Cybersecurity and Privacy Threat Modeling: A Genomics Use Case

***Abstract*—This presentation will discuss cybersecurity and privacy threat modeling for biocybersecurity using a real-world genomics lab as a case study. These forms of threat modeling have several commonalities, but also have crucial differences in perspective, priorities, and approach. This presentation introduces both types of threat modeling and covers these similarities and differences in more detail. The insights shared were gained through interaction with an operational genomics lab over several years and multiple projects where cybersecurity and privacy threat models were developed and publicly shared.**

1. Introduction

While privacy and cybersecurity threat modeling have similarities, the perspectives and concerns for each can differ. For instance, while a cybersecurity threat model may be very concerned with traditional intentional data breaching cyberattacks, a privacy threat model may show more concern and attention to internal data privilege and access levels when human data are concerned.

This difference in concern results in different applicable tools to accomplish similar threat modeling goals. Although these tools fill similar niches within the respective methodologies, they tangibly show this difference in perspective. Both privacy and cybersecurity have multiple threat identification, attack or privacy activity classification, and mitigation or intervention frameworks available and the choice of which frameworks to use is dependent upon the goals of the threat modeler as well as the traits of the target environment. This talk discusses these topics using a genomics lab as a case study.

2. Background

The following section introduces the background information necessary to understand privacy and cybersecurity threat modeling.

2.1. Privacy Threat Modeling

The Threat Modeling Manifesto defines threat modeling as ”analyzing representations of a system to highlight concerns about security and privacy characteristics” [4] and outlines the Four Question Framework that guides the process of threat modeling. The core components of the threat modeling process provided by the Threat Modeling Manifesto generally involve fully identifying the target environment, brainstorming as many threats as possible to the environment, determining responses for each of those threats, and assessing the produced threat model.

This threat modeling approach can be used to model both security threats and privacy threats for the target environment. Although this threat modeling approach can be used for security and privacy, a threat modeler will find it beneficial to leverage security and privacy frameworks to enhance their threat model. For example, a security threat model may use STRIDE [5] to categorize threats and MITRE ATT&CK [6] to label attacks. The same threat modeler focusing on privacy threat modeling may choose to use the LINDDUN [1] framework for categorizing privacy threats and MITRE’s Pattern and Action Nomenclature of Privacy Threats (PANOPTIC) [2] framework for labeling privacy activities.

The LINDDUN framework separates privacy threats into seven distinct categories: Linking, Identifying, Non-Repudiation, Detecting, Data Disclosure, Unawareness/Unninterveneability, and Non-Compliance. Each category is then broken down further into subcategories, with each having its own threats, criteria, and potential impact should the threat come to fruition. The PANOPTIC framework takes a different approach and contains two sections: Privacy Contextual Domains (PCDs) and Privacy Activities (PAs). The five PCDs provide crucial situational awareness, while the PAs are a group of thirteen different privacy threat categories. Both frameworks are used in conjunction to establish a well-rounded privacy threat model.

2.2. Cybersecurity Threat Modeling

The process defined in the Threat Modeling Manifesto [4] also provides a functional outline for the cybersecurity threat modeling process. The main differences appear in the perspective and main concerns of the threat modeling endeavor and the individual tools and frameworks used.

The perspective used when creating a cybersecurity threat model differs from the privacy threat modeling perspective. When conducting privacy threat modeling, the threat modeler will be considering human data and how it, and relevant derivatives and observable effects from it, move through the environment and are reflected and managed through both technical and non-technical controls and interventions. The cybersecurity threat modeler will be more concerned with the state of the technical systems involved and technical attacks that may be conducted against these

systems. While there is some conceptual overlap between these, the main concern of the threat modeler should be on capturing the threats within either model rather than being halted by extended indecision on which model is more appropriate to capture a given threat.

As far as threat identification and classification frameworks and techniques go, STRIDE [5] is one potential threat categorization framework for cybersecurity threat modeling, but several alternatives exist depending on the industry or individual concerns of the target environment. While these and other frameworks and techniques exist, the most important concern is to enumerate as many relevant threats for the environment as possible.

Once the threats have been identified and classified, a framework such as the MITRE ATT&CK [6] framework allow the threat modeler to label attacks. Attack trees can also be generated to show how potential attack scenarios may move through the environment. In applying attack labeling techniques and frameworks such as these, the threat modeler may discover additional threats that have not yet been captured in the threat identification portion of the model; in this case, such new threats should be added to the model and tracked. Each phase of the threat modeling process may bring about new insights that are useful to previous sections and these new insights should be captured.

After attack labeling, potential actions to take to address individual threats can be decided; e.g., whether to accept, transfer, mitigate, or avoid. These choices should be clearly documented such that they can be reviewed and even revised as the environment changes in the future. Avoidance decisions should include explanations of how the respective threat is avoided. In the event of mitigate decisions, a threat model can either concisely describe the mitigation plan for each relevant threat or reference known cybersecurity control frameworks such as NIST SP 800-53 [3], ISO 27001 [8], or more domain-specific frameworks.

3. Cyberbiosecurity Applications

The genomics lab used as a case study for this work processes human physical samples to obtain digital sequence data and generate personalized insights that are provided back to the data subject. To conduct this threat modeling, the [REDACTED FOR DOUBLE BLIND REVIEW] was a partner and allowed access into their genomics environment for tours and interviews with the scientists that work daily in the labs. The aspects of genomic data that are relevant to a threat modeling endeavor are discussed in [REDACTED FOR DOUBLE BLIND REVIEW]. Table 1 and Table 2 show the methodological choices that were made in cybersecurity and privacy threat modeling, respectively, for this case study.

The full threat models for this case study are available in the currently public draft version of [REDACTED FOR DOUBLE BLIND REVIEW] and [REDACTED FOR DOUBLE BLIND REVIEW]. More in-depth discussion of the methodological choices made and the results that followed from those choices can be found in that document. A threat modeler can use this as an example of following a cybersecurity and privacy threat modeling methodology through for a given target environment, which is a genomics lab in this case.

TABLE 1. CYBERSECURITY THREAT MODELING FRAMEWORKS AND TECHNIQUES

Threat Modeling Step	Technique/Framework
Threat Identification and Categorization	STRIDE
Attack Labeling	MITRE ATT&CK
Control Identification	NIST SP 800-53

TABLE 2. PRIVACY THREAT MODELING FRAMEWORKS AND TECHNIQUES

Threat Modeling Step	Technique/Framework
Threat Identification and Categorization	LINDDUN
Attack Labeling	MITRE PANOPTIC
Control/Intervention Identification	NIST SP 800-53

4. Conclusion

After this talk, attendees will walk away with significant knowledge of both cybersecurity and privacy threat modeling, including how they are relevant and useful in the cyberbiosecurity domain. Attendees will hear first-hand accounts of conducting threat modeling on a real-world genomics lab environment. These accounts and subsequent discussion of the threat modeling process and choices made for a genomics lab threat modeling effort will help attendees when making similar choices in their own environments.

References

[1] Laurens Sion and Wouter Joosen, *LINDDUN PRO privacy threat modeling tutorial*, Technical Report, Department of Computer Science, KU Leuven, April 2023

[2] MITRE, "PTM Workshop," *Gitlab.io*, 2026. https://ptmworkshop.gitlab.io/#/panoptic.

[3] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," *Security and Privacy Controls for Information Systems and Organizations*, vol. 5, no. 5, Sep. 2020, doi: https://doi.org/10.6028/nist.sp.800-53r5.

[4] "Threat Modeling Manifesto," *www.threatmodelingmanifesto.org*. https://www.threatmodelingmanifesto.org/

[5] Microsoft, "The STRIDE Threat Model," *learn.microsoft.com*, Nov. 12, 2009. https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[6] MITRE, "MITRE ATT&CK," *Mitre.org*, 2025. https://attack.mitre.org/

[7] Pulivarti R, Martin N, Byers F, Wagner J, Maragh S, Wilson K, Wojtyniak M, Kreider B, Frances A, Edwards S, Morris T, Sheldon J, Ross S, Whitlow P, "Cybersecurity of Genomic Data," 2023, doi: https://doi.org/10.6028/nist.ir.8432.

[8] ISO/IEC, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," *iso.org*, Oct. 2022. https://www.iso.org/standard/27001