Putting Privacy on the MAP

A Persona Based Approach to Threat Modeling

Jayati Dev, Bahman Rashidi, and Vaibhav Garg
COMCAST Cable
How does my app work?

What kinds of data does it collect and process?
How do I find privacy threats in my application?

A manual privacy threat model is a way to identify these kinds of privacy violations at the design or architecture level.
However...

- Happens late stage
- Resource intensive
- Needs common language
- Demands privacy expertise
Privacy Shift Left

- **Happens late stage**
  - Integrate privacy early by empowering developers

- **Resource intensive**
  - Reduce overhead for threat modelers by potentially reducing action items and time

- **Needs common language**
  - Better efficiency due to consistent, repeatable threats across apps

- **Demands privacy expertise**
  - Use terms that are established and familiar
MAP Draws on Existing Frameworks
Existing Privacy Frameworks

- OWASP Top 10 Privacy Risks
- MITRE Privacy Threat Taxonomy
- NIST Privacy Risk Assessment Methodology
- LINDDUN
Models of Applied Privacy (MAP)

Holistic framework that builds on existing mechanisms for doing privacy threat modeling

Complements the privacy threat modeling process by guiding developers to **find** and **formalize** threats in the requirement gathering stage

- List of Findings
- Application
- List of Threats (Personas)
- Classify and risk-rank threats (MAP)
MAP Structure

There are three components

- **Actor**: CSAN Threat Actor List + Classify
- **Mechanism**: LINDDUN + PRAM
- **Impact**: Citron-Solove Taxonomy + Classify
MAP – Privacy Threat Modeling Framework

What threat(s) can occur?

- Threat Mechanism
- Linkability
- Identifiability
- Non-repudiation
- Detectability
- Disclosure of Information
- Unawareness
- Non-compliance
- Distortion
- Stigmatization
- Unanticipated Revelation
MAP – Privacy Threat Modeling Framework

Who can cause this threat?

Are they present inside the organization?
Do they intend to cause harm to the organization or to a person?

Someone with 5 years of Computer-related experience who uses that skill for a privacy threat
MAP – Privacy Threat Modeling Framework

What harm can this threat cause?

Is the harm related to an organization or to a person?

Is the harm measurable or not?
MAP – Privacy Threat Modeling Framework

Models of Applied Privacy (MAP)(CHI ’23). [https://doi.org/10.1145/3544548.3581484]
Advantages

Flexible
- Makes it easier to add and delete categories as required.

Scalable
- Forms a piece-wise architecture that is easy to code.

Customizable
- Independent of industry type and scale.

Moving away from an attacker-only approach
- Accounts for both malicious and benign actors.
How Do I Use MAP?

MAP uses personas to go from abstract to concrete visualization of the threat.

**Personas** are fictional characters, which you create based upon your research to **represent the different user types that might use your service, product, site, or brand in a similar way.**

Personas are commonly used in product development to ensure that the product meets the needs of all potential customers.
How can developers use this?

Note: Security TM is always the first step!

- Review the application
- Select relevant subcategories
- Create personas
- Review MAP
- Select one category from each of the three components
- Apply: Discuss with threat modeling to rank findings based on personas and recommend mitigations
Let’s do an example!

April uses a social media app
Example Persona

Outside Neutral (Expert) - Researchers, Non-compliance

Kiwi is a researcher who recently found company ABC’s user data in a large breach. Interestingly, on further investigation, Kiwi found that the types of data released in the breach was a lot more than what ABC had said they collect from users.

Consider this persona for your application.

1. Have you documented all the data types collected by your application?
2. Is your application collecting only the minimum data necessary for the app to function?
3. If no, have you documented the reason for collecting additional information?
4. For any information not necessary for the functioning of the is the user aware of the additional data collection and has consent been obtained?

Real World Breach:

Have an audit process for databases to ensure that minimization and retention policies are followed
**Example Persona**

**Inside Neutral (Non-expert) - Employees, Identifiability**

Avocado is a developer at a learning solution provider ABC. They maintain a public database of student information which is de-identified and does not contain personal information directly. However one of the columns in the database contains links and when someone clicks on these links, it redirects to personal documents stored elsewhere, like passport scans, application forms, visas, emails, and even medical information.

Consider this persona for your application.

1. Does any component in your application contain links?
2. Do these links redirect to any sensitive information?
3. If yes, is there authentication in place for who can access this information?

**Real World Breach:**

Anonymize and minimize the amount of personal information viewable by users on need-to-know basis
Example Persona

Inside Neutral (Expert) - Related Entities, Unawareness

Mango provides identity verification services as a vendor for social media platform ABC. During a breach at ABC, Mango requests personal information from ABC's customers in order to verify their account. However, Mango also sends this data to a marketing company who is now able to target advertisements to customers based on this new information. This purpose was not disclosed to customers and it may cause a privacy issue.

Consider this persona for your application.

1. If your application has a vendor who uses customer data beyond functionality, do customer know about this in their privacy policy? Have they provided consent to this extended use?
2. Can customers limit their data from being shared by vendors to other applications?
3. Are customers able to access/modify their data that is sent to vendors?
4. Has the vendor gone through TPSA?

Real World Breach:

Be transparent with customers – inform the user and give control
Ad Delivery Network

Profile Database

Profile tags
Behavior tags

Website cookies

Photos licensed under CC BY-SA, CC BY. Example is for illustrative purposes only.
Testing on Real-World Incidents

We tested the model against the Verizon Community Data Base for 207 privacy related incidents*

*Note there can be multiple threat impacts
Categorizing Privacy Incidents Using MAP

Frequency of occurrence of the components of the framework in VCDB

Showing categories that account for > 80% of 183 incidents.
Thank you for Listening!

Key Takeaways

• Unified framework for developers to conduct threat modeling

• Personas help operationalize threats across various sectors

• Use MAP to classify existing findings

Resources

Open-source project on GitHub: https://github.com/Comcast/MAP

More information on the SPIDER team: https://corporate.comcast.com/ccs-research

Reach us on LinkedIn:
jayati-dev
bahman-Rashidi
gargvaibhav