Toward Normative Threat Models to Prevent Misuse

Extended Abstract

Özgür Kafalı, Munindar P. Singh, and Laurie Williams
Department of Computer Science
North Carolina State University
Raleigh, NC 27695-8206, USA
{rkafali,singh,laurie_williams}@ncsu.edu

ABSTRACT

Creating a set of comprehensive security requirements is the first step for implementing the necessary protocols to prevent, detect, and respond to misuses. Current approaches to tackle this task via threat modeling techniques lack formal semantics, which prevents formal understanding and aggregation of threat models needed to help security practitioners make informed decisions. We propose threat models formalized via norms, where a norm captures who is accountable to whom and for what. We discuss the merits of a normative representation and list promising directions of research.

Categories and Subject Descriptors

D.2.1 [**Software Engineering**]: Requirements/Specifications—*Elicitation methods*

Keywords

Security requirements, sociotechnical systems

1. APPROACH

The variety of accidental misuses has increased noticeably in recent years. According to a recent report by the United States Department of Defense [1], accidental misuses caused by poor user practices, poor network and data management practices, and poor data network implementation account for 80% of security incidents. We approach security from a sociotechnical standpoint [2] to capture such misuse cases via normative models. Norms regulate the interactions of autonomous parties, and describe who is accountable to whom and for what.

Significance: A normative representation will enable automatic translation of threat models into security protocols to prevent, detect, and respond to accidental misuses.

Novelty: Formal understanding and aggregation of normative threat models will reveal additional threats (not identified by individual threat models) via domain ontologies.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

HotSoS '17 Hanover, MD, USA

© 2017 ACM. ISBN .

DOI:

2. PROMISING DIRECTIONS

We propose norms (commitments, authorizations, and prohibitions) as a way to formalize threat models. Our findings from a recent study indicate that norms are useful for formalizing security requirements [2], and connecting requirements with misuses [4]. The following research directions are promising toward normative threat modeling:

1. Aggregation of threat models: Aggregation of threat models would increase knowledge of potential threats by identifying commonalities and differences among threats.

2. Analysis of misuses: While automatic generation of potential misuses [5] is helpful, formal analysis of real misuse incidents would help create a comprehensive set of security requirements.

3. Automatic generation of defenses: Characterization of cybersecurity attacks has been extensively studied, whereas little attention has been given to formal understanding of defense components. Relations among norms such as conflicts and tradeoffs [3] would reveal which defenses are best suited according to the needs of the underlying sociotechnical system. Sanctions can be generated as defenses.

4. Game playing : would incorporate security risk analysis into threat models as well as raise awareness among the general public for accidental misuses.

Acknowledgments

This research is supported by the US Department of Defense under the Science of Security Lablet grant. We thank Samuel Rappl for his help with our security card game.

3. REFERENCES

[1] DoD. The United States Department of Defense cybersecurity culture and compliance initiative, 2015.

[2] Ö. Kafalı, N. Ajmeri, and M. P. Singh. Revani: Revising and verifying normative specifications for privacy. *IEEE Intelligent Systems*, 31(5):8–15, 2016.

[3] Ö. Kafalı, N. Ajmeri, and M. P. Singh. Kont: Computing tradeoffs in normative multiagent systems. In *AAAI'17*, pages 3006–3012, 2017.

[4] Ö. Kafalı, J. Jones, M. Petruso, L. Williams, and M. P. Singh. Nane: How Good is a Security Policy against Real Breaches? A HIPAA Case Study. In *ICSE'17*.

[5] Ö. Kafalı, M. P. Singh, and L. Williams. Nane: Identifying misuse cases using temporal norm enactments. In *RE'16*, pages 136–145, 2016.