



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
 -

Reconnaissance 10 techniques	Resource Development 10 techniques	Initial Access 11 techniques	Execution 14 techniques	Persistence 13 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 37 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 17 techniques	Impact 13 techniques
Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)	Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2) Active Directory Enumeration (2)



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 Inpiazza 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: 158

Summary

Attack patterns within this category focus on malicious interactions with a target in a take actions based on the level of trust that exists between the target and the other party and that the content / functionality is trusted by the target because of this association. Identify 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 detect these type may involve an adversary crafting the content from scratch or capturing and

Membership

Notes	Type	ID	Name
MemberOf	1	1000	Mechanisms of Attack
HasMember	1	148	Content Spoofing
HasMember	1	151	Identity Spoofing
HasMember	1	154	Resource Location Spoofing
HasMember	1	173	Action Spoofing
HasMember	1	416	Manipulate Human Behavior
HasMember	1	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

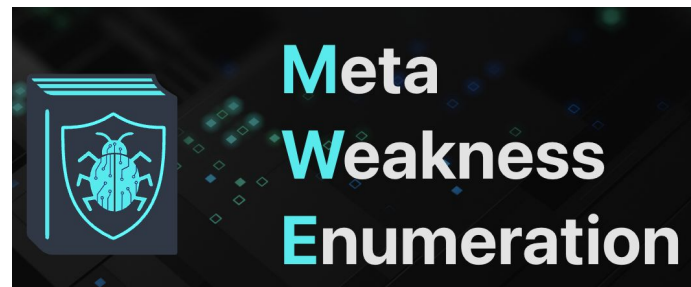
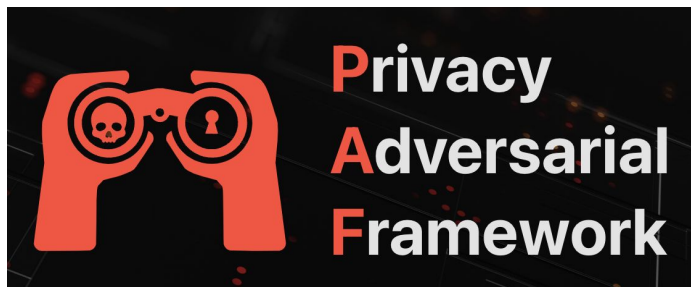
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor



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

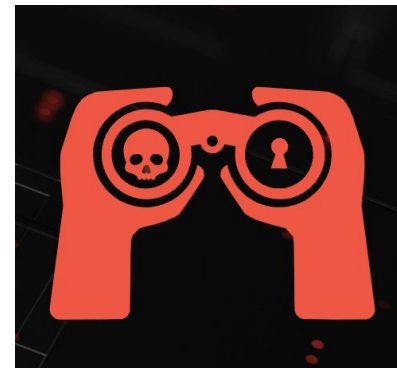


Agenda

- 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

layer								
selection controls								
layer controls								
technique controls								
Reconnaissance 14 techniques	Establish Infrastructure 10 techniques	Asset Takeover 10 techniques	Detection / Enforcement Evasion 12 techniques	Access Data 35 techniques	User Engagement 6 techniques	Maintain Persistence 5 techniques	Process Data 7 techniques	Build Revenue / Monetization 7 techniques
Abuse Account Recovery Flows (C2)	Acquire On Platform Assets (C2)	Abuse Account Recovery Flows (C2)	Bypass SPAM Filter/Controls	Abuse 'Invites'	Artificial Engagement (C6)	Add Contact Points to User Account	Build Dataset	Extortion (C2)
Abuse Cached Data (C4)	Compromise User Account (C1)	Abuse Redirects	Circumvent Platform Controls (C1)	Abuse Account Recovery Flows (C2)	Change User Settings (C1)	Change User Settings (C1)	Combine Datasets	Freemium Model
Abuse Error Handling Messages (C4)	Create End User GUI (C4)	Brute Force (C2)	Obfuscate Identity (C4)	Abuse Cached Data (C6)	Delete User Data	Lockout User	Data Inference	Integrate Payment Processor (C1)
Brute Force (C2)	Create Malicious App (C2)	Bypass 2FA (C2)	Obfuscate Tool (C2)	Abuse Error Handling Messages (C1)	Forced Engagement (C1)	Maintain Valid Access Token	Deanonimization (C2)	Publish Data (C1)
Deanonimization (C2)	Impersonation (C2)	Exploit Vulnerability	Operate Within Rate Limits (C1)	Abuse Machine Learning Models	Post Content as User	Recreate On-Platform Enforced Assets	Exfiltration	Run Ads (C2)
Enumerate On-Platform Accounts (C1)	Promote Adversarial Tool/Service	Obtain Access Token	Spoofing (C6)	Abuse Misconfigured Platform Privacy Policies	Targeted Advertising		Infer Data From Metrics	Sell Data
Enumerate On-Platform Assets	Public Unsecured Dataset	Privilege Escalation (C1)	Switch Infrastructure (C2)	Abuse Real-time Communications			Structure/Index Scraped Data	Subscription Model
Identify Individuals Belonging to a Group (C1)	Request Manipulation	Privileged Assets (C2)	Use Device Emulation (C2)	Abuse Typeahead Suggestions				
Identify Rate Limits (C1)	Use Cloud Infrastructure	Spoofing (C6)	Use Legacy Tools (C2)	Access Private Information (C1)				
Identify Server Endpoints	Utilize Official SDK (C1)		Utilize Batched Requests	Access Token Abuse (C1)				
Open-source Intelligence			Virtual Phone Numbers	Authenticate Through Automation				
Public Unsecured Dataset				Bypass Authentication Controls				
Reverse Engineer Software				Collect Platform Metrics (C1)				
Test Anti-abuse Controls (C1)				Create Malicious App (C2)				
				Cross Platform Abuse				
				Enumerate Contact Points				
				Exploit Vulnerability				
				Faulty Privacy Policy Implementation (C1)				
				First Party Tools				
				Geolocate User (C1)				
				Impersonation (C2)				
				Logged-in Access				
				Logged-out Access				
				Monitor Availability Status				
				Query GraphQL Endpoints				

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



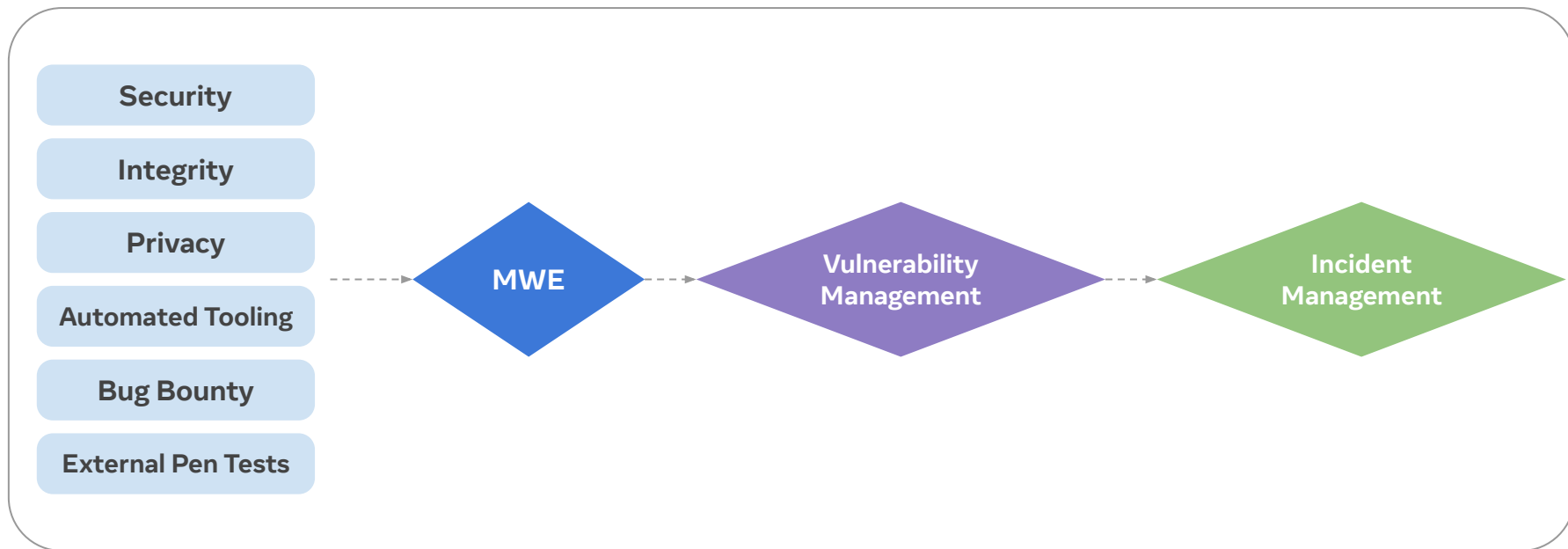


Why privacy-inclusive?

- 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

