

Industrial practitioners' mental models of adversarial machine learning

Lukas Bieringer*
QuantPi

Kathrin Grosse*
University of Cagliari

Michael Backes
*CISPA Helmholtz Center
for Information Security*

Battista Biggio
*University of Cagliari,
Pluribus One*

Katharina Krombholz
*CISPA Helmholtz Center
for Information Security*

Abstract

Although machine learning is widely used in practice, little is known about practitioners' understanding of potential security challenges. In this work, we close this substantial gap and contribute a qualitative study focusing on developers' mental models of the machine learning pipeline and potentially vulnerable components. Similar studies have helped in other security fields to discover root causes or improve risk communication. Our study reveals two facets of practitioners' mental models of machine learning security. Firstly, practitioners often confuse machine learning security with threats and defences that are not directly related to machine learning. Secondly, in contrast to most academic research, our participants perceive security of machine learning as not solely related to individual models, but rather in the context of entire workflows that consist of multiple components. Jointly with our additional findings, these two facets provide a foundation to substantiate mental models for machine learning security and have implications for the integration of adversarial machine learning into corporate workflows, decreasing practitioners' reported uncertainty, and appropriate regulatory frameworks for machine learning security.

1 Introduction

Adversarial machine learning (AML) studies the reliability of learning based systems in the context of an adversary [6, 12, 69]. For example, tampering with some features often

suffices to change the classifier's outputs to a class chosen by the adversary [9, 24, 80]. Analogously, slightly altering the training data enables the attacker to decrease performance of the classifier [11, 72]. Another change in the training data allows the attacker to enforce a particular output class when a specified stimulus is present [20, 36]. Most state-of-the-art attacks and mitigations are in an ongoing arms race [5, 19, 82].

Although machine learning (ML) is increasingly used in industry, very little is known about ML security in practice. At the same time, previous works show that practitioners are concerned about AML [47, 60], and failures already occur [53], very little is known about ML security in practice. To tackle this question, we conduct a first study to explore mental models of AML. Mental models are relatively enduring, internal conceptual representations of external systems that originated in cognitive science [30, 38]. In other security related areas, correct mental models have been found to ease the communication of security warnings [16] or enable users to implement security best-practices [81]. Mental models also serve to enable better interactions with a given system [87], or to design better user interfaces [29].

Our methodology builds upon these previous works by using qualitative methods to investigate the perception of vulnerabilities in ML applications. More concretely, we conducted 15 semi-structured interviews and drawing tasks with industrial practitioners from European start-ups and coded both drawings and the transcripts of the interviews. As the first work in this direction, we lay the foundations for practitioners' mental models of AML by describing two facets of these models. The first concerns the separation of ML related security (AML) and security unrelated to ML (non-AML security). In many cases, the borders between these two fields are blurry: a participant may start talking about evasion and finish the sentence with a reference to cryptographic keys. The second facet concerns the view of the ML model within a project. In contrast to the focus on an isolated model in AML research [5, 6, 12, 19, 69], our practitioners often describe one or more pipelines with potentially several applications of ML. Finally, we found more facets which are left for an in-depth

*First two authors contributed equally.

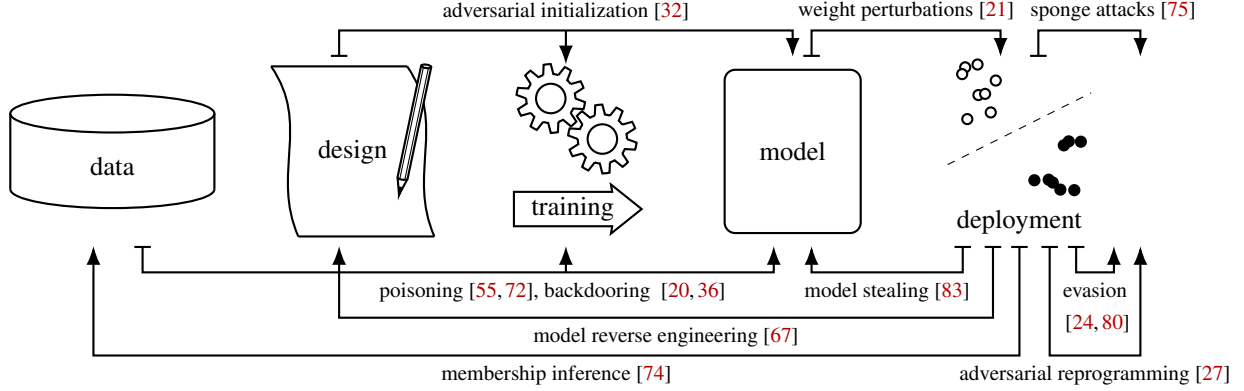


Figure 1: AML threats within the ML pipeline. Each attack is visualized as an arrow pointing from the step controlled to the point where the attack affects the pipeline.

investigation by future work. These include the application setting, prior education, and the perceived relevance of AML.

Our interviews showed that most of our participants lack an adequate and differentiated understanding to secure ML systems in production. At the same time, more than a third of our participants feels insecure about AML. These concerns seem justified as we found evidence for semi-automated fraud on ML systems in the wild. However, our findings have more practical implications. Our results allow us to address the current lack of understanding by (I) increasing awareness for AML and decreasing uncertainty about AML, (II) developing tools that help practitioners to assess and evaluate security of ML applications, and (III) drafting regulations that contain adequate security assessments and reduce insecurity about AML. However, more work is needed to understand the individual and shared mental models of practitioners and assess the real world security risks when applying ML.

2 Background and related work

In this section, we review related work on AML and recall different attacks that have recently been discussed. We also review literature on mental models with regard to human-computer interaction, usable security and ML.

2.1 Adversarial machine learning

AML studies the security of ML algorithms [6, 12, 69]. We attempt to give an informal overview of all attacks in AML, and additionally illustrate them in Figure 1.

Poisoning/backdooring. Early works in poisoning altered the training data [72] or labels [11] to decrease accuracy of the resulting classifier, for example SVM. For deep learning, due to the flexibility of the models, introducing backdoors is more common [20, 36]. Backdoors are chosen input patterns that reliably trigger a specified classification output. Defending such backdoors has lead to an arms race [82].

Evasion/adversarial examples. Early work in evasion decreased the test-time accuracy of spam classification [24]. It was later shown that also more complex models change their output for small, malicious input perturbations [9, 80]. Albeit all classifiers are principally vulnerable towards evasion, recent works focus on the arms race in deep learning [5, 19].

Membership inference. After first inferring attributes [4] of the training data, research later showed that entire points can be leaked from a model [74]. More concretely, the attacker deduces, given the output of a trained ML model, whether a data record was part of the training data or not. As for other attacks, numerous defenses are being proposed [37, 64].

Model stealing. Tramèr et al. [83] recently introduced model stealing. During this attack, the attacker copies the ML model functionality without consent of the model’s owner. The attacker, given black box access to the original model, tries to reproduce a model with similar performance. As for the previous attacks, mitigations have been proposed [39, 68].

Weight perturbations. Fault tolerance of neural networks has long been studied in the ML community [17, 65]. Recently, maliciously altered weights are used to introduce a specific backdoor [35]. Few works exist to defend malicious change to the weights in general, not only related to backdoor introduction [78, 88].

For the sake of completeness, we conclude with a description of additional, recent attacks, some of which are part of our questionnaires (see Appendix D.3). In **adversarial initialization**, the initial weights of a neural network¹ are targeted to harm convergence or accuracy during training [32, 54]. In **adversarial reprogramming**, an input perturbation mask forces the classifier at test time to perform another classification task than originally intended [27]. For example, a cat/dog classifier is reprogrammed to classify digits. In **model reverse engineering**, crafted inputs allow to deduce from a trained model the usage of dropout and other architectural choices [67]. Fi-

¹Classifiers with convex optimization problems (for example SVM) cannot be targeted, as the mathematical solution to the learning problem does not depend on the initial weights.

nally, **sponge attacks** aim to increase energy consumption of the classifier at test time [75].

Practical Relevance of AML. In general, AML research has been criticized for the limited practical relevance of its threat models [28, 31]. A possible reason is our lack of knowledge about AI security in practice. Few works attempt to tackle this gap, including for example Lin and Biggio [53]. They give an overview about AI attacks that were carried out in practice based on AI related incidents covered in newspapers. Furthermore, Boenisch et al. [14] conducted a survey and developed an awareness score, which however encompasses AML, privacy, and non-AML security. Concerning which threats are relevant in practice in industry, Kumar et al. [47] and Mirsky et al. [60] found that practitioners are most concerned about model theft and poisoning. Yet, in academia, most work focused on evasion so far. To shed more light on AML in practice, we interview industrial practitioners and take a first step towards a theory of mental models of AML. To this end, we now introduce and review mental models.

2.2 Mental models

Mental models are relatively enduring and accessible, but limited, internal conceptual representations of external systems [26] that enable people to interact with given systems. Hence, the field of human computer interaction (HCI) studied this concept quite early [73]. Mental models, most recently, saw an increasing relevance in usable security. We now recall prior application scenarios and highlight relevant conceptual contributions in the context of security and ML.

Mental models in HCI and usable security. The relevance of mental models has been subject to a lengthy debate in HCI research [76, 85]. In many cases, the focus was to capture, depict and analyze mental models of specific objects of investigation. Examples of topics include, but are not limited to, the design of online search applications [7], interface design [44], and interfaces for blind people [25]. Research in usable security has recently focused on mental models of security in general [2, 87], privacy in general [71], security warnings [16], incident response [70], the internet [41], the design of security dashboards [58], the Tor anonymity network [29], privacy and security in smart homes [81, 90], encryption [1, 89], HTTPS [45], and cryptocurrency systems [57].

With regard to the respective object of investigation, these contributions paved the way for improvements of user interface designs [29], adequate security communication [16], as well as the development of security policies and implementation of best-practices [81]. It has been argued that security mental models contain structural and functional properties [89]. For each application, users develop a cognitive representation of its inherent components, their interconnection and correspondingly possible security threats. This representation helps them to understand where threats could emerge and how they could take effect. Mental models evolve dynamically

upon individual interaction with a given application [13].

Mental models in ML. In order to interact with an ML application, humans need a mental model of how it combines evidence for prediction [66]. This is all the more important for ML-based applications which often inherit a certain opacity. As Lage et al. [48] pointed out, the number of necessary cognitive chunks is the most important type of complexity in order to understand applications. During interaction with black-box processes, humans strive for reduced complexity which may lead to the development of inaccurate or oversimplified mental models [33, 42].

A dedicated line of research therefore elaborates on the relevance and nature of mental models in the context of explainable artificial intelligence. Mental models have been found to serve as scaffolds not only for a given ML application [84], but also for its embedding in organizational practices [91]. For data science teams, these workflows usually consist of predefined steps (Figure 1) and necessitate interpersonal collaboration [62]. Following Arrieta et al. [3], we argue that individual collaborators within these teams (e.g., ML engineers, software engineers) develop separate internal representations of a given workflow or application. The need for appropriate mental models thereby increases with the enlarged scope of ML applications [49] and involved stakeholders [51, 79].

Recent work in this line of research called for qualitative studies at the intersection of the HCI and ML communities, to better understand the cognitive expectations practitioners have on ML systems [8, 42]. Suchlike studies seem all the more relevant as various industry initiatives propagate a human-centric approach to AI, explicitly referring to mental models.² However, the current scientific discourse lacks a dedicated consideration of cognition in AML. In order to fill this gap, we present the first qualitative study to elicit mental models of adversarial aspects in ML.

3 Methodology

This section describes the design of our semi-structured interviews, the drawing task, our recruiting strategy, the participants, and the data analysis. Our methodology was designed to investigate the perception of ML security and is, to the best of our knowledge, the first mental model study of AML.

3.1 Study design and procedure

To assess participants' perceptions, we conducted semi-structured interviews enriched with drawing tasks. We draw inspiration from recent work in usable security which also investigated mental models [45, 89].

Before the interview, participants were informed about the general purpose of our study and the applied privacy measures. We further assured each participant that their answers would

²e.g., <https://pair.withgoogle.com/chapter/mental-models/>

Table 1: Participants with their random IDs. Capital letters denote that participants work in the same company. We denote the application domain and the working experience (Exp.) in years. Knowledge in ML, Security and AML is encoded as completed lectures (++) , seminar/self-study (+) or none ().

Company			Education				
ID	Application domain		Exp.	ML	Sec.	AML	Degree
1		Human resources	7	++	+		PhD
3	A	Healthcare	0.4				PhD
4	B	Cybersecurity	8	++	+		PhD
6	C	Business intelligence	15	++	++	+	PhD
7		Computer vision	12	++			BSc
9		Computer vision	9	++			MSc
10		Cybersecurity	no questionnaire handed in				
11		Business intelligence	1	++			PhD
12		Retail and commerce	1.4			++	PhD
14		AI as a service	5	++		+	PhD
15		Computer linguistics	5	+	+		MSc
16	C	Business intelligence	3	++	+	+	PhD
18	A	Healthcare	1.5	++			PhD
19	B	Cybersecurity	15	++	++	+	MSc
20	A	Healthcare	1.2	++			MSc

not be judged. Participants were then instructed to complete a questionnaire on demographics, organizational background and a self-reflected familiarity with field-related concepts (Appendix D) before the interview. This questionnaire was filled with or without the authors’ presence. The answers have later been used to put participants’ perceptions in context to their organizational and individual background.

The threefold structure of our interviews covered 1) a specification of a given ML project a participant was involved in, 2) the underlying ML pipeline of this project and 3) possible security threats within the project. We chose this approach as the different attack vectors form part of the ML-pipeline as shown in Section 2.1. The detailed interview guideline can be found in Appendix C. As a last step of our interviews, we confronted the participants with exemplary attacker models for some of the threats considered relevant in industrial application of ML [47]. To assess practitioners’ understandings of these threats, study participants had to elaborate on these attack vectors within their specific setup (Appendix D.2).

To assess the participants’ knowledge about (A)ML in general, participants were asked to fill an additional questionnaire after the interview (Appendix D.3). In this questionnaire, we tested general knowledge in ML and independently asked for a self-reflected familiarity rating with some of the attacks we discussed in Section 2.1. This questionnaire was handed to the participants after the interview as to avoid priming.

We conducted one pilot interview to evaluate our study design. This first participant met all criteria of our target population in terms of employment, education and prior knowledge. As his explanations and drawings matched our expectations, we only added a specific question regarding the collaborators within a given ML-based project.

The average interview lasted 40 minutes and was jointly conducted by the first two authors of this paper between April and July 2019. To minimize interviewer biases, we equally distributed the interviews, where one author was the lead interviewer and the other took notes. Due to the COVID-19 pandemic, interviews were conducted remotely and relied on a freely available digital whiteboard³.

3.2 Recruitment

Recruitment for a study on applied ML in corporate environments presents a challenge, as only a small proportion of the overall population works with ML. Furthermore, the topic touches compliance and intellectual property of participating organizations. Hence, many companies are skeptical about the exchange with third parties. Consequently, many current contributions with industrial practitioners as study participants are conducted by corporate research groups (e.g., [34, 47]).

We tried to initiate interviews with two large multinational companies. Unfortunately, both denied our request after internal risk assessments. Therefore, we focused on smaller companies where we could present our research project directly to decision-makers and convince them to participate in our study. We relied on the authors’ networks (pilot participant, *P11*) and public databases for start-ups (more details in Appendix A) to find potential participants and used direct-messaging on LinkedIn and emails to get in contact.

Recruitment of study participants happened in parallel to interview conduction. Some participants forwarded our interview request to internal colleagues, so that we talked to multiple employees of some participating companies (see Table 1). We aimed to recruit experienced and knowledgeable participants and hence our requirements were a background in ML or computer science and positions such as data scientists, software engineers, product managers, or tech leads. We did not require any prior knowledge in security. After 8 interviews, no new topics (in our case for example new pipeline elements, whether defenses were mentioned, or how attacks were depicted in drawings) emerged. The research team thus agreed after 15 interviews that saturation was reached [15], and we stopped recruiting. The participants were randomly assigned an ID (a number between 1 and 20) which was used throughout our analysis. All participants were offered an euro 20 voucher as compensation for their time.

3.3 Participants

We summarize demographic information in Table 1. One participant, *P10*, did not hand in the questionnaire and is consequently not included in the following statistics. 14 participants identified as male, one identified as female, our sample is thus skewed towards males when considering ML practitioners [40]. As previous work found security perception of

³<https://awwapp.com/>

women and men to exhibit only some differences [59], this bias is acceptable for a first exploration but should be studied in depth in future work. Our participants had an average age of 34 years (standard deviation (STD) 4.27). As intended for a first exploration of practitioners' perception of AML, our sample covered various application domains and organizational roles which we now describe in detail.

Education and prior knowledge. The majority of participants (9 of 14) has a PhD, with all participants holding some academic degree. While our sample skews towards PhDs compared to the overall population of ML practitioners [40], previous work reports no correlation between overall education and security awareness [14]. Most participants (12 of 14) reported that they had attended lectures or seminars on ML. Roughly half (6 of 14) reported to have a similar background in security. To obtain a more objective measure we conducted a test about ML knowledge and asked participants to rate their familiarity with AML attacks (details in Appendix B). While we found that all participants were indeed knowledgeable in ML, we found that few attacks were well known to them.

Employment. Regarding the size of the companies, four participants worked in companies with less than ten employees, five in companies with less than 50 and the remaining six participants in companies with less than 200 employees. The companies' application areas were as diverse as healthcare, security, human resources, and others. Most participants were working in their current positions 6 years (STD 4.9). Their roles were diverse: Most (8 of 15) were in managing positions. Three were software or ML engineers, three more researchers. One of the participants stated to be both a researcher and a founder. One participant did not report his role.

Finally, we asked participants to report which goals were part of their companies' AI/ML checklist. Almost all participants (13 of 14) reported that performance mattered in their company. Half (7 of 14) stated that privacy was important. Slightly less than half (6 of 14) focused on explainability and security. Least participants (4 of 14) listed fairness as a goal in their products. To conclude, when interpreting these numbers, one should keep in mind that not all five goals apply equally to all application domains. Furthermore, our sample is too small to derive per area or per company insights, and we thus leave a detailed analysis for future work.

3.4 Data analysis

We adopted an inductive approach, where we followed recent work in social sciences and usable security that constructed theories based on qualitative data [45, 63]. To distill observable patterns in interview transcripts and drawings, we applied two rounds of open coding, e.g. we assigned one or several codes to sentences, words, or parts of the drawings. We then performed Strauss and Corbin's descriptive axial coding to group our data into categories and selective coding to relate these categories to our research questions [77]. Throughout

the coding process, we used analytic memos to keep track of thoughts about emerging themes. The final set of codes for interview transcripts and drawings is listed in Appendix E.

As a first step, the first two authors independently conducted open coding sentence by sentence and sketch by sketch. This allowed for the generation of new codes without predefined hypotheses. Afterwards, the resulting codes were discussed and the research team agreed on adding specific codes for text snippets relating to the confusion of standard security and AML. As a second step, two coders independently coded the data again. After all iterations of coding, conflicts were resolved and the codebook was adapted accordingly.

During axial coding, the obtained codes were grouped into categories. The first two authors independently came up with proposed categories which have then been discussed within an in-person meeting. While the grouping was undisputed for some of the categories presented in Appendix E (e.g. AML attacks, pipeline elements), for others the research team decided for (e.g. confusion, relevance) or against (e.g. type of ML model applied) the inclusion of a corresponding category only after detailed discussion. In addition, dedicated codes for the perception of participants (e.g. perceives AML as a feature, not a bug or security issue) were added to the codebook. Once the research team agreed on a final codebook, all transcripts and drawings were coded again using corresponding software.⁴ In doing so, we aimed for inferring contextual statements instead of singular entities.

The codes and categories served as a baseline for selective coding. Independently, the researchers came up with observations and proposals for specific mental models. Every proposal included a definition of the observation, related codes, exemplary quotes and drawings. The first two authors then met multiple times to discuss the observations and the corresponding relations of codes and categories. The resulting code tree contains 77 interview codes in 12 groups, 44 for drawings (in 5 groups), as depicted in Appendix E.

Over all interviews, the coders agreed on 989 codes while disagreeing on 136. Analogously, there were 275 codes on drawings in total, with 42 disagreements. We further calculated Cohen's kappa [23] to measure the level of agreement among the coders. For interview transcripts, we reached $\kappa = 0.71$; for the codes assigned to drawings $\kappa = 0.85$. These values indicate a good level of coding agreement since both values are greater than 0.61 [50]. Given the semi-technical nature of our codebook, we consider these values as substantial inter-coder agreement. Irrespective of this and in line with best practices in qualitative research, we believe that it is important to elaborate how and why disagreements in coding arose and disclose the insights gained from discussions about them. Each coder brought a unique perspective on the topic that contributed to a more complete picture. Due to the diverse background of our research team in AML, usable security and

⁴Available at <https://www.taguette.org/> and <https://www.maxqda.com/>.

economic geography, most conflicts arose regarding the relevance of technical and organizational elements of transcripts and drawings. These were resolved during conceptual and on-the-spot discussions within the research team.

3.5 Expectations of mental models

Given previous work on mental models and ML, we designed our study in a way that participants would first visualize their pipeline and later add corresponding attacks and defenses. For the pipeline, we expected that participants would name basic steps or components, such as data (collection), training, and testing. In general, we assumed participants’ descriptions would vary in technical detail. Regarding AML, one of our motivations to conduct this study was to learn which knowledge our participants had. As a recent phenomenon, AML might not be known at all in practice, although practitioners might be aware of attacks relevant to their specific application. In particular, we did not expect practitioners to depict attacks using a starting and target point, as done in Figure 1.

3.6 Ethical considerations

The ethical review board of our university reviewed and approved our study design. We limited the collection of personal data as much as possible and used ID’s for participants throughout the analysis. Since all participants were employed at existing companies and partially shared business-critical information, we aimed to avoid company-specific disclosures in this paper. Finally, we complied with both local privacy regulations and the general data protection regulation (GDPR).

4 Empirical results

In this section, we discuss our findings from the interviews and drawings. Given the unexplored nature of mental models of AML, we focus on two main facets, and discuss additional findings that require a more in depth analysis (in the sense of future work) at the end of this section.

The first of the two main facets is the (mingled) relationship between ML security (AML) and security unrelated to ML (non-AML security). We found that our participants, while not referring to AML and non-AML security interchangeably, still exhibited an often vague boundary between the two topics. The second facet concerns the view on ML as part of a larger workflow or product in industry, as opposed to the focus on an isolated model in academia. As a description of a high level workflow requires a high level perspective, we investigate whether it is equivalent to one, which we find not to be true. Afterwards, we then discuss potential facets requiring a more in depth investigation: the application setting, prior knowledge of the participant, and the perceived relevance of AML.

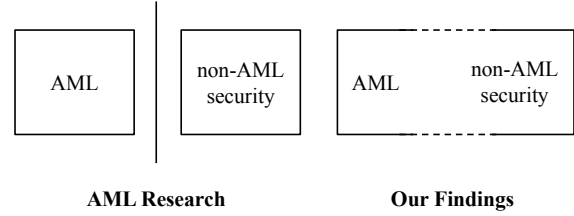


Figure 2: High-level intuition Section 4.1. While in research, non-AML security and AML are rather distinct, our participants do not always clearly distinguish the two fields.

4.1 Non-AML security and AML

Non-AML security deals with the protection against digital attacks in general. In our case, it encompasses topics like access control, cryptography, malicious code execution, etc. Non-AML security provides sound solutions by deploying defenses or implementing design choices. In AML, threats are much more connected with the functioning of ML. For many AML attacks, it is unclear which defenses work due to the ongoing arms-race. Although both topics are conceptually different, we found that our participants did not distinguish between security unrelated to ML and AML, as visualized in Figure 2. In our interviews, on the one hand, the boundary between non-AML security and AML often appeared blurry or unclear, with the corresponding concepts intertwined. On the other hand, there were crucial differences in the perception between non-AML security and AML threats. One difference is that whereas security defenses were often clearly stated as such, AML mitigations⁵ were often applied without security incentives. Finally, we find a tendency to not believe in AML threats. Many participants denied responsibility, doubted an attacker would benefit, or stated the attack does not exist in the wild. There was no such tendency in non-AML security.

4.1.1 Mingling AML and non-AML security

We first provide examples showing that non-AML security and AML were not distinguished by our participants. Afterwards, we investigate if non-AML security and AML are used interchangeably, by investigating the co-occurrence of codes.

Vagueness of the boundary between security and AML.

There are many examples for a vague boundary between non-AML security and AML. For example *P20* reasoned about evasion: “*this would require someone to exactly know how we deploy, right? and, where we deploy to, and which keys we use.*” At the beginning, the scenario seems unclear, but the reference to (cryptographic) keys or access tokens shows that the participant has moved to classical security. Analo-

⁵We are aware that AML is far from being solved, and communicated this to our participants if required. In this study, we define defenses as techniques which increase the difficulty for an attacker, like retraining or explainability.

gously, when *P18* reasoned about membership inference: “*but that could be only if you break in [...] if you login in to our computer and then do some data manipulation.*” Again, this participant was reasoning about failed access control as opposed to an AML attack via an API. Sometimes, ambiguity in naming confused our participants. For example, *P11* thought aloud: “*poisoning [...] the only way to install a backdoor into our models would be that we use python modules that are somewhat wicked or have a backdoor.*” In this case, the term ‘backdoor’ in our questionnaire caused a non-AML security mindset involving libraries in contrary to our original intention to query participants about neural network backdoors. The same reasoning can also be seen in *P11*’s drawing (compare Figure 3), where ‘backdoor’ points to python modules. Finally, *P12* stated: “*maybe the poisoning will be for the neural network. From our point of view you would have to get through the Google cloud infrastructure.*” From an AML perspective, the attack is carried out via data which is uploaded from the user. Yet, the infrastructure is perceived as an obstacle for the attack.

Correlations between non-AML security and AML attacks. In the previous paragraph, we showed that the boundaries between AML and non-AML security are blurred in our interviews. Another example is *P6* reasoning about IP loss: “*we are very much concerned I’d say the models themselves and the training data we have that is a concern if people steal that would be bad.*” In this case, it is left out how the attack is performed. Analogously, *P9* remarked: “*We could of course deploy our models on the Android phones but we don’t want anybody to steal our models.*” To investigate whether our participants are more concerned about some property or feature (data, IP, the model functionality) than about how it is stolen or harmed, we examined the co-occurrence of AML and non-AML security codes that refer to similar properties in our interviews. For example, the codes ‘model stealing’ and ‘code breach’ both describe a potential loss of the model (albeit the security version is broader). Both codes occur together six times, with ‘code breach’ being tagged one additional time. Furthermore, the code ‘model reverse engineering’, listed only two times, occurs both times with both ‘model stealing’ and ‘code breach’. However, not all cases are that clear. For example ‘membership inference’ and ‘data breach’ only occur together two times. The individual codes are more frequent, and were mentioned by three (‘membership inference’) and eleven (‘data breach’) participants. Analogously, attacks on availability (such as DDoS) in ML and non-AML security were only mentioned once together. Such availability attacks were brought up in an ML context twice, in non-AML security four times. Codes like ‘evasion’ and ‘poisoning’, in contrast, are not particularly related to any non-AML security concern. We conclude that AML and security are not interchangeable in our participants’ mental models to refer to attacks with a shared goal.

4.1.2 Differences between AML and non-AML security

In the previous subsection, we found that our participants did not distinguish non-AML security and AML. To show that this is not true in general, we now focus on the differences between the two topics. To this end, we start with the perception of defenses and then consider the overall perception of threats in AML and security. We conclude with a brief remark on the practical relevance of AML.

Defenses. Out of fifteen interviews, in thirteen some kind of defense or mitigation was mentioned; whereas all corresponding interviewees mentioned a non-AML security defense (encryption, passwords, sand-boxing, etc). An AML mitigation appeared in eight. In contrast to security defenses, however, AML defenses were often implemented as part of the pipeline, and not seen in relation to security or AML. As an example, *P9*, *P15*, and *P18* reported to have humans in the loop, however not for defensive purposes. *P10* and *P16* were aware that this makes an attack more difficult. For example, *P16* stated: “*maybe this poisoning of the data [...] is potentially more possible. There, we would have to manually check the data itself. We don’t [...] blindly trust feedback from the user.*” Analogous observations hold techniques like explainable models (3 participants apply, 1 on purpose) or retraining (2 apply, additional 2 as mitigation). For example, *P14* said: “*when we find high entropy in the confidences of the data [...] for those kind of specific ranges we send them back to the data sets to train a second version of the algorithm.*” In this case, retraining was used to improve the algorithm, not as a mitigation. We conclude that albeit no definite solution to vulnerability exists, many techniques that increase the difficulty for an attacker are implemented by our participants. At the same time, many practitioners are unaware which techniques potentially make an attack harder.

Perception of threats. There is also a huge difference in the perception of threats in non-AML security and AML. In security, threats were somewhat taken for granted. For example, *P9* was concerned about security of the server’s passwords “*because anybody can reverse-engineer or sniff it or something.*” Analogously, *P6* said to pay attention to “*the infrastructure so that means that the network the machines but also the application layer we need to look at libraries.*” On the other hand, almost a third of our participants (4 of 15) externalized responsibility for AML threats. For example, *P3* said their “*main vulnerability from that perspective would probably be more the client would be compromised.*” Analogously, *P1* remarked that ML security was a “*concern of the other teams.*” In both cases, the participants referred to another entity, and reasoned that they were not in charge to alleviate risks. Other reasons not to act include participants not having encountered an AML threat yet, and concluded AML was not relevant. More concretely, *P9* remarked: “*we also have a community feature where people can upload images. And there could be some issues where people could try*

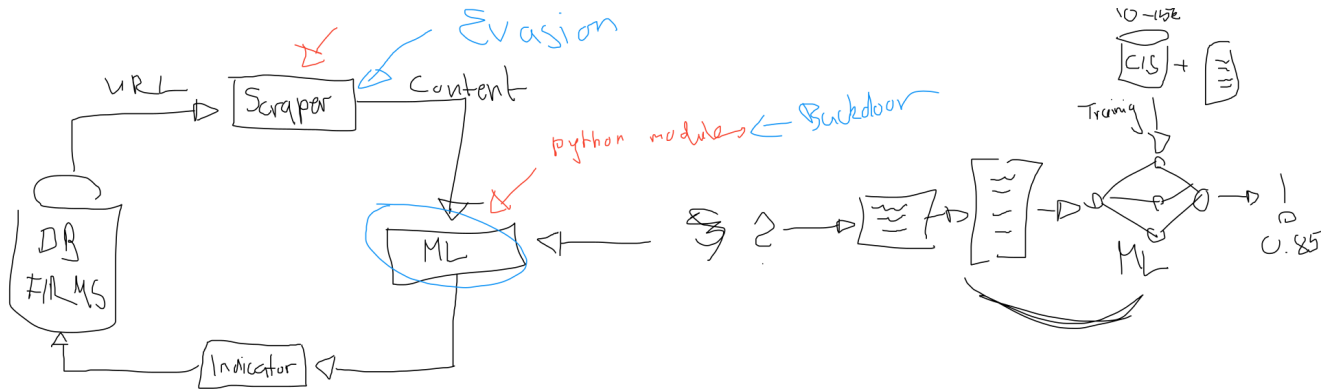


Figure 3: Drawing of P11. Red markings were added by the participant before, blue after being confronted with selected attacks.

to upload not safe or try to get around something. But we have not observed that much yet. So it's not really a concern, poisoning." Roughly half of the participants (7 of 15) reported to doubt the attackers' motivation or capabilities in the real world. For example, P1 said: "I have a hard time imagining right now in our use-cases what an attacker might gain from deploying such attacks." P20, who worked in the medical domain, stated: "I'm left thinking, like, why, what could you, achieve from that, by fooling our model. I'm not sure what the benefit is for whoever is trying to do that." Finally, many participants (9 of 15) believed that they have techniques in place which function as defenses. As an in-depth evaluation of which mitigations are effective in which setting is beyond the scope of this paper, we leave it for future work.

Practical relevance of AML. The fact that most participants did not consider AML threats relevant might be an expression of these threats being academic and not occurring in practice. Yet, our interviews showed that there are already variants of AML attacks in the wild. More concretely, P10 stated: "What we found is [...] common criminals doing semi-automated fraud using gaps in the AI or the processes, but they probably don't know what AML, like adversarial machine learning is and that they are doing that. So we have seen plenty of cases are intentional circumventions, we haven't quite seen like systematic scientific approaches to crime." Our participants lack of concern might then be an indicator that harmful AML attacks are (still) rare in practice.

4.1.3 Summary

We found that non-AML security and AML were mingled in our participants' mental models: the boundaries between the corresponding threats were often unclear. Yet, security and AML were not interchangeably used to refer to attacks with a shared goal. Furthermore, non-AML security threats were treated differently than AML threats: the latter were often considered less relevant. Whereas it remains an open question whether AML and non-AML security *should* be treated differently in practice, the fact that they are currently

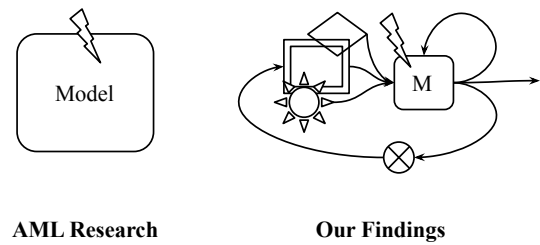


Figure 4: High-level intuition of Section 4.2. While AML research studies individual models, our participants often describe workflows with potentially several models, sometimes even the embedding system of the ML project.

poorly distinguished might due to low exposure to AML. At the same time, our interviews provided evidence for AML attacks in practice.

4.2 ML models and ML workflows

Many of our participants did not only refer to an ML model, but discussed a workflow or an entire system. This is in stark contrast to AML research, where models are often studied in isolation, possibly due to a lack of available data. This finding is visualized in Figure 4. In this subsection, we first discuss our participants view on ML models and the described systems. We then investigate whether such views are equivalent to a high level view on ML related projects, and conclude the section with a short discussion on some of our participants' struggles to assess threats at a high level.

4.2.1 Model versus system view

We first focus on the description of the ML model itself. Afterwards, we describe practitioners' views of ML models within larger systems and conclude the section with relating both findings to the technical level of abstraction.

ML model perspective. The general perception of the ML

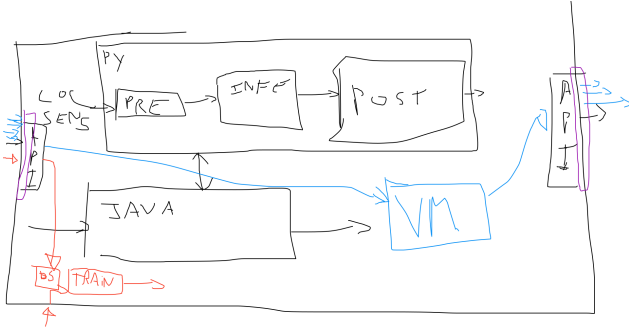


Figure 5: Drawing of *P16*. Colors were added after selected attack were presented to the participant. Red refers to evasion, purple to reverse engineering, blue to membership inference.

pipeline (Figure 1) seems to affect mainly the relevance of ML-models as such within the pipeline. More concretely, participants talked about models as pipeline components. Many (11 of 15) of our participants presented their projects in chronological order or with an implicit flow. Examples are visible in Figure 3 or Figure 6. Moreover, 6 out of 15 participants explained a pipeline not only as being composed by several steps, but remarked potentially several applications of ML within, or that several (different) pipelines exist. For example, *P14* reported that “the models are chained one after the other,” and *P7* stated that “we have both like unsupervised training and unsupervised training.” We conclude that often there is not a single model deployed, but data may be processed by several models, potentially in sequential order.

System perspective. Moreover, participants showed a strong focus on the surrounding or embedding of their ML-based project. In other words, not only the pipeline around the model was important, but also the surrounding infrastructure of the project. Out of 15 participants, 5 described their ML pipeline as a classifier as embedded into the larger project context (for example visible in Figure 3 or Figure 5). Related to this embedding, in two of the interviews, the topic of technical debt (or long-term maintenance) arose. In this context, *P6* stated: “how [...] we can also have to something that is maintainable in the long term.”

4.2.2 Technical abstraction level

The previous findings suggest a high level of technical abstraction in our interviews. While this is true on average, some (5 of 15) participants described their project minutely. For example *P12* described their application almost at the code level: “[...] we want to have for each node, that is basically the union of those two columns [...]”. However, whereas the same participants also described their project as a workflow, they did not talk about the embedding of the project. On the other hand, *P18* remarked on their “supervising” (e.g., high level) perspective, yet provided no context. We conclude that our

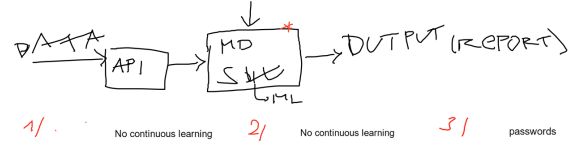


Figure 6: Drawing of *P18*. Red star indicates the most important component of the pipeline, not an attack.

sample does not allow conclusions about the level of technical abstraction and perspective on ML model, which is thus left for future work. We did find, however, that a high level perspective seemed to make threat assessment harder for at least some participants. Asked to specify a certain threat model, *P19* stated for example: “It’s like everywhere. Internal threats, external threats. Trying to mess with the communication, trying to mess if we model something.” In a similar manner, *P14* explained that an adversary could “try to put some pythons in non conforming ways to trigger networks.” Both descriptions are hard to interpret in technical terms, although both participants seemed aware of security threats in general. The same problem persists for defenses that our participants apply to encounter AML-specific security threats. *P18*, for example, first explained that “the countermeasures are all in the API.” After rechecking the documentation, the participant was able to provide further details on the applied defenses.

4.2.3 Summary

Our findings illustrate an important point which at the same time is very intuitive. Whereas most research papers focus on a single model when investigating ML security, in practice, models are trained and deployed in the context of other models or as components of larger workflows. At the same time, one pipeline may also contain several applications of ML. These views are not to be confused with the technical detail of a projects’ description. We furthermore find evidence that the right level of detail is crucial to providing useful information.

4.3 Additional facets of mental models

Eliciting mental models with only fifteen interviews seems ambitious, in particular in the context of a technique so versatile as ML. In the following, we thus discuss potential aspects of mental models that have to be studied in more depth in future work. These aspects include, but are not limited to the application setting, the effect of prior knowledge, and the perceived relevance of AML. We also found evidence of structural and functional components in our participant’s mental models. As the occurrence of these in AML mental models can be anticipated from prior work in mental models [89], we leave the corresponding discussion to Appendix F.

4.3.1 Application setting

Our sample is too small to make general statements about the application area. However, since almost a third (4 of 15) participants work in cybersecurity, we attempt to investigate whether working in security affects sensitivity to AML. Hence, we first divide the participants into security and non-security groups, starting with participants working in security-related fields. *P10*, who worked in a setting with cybersecurity reported: *“there is some standard AML attacks on ML you can use, but we design our system knowing that very well; on the other hand, we know that there is no perfect security, so, again defense is in monitoring and vigilance, but it’s not something that can be fully automated in our opinion.”* *P10* was in general very sensitive towards AML. *P4*, also from a cybersecurity setting, was less concerned about evasion: *“I can’t imagine yet how it can be applied for real life, for example [...] since we are pretty close on our development.”* Yet, *P4* also stated the need to gather more information about AML. Hence, also participants who worked in security-related areas had diverse mental models with respect to concrete attacks.

Participants from non-security fields have similarly diverse mental models. This diversity is also reflected in the drawings. *P11* (Figure 3) added some attacks (in red) before we provided explanations of evasion, backdooring and membership inference (added in blue). *P18* (Figure 6), on the other hand, did not add any threats in their drawing. Analogously, opinions also differ in the interviews; e.g., *P15* who worked in a non-security setting, was aware of security issues: *“one interesting thing of course is that the solution is in some ways constraint by adversarial security considerations so for example you cannot use natural language generation very much because of potential adversarial behavior.”* On the other hand, and confirming the drawing, *P18* reported that *“we do not really protect the machine learning part.”* Investigating the diversity of mental models induced by the application area in more depth is thus left for future work.

4.3.2 Prior knowledge

Another potential factor on a practitioner’s mental model is knowledge about or exposure to the topic at hand. However, we find no strong relation between education and capability or knowledge about AML in our sample. For example, one participant self-reported high knowledge in AML, but also stated: *“maybe the poisoning will be for the neural network.”* Here, a general attack, poisoning, is related to a specific model (neural networks). On the other end of the spectrum, *P9* did not self-report any knowledge about security or AML, but correctly remarked: *“Somebody could send us 100.000 images and collect all the results and try to build a model from that.”* We conclude that in our sample, self-reported prior knowledge is not related to AML knowledge. Yet, more work is needed to understand more in depth the complex relationship between exposure, education, and mental models of AML.

4.3.3 Perceived relevance of AML

Last but not least, we found little awareness of AML in our sample. As already discussed in section 4.1.2, this might be a consequence of little exposure to AML attacks in the wild. On the other hand, we found all levels of concern about AML in our sample. More concretely, a third of our the practitioners (5 of 15) did not mention AML at all before we explicitly asked. Another third reported that they were not very concerned about AML. For example, *P1* stated that evasion, or *“injecting malicious data to basically make the model [...] predict the wrong things”* was *“a concern that is not as high on my priority list.”* *P15*, analogously, said: *“mainly the machine learning pipeline this is the less critical security problem,”* reasoning that *“simply a performance would be unexpected.”* Yet, over a third (6 of 15) of the participants reported to feel insecure about AML when confronted with the topic. Of these six participants, two previously showed low priority on AML, and three did not mention AML at all. An example of insecurity is *P4*, who stated they needed *“some more research on it.”* Some participants, like *P19*, were concerned about specific attacks: *“I maybe need to learn more about this membership.”* In summary, some practitioners consider AML threats important, whereas some participants did not know AML well, and yet others did not consider it an important threat. From each of these three groups, there was at least one participant that felt not well informed. After the interviews (e.g., off the record) some participants stated that their awareness for AML had increased due to the interview. Many also inquired about defenses against specific threats, further confirming that they were indeed concerned about specific attacks.

5 Future work

Our findings expose the lack of knowledge about AML in practice, and thus show the need for additional research at the intersection of AML and cognitive science. In this section, we summarize these potential directions of future work. We first discuss theoretical research on mental models of AML and secondly more practical research that applies findings derived from mental models to AML.

5.1 A theory on mental models of AML

Our work is a first step to describe mental models of AML. For well-grounded mental models, more research is needed to investigate different aspects, as discussed in the previous section about the technical detail, application area and prior knowledge, for example. However, more research is also required concerning the development of mental models, and how a user based threat taxonomy (as opposed to a research based taxonomy) could look like.

Temporal involvement of mental models of AML. A better understanding about the development of individual mental

models could help to assess necessary steps to make practitioners take into account AML. In addition, research on how mental models are shared between various AI practitioners might help to implement adequate defenses within and across corporate workflows. Corresponding starting points can be found in cognitive science [61], where the convergence of mental models has been studied as a three-phase process of orientation, differentiation and integration [43].

Inherent threat taxonomies of mental models. Whereas academia has proposed clear threat models in ML security, it is unclear whether or to which degree these are also used or useful in practice. In this context, it could be interesting to consider existing taxonomies by Biggio et al. [10] and Barreno et al. [6]. These frameworks seem promising to investigate which specific structural elements practitioners consider relevant for specific attack vectors and how they perceive the causal evolution of these attacks. In line with recent work by Wang et al. [86], such user-centric attack taxonomies might help to understand practitioners’ reasoning on AML.

5.2 Applying mental models to AML

Secondly, but not less important, is the question how AML research can benefit from the study of mental models and which problems could be tackled in this context. Examples include the usability of AML tools and libraries, a more realistic threat modelling in AML research as well as a general assessment of AML attacks in the wild.

Utility and usability of AML tools and libraries. We found that practitioners’ mental models depend on available and provided information. Future research should therefore elaborate on the needed specificity of the available information. Furthermore, an evaluation of the available AML tools and libraries with regards to capabilities and needs of industrial practitioners might ease their usage across application domains. In line with recent work on fairness [52] and ethics [22], we consider this crucial for designing usable and accessible tools, corporate guidelines and regulations.

Practical threat modelling for AML research. As stated in Section 2, AML research has been criticized for the limited practical relevance of its threat models [28, 31]. Mental models could alleviate this issue in two ways. On the one hand, understanding which threats occur in which applications and how they are perceived helps to shift research towards designing practical and usable defenses. On the other hand, a deeper understanding of why non-AML security and AML are mingled allows us to adapt and improve current threat modelling. To this end, however, it is also important to know which threats need to be studied in the first place.

AML in the wild. Given the previous insight and evidence of semi-automated, ML-related fraud, a more detailed assessment of which attacks are conducted in the wild would be beneficial. Future work could investigate this with a focus on different groups of ML practitioners, including for example

ML engineers, auditors, and researchers, or dependant on the application. Furthermore, our work outlines that the model perspective usually taken in AML is of limited use in practice. More work is needed to study AML in the context of entire ML pipelines and end-to-end workflows.

6 Practical implications

Similar to Kumar et al. [47], we find that most of our participants lack an adequate and differentiated understanding to secure ML systems in production. Given that we found only reports of semi-automated fraud in our sample in Section 4.1.2, the absence of strong AML in practice might explain this lack of knowledge. Yet, as discussed in Section 4.3.3, 6 of 15 participants felt insecure about ML security. We thus now discuss the diverse implications of our study on how to tackle these insecurities and the overall lack of knowledge. We start with the question how to raise awareness for AML. Afterwards, discuss the implications of our findings for the embedding of AML in corporate workflows and finish with implications for regulatory frameworks of AML.

Raising awareness of and increasing confidence about AML. Although we did not ask about privacy specifically, the general data protection regulation was often mentioned by our participants. For example, *P6* stated: “*we are also subject to GDPR so we cannot just ignore the security aspects of the process.*” Like other participants (*P12*, *P18*), *P6* mentioned GDPR before we had asked about membership inference and thus privacy. Legislation might thus be a tool to increase awareness of AML. Independently, a third of our participants felt insecure about AML (Section 4.3.3). Given that several participants reported used software (*P9*, *P14*, for example “*TensorFlow*”), infrastructure (*P14*) or service provider (*P3*, *P12*, *P20*, for example “*Google*”), advertising tools to assess AML risks might be helpful for our participants. In particular as AML libraries⁶, but also overviews like the Adversarial ML Threat Matrix⁷ already exist. Our findings on the confusion between AML and non-AML security (Section 4.1.2) suggest these tools need to either enforce dedicated audits for both AML and non-AML security or combined countermeasures to address both areas jointly. Another solution to the feeling of insecurity, reported by our participants themselves (Section 4.3.3, *P19*: “*I maybe need to learn more about this membership*”), could be to provide materials for education.

Embedding AML into corporate workflows. Whereas academia generally studies AML with the perspective of an individual model, in practice, the entire ML pipeline and broader AI workflow need to be considered. As discussed in Section 4.2, in our interviews, for example *P6* and *P16* (see Figure 5) described the entire workflow of their AI application, whereas other participants focused on the ML pipelines

⁶For example the Adversarial Robustness Toolbox, CleverHans, Robust-Bench, or the SecML library, just to name a few.

⁷<https://github.com/mitre/advmthreatmatrix>

(for example *P18*, as visible in Figure 6). To successfully integrate AML into corporate workflows, however, more effort is needed. All actors working on an ML product need to be able to identify relevant and possible attacks and implementable defenses. Potential factors to consider here are for example different applications areas, as discussed in Section 4.3.1. Also the existing knowledge of the target audience should be considered, as the in Section 4.3.2 discussed variation of knowledge in our sample shows.

Creating appropriate regulatory and standardization frameworks for AML. Lastly, our study has implications for regulatory approaches that enable appropriate security assessments. The differences in application (Section 4.3.1) and prior knowledge (Section 4.3.2) we found imply that regulatory frameworks need to find a way to formally encompass these differences with regards to necessary security measures. The currently proposed ‘Legal Framework for AI’ by the European Commission, for example, differentiates certain types of ML applications of which some are prohibited or classified as high-risk and thus require a certain risk management. Furthermore, as discussed in Section 4.2, our results indicate that it is essential to communicate such frameworks at the right technical abstraction level to encompass both technical ML practitioners and non-technical stakeholders. Standardization efforts could incorporate this requirement by providing adequate information at multiple mental abstraction levels [18]. For example, recently proposed frameworks like the NIST Taxonomy and Terminology of AML⁸ explicitly lists references that might help practitioners develop more complex mental models. As mentioned above, a similar regulatory approach to privacy, the European general data protection regulation, had served as a scaffold for their privacy perception.

7 Limitations

We followed an inductive approach to investigate mental models through qualitative analysis. Hence, the data collected is self-reported and subjected to a coding process. We continued coding and refining codes until a good level of inter-coder agreement was reached. Nonetheless, all our findings are subject to interpretation and do not generalize beyond the sample, both of which is inherent to qualitative analyses. Finally, due to the COVID-19 pandemic, all interviews were conducted remotely and the interface limitations of the digital whiteboard might have impacted the participants’ sketches.

Given the qualitative approach and reached saturation, the small sample size of 15 is indeed acceptable [29, 89]. Due to the small sample size, however, several factors cannot be addressed in depth, as discussed in Section 4.3. Examples include, but are not limited to, the application setting and the perceived relevance. Ideally, future work provides a more in depth analysis of these topics in a larger quantitative study.

All participants were employed at European organizations with <200 employees. This is due to the fact that while several multinational companies stated great interest in our research, they denied participation after internal risk assessments. As mental models of ML systems are always embedded in organizational practices [91], we strongly encourage future research to assess our findings within larger samples including more variety, for example academics, small and large companies. Given that previous work found differences in general security behavior depending on gender [59], and cultural background [46], we also strongly encourage a more in depth analysis of these aspects.

Furthermore, AML itself is a subject of study of which the perception evolves continuously. With an increasing awareness for security within applied machine learning, the findings presented can only be valid temporarily. Machine learning is applied in a wide range of settings. Consequently, not all attacks are relevant within each application domain. For example, a healthcare setting is subjected to other threats than a cybersecurity setting. For the sake of studying abstract facets of mental models, we did not consider the application in the present work. Yet, we would like to point out the necessity to study this aspect of AML in general.

8 Conclusion

Based on our semi-structured interviews with industrial practitioners, we take a first step towards a theory of mental models of AML. We described two facets of practitioners’ mental models and sketched more facets as an anchor for in-depth investigation by future work. These include the technical abstraction level, application setting, prior education, and the perceived relevance of AML. We provided more details on the first facet, or the blurry relationship between AML and non-AML security. These two topics were often mingled, yet not used interchangeably by our participants. The second facet can be understood as a first step to refined threat models in AML research. As apposed to a single model, our participants instead described workflows and relationships between potentially several ML models in a larger system context.

A clear understanding of the elicited mental models allows to improve information for practitioners and adjustments of corporate workflows. More concretely, our results help to raise awareness for AML, thus making practitioners feel less insecure. We further suggest that both application area and prior knowledge are considered when embedding AML into corporate workflows. Finally, regulatory frameworks might reduce uncertainty about AML and increase the awareness for possible AML threats. However, a wide range of subsequent research towards an encompassing theory of mental models in AML is still required. Last but not least, we are convinced that the AML community will benefit from further practical assessment of attacks in practice, as our work already provides evidence of semi-automated fraud in the wild.

⁸<https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8269-draft.pdf>

Acknowledgements

The authors would like to thank Antoine Gautier, Michael Schilling, the anonymous reviewers and the shepherd for the insightful feedback. This work was supported by the German Federal Ministry of Education and Research (BMBF) through funding for the Center for IT-Security, Privacy and Accountability (CISPA) (FKZ: 16KIS0753) and by BMK, BMDW and the Province of Upper Austria within the COMET program managed by FFG in the COMET S3AI module.

References

- [1] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. Exploring user mental models of end-to-end encrypted communication tools. In *USENIX*, 2018.
- [2] Simon Anell, Lea Gröber, and Katharina Krombholz. End user and expert perceptions of threats and potential countermeasures. In *EuroS&P Workshops*, 2020.
- [3] Alejandro Barredo Arrieta, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, et al. Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. *Information Fusion*, 58, 2020.
- [4] Giuseppe Ateniese, Luigi V Mancini, Angelo Spognardi, Antonio Villani, Domenico Vitali, and Giovanni Felici. Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers. *International Journal of Security and Networks*, 10, 2015.
- [5] Anish Athalye, Nicholas Carlini, and David Wagner. Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. In *ICML*, 2018.
- [6] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D Joseph, and J Doug Tygar. Can machine learning be secure? In *CCS*, 2006.
- [7] Marcia J Bates. The design of browsing and berrypicking techniques for the online search interface. *Online review*, 1989.
- [8] Umang Bhatt, Alice Xiang, Shubham Sharma, Adrian Weller, Ankur Taly, Yunhan Jia, Joydeep Ghosh, Ruchir Puri, José M. F. Moura, and Peter Eckersley. Explainable machine learning in deployment. In *FAccT*, 2020.
- [9] Battista Biggio, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Srndic, Pavel Laskov, Giorgio Giacinto, and Fabio Roli. Evasion attacks against machine learning at test time. In *ECML PKDD*, 2013.
- [10] Battista Biggio, Giorgio Fumera, and Fabio Roli. Pattern recognition systems under attack: Design issues and research challenges. *International Journal of Pattern Recognition and AI*, 28, 2014.
- [11] Battista Biggio, Blaine Nelson, and Pavel Laskov. Support vector machines under adversarial label noise. In *ACML*, 2011.
- [12] Battista Biggio and Fabio Roli. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 2018.
- [13] Reuben Binns, Max Van Kleek, Michael Veale, Ulrik Lyngs, Jun Zhao, and Nigel Shadbolt. ‘it’s reducing a human being to a percentage’ perceptions of justice in algorithmic decisions. In *CHI*, 2018.
- [14] Franziska Boenisch, Verena Battis, Nicolas Buchmann, and Maija Poikela. “i never thought about securing my machine learning systems”: A study of security and privacy awareness of machine learning practitioners. In *Mensch und Computer 2021*. 2021.
- [15] Glenn A Bowen. Naturalistic inquiry and the saturation concept: a research note. *Qualitative research*, 8, 2008.
- [16] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. In *S&P*. Ieee, 2010.
- [17] Jakub Breier, Xiaolu Hou, Dirmanto Jap, Lei Ma, Shivam Bhasin, and Yang Liu. Practical fault attack on deep neural networks. In *CCS*, 2018.
- [18] David A Broniatowski et al. Psychological foundations of explainability and interpretability in artificial intelligence. *NIST: National Institute of Standards and Technology, US Department of Commerce*, 2021.
- [19] Nicholas Carlini and David Wagner. Adversarial examples are not easily detected: Bypassing ten detection methods. In *ACM Workshop on Artificial Intelligence and Security*, 2017.
- [20] Xinyun Chen, Chang Liu, Bo Li, Kimberly Lu, and Dawn Song. Targeted backdoor attacks on deep learning systems using data poisoning. *arXiv preprint arXiv:1712.05526*, 2017.
- [21] Nicholas Cheney, Martin Schrimpf, and Gabriel Kreiman. On the robustness of convolutional neural networks to internal architecture and weight perturbations. *arXiv preprint arXiv:1703.08245*, 2017.

- [22] Shruthi Sai Chivukula, Ziqing Li, Anne C Pivonka, Jingning Chen, and Colin M Gray. Surveying the landscape of ethics-focused design methods. *arXiv preprint arXiv:2102.08909*, 2021.
- [23] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and psychological measurement*, 20, 1960.
- [24] Nilesh Dalvi, Pedro Domingos, Mausam, Sumit Sanghai, and Deepak Verma. Adversarial classification. In *KDD*, 2004.
- [25] Hilko Donker, Palle Klante, and Peter Gorny. The design of auditory user interfaces for blind users. In *NordiCHI*, 2002.
- [26] James K Doyle and David N Ford. Mental models concepts for system dynamics research. *System dynamics review*, 14, 1998.
- [27] Gamaleldin F Elsayed, Ian Goodfellow, and Jascha Sohl-Dickstein. Adversarial reprogramming of neural networks. *arXiv preprint arXiv:1806.11146*, 2018.
- [28] Ivan Evtimov, Weidong Cui, Ece Kamar, Emre Kiciman, Tadayoshi Kohno, and Jerry Li. Security and machine learning in the real world. *arXiv preprint arXiv:2007.07205*, 2020.
- [29] Kevin Gallagher, Sameer Patil, and Nasir Memon. New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In *SOUPS*, 2017.
- [30] Dedre Gentner and Albert L Stevens. *Mental Models*. Erlbaum, 1983.
- [31] Justin Gilmer, Ryan P Adams, Ian Goodfellow, David Andersen, and George E Dahl. Motivating the rules of the game for adversarial example research. *arXiv preprint arXiv:1807.06732*, 2018.
- [32] Kathrin Grosse, Thomas A Trost, Marius Mosbach, Michael Backes, and Dietrich Klakow. On the security relevance of initial weights in deep neural networks. In *ICANN*. Springer, 2020.
- [33] Tom Hitron, Yoav Orlev, Iddo Wald, Ariel Shamir, Hadas Erel, and Oren Zuckerman. Can children understand machine learning concepts? the effect of uncovering black boxes. In *CHI*, 2019.
- [34] Kenneth Holstein, Jennifer Wortman Vaughan, Hal Daumé III, Miro Dudik, and Hanna Wallach. Improving fairness in machine learning systems: What do industry practitioners need? In *CHI*, 2019.
- [35] Yujie Ji, Xinyang Zhang, Shouling Ji, Xiapu Luo, and Ting Wang. Model-reuse attacks on deep learning systems. In *CCS*, 2018.
- [36] Yujie Ji, Xinyang Zhang, and Ting Wang. Backdoor attacks against learning systems. In *CNS*, 2017.
- [37] Jinyuan Jia, Ahmed Salem, Michael Backes, Yang Zhang, and Neil Zhenqiang Gong. Memguard: Defending against black-box membership inference attacks via adversarial examples. In *CCS*, 2019.
- [38] P. N. Johnson-Laird. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press, USA, 1986.
- [39] Mika Juuti, Sebastian Szyller, Samuel Marchal, and N Asokan. Prada: protecting against dnn model stealing attacks. In *EuroS&P*, 2019.
- [40] Kaggle. State of machine learning and data science. <https://storage.googleapis.com/kaggle-media/surveys/Kaggle's%20State%20of%20Machine%20Learning%20and%20Data%20Science%202021.pdf>, 2021.
- [41] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *SOUPS*, 2015.
- [42] Harmanpreet Kaur, Harsha Nori, Samuel Jenkins, Rich Caruana, Hanna Wallach, and Jennifer Wortman Vaughan. Interpreting interpretability: understanding data scientists' use of interpretability tools for machine learning. In *CHI*, 2020.
- [43] Deanna M Kennedy and Sara A McComb. Merging internal and external processes: Examining the mental model convergence process through team communication. *Theoretical Issues in Ergonomics Science*, 11, 2010.
- [44] Julie Khaslavsky. Integrating culture into interface design. In *CHI*, 1998.
- [45] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz. "if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In *S&P*, 2019.
- [46] Hennie A Kruger, L Drevin, S Flowerday, and Tjaart Steyn. An assessment of the role of cultural factors in information security awareness. In *ISSA*, 2011.
- [47] Ram Shankar Siva Kumar, Magnus Nyström, John Lambert, Andrew Marshall, Mario Goertzel, Andi Comissioneru, Matt Swann, and Sharon Xia. Adversarial machine learning-industry perspectives. In *S&P Workshops*, 2020.

- [48] Isaac Lage, Emily Chen, Jeffrey He, Menaka Narayanan, Been Kim, Samuel J Gershman, and Finale Doshi-Velez. Human evaluation of models built for interpretability. In *AAAI*, 2019.
- [49] Himabindu Lakkaraju, Stephen H Bach, and Jure Leskovec. Interpretable decision sets: A joint framework for description and prediction. In *KDD*, 2016.
- [50] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *biometrics*, 1977.
- [51] Markus Langer, Daniel Oster, Timo Speith, Holger Hermanns, Lena Kästner, Eva Schmidt, Andreas Sesting, and Kevin Baum. What do we want from explainable artificial intelligence (xai)?—a stakeholder perspective on xai and a conceptual model guiding interdisciplinary xai research. *Artificial Intelligence*, 296, 2021.
- [52] Michelle Seng Ah Lee and Jatinder Singh. The landscape and gaps in open source fairness toolkits. In *CHI*, 2021.
- [53] Hsiao-Ying Lin and Battista Biggio. Adversarial machine learning: Attacks from laboratories to the real world. *Computer*, 54, 2021.
- [54] Shengchao Liu, Dimitris Papailiopoulos, and Dimitris Achlioptas. Bad global minima exist and sgd can reach them. *ICML*, 2019.
- [55] Yingqi Liu, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, and Xiangyu Zhang. Trojaning attack on neural networks. In *NDSS*, 2018.
- [56] Yuntao Liu, Yang Xie, and Ankur Srivastava. Neural trojans. In *ICCD*, 2017.
- [57] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. User mental models of cryptocurrency systems - a grounded theory approach. In *SOUPS*, 2020.
- [58] Janosch Maier, Arne Padmos, Mortaza S Bargh, and Wolfgang Wörndl. Influence of mental models on the design of cyber security dashboards. In *VISIGRAPP (3: IVAPP)*, 2017.
- [59] Tanya McGill and Nik Thompson. Exploring potential gender differences in information security and privacy. *Information & Computer Security*, 2021.
- [60] Yisroel Mirsky, Ambra Demontis, Jaidip Kotak, Ram Shankar, Deng Gelei, Liu Yang, Xiangyu Zhang, Wenke Lee, Yuval Elovici, and Battista Biggio. The threat of offensive ai to organizations. *arXiv preprint arXiv:2106.15764*, 2021.
- [61] Susan Mohammed, Lori Ferzandi, and Katherine Hamilton. Metaphor no more: A 15-year review of the team mental model construct. *Journal of management*, 36, 2010.
- [62] Nadia Nahar, Shurui Zhou, Grace Lewis, and Christian Kästner. Collaboration challenges in building ml-enabled systems: Communication, documentation, engineering, and process. *Organization*, 1, 2022.
- [63] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. Why do developers get password storage wrong? a qualitative usability study. In *CCS*, 2017.
- [64] Milad Nasr, Reza Shokri, and Amir Houmansadr. Machine learning with membership privacy using adversarial regularization. In *CCS*, 2018.
- [65] Chalapathy Neti, Michael H Schneider, and Eric D Young. Maximally fault tolerant neural networks. *Transactions on Neural Networks*, 3, 1992.
- [66] An T Nguyen, Aditya Kharosekar, Saumyaa Krishnan, Siddhesh Krishnan, Elizabeth Tate, Byron C Wallace, and Matthew Lease. Believe it or not: Designing a human-ai partnership for mixed-initiative fact-checking. In *UIST*, 2018.
- [67] Seong Joon Oh, Max Augustin, Mario Fritz, and Bernt Schiele. Towards reverse-engineering black-box neural networks. In *ICLR*, 2018.
- [68] Tribhuvanesh Orekondy, Bernt Schiele, and Mario Fritz. Prediction poisoning: Towards defenses against model stealing attacks. In *ICLR*, 2020.
- [69] Nicolas Papernot. A marauder’s map of security and privacy in machine learning: An overview of current and future research directions for making machine learning secure and private. In *Workshop on Artificial Intelligence and Security*, 2018.
- [70] Elissa M Redmiles. " should i worry?" a cross-cultural examination of account security incident response. In *S&P*, 2019.
- [71] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why doesn’t jane protect her privacy? In *PETS*. Springer, 2014.
- [72] Benjamin IP Rubinstein, Blaine Nelson, Ling Huang, Anthony D Joseph, Shing-hon Lau, Satish Rao, Nina Taft, and J Doug Tygar. Antidote: understanding and defending against poisoning of anomaly detectors. In *IMC*, 2009.

- [73] Martina-Angela Sasse. How to tap users' mental models. In *Human Factors in Information Technology*, volume 2. 1991.
- [74] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *S&P*, 2017.
- [75] Ilia Shumailov, Yiren Zhao, Daniel Bates, Nicolas Papernot, Robert Mullins, and Ross Anderson. Sponge examples: Energy-latency attacks on neural networks. *arXiv preprint arXiv:2006.03463*, 2020.
- [76] Nancy Staggers and Anthony F. Norcio. Mental models: concepts for human-computer interaction research. *International Journal of Man-machine studies*, 38, 1993.
- [77] Anselm Strauss and Juliet Corbin. *Basics of qualitative research*. Sage publications, 1990.
- [78] David Stutz, Nandhini Chandramoorthy, Matthias Hein, and Bernt Schiele. Bit error robustness for energy-efficient dnn accelerators. In *MLSys*, 2021.
- [79] Harini Suresh, Steven R Gomez, Kevin K Nam, and Arvind Satyanarayan. Beyond expertise and roles: A framework to characterize the stakeholders of interpretable machine learning and their needs. *arXiv preprint arXiv:2101.09824*, 2021.
- [80] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian J. Goodfellow, and Rob Fergus. Intriguing properties of neural networks. In *ICLR*, 2014.
- [81] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "i don't own the data": End user perceptions of smart home device data practices and risks. In *SOUPS*, 2019.
- [82] Te Juin Lester Tan and Reza Shokri. Bypassing backdoor detection algorithms in deep learning. In *EuroS&P*, 2020.
- [83] Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. Stealing machine learning models via prediction apis. In *USENIX*, 2016.
- [84] Jennifer Villareale and Jichen Zhu. Understanding mental models of ai through player-ai interaction. *arXiv preprint arXiv:2103.16168*, 2021.
- [85] Melanie Volkamer and Karen Renaud. Mental models—general introduction and review of their application to human-centred security. In *Number Theory and Cryptography*. Springer, 2013.
- [86] Danding Wang, Qian Yang, Ashraf Abdul, and Brian Y Lim. Designing theory-driven user-centric explainable ai. In *CHI*, 2019.
- [87] Rick Wash and Emilee Rader. Influencing mental models of security: a research agenda. In *New Security Paradigms Workshop*, 2011.
- [88] Tsui-Wei Weng, Pu Zhao, Sijia Liu, Pin-Yu Chen, Xue Lin, and Luca Daniel. Towards certificated model robustness against weight perturbations. In *AAAI*, 2020.
- [89] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *SOUPS*, 2018.
- [90] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *SOUPS*, 2017.
- [91] Amy X Zhang, Michael Muller, and Dakuo Wang. How do data science workers collaborate? roles, workflows, and tools. *ACM on Human-Computer Interaction*, 4, 2020.

A Details on recruiting

We searched online databases like crunchbase⁹, Alhubs¹⁰, and lists with promising AI start-ups (for example the list by Forbes¹¹) to find potential participants.

B Participants' prior knowledge in (A)ML

To measure our participants' knowledge in ML, we constructed a questionnaire based on ML job interview questions¹²(Appendix D.3). Given that participants were not informed they had to take a test, we aimed to select a broad range of topics easy to query with multiple choice answers that were not too hard. The questionnaire had 8 questions, with the participants correctly answering on average 6.64 questions (STD 1.14). Guessing would yield an average of 2.66 correct questions. Thus, while we do not know how reliable our questionnaire estimates ML knowledge, we conclude that our participants are indeed knowledgeable in ML.

We also investigated the familiarity of our participants with AML attacks. To avoid priming, we asked participants to rate their familiarity after the interview. As sanity checks,

⁹<https://www.crunchbase.com/> for European companies operating in AI and having raised more than 1 million dollar funding

¹⁰<https://www.appliedai.de/hub/2020-ai-german-startup-landscape>

¹¹<https://www.forbes.com/sites/alanohnsman/2021/04/26/ai-50-americas-most-promising-artificial-intelligence-companies/?sh=653894c477cf>

¹²For example <https://www.springboard.com/blog/machine-learning-interview-questions/>

we added two rather unknown terms, adversarial initialization [32] and neural trojans [56] (similar to backdoors). The results are depicted in Figure 7. Only one participant reported to be familiar with one attack (evasion). In general, most participants reported to have heard of most common attacks (evasion, poisoning, membership inference, and model stealing). As expected for the sanity check, adversarial initialization and neural trojans were largely unknown.

C Interview protocol

Thank you so much for taking the time to give us your perspective on security in machine learning. This study consists in III parts. Part I aims at exploring your role in ML-projects. Part II addresses the underlying machine learning pipeline. In part III, we want to know how you perceive the security of machine learning. In part II and III, please visualize the topics (and relationships between them) that we ask you about. There are no rules, no wrong way to do it, and don't worry about spelling things perfectly. Nothing is off limits and you can use any feature of the digital whiteboard. After this last part, we will ask you about your knowledge about security of machine learning before this study.

Part I: Machine learning project

- Can you briefly describe what AI- or machine learning-based project you are currently involved in?
- Can you tell us a bit more about the goal of this project?
- Who else is involved in this project?
- What is your collaborators role in the project?

Part II: Machine learning pipeline

- What kind of pipeline do you currently apply within this machine learning based project?
- Which part of this pipeline is crucial for your business, or identical to your product?

Part III: Security within project and pipeline

- Is security something you regularly incorporate into your workflow?

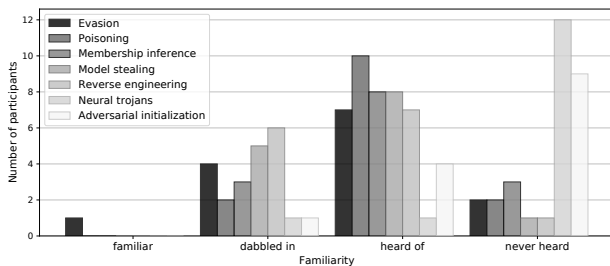


Figure 7: Self-reported familiarity of interviewed participants with different attacks on ML. Total of participants is 14, as one participant did not hand in questionnaire.

• Have you encountered any issues relating to security in the projects you described?

• Where in the pipeline did these security-related issues originate?

• Can you specify the cause of the security-related issues?

• Can you specify how these security-related issues evolve in your pipeline?

• Which goal pursues an adversary with a such a threat?

• What is the security violation of the threat?

• How specific is the depicted threat?

• Are you aware of any further possible security threats in the scope of your project or pipeline?

• Which countermeasures do you implement against any of the aforementioned threats?

Thank you so much for taking the time to give us your perspective on security in machine learning.

D Questionnaires

D.1 Demographics questionnaire

Thank you for participating in our research study about security in machine learning. Please take a couple of minutes to respond to the following questions.

- How old are you? _____
- What gender do you identify with?
 - ☐ male ☐ female ☐ _____
- What is your level of education? (please specify highest)
 - ☐ Highschool
 - ☐ Bachelor in _____
 - ☐ Master / Diploma in _____
 - ☐ Training / Apprenticeship in _____
 - ☐ PhD, area: _____
- What is your profession? _____
- What is your role in your team? _____
- How long have you been working in your current profession? _____
- What is the number of employees at your company/organization? _____
- What is the application domain of your product? _____
- Which of these goals are part of your organization's AI/ML-model checklist?
 - ☐ Explainability ☐ Fairness ☐ Privacy
 - ☐ Security ☐ Performance
- In which of these areas have you taken a lecture or intense course? Please add the title of the course if applicable.
 - ☐ Machine Learning _____
 - ☐ Security _____
 - ☐ Adversarial Machine Learning _____
- In which of these areas have you taken a seminar, or read up on? Please add the title of the seminar/book if applicable.
 - ☐ Machine Learning _____
 - ☐ Security _____

D.2 Attacks used in Interviews

Please read through the following selection of attack vectors and machine learning and explain whether you consider them relevant in your specific project. If yes, please add them to your sketch in a different color.

Evasion/ Adversarial Examples. This attack targets a model during deployment. The goal of the attacker is to fool the model: changing its output significantly by altering the input only slightly. An example is to change a picture containing a dog, present it to a cat-dog-classifier, and the model's output changes from dog to cat.

Poisoning. This attack targets the training or optimization phase of the model. The goal of the attacker is to either decrease accuracy significantly, or to install a backdoor. An example is a cat-dog classifier that always classifies images containing a smiley as cat.

Privacy/ Membership Inference. This attack targets a model at test-time. The attacker's goal is to identify individual samples from or even the whole training set. An example is to measure the confidence on an input, as some algorithms tend to be more confident on data they have seen during training. Also over-fitting eases to determine what a classifier was trained on.

D.3 ML quiz

Please answer the following questions about ML. For each question, please tick **at least** one box.

Question 1. Which loss is used to train DNN?

- ☐ 0/1-loss.
- ☐ Cross-entropy loss.
- ☐ Hinge-loss.

Question 2. What is the difference between classification and regression?

- ☐ The kind of labels we fit: reals vs discrete classes.
- ☐ Regression is the name of classification in psychology / medical science.
- ☐ Regression is for discrete labels, classification for real valued ones.

Question 3. What is the difference between L_1 and L_2 regularization?

- ☐ L_1 yields sparser solutions.
- ☐ L_2 yields sparser solutions.
- ☐ none - they differ only in few practical applications.

Question 4. In the bias-variance trade-off, what does high variance imply?

- ☐ The analyzed data shows high variance.
- ☐ The clf is overly complex and potentially overfits.
- ☐ The data is likely to be classified fair (e.g., low bias).

Question 5. Why is Naive Bayes naive?

- ☐ Due to historic reasons.

☐ Due to the assumption that all features are independent.

☐ Because the application is simple and straightforward.

Question 6. What is cross-validation?

- ☐ Training on one task and then transferring the model to another task.
- ☐ Splitting the dataset and training/evaluating on different subsets.
- ☐ A method to reduce overfitting or choosing hyper-parameters.

Question 7. What are kernels in machine learning?

- ☐ Essentially similarity functions.
- ☐ A part of SVM, potentially yielding non-linear SVM.
- ☐ A specific instance of a similarity function used in SVM.

Question 8. What is pruning?

- ☐ Deletion of for example weights in a model.
- ☐ Deletion of specific points of the data.
- ☐ A technique to get a smaller from a large model with similar performance.

To conclude the study, we will ask you to rate your background knowledge on attacks *before* this study according to the following four classes:

Familiar. You are familiar with this concept, and can write down the mathematical formulation.

Dabbled in. You could explain in a five minute talk what the concept is about.

Heard of. You have heard of the concept and you could put it into context if necessary.

Never heard. You did not know about this concept before this survey.

For each concept, please tick **one** box. *The original questionnaire was formatted as table. To ease readability, we list them as questions here.*

Evasion / adversarial examples.

☐ familiar ☐ dabbled in ☐ heard of ☐ never heard

Poisoning / backdooring

☐ familiar ☐ dabbled in ☐ heard of ☐ never heard

Model stealing

☐ familiar ☐ dabbled in ☐ heard of ☐ never heard

Model reverse engineering

☐ familiar ☐ dabbled in ☐ heard of ☐ never heard

Neural trojans

☐ familiar ☐ dabbled in ☐ heard of ☐ never heard

Adversarial initialization

☐ familiar ☐ dabbled in ☐ heard of ☐ never heard

E Final set of codes

The final set of codes for the interviews is depicted in Table 2, the codes for the drawings in Table 3.

Table 2: Final set of codes for the interviews.

A. AML attacks A.1 poisoning A.2 evasion A.3 model stealing A.4 reverse engineering A.5 membership inference A.6 availability B. AML defenses B.1 retraining B.2 interpretability B.3 basic models B.4 ensemble B.5 human in the loop B.6 regularization B.7 own implementation B.8 on purpose C. security threats C.1 data capturing C.2 access C.3 data breach C.4 code breach C.5 libraries C.6 denial of service C.7 SDK C.8 customer	D. security defenses D.1 sandboxing D.2 access control D.3 development policy D.4 server register D.5 security testing D.6 data anonymization D.7 input data format restrictions E. pipeline elements E.1 training E.2 design E.3 model E.4 data E.5 data labelling E.6 data collection E.7 data preprocessing E.8 feature extraction E.9 testing E.10 deployment E.11 API E.12 database F. pipeline properties F.1 iterative F.2 several within project	G. organization G.1 ML role in project G.2 security role in project G.3 other role on project G.4 legal constraints G.5 technical dept of ML H. customer H.1 requirements H.2 privacy relevant data I. cloud I.1 used for security I.2 used but potential security risk I.3 not used because of security I.4 neutral J. relevance J.1 mentioning AML J.2 security low priority J.3 AML low priority J.4 encountered security issue K. confusion K.1 across ML attacks K.2 security and AML K.3 vagueness of concepts K.4 what security means	L. perception L.1 security externalized L.2 AML feature not bug L.3 doubting attacker L.4 believing defense is effective L.5 has not encountered threat L.6 attacks too specific L.7 insecurity about AML L.8 unspecific attack L.9 holistic attacker specificity L.10 pipeline specific defense L.11 importance of data L.12 high level perspective L.13 coding perspective
--	--	--	--

F Structural and functional components

We found structural and functional components in our participants’ mental models. Structural components cover multiple, constituting entities that an individual perceives as relevant within a given application. In interaction with an ML system, functional components describe an individual’s perception of the relations between the structural elements. As intended, the structure of our interview and drawing task (Appendix C) allowed to investigate these properties on the level of the ML pipeline, of the attack vectors as well as of the defenses.

F.1 ML pipeline

All participants distinguish clearly separable elements within their ML workflow. The specific composition of these steps defines the structure of a certain ML pipeline. For two participants, this structure reflects the ML pipeline that we introduced in Figure 1. When asked to sketch the kind of pipeline applied, *P4* talked about “*data*”, “*training*”, “*testing*”, and “*visualization*”. We argue that these structural components serve as a scaffold for an individual’s mental model. Interestingly, the mental models of 12 out of 15 participants covered additional components that we did not expect prior to the study. The sketches of *P3*, *P7*, and *P11* (Figure 3), for example, contain explicit elements for data capturing, *P1*, *P9*, *P12*, as well as *P20* included dedicated elements representing a specific database to their drawing. Five participants also highlighted structural elements within the deployment environment during the interviews. *P14*, for example, specified on an API for deployment “*on several kinds of hardware architectures*”.

Analogously, *P1* described an API that “*can be used to allow the user to interact with the models*” Hence, these structural elements concerning data and deployment seem to be of importance for the corresponding mental models. However, the perception of industrial practitioners does not only focus on these structural components but also covers functional aspects. *P6* for instance stated that his ML pipeline “*forks into a number of different directions and there are also interactions between the different components*”. In the corresponding sketch, multiple arrows within and across specific ML models indicate this interconnection of single components. Other drawings include this functional perspective through straight lines connecting the structural components, arrows connecting some of the structural components in a subsequent manner (e.g. *P14*), and arrows connecting all structural components in a subsequent manner (*P18* in Figure 6).

F.1.1 Attack vectors

The identified structural and functional components seem to be similarly relevant for mental models on attack vectors. For any kind of ML-specific threat, participants were able to precisely locate where they situated the corresponding, structural starting point. These have been specifically named during the interview and sketched via labelled arrows (e.g. Figure 3, *P11*), additional annotations (*P11*, *P15*), highlighted parts of potentially vulnerable pipeline components (e.g. Figure 8, *P10*) or as entire steps within a given ML workflow that have been marked as vulnerable (*P9*, *P20*). Strikingly, we saw a wide overlap in the perception of potential focal starting points for attack vectors. Study participants consid-

Table 3: Final set of codes for the drawings.

A. pipeline elements	B. pipeline properties	C. named explicitly	D. attacks	E. drawing
A.1 training	B.1 iterative	C.1 hardware	D.1 no attacks	E.1 boxes
A.2 design	B.2 linear	C.2 software	D.2 poisoning	E.2 symbols
A.3 model	B.3 abstracted	C.3 human	D.3 evasion	E.3 inner/outer
A.4 data	B.4 several	C.4 privacy sanitization	D.4 membership inference	E.4 flow within pipeline
A.5 data labelling	B.5 explainable	C.5 output	D.5 libraries	E.5 workflow embedding
A.6 data collection	B.6 MLaaS	C.6 classification	D.6 data collection	E.6 attacks graphical
A.7 data preprocessing		C.7 server	D.7 input/output	E.7 attacks words
A.8 feature extraction			D.8 unspecific attack	E.8 attacks causal
A.9 testing			D.9 defenses	E.9 attacks pointwise
A.10 deployment			D.10 exit points	
A.11 deployment environment			D.11 input points	

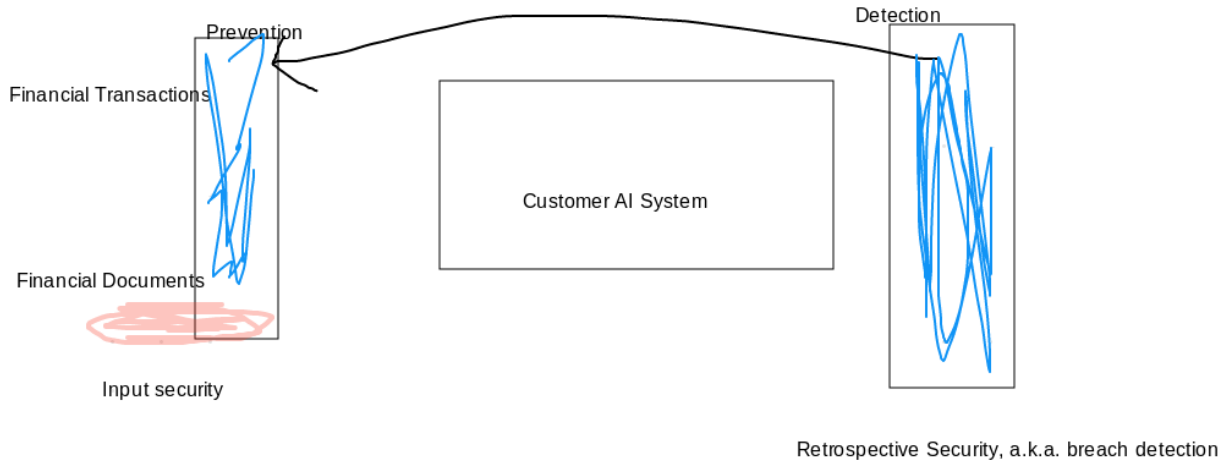


Figure 8: Drawing of *P10*. Important components of the workflow added in blue, possible starting points for attacks in red.

ered the model itself, the input of their ML pipeline, or the deployment environment to be particularly vulnerable. Figure 5 (*P16*) shows this for the latter. When confronted with poisoning and reverse engineering attacks, *P16* marked the input and output of his pipeline as possible starting points for threats (purple rectangles) and talked about how a competitor could “screw our labeled dataset” or a customer might “ask a lot of questions to the API”. However, the perception of attack vectors did also cover functional components. *P1*, for example, depicted the causal sequence of a “data injection attack” as three consecutive red arrows connecting different components of his ML pipeline. This is all the more relevant, as *P1* provided such a functional explanation and drawing for each of the attack vectors we presented to him. His mental models, hence, clearly seem to contain functional components. This is also the case for *P16*, who similarly provided explanations on the functional involvement of certain attacks within his workflow and even added corresponding functional elements to his sketch (blue and red arrows in Figure 5).

F.1.2 Defenses

Although we found participants’ defenses explanations and sketches to be rather sparse, structural and functional properties are also relevant for the corresponding mental models. As visible in the sketch of *P18*, defenses are often thought of as structurally bound to specific components of a workflow/pipeline (Figure 6, *P18*). Data (*P14*), training (*P6*) and the models themselves (*P10*) have been specifically named as focal points for implementing defenses. In the case of defenses implemented at the model component, *P14* stated to “regularize in a way that makes it less sensitive to an adversary”. Hence, these implemented defenses are cognitively attached to the classifier as a focal pipeline component. However, security mental models also contain functional properties. In the case of human-in-the-loop-defenses, for example, *P14* stated to send certain classifications “back to the data sets to train a second version of the algorithm” if the output confidence for certain data exhibited high entropy. This is depicted in the corresponding sketch by an arrow pointing from a rectangle with the caption “CPU” at the end of the pipeline to “raw data” (initial step of the pipeline). Similarly, *P7*, a participant working in video surveillance, explained the defense they had implemented to secure the transfer of

input data (from cameras and on-site computers) into their pipeline: “*This can only go out, never go in. [...] Nothing from the internet can connect to that server*”. Industrial practitioners, hence, perceive defenses as containing functional components to unfold their full effect.

F.1.3 Summary

We conclude that mental models in AML contain of structural components which are cognitively put into (internal) relation.

However, the specific unfolding of these internal conceptual representations seems to depend on the corresponding application and its underlying ML pipeline.