# Where Do Threat Models Come From?

## Challenging Implicit Assumptions

Lucy Qin
Leah Namisa Rosenbloom
Kris Shrishak

HotPETs 2023

How do privacy researchers engage in the process of **threat modeling**?

Where do the **underlying assumptions** of threats, and the **implicit assumptions** about the populations facing those threats, come from?

How might we bring the threat modeling process **"back to basics"**—such that our work addresses the **specific needs** of the population(s) it claims to serve?

**Threat Model Mismatch:** When the threat model of researchers trying to solve Problem X faced by Population Y does not align with the threat model of Population Y

## Common Mismatches

- Foundational Mismatch: Population Y is more concerned about Problem Z (and may or may not care about X)
- Solutional Mismatch: From the perspective of Population Y, researchers' proposed solution does not solve Problem X

# Threat Model Mismatch Example #1: Grassroots Organizing

- Activists, leakers, whistleblowers, and dissidents have to think about device compromise and therefore **compromise security**

- Cryptographers typically consider **post-compromise security**, modeled with a property called <u>forward secrecy</u>

<u>Forward secrecy:</u> a key compromise at time T does not allow an adversary to decrypt messages sent before time T

<u>Implicit assumptions:</u> adversary dragnet collects ciphertexts; later **corrupts** device with secret key(s) and attempts to decrypt them

# Threat Model Mismatch Example #1: Grassroots Organizing

- Activists, leakers, whistleblowers, and dissidents have to think about device compromise and therefore **compromise security**

- In reality, compromise **(semi-locked or unlocked device)** can reveal contacts, messaging history, metadata, documents, etc. (in plaintext)

Full-compromise security: activists want compromise awareness and remote deletion capabilities (Albrecht, Blasco, Jensen, and Mareková '21)

Reality: arrest leads to compromise of historical plaintext records; flexible deletion more important than forward secrecy (foundational mismatch)

# Threat Model Mismatch Example #2: Compelled Decryption

- When designing against a compelled decryption threat in which a subpoena is issued such that an individual must decrypt encrypted content, deniable encryption is a cryptographic tool that has been proposed

Deniable Encryption: enables a ciphertext to be decrypted to two or more plaintexts, using different keys

Implicit assumptions: the entity compelling the decryption does not know information about the underlying plaintext

Reality: when used in a situation where the entity compelling the decryption (such as a judge) knows something about the plaintext, giving keys that decrypt to false plaintexts could lead to negative consequences

# Think-Pair-Discuss Activity

1. Think (5 min)
    a. When you sit down to start a new project, how do you determine the threat model?
        - What are the pieces of tangible evidence that go into threat modeling decisions?
        - What are the implicit assumptions that go into threat modeling decisions?

    b. Have you noticed any example(s) of mismatches between threat models in research and threat models in practice? If so, what are they?

2. Pair (5 min)
    a. Introduce yourself to your partner and share your example(s) from Question 1b.

    b. What implicit assumptions might have created the mismatches in your examples?

3. Discuss (10 min)
    a. <u>Key insights:</u> what did you learn from your reflection and discussion?

    b. How accurately do our collective threat modeling processes reflect the needs of the population(s) that our work claims to serve? Why do you think that is?

    c. How might we reimagine the threat modeling process to address implicit assumptions and introduce more tangible evidence?