Know Thy Enemy: The Taxonomies That Meta Uses to Map the Offensive Privacy Space

Zach Miller - Privacy Red Team, Meta
David Renardy - Privacy Red Team, Meta

This talk is...

- About design decisions we made on offensive privacy frameworks.
- A reflection on the use-cases of those frameworks.
- A jumping off point for driving more discussions in the space.

This talk is not...

- A product or service pitch.
- A takedown or criticism of preceding frameworks.
- About absolutes.

Agenda

01 **Who are Offensive Privacy Threats and how are they tracked?**

02 What are their tactics? (**Privacy Adversarial Framework** - PAF)

03 What weaknesses do they leverage? (Meta Weakness Enumeration - MWE)

04 What can I do for my organization?

What data do you have and who wants it?

Industry / Company

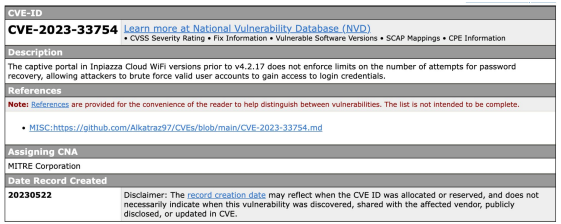
- Health
- Financial
- Social media
- Defense
- Government

Potential Adversaries

- Data brokers
- Nation state actors
- Private Investigation firms
- Stalkers
- Advertising agencies
- Political campaign firms

How do we understand threats in Cybersecurity?

- **Adversary Behaviors** (TTPs)
  - MITRE ATT&CK®
- **Weaknesses enumeration and root causes**
  - CVE® CAPEC™



CVE-ID

CVE-2023-33754 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The captive portal in Inplazza Cloud WiFi versions prior to v4.2.17 does not enforce limits on the number of attempts for password recovery, allowing attackers to brute force valid user accounts to gain access to login credentials.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

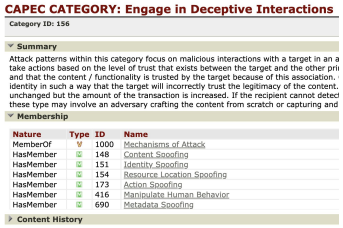
- MISC:https://github.com/Alkatraz97/CVEs/blob/main/CVE-2023-33754.md

Assigning CNA

MITRE Corporation

Date Record Created

20230522	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.



CAPEC CATEGORY: Engage in Deceptive Interactions

Category ID: 156

Summary

Attack patterns within this category focus on malicious interactions with a target in an a
take actions based on the level of trust that exists between the target and the other pri
and that the content / functionality is trusted by the target because of this association.
identity in such a way that the target will incorrectly trust the legitimacy of the content.
unchanged but the amount of the transaction is increased. If the recipient cannot detec
these type may involve an adversary crafting the content from scratch or capturing and

Membership

Nature	Type	ID	Name
MemberOf	V	1000	Mechanisms of Attack
HasMember	S	148	Content Spoofing
HasMember	S	151	Identity Spoofing
HasMember	S	154	Resource Location Spoofing
HasMember	S	173	Action Spoofing
HasMember	S	416	Manipulate Human Behavior
HasMember	S	690	Metadata Spoofing

Content History

Privacy friction with existing frameworks

Privacy-centric tactics or vulnerabilities not present

OR

Not enough granularity on Privacy

Privacy-centric tactics

Example: Adversary downloads data from legacy endpoints via an internet archive

Difficult to express in e.g. Mitre ATT&CK (closest is “Search Open Websites/Domains”)

Privacy-centric vulnerabilities

Example: Insufficient Anonymization

CWE ???

Insufficient Granularity

Example: Contact point exposure

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Privacy Threat Intelligence

- Less open reporting than in Security
- Lucky if root cause or technical weakness is identified in reporting
- Common adversary tactics not tracked across cases

Creating our own Privacy taxonomies

Design Decisions:

- Who are the data providers? Who are the data consumers?
- Privacy-exclusive vs. Privacy-inclusive

Agenda

01 Who are Offensive Privacy Threats and how are they tracked?

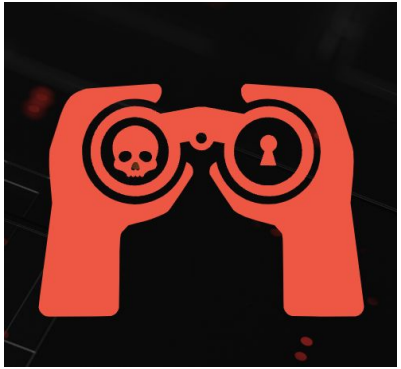
02 What are their tactics? (Privacy Adversarial Framework - PAF)

03 What weaknesses do they leverage? (Meta Weakness Enumeration - MWE)

04 What can I do for my organization?

Privacy Adversarial Framework (PAF)

- Inspired by MITRE ATT&CK®, TTP framework for Offensive Privacy.
  - Tactics
  - Techniques
    - Subtechniques
- Designed to be privacy-exclusive and to supplement existing cybersecurity frameworks.
- Plan for public release with ATT&CK Navigator integration.



Why Privacy-exclusive?

- Privacy threat actors don’t always need a complete “kill-chain”.
  - E.g. Stalker may only want to access data
- Choke points for detection and mitigations are different than for cybersecurity.
  - E.g. Spoofing User Agents

Who provides data? Who consumes data?

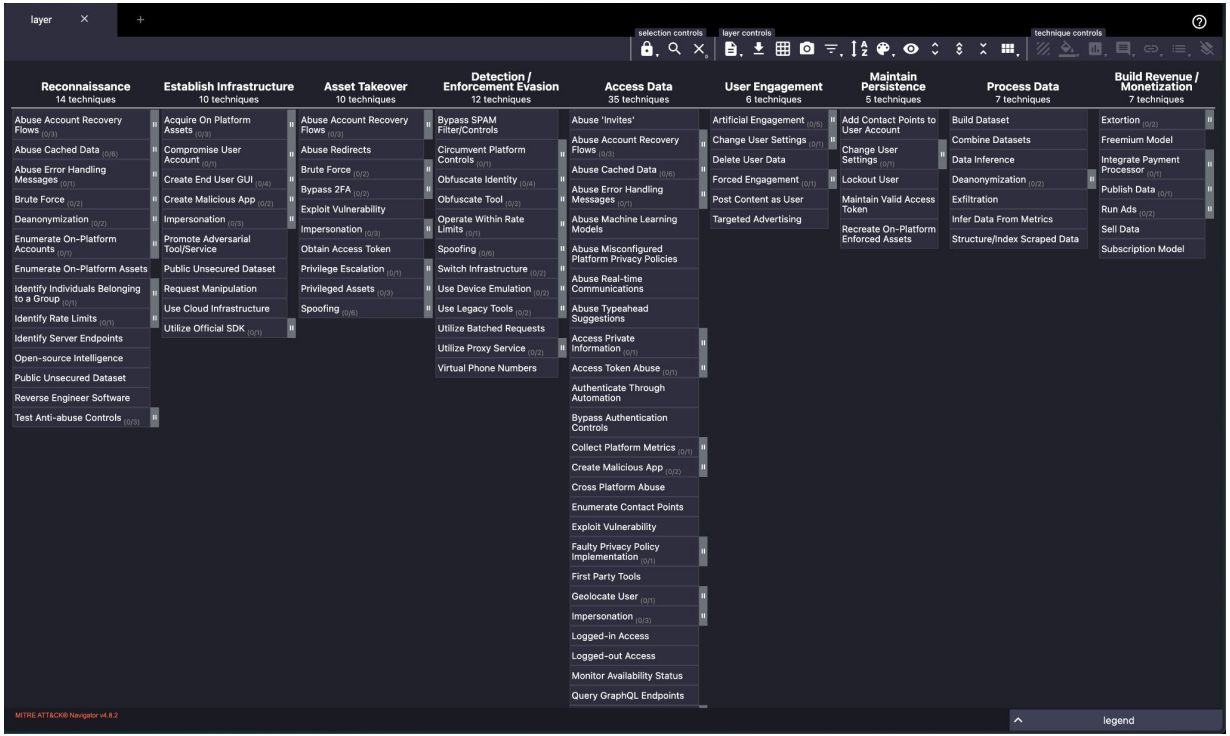
Data sources (tagging examples and incidents):

- Red Team
- Threat Intel
- Investigations

Data sinks:

- Red Team
- Threat Intel
- Investigations
- Insights / Detections
- Purple Team

Privacy Adversarial Framework



Using PAF

Ex 1: Adversary downloads data from legacy endpoints via an internet archive

PTA0005
Access Data

PTA0083
Abuse Cached Data

PT0083.001
Archived Site

Using PAF

Ex 2:

PTA0002 Establish Infrastructure

PT0061.003
Create Account

PT0063
Utilize Official SDK

PTA0004 Detection / Enforcement Evasion

PT0052.002
Spoof User Agent

PT0005 Access Data

PT008 Logged-In Access

PT0040.023 Scraping - Use Open Source Tooling

PT003 Access Token Abuse

PAF Outcomes

- Identify common adversarial behaviors.
- Link behaviors to common products and surfaces.
- Identify emerging behaviors as they manifest.
- Find “choke points” for detection, mitigation and enforcement.
- Develop privacy threat intel feed within your org.

Agenda

01 Who are Offensive Privacy Threats and how are they tracked?

02 What are their tactics? (Privacy Adversarial Framework - PAF)

03 What weaknesses do they leverage? (Meta Weakness Enumeration - MWE)

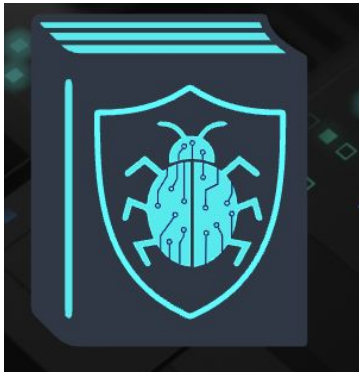
04 What can I do for my organization?

What weaknesses do they leverage?

- Adversaries are outcome-driven
- Data is our adversaries' main target

Meta Weakness Enumeration (MWE)

- Inspired by MITRE's CWE® and CAPEC® systems
- Designed to be privacy-inclusive
- Includes types unique to Meta and our custom, internal systems

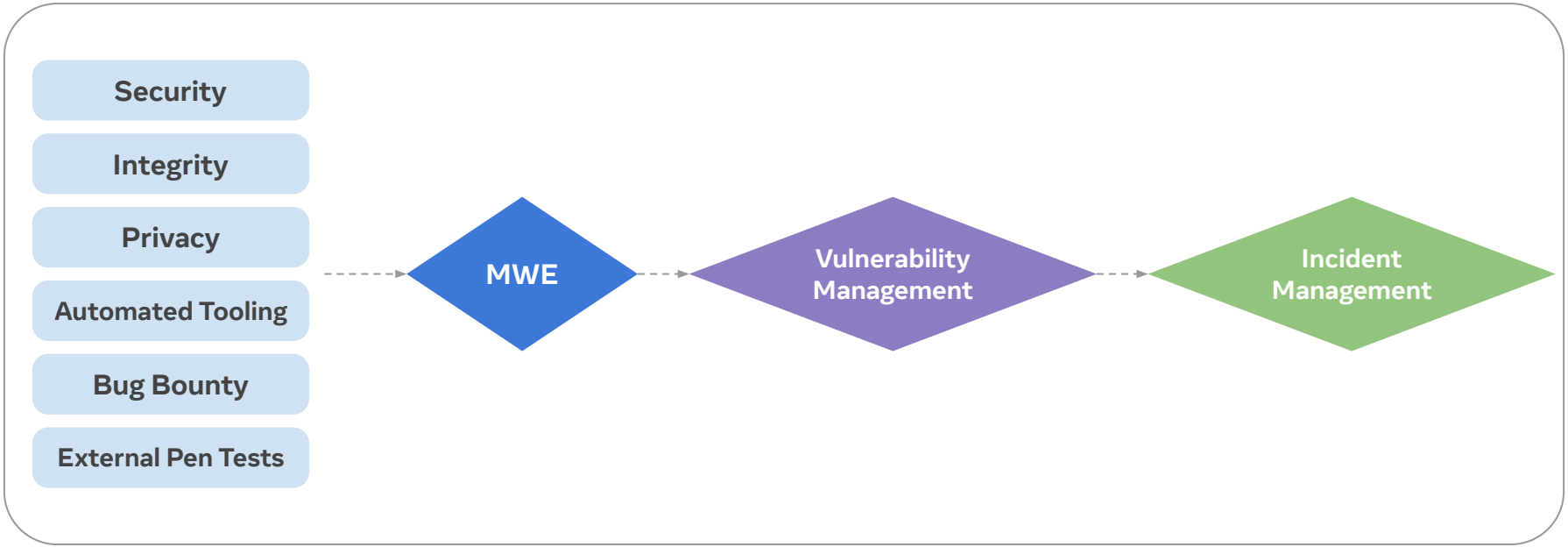


Why privacy-inclusive?

- Vulnerabilities encountered by security, privacy, and integrity teams often overlap
- Approaches towards detecting, preventing, and remediating vulnerabilities can also overlap

Who do we expect to use it?

Meta Internal Processes



Who do we expect to use it?

Who will actually be applying the taxonomy

- Engineers?
- PMs?
- Someone else?

What specifically are we trying to measure?

- Vectors - the method of abuse
- Root Weakness - the underlying technical cause which enabled the Vector to exist

Vector

Contact Point Exposure

Root Weakness

Response Side Channel

Summary of MWE Design

- Privacy-inclusive system applicable across company
- Technically-focused system to identify trends, inform tech investment, spread awareness
- Categorize vectors of abuse and weaknesses that cause them

MWE Outcomes

- Educational efforts on privacy-centric vulnerabilities
- Cross-organizational collaboration on shared issues
- Efficiency gains due to aligning on unified system

Agenda

01 Who are Offensive Privacy Threats and how are they tracked?

02 What are their tactics? (Privacy Adversarial Framework - PAF)

03 What weaknesses do they leverage? (Meta Weakness Enumeration - MWE)

04 What can I do for my organization?

What can I do?

- Investigate the Privacy threats your product / organization is up against.
- Think about privacy-inclusive vs. privacy-exclusive approaches.
- Consider adopting PAF via Mitre ATT&CK Navigator integration.
- Incorporate MWE design decisions in your own vulnerability management framework.

Let's continue the conversation.

David: drenardy@meta.com
Zach: zjmiller@meta.com

Meta