**Cybersecurity Metrics: Why Is It So Hard?**
**SaTC 2019 PI meeting breakout group report**
**Co-leads: Shouhuai Xu (Univ Texas at San Antonio) and Kishor Trivedi (Duke)**
**Scribe: Adwait Nadkarni (William & Mary)**

## 1. Problem/Domain Summary

**Breakout session background and topic motivation**.
The breakout session is on *cybersecurity metrics* addressing the following question: "why cybersecurity metrics is so hard to tackle?" This topic is important to SaTC and to the society as a whole as being able to measure and quantify cybersecurity aspects of a system is the first step towards accomplishing a number of different goals, such as comparing alternative systems and addressing tradeoffs. Given that the problem of cybersecurity metrics is so hard, asking "why the problem is so hard" or "what are the technical barriers on the way towards solving the cybersecurity metrics problem" may shed light on new approaches to tackle the problem. Putting into the context of cybersecurity metrics, understanding the barriers to measure cybersecurity leads to a deeper understanding and possibly new technical approaches.

**Is there is an existing body of research and/or practice? What are some highlights or pointers to it?**

Although there is no literature on systematically examining why the cybersecurity metrics problem is so hard, there are positive results in measuring certain things in certain models, such as:

- The cybersecurity community has made significant progress. There are a few surveys that have systematized the existing metrics from different perspectives and the gaps between "what needs to be done" and "what we can do", including:
    - M. Pendleton et al., A Survey on Systems Security Metrics, ACM CSUR (2017).
    - A. Ramos et al., Model-based quantitative network security metrics: A survey. IEEE CST (2017).
    - J. Cho et al, STRAM: Measuring the Trustworthiness of Computer-based Systems. ACM CSUR (2019).

  As another example, there is a study (Sugrim et al., NDSS'19) showing that many papers used metrics that are confusing.
- The fault-tolerance community has made significant progress towards quantifying cybersecurity properties. Models, methods and tools have been developed and applied to several case studies. The community investigated the notion of survivability in certain threat models, which is related to the notion of resilience in cybersecurity. Two examples are:
    - D. Nicol et al., Model-Based Evaluation: From Dependability to Security. IEEE TDSC (2004).
    - Madan et al., A method for modeling and quantifying the security attributes of intrusion tolerant systems, Performance Evaluation (2004)

- A. Roy, D. Kim, K. Trivedi: Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees, Proc. DSN 2012
- Mitchell & Chen, Effect of Intrusion Detection and Response on Cyber Physical System, IEEE-TR, March 2013

- The software engineering community has made some significant progress in empirical measurement of software properties (e.g., "code smell"). According to Brooks, "software reflects the organization that developed it". Researchers are systematically evaluating the reasons that certain software components are considered flawed (e.g., "this type of code is bad because of XYZ"). We envision that something similar may be achievable in the realm of cybersecurity.

**2. Key Research Challenges**

The breakout session has identified the following barriers:

1. Systems security is about emergent properties, meaning that the properties of a system may not be directly derived from the properties of its components?
2. Do we know what metrics we have to measure?
3. Hard to precisely define what metrics are *useful*, i.e., what metrics best measure confidentiality, integrity, and availability
4. Walls between sub-disciplines (or silos)
5. Technical-business semantic gap, due to misaligned objectives. That is, how do you map business objectives to technical metrics
6. Hard to create/parameterize/validate useful models
7. Developing metrics that are reproduceable
8. How to deal with the unknown and future vulnerabilities, attacks?
9. High dimensionality, i.e., there are many facets of security that you cannot capture in on metric (e.g., CIA, privacy, trust, resilience)
10. Context-dependent metrics. Security is context-sensitive; if you are building a new technology and tool and need to evaluate it, you need to provide evidence, but that evidence would not really be a metric.
11. Indefinite system complexity
12. Hard to completely specify threat models
13. Hard to relate metrics to threat models?
14. Hard to relate vulnerability and exploitability and attack metrics
15. Hard to do experiments at scale?
16. Hard to translate intuitive metrics into precise ones
17. The lack of quality, publicly available datasets

**3. Potential Approaches to Overcoming those Barriers**

The breakout session identified the following potential approaches to overcoming those barriers:

1. Define metrics at multiple levels of abstractions, and a spectrum of metrics at each level of abstraction
2. Conduct case studies. If we can get examples of concrete solutions, we can then make metrics (i.e., what criteria should I use to buy this software).
3. Support a metrics research community
4. Publish papers with explicit metrics definitions?
5. Break walls between disciplines (or break down silos) – make researchers from different sub-disciplines work with each other.
6. Making more datasets available

**4. Long-Term (> 10 years) Significance**

The problem will remain relevant for many years.

**5. Other Important Aspects of This Topic *(specify)***

No.

**Acknowledgement**. We thank the breakout session participants for their insightful discussion and contributions, and Daniel Sadoc for helping edit this report.