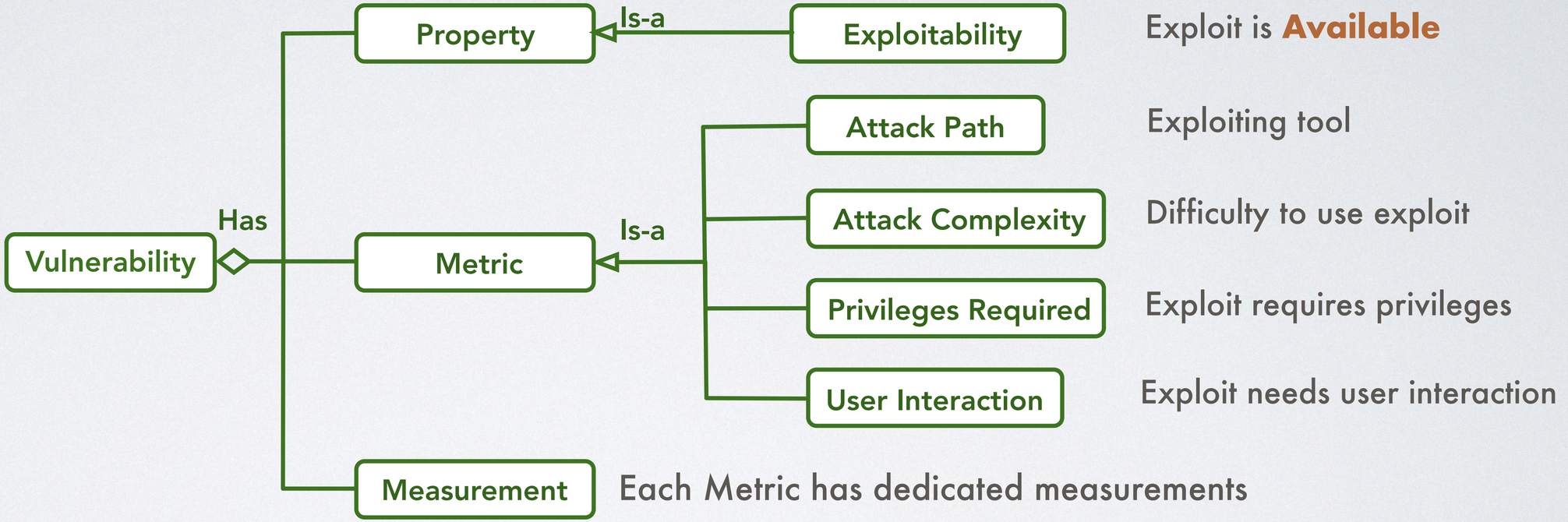
- To enhances compatibility across different CVSS versions, while streamlining vulnerability analysis;
- To consolidate scores in a way that better describe the actual severity of vulnerability instance;
- To explore patterns of cyber-physical system (CPS) vulnerabilities.

Vulnerability Characteristics



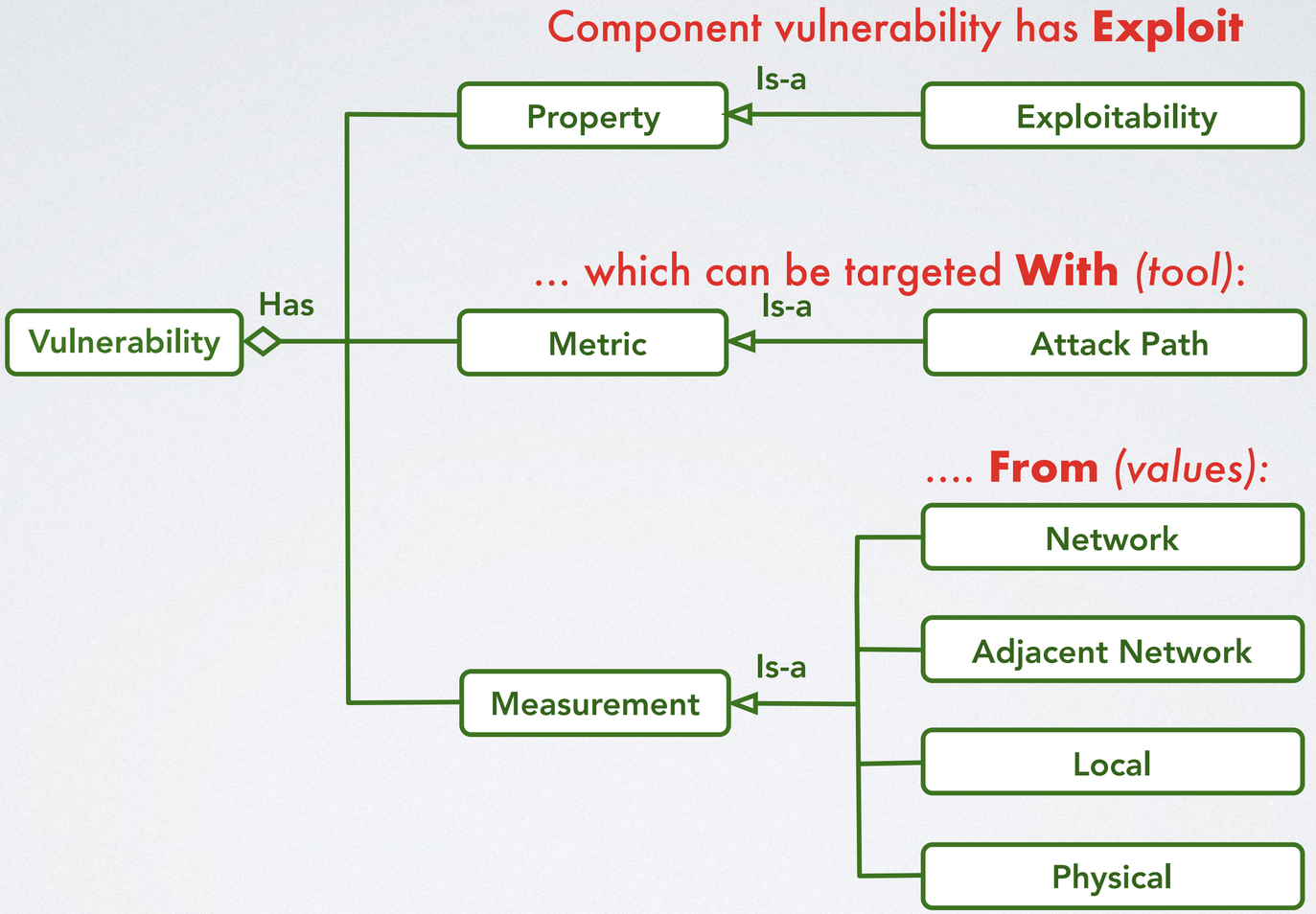
Adapted from CVSS Version 3 (https://www.first.org/cvss/)

Vulnerability Characteristics - Exploitability



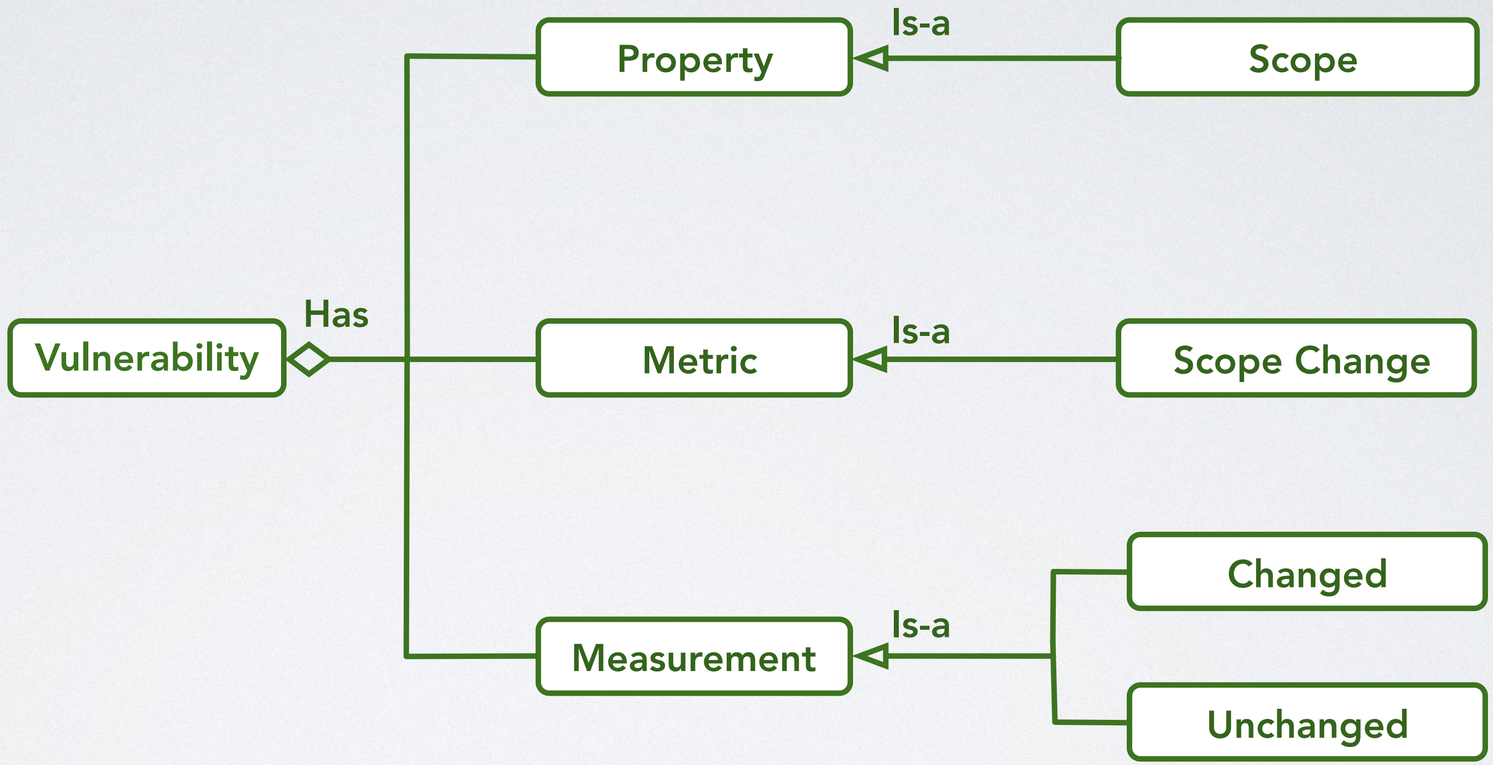
Adapted from CVSS Version 3 (https://www.first.org/cvss/)

Vulnerability Characteristics - Attack Path



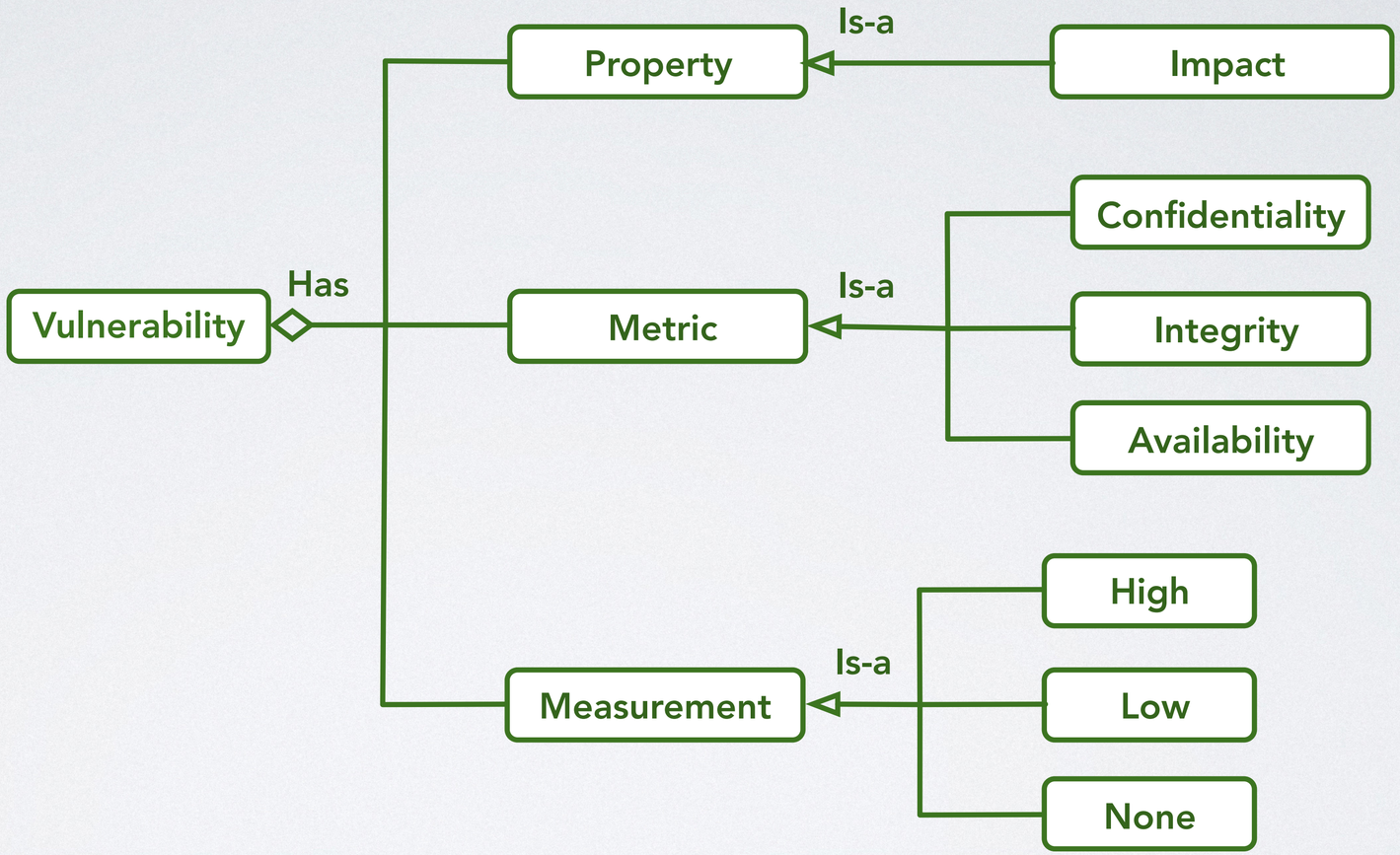
Adapted from CVSS Version 3 (https://www.first.org/cvss/)

Vulnerability Characteristics - Scope



Adapted from CVSS Version 3 (https://www.first.org/cvss/)

Vulnerability Characteristics - Impact

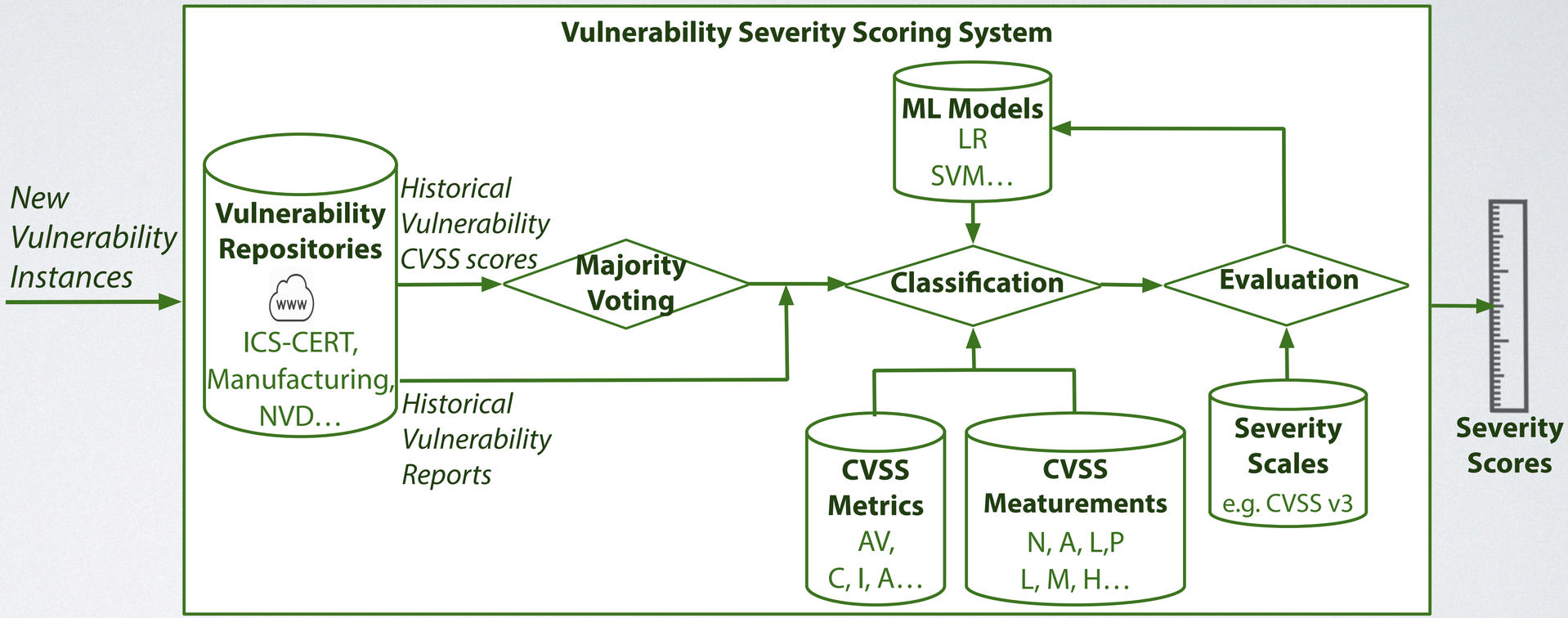


Adapted from CVSS Version 3 (https://www.first.org/cvss/)

Existing Works

- Vulnerability severity analysis using CVSS mechanism.
  - Compatibility issues among existing CVSS versions was overlooked.
- Correlation studies between multiple cybersecurity data-sources.
  - Correlation studies considering different terminology used in cybersecurity and CPS domains are limited.
- Artificial-Intelligence Approaches for Cybersecurity:
  - Directly adopted CVSS scores from NVD as training ground.

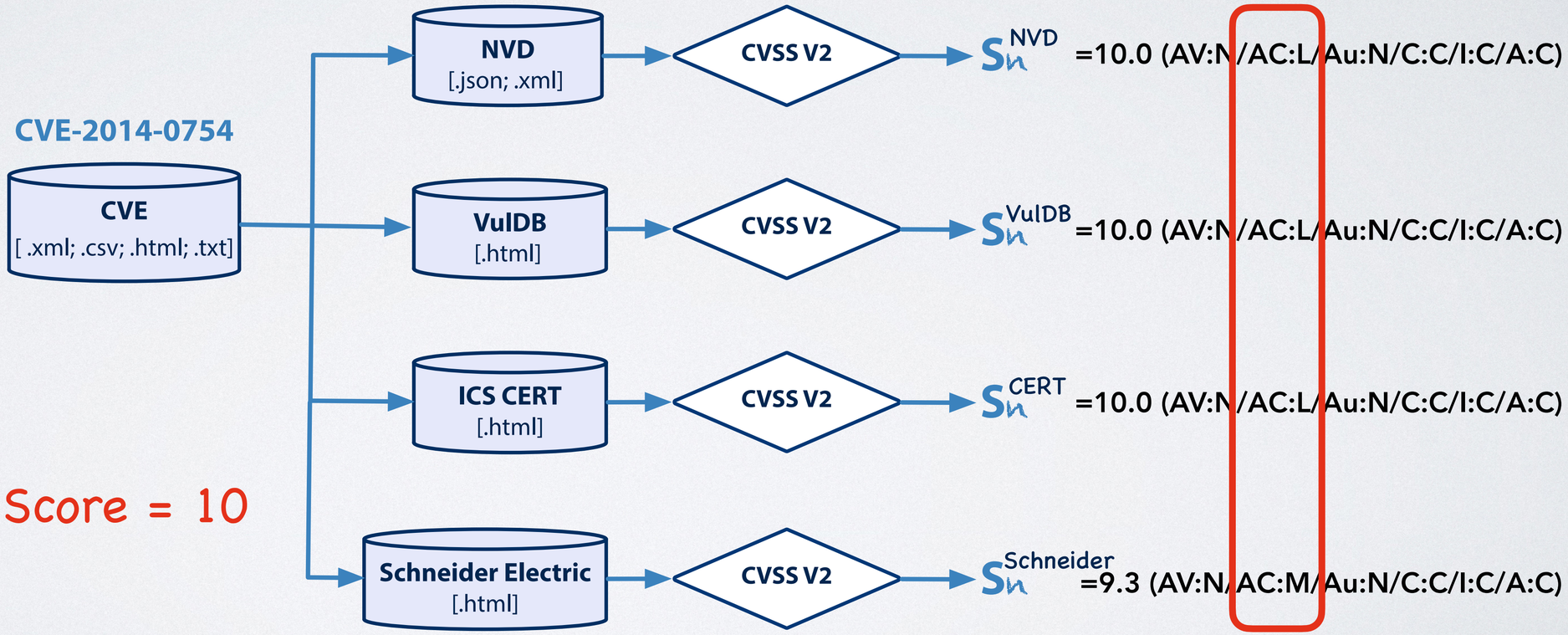
Discovering Vulnerability Severity



Vulnerability Severity Computing Pipeline

Majority Voting for Inconsistent Scores

- =2 inconsistent scores → Average of inconsistent scores
- >2 inconsistent scores → Majority voting of inconsistent scores



Vulnerability Severity Computing

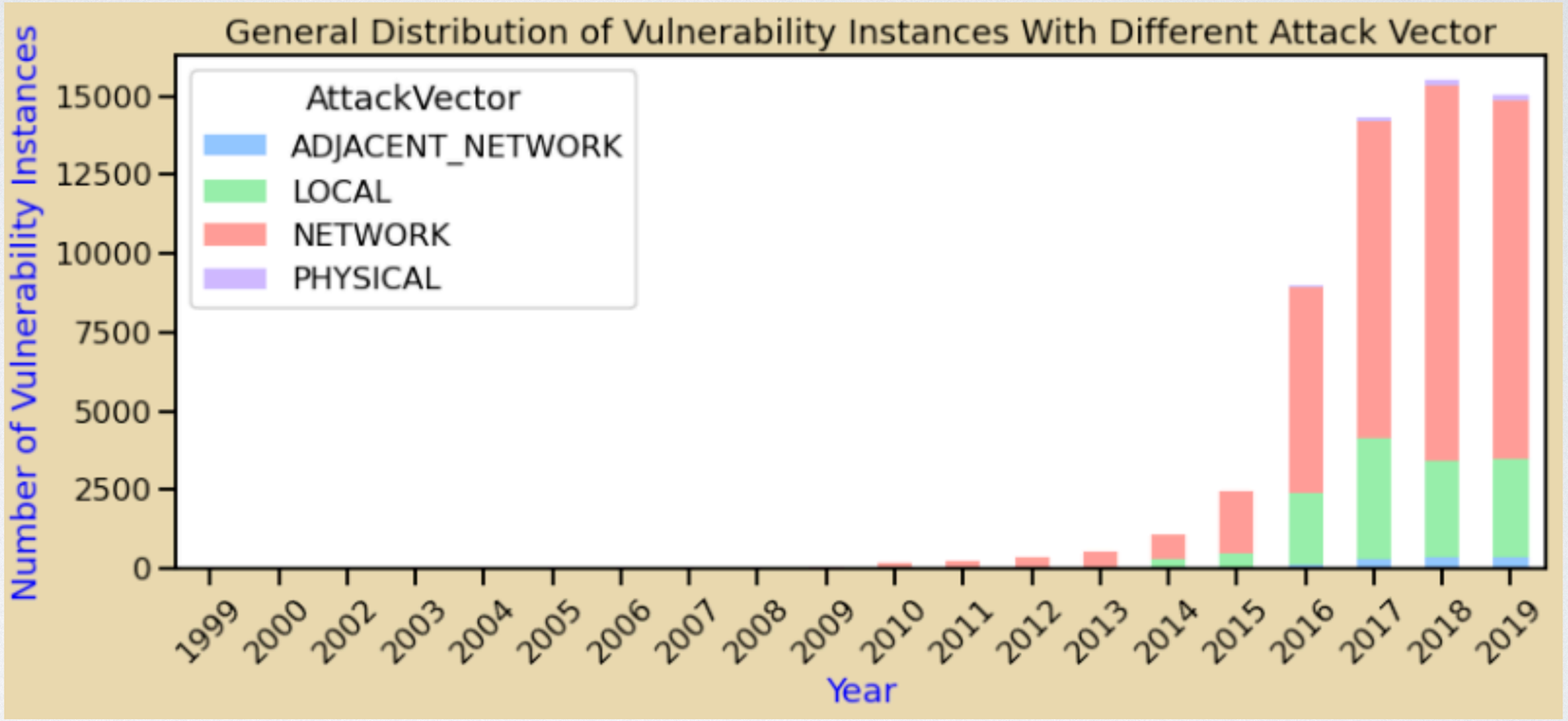
Algorithm 1 Automatic Vulnerability Severity Computing

1: **procedure** SEVERITYCOMPUTING($\mathcal{ML}, D, m, K$)
▷ $\mathcal{ML}$ is a machine learning model $f()$, m is a set of CVSS metrics m_j $(0 < j \leq M)$ where each metric m_j has a set of K^{m_j} classes, and D is a dataset with n vulnerability instance where each instance (x_i, Y_i) $(0 < i \leq N)$ has a vulnerability report x_i and a ground truth vector Y_i.
2: $N = |D|, M = |m|$
3: **for** $j = 1, \ldots, M$ **do**
4: Train(ML_j)
5: $f(x)^j = \arg\max_{K^{m_j}} f_{K^{m_j}}(x)^j$
6: **end for**
7: **for** $i = 1, \ldots, N$ **do**
8: **for** $j = 1, \ldots, M$ **do**
9: $Z_i^{(m_j)} = f(x_I)^j$
10: **end for**
11: $Z_i = [Z_i^{(m_1)}, \ldots, Z_i^{(m_j)}, \ldots, Z_i^{(m_M)}]$
12: **end for**
13: Severity Score $S_i = CVSSCALCULATION(Z_i)$
14: **end procedure**

- Allows customisation on selecting a preferable CVSS version.

Evaluation Metrics of Text Mining

- Imbalanced classes of CVSS categorisations:



- Selected evaluation metrics: Balanced Accuracy & Micro F1-Score.

Evaluation Metrics of Text Mining

- Binary-class classification: apply the confusion matrix.
  - CVSS V3 AttackComplexity: Low; High.
  - CVSS V3 UserInteraction: None; Required.
- Multi-class classification: use micro-average to calculate the average of per class evaluation.
  - CVSS V3 PrivilegesRequired: None; Low; High.
  - CVSS V3 IntegrityImpact: None; Low; High.

Dataset of LR-Based Algorithm are retrieved till Oct 27th 2020

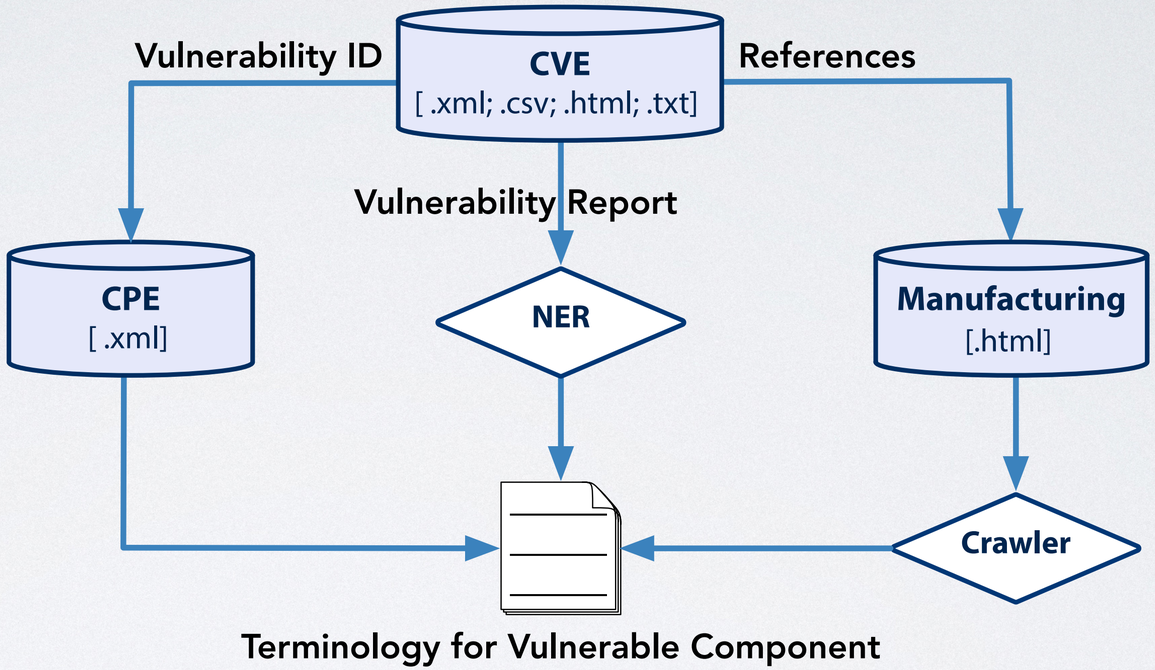
- Download Vulnerability score reports from NVD (2002-2019)
  - CVSS V2 (127 907 items)
  - CVSS V3 (58 813 items)
- Crawl ICS CERT vulnerability analysis
- Crawl Manufacturing vulnerability analysis

Results of LR-Based Algorithm

CVSS-Metric	Balanced Accuracy	Micro F1-Score
V2 AccessVector(AV)	80.87%	95.76%
V2 AccessComplexity(AC)	63.68%	83.63%
V2 Authentication(Au)	56.34%	95.00%
V2 ConfidentialityImpact(C)	81.03%	82.98%
V2 IntegrityImpact(I)	82.40%	84.60%
V2 AvailabilityImpact(A)	80.12%	81.08%
V3 AttackVector(AV)	75.92%	93.68%
V3 AttackComplexity(AC)	78.78%	95.58%
V3 PrivilegesRequired(PR)	78.79%	90.71%
V3 UserInteraction(UI)	93.45%	94.13%
V3 Scope(S)	93.65%	97.48%
V3 ConfidentialityImpact(C)	88.36%	91.46%
V3 IntegrityImpact(I)	90.58%	92.02%
V3 AvailabilityImpact(A)	75.75%	93.01%

Cyber-Physical System (CPS) Vulnerability

- CPS vulnerability filter for vulnerable component.



- Filter for vendor information, combined with manual checking.
  - Schneider Electric SE ('schneider-electic', 'chneider-electric', and 'schneider-electric', etc,.)

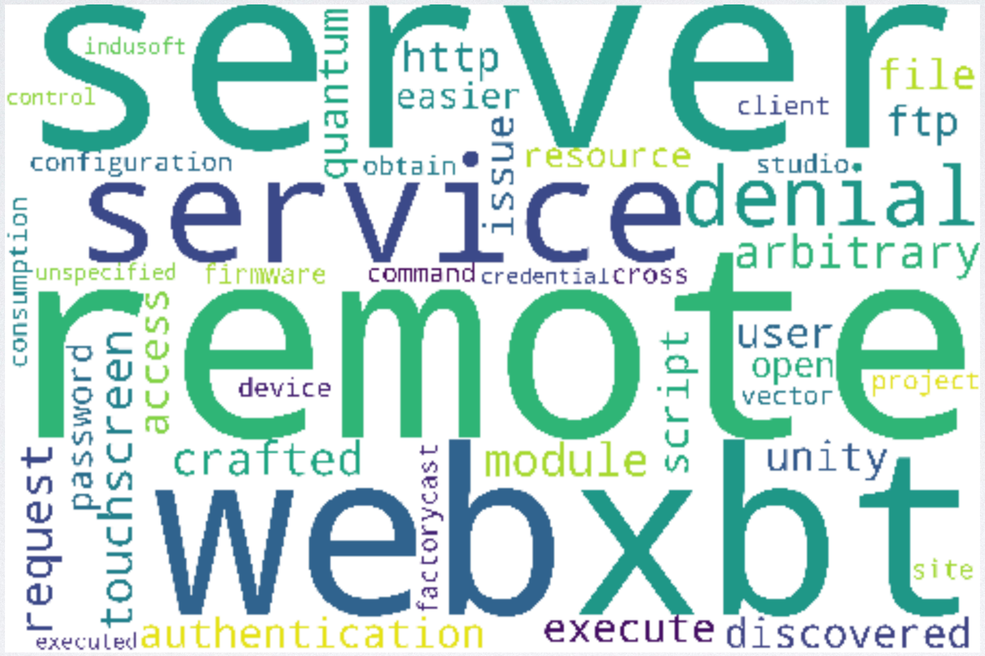
Cyber-Physical System (CPS) Vulnerability

- Retrieved CPS vulnerability instances (till Oct 27th 2020).

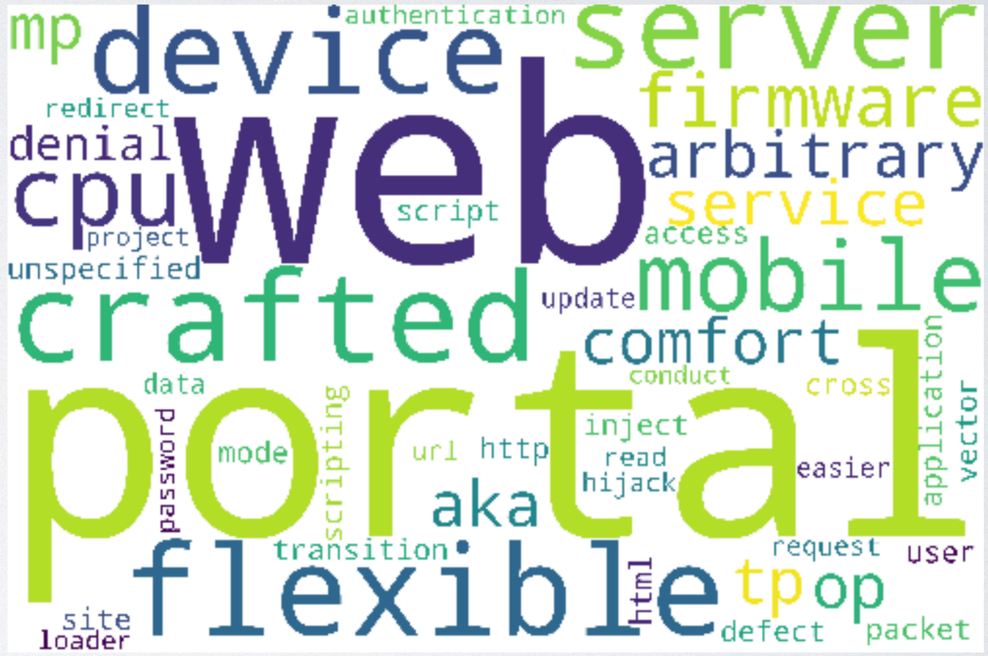
CPS Asset	Number
Programmable Logic Controller (PLC)	89
Remote Terminal Unit (RTU)	32
Master Terminal Unit (MTU)	8
Human Machine Interface (HMI)	105

CPS Vendors Characteristics Using Top Keywords

- Schneider Electric SE (24 instances)



- Siemens AG (39 instances)



Characteristic Analysis for CPS Vulnerabilities

CPS on average

Metric	Measurement	PLC	RTU	MTU	HMI	CPS	CVE
AttackPath	Network	93.26%	100%	87.50%	84.76%	90.17%	74.35%
	AdjacentNetwork	0%	0%	0%	0.95%	0.43%	22.57%
	Local	5.62%	0%	12.50%	13.33%	8.55%	2.01%
	Physical	1.12%	0%	0%	0.95%	0.85%	1.06%
AttackComplexity	Low	97.75%	100%	100%	99.05%	98.72%	91.21%
	High	2.25%	0%	0%	0.95%	1.28%	8.79%
PrivilegesRequired	None	95.51%	78.13%	100%	92.38%	91.45%	69.55%
	Low	4.49%	12.50%	0%	7.62%	7.26%	25.18%
	High	0%	9.37%	0%	0%	1.28%	5.28%
UserInteraction	None	83.14%	100%	87.50%	67.62%	78.63%	62.80%
	Required	16.85%	0%	12.50%	32.38%	21.37%	37.20%
ScopeChange	Unchanged	92.13%	100%	100%	85.71%	90.60%	83.64%
	Changed	7.87%	0%	0%	14.29%	9.40%	16.36%

Overall in CVE

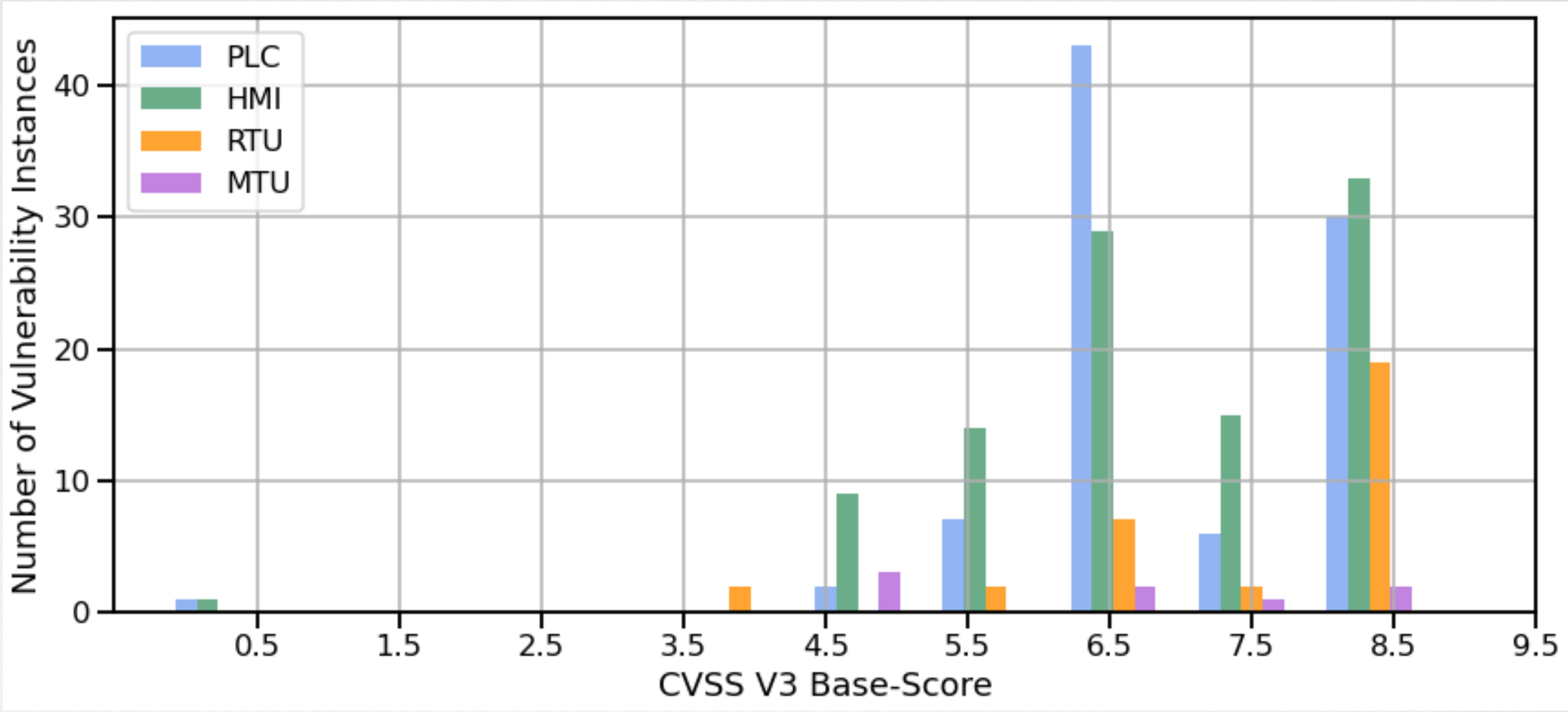
Characteristic Analysis for CPS Vulnerabilities

CPS on average

Metric	Measurement	PLC	RTU	MTU	HMI	CPS	CVE
ConfidentialityImpact	None	43.82%	21.87%	50.00%	17.14%	26.92%	22.15%
	Low	7.87%	0%	0%	10.48%	8.97%	19.10%
	High	48.31%	78.13%	15.00%	72.38%	64.10%	58.75%
IntegrityImpact	None	42.70%	46.88%	50.00%	39.05%	43.16%	31.14%
	Low	7.87%	0%	0%	10.48%	7.69%	17.20%
	High	49.45%	53.12%	50.00%	50.48%	49.15%	51.66%
AvailabilityImpact	None	13.48%	28.13%	37.50%	29.52%	22.65%	38.22%
	Low	0%	0%	0%	1.90%	0.85%	2.30%
	High	86.52%	71.87%	62.50%	68.57%	74.36%	61.19%

Overall in CVE

Characteristic Analysis for CPS Vulnerabilities



CVSS Version3 Base-Scores Distribution of CPS Vulnerabilities (2002-2020)

Planned Works

- Optimising majority voting method.
  - Apply majority voting to the sub-metrics of CVSS.
  - Use the weighted arithmetic mean of different scores from several sources.
  - Adjust the tie of majority voting under experts' supervision.

UNIVERSITY
OF SKÖVDE

Thanks!