HAW
HAMBURG

MASTER THESIS
Jakob Otto

Possession: The Overlooked Element in Information Security

Faculty of Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE
WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Jakob Otto

Possession: The Overlooked Element in Information Security

Master thesis submitted for examination in Master´s degree
in the study course Master of Science Informatik
at the Department Computer Science
at the Faculty of Engineering and Computer Science
at University of Applied Science Hamburg

Supervisor: Prof. Dr. Klaus-Peter Kossakowski
Supervisor: Prof. Dr. Bettina Buth

Submitted on: 28. March 2025

Jakob Otto

Titel der Arbeit

Possession: Das übersehene Element in der Informationssicherheit

Stichworte

Informationssicherheit, CIA Triade, Parkerian Hexad, Besitz, Kontrolle

Zusammenfassung

In den letzten 20 Jahren basierte die Informationssicherheit nur auf einer Handvoll von Modellen. Insbesondere die traditionelle CIA-Triade - bestehend aus Vertraulichkeit, Integrität und Verfügbarkeit - ist nach wie vor ein beliebtes Instrument zur Beschreibung der Einsetzbarkeit von Security-Modellen. Seitdem hat sich die Landschaft der Informationssysteme jedoch rapide verändert, was zu neuen Risiken und damit zu neuen Anforderungen an Informationssicherheitsmodelle geführt hat. Donn B. Parker *et al.* schlug bereits in den 1990er Jahren ein alternatives Modell vor, das als Parkerian Hexad bekannt wurde und die CIA-Triade durch die Einführung zusätzlicher Dimensionen erweitert: Besitz, Authentizität und Nützlichkeit. Diese breitere Perspektive zielt darauf ab, moderne Sicherheitsherausforderungen zu beschreiben, die sich aus der Entwicklung von Bedrohungen ergeben, wie z.B. Schwachstellen in Informationssystemen und Bedenken hinsichtlich des Eigentums an Daten.

In dieser Arbeit untersuchen wir, wie die Hinzufügung von Besitz die derzeitige Landschaft der Sicherheitsmodelle verbessern könnte, und diskutieren die daraus resultierenden Modelle im Vergleich zu den traditionellen Ansätzen. Unsere Ergebnisse sollen zu einem umfassenderen Ansatz für Sicherheitsmodelle und deren Anwendbarkeit und Umsetzung in der sich ständig verändernden digitalen Landschaft beitragen.

Jakob Otto

Thesis title

Possession: The Overlooked Element in Information Security

Keywords

Information Security, CIA Triad, Parkerian Hexad, Possession, Control

Abstract

In the last 20 years, information security was based on only a handful of models. Especially the traditional CIA Triad – consisting of confidentiality, integrity, and availability – has always been (and still is) a popular model to describe the feasibility of security patterns. Since then, however, the landscape of information systems has changed rapidly, leading to new risks and thus new requirements for information security models. Donn B. Parker *et al.* proposed an alternative model in the 1990's, known as the Parkerian Hexad, which expands upon the CIA Triad by introducing additional dimensions: Possession, Authenticity, and Utility. This broader perspective aims to address modern security challenges that arise from evolving risks, such as information system vulnerabilities and data ownership concerns.

In this thesis, we explore how the addition of possession could improve upon the current landscape of security models, discussing the resulting models to the traditional approaches. Our findings aim to contribute to a more comprehensive approach to security models and their applicability in the ever-changing digital landscape.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

Information security is a cornerstone of modern society, ensuring confidentiality, integrity, and availability of data in an increasingly interconnected digital world. The CIA Triad, coined by these three basic requirements, has long been recognized as the foundation of information security. It offers a simple framework for understanding essential objectives of protecting information. The rapid evolution of technology and the rise of decentralized systems such as cloud storage and computing, artificial intelligence and the management of other digital assets continues to expose gaps in current information security models. Over time, extensions such as the Parkerian Hexad have been proposed with elements such as authenticity, utility, and possession, aiming to address more specialized aspects of security, aiming to address these new requirements.

While traditional security principles address ownership, control, and access by following the traditional CIA framework, they often overlook the importance of physical or digital possession, particularly in scenarios where possession plays a crucial role exceeding the traditional models. For example, the aspect of possession (*i.e.,* having the control and ownership of an asset) of encryption keys, hardware tokens, or other sensitive assets can directly impact the security of digital systems, yet it seems this aspect remains largely implicit or plain forgotten in current information security frameworks. We think that the inclusion of such principles can improve upon the existing landscape of information security models, and thus want to explore the inclusion of the principle of possession in the current state of security models.

In this thesis we investigate whether the omission of possession as a key requirement in information security frameworks represents a significant gap. We want to explore whether extension of existing models with a possible possession-aware approach could achieve a more holistic approach to information security. Additionally, we propose a novel possession-based security model that aims to apply the concept to security modeling.

1.1 Problem Statement

This thesis argues that possession is an often overlooked but critical concept in information security. Omitting the requirement may result in gaps in the existing security models in scenarios where possession could play a key role in addressing negative security outcomes, such as physical theft of devices or misuse of digital assets. By analyzing existing frameworks, this work demonstrates the relevance of possession and proposes its inclusion as a formal component of security models.

Essentially, we explore whether the addition of possession as an explicit security element in current information security models can result in a more holistic approach to information security. We consider completeness and effectiveness of current information security models, as well as the usability of extended models and aim to answer this question with a proposal of a new model.

1.2 Organization of this Thesis

Chapter 2 explores the foundations of information security, providing an overview of the CIA Triad and its extensions while discussing the importance of completeness in security models.
Chapter 3 introduces the concept of possession in information security, defining it and exploring its practical relevance in digital and physical contexts.
Chapter 4 evaluates the current landscape of information security models, analyzing their strengths, weaknesses, and gaps through case studies and practical examples.
Chapter 5 proposes a new possession-aware security framework and possession-aware extensions to existing security frameworks.
Chapter 6 addresses counterarguments and limitations, critically analyzing potential objections to the inclusion of possession in security models.
Chapter 7 concludes the thesis by summarizing key findings, discussing implications for information security, and proposing directions for future research.

2 Foundations of Information Security

In today's increasingly distributed and interconnected world, protecting assets from unauthorized disclosure and other threats has become one of the most critical aspects of information system governance. This process of securing, safeguarding, and protecting computer systems and their managed assets, as well as responding to attacks and incidents is called information security. The goal of information security is to ensure that all information remains secured, accurate, and accessible for authorized users, while protecting it from unauthorized access, modification, and – in the worst case – destruction or loss.

At its core, information security practices involve the identification and assessment of risks and threats, the implementation of appropriate countermeasures, and the continuous monitoring of systems to achieve its goal. The discipline is required across industries, affecting organizations (*e.g.,* businesses, governments, healthcare systems, education, *etc.*) and, especially in current times, individuals.

In this section we want to motivate the importance of information security and show why it is such an important cornerstone in the current landscape of information systems. Starting with the background on the topic of information security, we will provide an overview of the roots and foundations of the topic. Afterwards, we will go over the key objectives, enforced by information security.

2.1 Historical Background

The need to protect critical information and to keep assets secured has existed for as long as civilization itself. Beginning in ancient times, societies have come up with ways to safeguard sensitive information, whether it was military strategies, trade secrets, or political communications. Early examples for this were ciphers used by the ancient Egyptians and Greeks, such as the Spartan scytale, a device that enabled secret communication

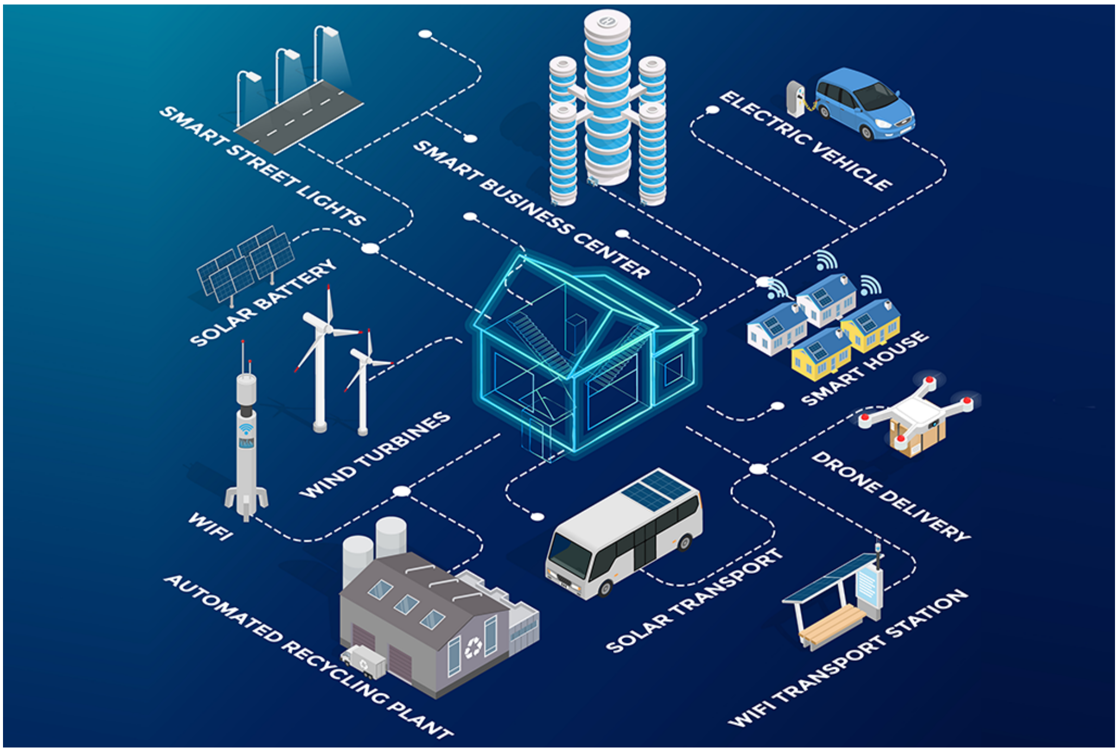


Figure 2.1: Visualization of a smart city layout, exemplary for the interconnected nature of current information systems.

Source: https://innovationatwork.ieee.org/what-makes-a-city-smart/

through transposition ciphers [12]. Perhaps the best known example in computer science was used by the Roman Empire: the Caesar cipher [21], which has been applied to secure military messages and is still used, for example, in ROT13 ciphers [15].

With increasing dependencies of governments and organizations, the need for more sophisticated means of securing information has grown as well. During the Renaissance, advances in cryptography, most notably with the work of Blaise de Vigenère, whose polyalphabetic cipher [22] remained difficult to break for centuries. During World War II, encryption and code-breaking became central to warfare, with machines like the German Enigma [13] and the Allied Colossus shaping the outcome of battles.

The transition to the digital age in the 1960's and 70's marked a pivotal turning point, by then, the typical approach to information security was managing physical access to secured assets. Before that time, computers were still floor-filling machines that could only be operated by a limited number of trained specialists with direct access to the systems terminal. Securing assets could thus be achieved by placing security personnel at the entrance.

As computers became more prevalent in military and government operations though, this approach had to shift to protecting data digitally instead. This introduced new challenges, as information was no longer stored in locked safes or hidden messages but rather on interconnected systems which were vulnerable to remote access and manipulation.

The U.S. Department of Defense recognized this risks of unauthorized access and cyber espionage and began commissioning research into the field of computer and information security. This effort led to the Anderson Report in 1972 [3], which formally introduced computer security as a discipline and set the stage for modern cybersecurity principles. By the late 1970s, the fundamental ideas of information security – confidentiality, integrity, and availability (CIA) – began taking shape. This shift from securing physical information to safeguarding digital assets laid the foundation for the modern cybersecurity landscape.

2.2 Distinguishing Security, information security, and Cybersecurity

The terms security, information security, and cybersecurity are closely related, but they differ in scope and application. Understanding these distinctions is crucial to be able to implement effective security measures for physical and digital assets.

Security Security is a broad concept that refers to protecting assets – whether physical, digital, or human – from harm, theft, or unauthorized access. It includes physical security (*e.g.,* locks, guards, surveillance) and broader risk management strategies.

Information Security Information security specifically concerns the protection of information, whether digital or physical, from unauthorized access, disclosure, alteration, or destruction. It is often governed by principles like the CIA Triad (confidentiality, integrity, and availability). InfoSec applies to both digital and non-digital formats, including paper records and verbal communication.

Cybersecurity Cybersecurity is a subset of information security that focuses on protecting digital systems, networks, and data from cyber threats such as hacking,

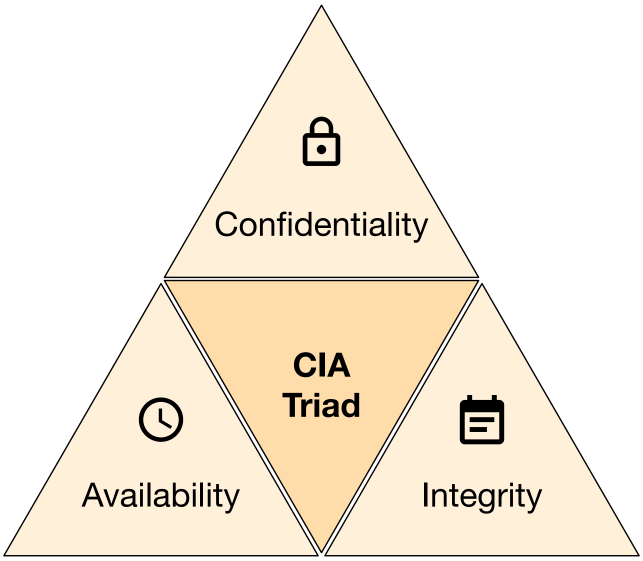


Figure 2.2: Visualization of the CIA Triad.

malware, and cyber attacks. It deals specifically with securing internet-connected systems, including hardware, software, and sensitive data.

Thus, the three terms are related but have different focuses. While security can be regarded as the general protection of assets, information security aims to protect all forms of digital or physical information. Cybersecurity narrows this focus again to the protection of digital systems and data from cyber threats in particular.

2.3 CIA Triad

The CIA Triad [27] is the most widely used and regarded information security model of them all, most of the current security models reach back to the ideas of the triad. It is derived directly from the ideas in the early 1970's, where the US-American military researched and developed approaches to secure classified information. The model proposes the three objectives (*i*) confidentiality, (*ii*) integrity, and (*iii*) availability, which have been visualized in Figure 2.2. We want to briefly describe the concepts and explain them in more detail:

Confidentiality The act of ensuring that sensitive information is only accessible to those with authorized access. The concept places a strong focus on preventing unauthorized or unintended disclosure of data, whether intentional or unintentional. Access control and encryption are good examples that implement the concept, ensuring confidentiality.

Integrity The act of ensuring that data remains accurate, reliable, and unaltered during during any part of its lifetime (*i.e.,* storage, processing, or transmission). This objective is essential for maintaining trust in information systems while ensuring that the managed data can be relied upon. Often integrity is achieved by implementing checksums and hash functions, allowing data verification, while digital signatures ensure the authenticity and of the data.

Availability The act of ensuring that information and systems are accessible, whenever they are needed. This objective is critical for organizations that rely on real-time data access, *e.g.,* financial institutions or emergency services, where downtime results in loss of life or money. Redundancy of the systems and a reliable disaster recovery plan can ensure that downtime can be minimized, while the system can be recovered in case it is actually lost.

Addressing all three CIA objectives is considered the gold-standard in information security. Most current models base their ideas on these three objectives, making the CIA triad the most widely accepted and applied model currently.

2.4 Parkerian Hexad

The Parkerian Hexad was an extension of the now infamous CIA triad proposed by Donn B. Parker in 1998 [25] that was later named after him. It was the result of him criticizing the traditional approach to information security for being limited to the CIA-triad that he claimed to be “dangerously incorrect”. Parker argued that the technical security controls have significantly improved over the years, however the underlying model (CIA) that is applied in almost all models did not. According to him, the then current landscape of information security essentially outgrew the old ideas from the 1960s’ and 1970s’, but never evolved past their ideas.

The Parkerian Hexad is a model that extends on the ideas and concepts of the traditional CIA model. While the already known goals of confidentiality, integrity, and availability are also part of this model, he extended them with (*i*) possession, (*ii*) Authenticity, and (*iii*) Utility. He defined the three objectives as follows:

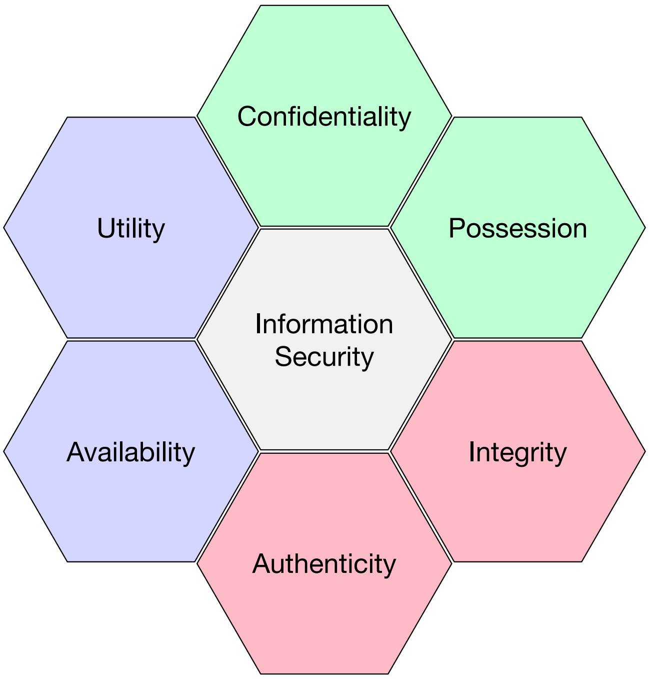


Figure 2.3: Visualization of the Parkerian Hexad. Correlation between objectives is visualized by using the same colors for related objectives.

Possession The holding, control, and ability to use information.

Authenticity The validity, conformance, and genuineness of information.

Utility The usefulness of information for a specific purpose.

Figure 2.3 visualizes the proposed objectives of the model. Special consideration must be given to the coloring of the objectives that indicate the strong relation between them. For example, confidentiality and possession can often be addressed similarly and pose overlaps in their application. While Utility and availability are – by design – both regarding the interruptions by unusable assets. Authenticity and integrity are both objectives that are closely coupled again, by the means of implementation through cryptography and digital signing mechanisms.

The many overlaps between both models are only one side, especially the Hexad expands on the ideas and creates valuable distinctions of the previously cumulated objectives. Confidentiality ensures that only authorized users can access data, possession refines this idea and refers to control over the data, meaning a breach could occur even if confidentiality remains intact. Both Utility and integrity address and ensure access to data when needed; utility adds to this idea by ensuring that the data is useful and meaningful – securing against uselessness of data if corrupted or destroyed. Lastly, Authenticity and integrity focus on ensuring access; authenticity ensures that the data is genuine and unaltered. The Parkerian Hexad thus provides a more comprehensive framework for modern cybersecurity concerns.

3 Possession in the Context of Information Security

In this chapter, we want to introduce the concept of possession in the context of information security. Beginning with a general definition of the term, we follow with a more scoped approach to possession in the field of information security and review existing applications. We provide some real-world examples, for which possession was taken explicitly into consideration, or it would have aided in preventing adverse outcomes. Essentially, we want to motivate what the concept of possession is all about and why it matters – especially in information security.

3.1 Possession: A Definition

According to the Merriam-Webster dictionary[1], the term possession is defined as "the act of having or taking into control". The Cambridge dictionary[2] defines the term similarly as "the fact that you have or own something". Possession is thus concerned with the physical ownership of an object, having the ability and right to control what happens with-, and who is allowed to have it or make use of it.

In information security, the concept refers to having control over an asset, such as data, cryptographic keys, or physical devices. It is thus applied more specifically to the requirements of information security, where ownership and possession of something is not always physical or tangible. Possession of digital assets can be manifested in different ways, the key idea is: Digitally stored assets are not tangible as such, but giving away a digital representation of said assets makes them available in undesired ways. Essentially, passing a digital representation (*i.e.,* by copying) passes ownership and thus, possession

[1] https://www.merriam-webster.com/dictionary/possession

[2] https://dictionary.cambridge.org/us/dictionary/english/possession

on to another participant, making it difficult to maintain other goals such as confidentiality.

In the 1990's, Parker *et al.* [25] proposed a generalized definition, in which they defined possession as "the holding, control, and ability to use information". With this, possessing an asset is not only a question of holding or having access to it, but also the ability to read, interpret, and use it. It expands the basic concept to also consider usability of assets, which – for example, when encryption is applied – is not guaranteed without holding control of the asset itself (or, by extension, the encryption keys). Possession thus enables organizations to manage assets in a fine granular way, which is relevant, because it allows to keep information secure by design and thus, out of control of unauthorized individuals.

Taking a step back and considering the history of information security shows that the concept has been leveraged in the field of information security *implicitly* for a long time. Confidentiality has mostly been implemented with an implicit consideration for possession. Ownership of credentials, ID cards, passwords, or other additional authentication factors has been considered a prerequisite for the process of identification and authentication of human users. This dates back to times where securing confidential assets relied on the physical exclusion of personnel, where possession of specific uniforms or badges were used to identify personnel that tried gaining access to confidential assets. The problem is that this has always only been an implicit byproduct of the concept, never an explicit consideration.

3.2 Why Possession Matters

Especially in recent years, the evolution of digital systems being increasingly interconnected and distributed has surpassed the previous requirements. Assets are typically not stored on disconnected devices with a single access terminal, but rather on cloud-servers that can be accessed from anywhere in the world. This leads to the requirement of more appropriate controls that explicitly considers possession of assets, not just implicitly as a byproduct of another concept.

Authentication, access control, usability, *etc.*are concerned with the idea of *who* has possession of the asset. Taking the concept out of this often implicit form, opens possibilities for how data is managed and stored: Applying possession through physical access restriction, *i.e.,* by storing information on a storage device that is secured physically simplifies access control within the information system, as well as limiting the overhead of digitally securing the network. Applying possession using cryptography, where information is rendered useless without the possession of the decryption key, simplifies other parts of information security since unauthorized data access is a non-issue, considering the used cryptography cannot be broken.

Considering the concept of possession explicitly, may allow significant simplification of other goals from information security (*e.g.,* authentication or confidentiality), which would lead to overall more manageable information systems. Leveraging encryption – and thus possession – of the encryption keys could support confidentiality and integrity of assets, since only users with possession of these can access the encrypted assets, which could allow to vastly simplify the data and access management aspects of information governance. Additionally, it could lead to a reduction of risks of unauthorized access by managing possession of physical assets explicitly. By ensuring that physical assets, such as memory sticks, HDDs, or phones are only in possession of authorized users, reduces possible attack vectors to contained confidential data. Managing this explicitly, could help ensuring a more holistic approach to information security.

3.3 Examples of Missing Consideration of Possession

To motivate the explicit consideration of possession, we want to provide some examples of recent developments in the field of information security. Some of which have considered possession explicitly, while others document recent incidents that could possibly have been mitigated if possession had been explicitly considered.

3.3.1 Datenschutz-Grundverordnung (DSGVO)

The Datenschutz-Grundverordnung (DSGVO) is the German implementation of the General Data Protection Regulation (GDPR). It came into effect across the European Union on May 25, 2018, establishing strict rules for the collection, processing, and storage of personal data to protect individuals' privacy rights. Key principles of the law include fairness and transparency in data processing, as well as data minimization to ensure that only necessary data is collected. Additionally, it requires companies to protect

Figure 3.1: Visualization of the Elektronische Patientenakte (ePA), which is intended to collect all medical data from patients in the german healthcare system.

Source: https://sozialministerium.baden-wuerttemberg.de/de/startseite/gesundheit-pflege/epa

any collected personal data from unauthorized access with technical and organizational measures.

The law tries to safeguard any individuals' personal data, stating a first shot at the ownership of this information. According to the law, personal information is taken as possession of the individual and may as such not be removed from the ownership of the individual. This is technically considered theft and is fined with severe fines up to 20 million Euro or 4% of the annual global turnover. It gives the end-users a tool with which they can enforce the ownership of their data.

3.3.2 Elektronische Patientenakte (ePA)

The elektronische Patientenakte (ePA)[3] is the electronic patient record system proposed in Germany, designed to store everyone's medical information digitally. It is currently being introduced as part of Germany's digital healthcare transformation, where the ePA

[3] https://www.bundesgesundheitsministerium.de/themen/digitalisierung/elektronische-patientenakte/epa-fuer-alle.html

enables patients and healthcare providers to access important health data securely, aiming to improve efficiency and quality of services. Goals of the ePA are to centralize health data storage, secure the data through means of encryption and strong authentication measures, while keeping the control of the data with the patients – every participant can control who has access to their data and which documents they share with whom.

The whole system is built around and with the DSGVO in mind, since the processing of data in Germany must follow this law. The special focus on keeping the control of the data with the individuals is essential – all data is encrypted before it is stored on the systems servers. Each user has to have authentication in the form of possession of the encryption keys for any piece of information they want to access or manage. Users identify themselves using their patient-ID, while doctors, nurses, and other healthcare workers have to apply for a digital ID that is issued by the GEMATIK itself. These precautions are intended to ensure the safety of any contained information, while making the system as user-friendly as possible.

The data contained in the ePA is especially confidential, which, if leaked or disclosed to unauthorized parties, would result in tremendous damage for individuals. Hackers have already shown that the system is vulnerable to a variety of attacks[4], such as impersonation or enumeration. Both attacks have been successfully carried out and gave the attackers access to the otherwise secured data of patients. This shows that even if possession is explicitly considered during the planning and implementation of a system, it has to be continuously monitored after it is set in place. For the ePA this has not been done, which resulted in a postponement of the initial plans, moving the time point for the introduction for all German citizens to some point in the future.

3.3.3 Volkswagen Position Leak

A significant data breach involving Volkswagen has been uncovered by security researchers in December 2024. The incident exposed sensitive information of approximately 800.000 electric vehicle owners across various brands under the Volkswagen Group – including Volkswagen, Audi, Seat, and Škoda. The compromised data included precise GPS location details, personal contact information such as names, email addresses, and phone numbers, as well as vehicle-specific data like battery status and odometer readings. This information was unknowingly left unprotected on an Amazon cloud server

[4] https://www.ccc.de/de/updates/2024/ende-der-epa-experimente

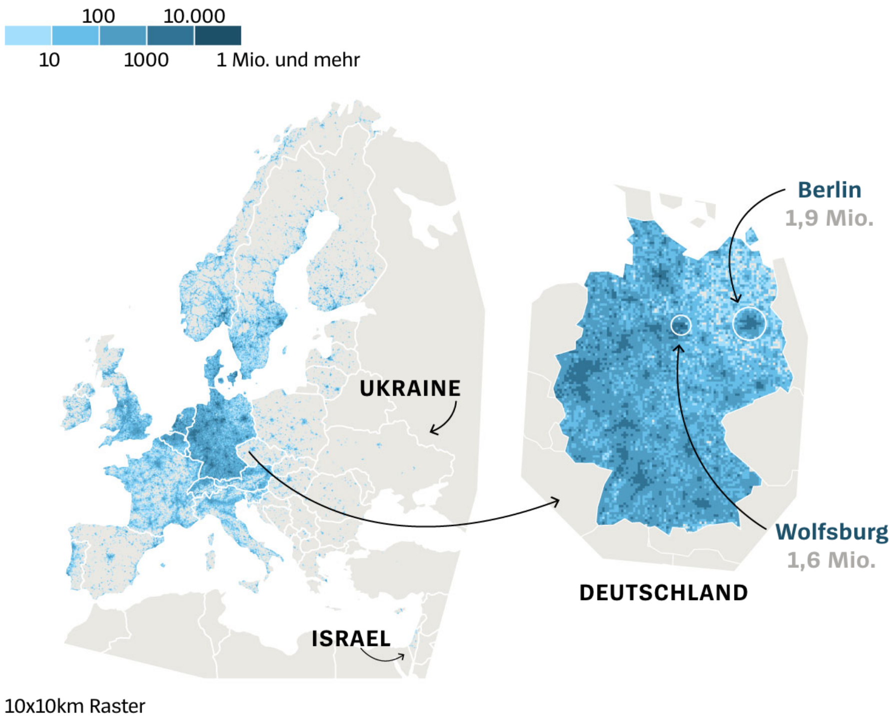


Figure 3.2: Visualization of leaked position data that has been collected without explicit consent from the users.

Source: https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027

maintained by Volkswagen's software company "Cariad" which was accessible freely on the internet due to a misconfiguration. The data exposure has been active for several months before being discovered by a whistleblower that reported the issue to the German magazine "Der Spiegel" and the "Chaos Computer Club (CCC)"[5], a German hacker collective.

The data leak itself was highly problematic and could have been avoided by a simple review of the server configurations by Volkswagen. The real issue with the incident however, was that the collected position data was collected without explicit consent from the owners. Position data collection and the correlation of Volkswagen's cars with the personal information of the owners was disclosed in contracts that had to be signed during the order process. The accuracy with which the data was collected was not disclosed and most likely another misconfiguration on Volkswagen's side – the collected position data should have been collected with a resolution of a few kilometers, but was

[5] https://www.ccc.de/de/updates/2024/wir-wissen-wo-dein-auto-steht

collected with a resolution of a few centimeters. Due to the high resolution and long time-span during which the data was collected, the data could be used to create motion profiles that were used to de-anonymize individuals and their families in some cases. Figure 3.2 shows the map containing all leaked data points. Each of the points from the map shows a single position of a Volkswagen vehicle that was collected over the timespan of the 5 years.

The problem in this case was twofold: (*i*) the misconfiguration lead to the breach and (*ii*) the data was collected without proper and explicit possession management. Misconfigurations of infrastructure can happen and will happen again in the future. With proper possession controls, the consequences could have been mitigated – especially through encryption or obfuscation, the data wouldn't have been usable for the creation of motion profiles.

4 The Current Landscape of Information Security

Many information security frameworks with varying goals have been proposed, since the beginning of research in the field in the 1970's and 80's. Especially in recent years the number of new models and concepts being proposed has soared, while many of the foundational models are still widely adopted and applied, as they still form the standard of information security.

In this chapter we want to provide an overview of the current landscape of information security models and risk modelling frameworks. We discuss their advantages and limitations, as well as categorize them according to their applied objectives from the Parkerian Hexad to allow a comparison.

4.1 Existing Critiques of Current Models

Despite the utility of existing information security models, they are not without limitations. Many models—such as the CIA Triad, Zero Trust, and Access Control Frameworks—are foundational, but they often fail to fully address the complexities of today's dynamic threat landscape. Key critiques of the current landscape of security models are:

Overemphasis on the CIA Triad The CIA Triad is a cornerstone of information security. Critics argue though that the CIA Triad doesn't fully address or plain forgets modern security challenges, such as privacy, accountability, or resilience. Moreover, it assumes a static environment, while threats are increasingly dynamic and sophisticated, as are the systems that are attacked. Especially emerging technologies like the IoT and cloud computing introduce new challenges (*e.g.,* shared responsibility models and resource constraints) that are not adequately covered by the model.

Lack of Focus on Usability Many models prioritize security over usability, leading to user resistance and operational inefficiencies. Complex or cumbersome security measures often result in users circumventing protocols, *e.g.,* by reusing passwords or disabling two-factor authentication, while strict policies can slow down workflows and create bottlenecks in system access and data sharing.

Failure to Address Human Factors Existing models often overlook the role of human behavior in security. Social engineering attacks, for example are a problem that models often do not adequately address. Phishing, impersonation, or other social engineering techniques are leading reasons for system breaches – even in well secured environments. Insider threats on the other hand, where malicious or negligent persons pose significant risks on the inside of the organization are another problem that many models are not designed to detect or mitigate effectively.

Inadequate Support for Emerging Technologies Traditional models were designed for centralized systems but struggle to accommodate increasingly decentralized systems. They often fail to address shared responsibility, data ownership, and isolation challenges in cloud computing. Limited processing power and storage are often not considered, posing problems for implementations in the areas of IoT or edge computing.

Reactive rather than Proactive Many models rely on reactive measures that merely respond to attacks, rather than to proactively prevent them. Traditional intrusion detection systems are based on known attack signatures, leaving systems vulnerable to new and unknown threats (zero-day attacks). Proactive strategies such as threat intelligence, behavior-based monitoring, and predictive analytics are often underrepresented.

Fragmentation of Frameworks Organizations often have to adopt multiple frameworks (*e.g.,* NIST, ISO/IEC 27001, COBIT) to achieve comprehensive security, leading to overlaps, inconsistencies, and overhead during implementation.

Lack of Scalability Traditional models often fail to scale effectively in larger, more complex environments. Models that work for small organizations may not apply to large enterprises with global operations. They often struggle to address security in distributed systems, such as hybrid cloud architectures or remote work setups. Additionally, due to the fragmentation, often different models address different (conflicting) security goals, that may hinder the development of thorough security measures.

4.2 Requirements for Information Security Models

Information security is not a singular thing that is to be achieved, it is a set of many objectives that may or may not be distinct in their goals. Hence, completeness in security models is an essential principle that ensures that a security framework addresses all relevant aspects of security, leaving no gaps that could be exploited. In our ever-evolving landscape of cybersecurity, completeness of information security models is crucial for ensuring robust protection against threats.

A security model serves as a structured framework that defines policies, controls, and mechanisms to safeguard (critical) assets. However, an incomplete model can leave critical gaps that attackers may exploit, undermining the resulting security infrastructure. By ensuring the completeness of a model, organizations can effectively address key security goals, such as confidentiality, integrity, availability, *etc.*

The following section explores essential goals that a security model should encompass for complete, well-structured and holistic results. A holistic and complete security model:

Covers All Aspects of Security The full spectrum of security objectives must be addressed that are relevant for the asset that shall be protected. This ensures that the security for the asset is complete and protects against all known and identified threats to the assets disclosure or loss.

Mitigates Known and Emerging Threats Any current threat, such as phishing, ransomware, and insider threats must be addressed, but must not be limited to these. Emerging risks, including those posed by zero-day vulnerabilities and evolving attack techniques may not be currently known, but have to be addressable by future expansions of the implementation. This extensibility of existing models allows to act and adapt the frameworks for such upcoming threats.

Prevents Security Gaps Any unaddressed vulnerabilities or overlooked attack vectors must be accounted for so that no security gaps are left in the resulting security implementation. For example, failing to address physical security could allow unauthorized access to servers, while ignoring insider threats might expose sensitive data to rogue but authorized employees.

Enhances Trust and Compliance Trust with stakeholders and compliance with standards and laws must be built by demonstrating a thorough approach to security. This helps organizations meet regulatory requirements and industry standards, such as GDPR or ISO/IEC 27001. Trust is essential because security models operate under assumptions about the reliability of users and systems. A breakdown in trust may lead to vulnerabilities and dissatisfied customers.

Supports Interoperability Components of the system must be able to interact securely enabling interoperability and composition of various mechanisms. For example, access control solutions and encryption protocols must work seamlessly to maintain both security and functionality.

Improves Resilience and Recovery Provisions for business continuity and disaster recovery must be included, ensuring that systems remain functional or can quickly recover from attacks, failures, or disasters.

All in all, completeness in security models is not a luxury; it is a necessity in an era of increasing cyber risks. By addressing all dimensions of security — people, processes, and technology — a complete model provides comprehensive protection, supports compliance, and ensures that organizations are resilient to both known and unforeseen threats. A holistic approach not only prevents vulnerabilities but also builds a strong foundation of trust and accountability.

4.3 Information Security Model Landscape

In this section we want to provide a set of information security models that are widely used and accepted in the current information security landscape.

4.3.1 Threat Modeling and Risk Management Frameworks

Threat Modeling and Risk Management Frameworks provide structured methodologies that may be used to assess information systems according to their safety. These frameworks can help organizations to proactively understand potential attack vectors to be able to implement security controls that reduce the identified risks. Typically, these models aim to identify threats for a system and assess them, to evaluate how likely they are and how big the impact of them would be. After identification, mitigation Strategies are formed, that implement controls to minimize the risks.

In this section we present some frameworks that are widely used in information security helping to enhance resilience against security threats.

STRIDE Threat Model

The STRIDE model is a threat modeling framework developed by Microsoft[1][2] that is intended to help identifying and categorizing potential security threats in software systems. It provides a structured approach to analyzing risks by breaking them down into six primary threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. Each category represents a different type of attack that a malicious actor may use to exploit vulnerabilities, allowing security teams to proactively design defenses:

Spoofing Impersonation of users or systems, allowing an intruder to gain unauthorized access by pretending to be someone else.

Tampering Unauthorized modification of data, either in storage or during transit.

Repudiation Denying to have performed an action, making it difficult to prove what happened without proper logging or auditing.

Information Disclosure Unauthorized access to sensitive data, compromising its confidentiality.

Denial of Service Disrupting the availability of systems or services, rendering them unusable.

[1] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
[2] https://www.microsoft.com/en-us/securityengineering/sdl/practices

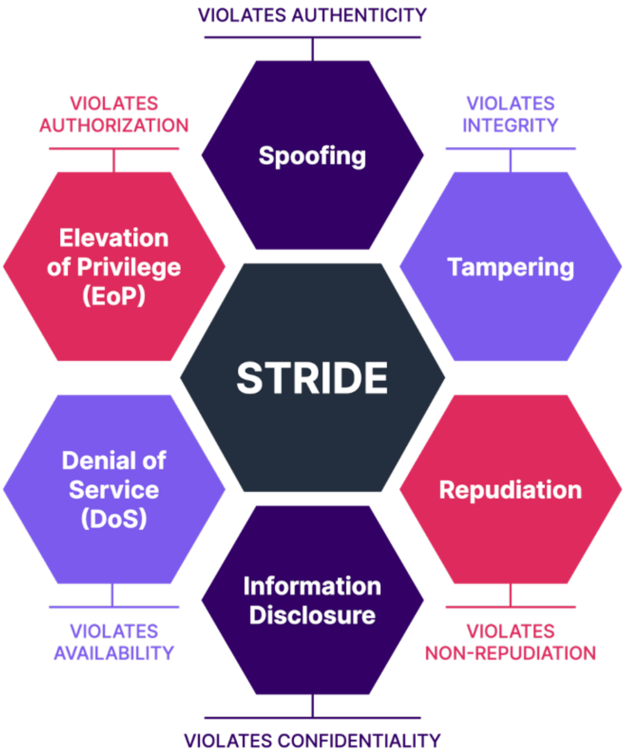


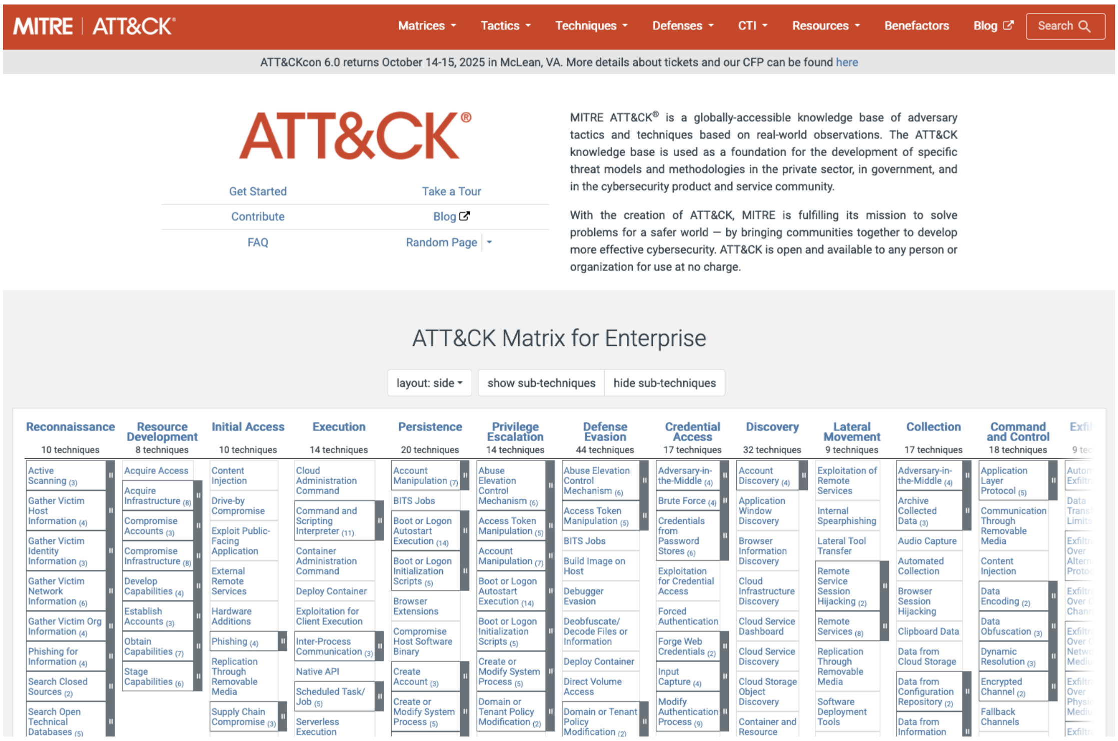
Figure 4.1: Visualization of the STRIDE threat modelling frameworks objectives correlated those from other information security models (*i.e., .* CIA and Parkerian Hexad).

Source: https://medium.com/@arielhacking/examples-of-stride-threats-for-payment-applications-87a0ad0c3a21

Elevation of Privilege Gaining a higher access level than was previously authorized, allowing an attacker to perform malicious activities.

By applying STRIDE to different system components, organizations can predict how an attacker might exploit weaknesses and implement appropriate countermeasures such as authentication, access controls, encryption, *etc.* This proactive approach helps to identify and address security concerns early in the development lifecycle, reducing risks before the deployment phase.

One of STRIDE's strengths is its adaptability across different types of applications, including cloud services, web applications [16, 1], and cyber-physical systems [18, 4]. While it is primarily used in software security, it can also be applied to network security, physical security, and operational technology environments. Using STRIDE in combination



ATT&CKcon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found here

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfil
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 tec
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Autom Exfiltr
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Trans Limits
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltr Over Altern Protoc
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltr Over C Chann
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltr Over C Netw Mediu
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltr Over Physic Mediu
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltr
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)		Direct Volume Access	Modify Authentication Process (9)	Container and Resource		Data from Configuration Repository (2)	Fallback Channels	
			Serverless Execution			Domain or Tenant Policy Modification (2)				Data from Information		

Figure 4.2: Screenshot of the MITRE ATT&CK framework website.

Source: https://attack.mitre.org/

with other security frameworks such as MITRE ATT&CK or NIST CSF, organizations can build a comprehensive cybersecurity strategy that addresses both technical and operational risks.

Figure 4.1 aims to visualize the six categories of the STRIDE model and connect each of them to the already known information security objectives found in Section 2.3. Noteworthy is the strong correlation between the STRIDE model and the three objectives of the CIA Triad (Confidentiality, Integrity, Availability).

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

MITRE ATT&CK[3] is a comprehensive open access knowledge base that documents real-world tactics, techniques, and procedures (TTPs) used by adversaries in the cyber

[3] https://attack.mitre.org/

space [31, 26]. It provides a structured framework for understanding how attackers typically operate, making it an essential tool for information security professionals working in threat intelligence, incident response, and security operations. The framework provides different matrices, with the most widely used being the Enterprise ATT&CK matrix that focuses on threats targeting Operating Systems (*e.g.,* Windows, Linux, macOS, *etc.*) and cloud infrastructure alike. Other matrices collect threats for more specialized environments such as mobile- or industrial control systems.

At the core of MITRE ATT&CK is its categorization of adversary behaviors into (*i*) tactics and (*ii*) techniques. Tactics represent the high-level objectives an attacker aims to achieve, such as gaining initial access, escalating privileges, or exfiltrating sensitive data. Techniques describe the specific methods adversaries use to accomplish these objectives. Each technique entry includes real-world examples, known threat actors that have used it, detection methods, and possible mitigations. This level of detail allows organizations to map out potential attack paths, simulate adversary behavior, and strengthen their defenses accordingly using a pattern based approach.

One of the most valuable aspects of MITRE ATT&CK is its role in attack simulation. Red teams and penetration testers (attackers) can use it to plan realistic attack scenarios, while blue teams (defenders) leverage it to improve detection and response strategies. By aligning security controls with proposed techniques from the framework, organizations can identify gaps in their defenses and enhance their threat-hunting capabilities.

MITRE ATT&CK has become a standard reference in cybersecurity due to its open-source nature and collaborative approach. It is constantly updated based on real-world attack data, ensuring it remains relevant in an ever-evolving threat landscape. Organizations worldwide use it as a foundation for developing security policies, conducting risk assessments, and improving their overall cyber resilience.

NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework 2.0 (CSF 2.0) [23] is an updated version of the original NIST CSF, designed to help organizations manage and reduce cybersecurity risk. Developed by the National Institute of Standards and Technology (NIST), this framework provides a structured approach for organizations of all sizes and sectors to enhance

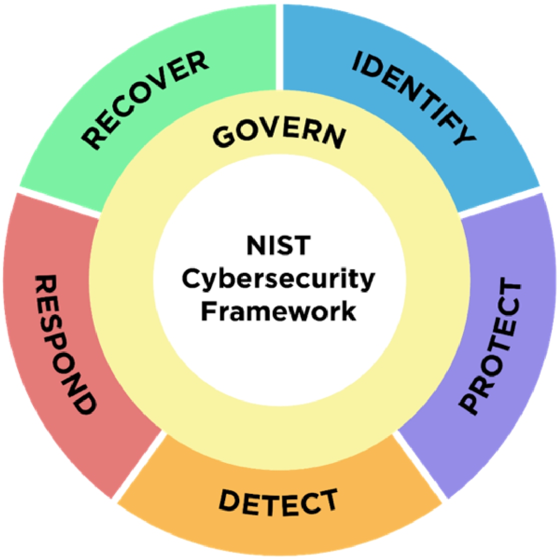


Figure 4.3: Visualization of the NIST CSF 2.0 framework and its six core functions.

Source: https://www.nist.gov/cyberframework

their cybersecurity posture. CSF 2.0 expands on the original framework by incorporating emerging threats, evolving best practices, and broader guidance for governance and supply chain security.

At the core of the framework are six key functions: Govern, Identify, Protect, Detect, Respond, and Recover:

Govern Emphasizes the importance of leadership, policies, and continuous improvement in cybersecurity decision-making. CSF 2.0 introduced this function.

Identify Focuses on understanding assets, risks, and vulnerabilities.

Protect Dedicated to implementing safeguards to defend against threats.

Detect Ensures organizations have monitoring capabilities to recognize cybersecurity events.

Respond Provides guidance on containment, mitigation, and communication strategies when an incident occurs.

Recover Outlines steps to restore normal operations and minimize long-term impact.

A visualization of the six functions can be found in Figure 4.3.

One of the defining aspects of NIST CSF 2.0 is its flexibility and adaptability. Unlike rigid compliance frameworks, it offers a set of guidelines that organizations can tailor to their unique risk profiles, regulatory requirements, and business objectives. The framework aligns with other standards, such as ISO 27001 [8, 11] and CIS Controls [14], making it easier for organizations to integrate it into their existing security programs. Additionally, CSF 2.0 places greater emphasis on supply chain risk management, ensuring that organizations account for third-party security risks in their overall cybersecurity strategy.

The NIST Cybersecurity Framework is widely used across industries, including government agencies, financial institutions, healthcare providers, and critical infrastructure sectors. By providing a common language for cybersecurity risk management, CSF 2.0 facilitates communication between technical teams, executives, and stakeholders. Its iterative approach encourages continuous improvement, allowing organizations to assess their cybersecurity maturity, identify gaps, and strengthen defenses against an increasingly complex threat landscape.

OCTAVE

The OCTAVE framework (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk management framework published in 2001 by the Carnegie Mellon University [2]. It is a framework designed to help organizations identify, assess, and address security risks to their critical assets. Aligning an organization's security strategy with its business objectives is a core feature of the model, emphasizing organizational self-assessment and strategic decision-making. OCTAVE is a particularly systematic and structured approach to assess risks that prioritizes actions to mitigate any identified risks.

The process described by the framework consists of three steps:

Build Asset-Based Threat Profiles Identify the organization's critical assets (*e.g.,* data, systems, processes). Assess the threats to these assets. Analyze how these threats might exploit vulnerabilities and the potential impact on the organization.

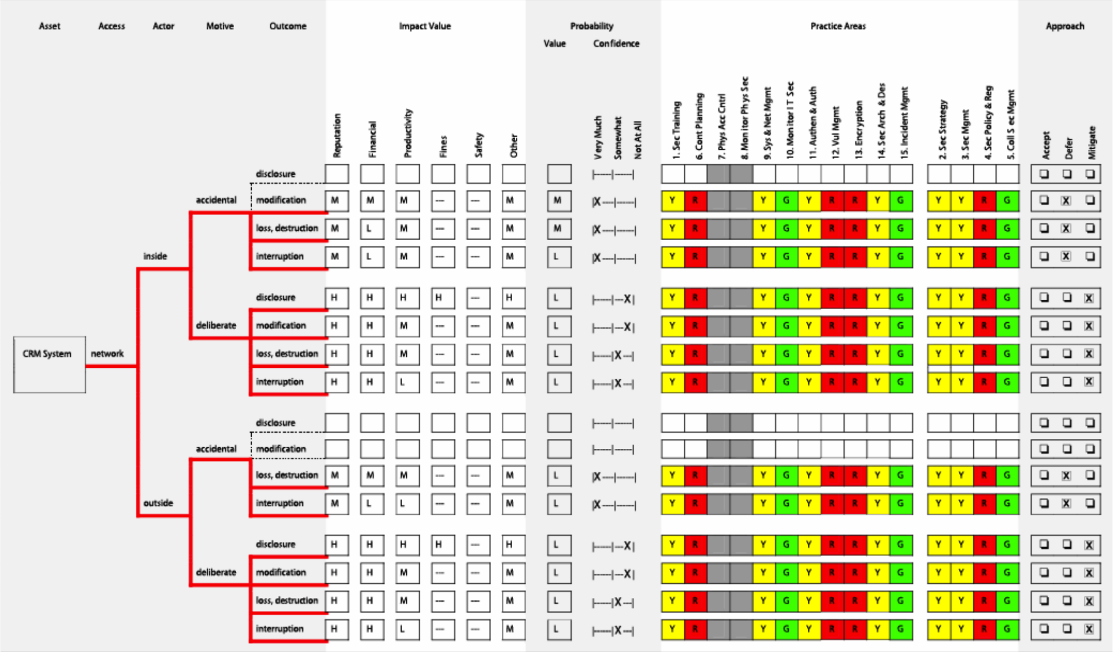


Figure 4.4: Visualization of the threat assessment process proposed by the OCTAVE framework.

Source: Taken from the script of the master's course *Management von Sicherheit und Zuverlässigkeit (MSZ)* in computer science at HAW Hamburg

Identify Infrastructure Vulnerabilities Evaluate the organization's IT infrastructure to identify vulnerabilities that could be exploited by threats. This includes assessing network configurations, software, hardware, and procedures.

Develop a Security Strategy and Plans Use the information from the first two phases to prioritize risks and define mitigation strategies. Develop a risk management plan that aligns with business goals and resources.

Figure 4.4 visualizes the process proposed by the framework. The framework itself is a risk assessment and requirements engineering framework, with strong coupling to the CIA's objectives. The four possible outcome column are take the impact – or rather the result – into consideration, where disclosure, modification, loss/destruction, and interruption are possible values. Taking the underlying requirements from CIA these can be directly mapped to its corresponding categories of the model: (*i*) disclosure ↔ confidentiality, (*ii*) modification ↔ integrity, and (*iii*) loss/destruction and interruption ↔ availability. Loss/destruction of assets is difficult to map in this regard, since while de-

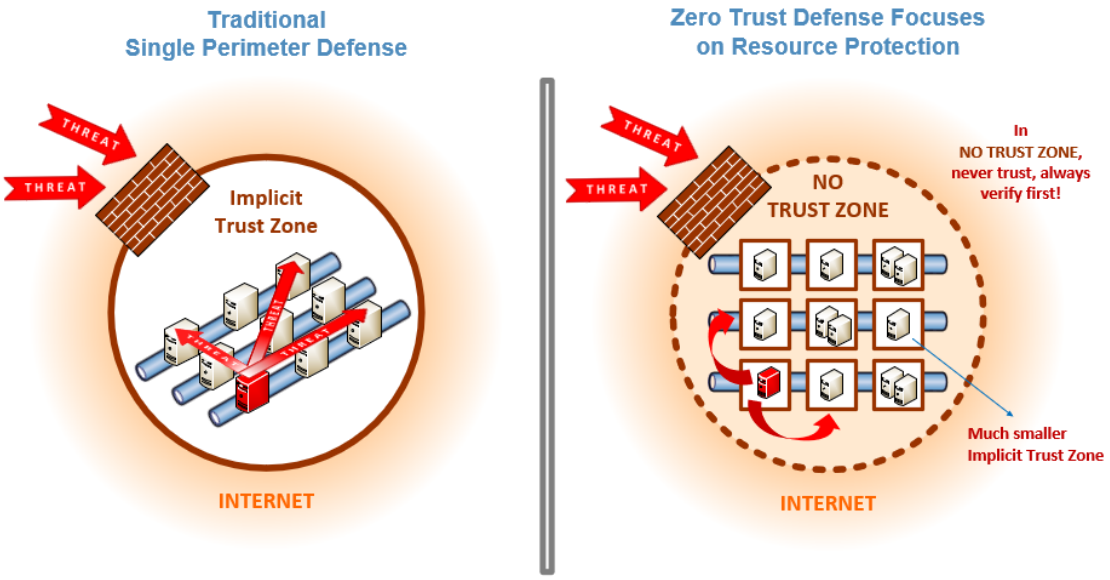


Figure 4.5: Visualization of the Zero Trust Model compared to the traditional approach of an implicit trust zone.

Source: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

struction of data may result in issues with integrity, but rather the access is what is interrupted due to the destruction. Both categorizations could be correct.

4.3.2 Security Architecture and Trust Models

Security Architecture and Trust Models provide structured frameworks for designing secure systems by defining how security principles, controls, and trust relationships are established and maintained. Such models can help organizations to enforce access control, data integrity, and confidentiality across IT environments.

In this section we present some frameworks that are commonly applied in information security helping to improve security in software systems.

Zero Trust

The Zero Trust model proposed by Kindevag *et al.* [19, 30] is a modern security framework following the idea of “never trust, always verify”. Traditional perimeter-based security, typically assumes users and devices within an internal network to be trustwothy which posed to be inherently unsafe. Applying zero trust requires continuous authentication and authorization, regardless of location or network, locking intruders in-place – even if they gained access to a part of the system. This approach minimizes the risk of insider threats, lateral movement by attackers (*i.e.,* moving from one device within the perimeter to another), and unauthorized access.

The model applies principles such as least privilege access [28], micro-segmentation [20, 29], and strong identity verification [10]. Users and devices alike must prove their authorization each time they attempt to access resources, while network access is strictly controlled, and communication between systems continuously monitored to detect anomalies.

By eliminating the idea of implicit trust, security in interconnected environments such as remote work settings, and hybrid infrastructures can be vastly enhanced. Organizations adopting this model benefit from reduced attack surfaces and greater resilience against intrusion – even if an attacker has already copromized parts of a system. Figure 4.5 visualizes and compares both approaches, showcasing the solved problem of lateral movement.

Bell-LaPadula Model

The Bell-LaPadula Model proposed by Bell *et al.* [6] is a security framework designed to enforce data confidentiality in computer systems and has been applied particularly within military and government environments. It follows a set of two rules that prevent unauthorized access to classified information by implementing strict access controls based on security clearances. The model enforces two main rules:

No read up Prevents users from accessing data at a higher classification level than their own, preventing unauthorized disclosure.

No write down Stops users from writing data to lower classification levels, ensuring integrity.

By structuring access to assets using hierarchical security levels, the Bell-LaPadula Model achieves an effective protection of sensitive information from unauthorized disclosure.

Biba Integrity Model

The Biba Model proposed by Biba *et al.* [7] is a security framework focused on maintaining data integrity by preventing unauthorized or untrusted modifications. It is closely related to the Bell-LaPadula Model, but comes with different requirements addressing data integrity - it ensures that higher-integrity data is not corrupted by lower-integrity sources. It enforces two main rules:

No read down Prevents users from accessing data at lower integrity levels, avoiding contamination of data.

No write up Stops users from writing data to higher integrity levels, maintaining data trustworthiness.

This model is commonly used in environments where data accuracy is critical.

4.3.3 Access Control and Authorization Models

Access control and authorization [17, 5] are core aspects of information security that are implemented to determine how users and systems interact with resources. These mechanisms ensure that only authorized entities can perform specific actions, reducing security risks such as data breaches, unauthorized modifications, and misuse of sensitive information.

At its core, access control involves three fundamental components:

Identification A user or system presents credentials (*e.g.,* usernames, biometrics, or device identities) to verify who they are.

Authentication The system validates the provided credentials, confirming that the entity is genuine (*e.g.,* via passwords, security tokens, or other factors).

Authorization Once authenticated, the system determines what actions the user or system is allowed to perform, based on predefined policies.

Access control systems rely on well-defined authorization models, which provide rules for who can access specific resources and under what conditions. These models aid organizations in enforcing security policies by structuring permissions in a way that aligns with operational needs, regulatory requirements, and security best practices.

A robust access control strategy incorporates principle-based security measures, such as:

Least Privilege Granting users only the minimum level of access necessary to perform their tasks.

Separation of Duties Ensuring that critical tasks require multiple individuals to prevent fraud and errors.

Context-Aware Access Factoring in real-time conditions such as user location, device type, and access patterns to refine security decisions.

In modern environments, access control extends beyond traditional on-premise systems to cloud-based infrastructures, mobile devices, and third-party integrations. As organizations evolve, they often adopt dynamic access control strategies that rely on continuous monitoring, risk-based authentication, and adaptive permissions to enhance security without compromising usability.

4.4 Possession in the Current Information Security Landscape

To understand commonalities between the proposed models, we categorized them according to the principles from the Parkerian Hexad. Table 4.1 shows the resulting categorization of all models discussed in Section 4.3. A number of additional models have been added to the table to expand on the categorization and emphasize the point of strong overreliance on the objectives of the CIA Triad.

This lack of consideration for objectives that lie outside the scope of the CIA Triad are an observation that has been criticized before (see Section 4.1). While almost all provided models address the CIA's objectives, the Hexad's objectives are sparsely considered – if at all. Apart from the Parkerian Hexad, which has been proposed out of critique of this realization, possession is only considered explicitly by access control models. Here possession plays a crucial role in terms of identifying and authorizing users and systems through the ownership of factors as trust-anchors (*e.g.,* ID cards, passwords, tokens *etc.*). This strong connection to possession as a requirement uncovers the problem with adhering to the CIA Triad alone. The model cannot express this underlying requirement

Security Model	**Confidentiality**	**Integrity**	**Availability**	**Authentication**	**Utility**	**Possession/Control**
CIA Triad	✓	✓	✓			
Parkerian Hexad	✓	✓	✓	✓	✓	✓
STRIDE	✓	✓	✓	✓		
MITRE ATT&CK	✓	✓	✓	✓		
NIST CSF 2.0	✓	✓	✓	✓	✓	
OCTAVE	✓	✓	✓	✓	✓	
Zero Trust	✓	✓		✓		
Bell-LaPadula Model	✓			✓		
Biba Integrity Model		✓		✓		
Access Control	✓	✓		✓		✓

Table 4.1: List of all patterns provided in Chapter 4. The patterns have been ordered according to their corresponding principle from the Parkerian Hexad (*i.e.*, (*i*) Confidentiality, (*ii*) Possession, (*iii*) Integrity, (*iv*) Authenticity, (*v*) Availability, and (*vi*) Utility).

of possession, which emphasizes the short-comings of the approach of following the CIA Triad exclusively.

We did include OCTAVE, Zero Trust, the Bell-LaPadula- and Biba Integrity models, and the access control mechanisms in this table to emphasize the point of missing consideration for the concept of possession. However, we will not consider these any further in the coming chapters. These models are well regarded in information security, but are either too broadly scoped or simply lack the requirements based approach that we want to explore in this thesis.

4.5 Discussion

In this chapter, we presented an overview of commonly implemented information security models. We provided background on their ideas, objectives and goals as well as a categorization according to CIA and Parkerian Hexad. During the categorization of the models, we could show that while the CIA is considered by all models, the Parkerian Hexad is not. Especially the objective of possession is only considered by the Hexad itself and access control mechanisms, which by definition rely heavily on possession of identifying factors.

5 Embracing Possession as Security Goal to Improve Existing Models

As discussed in Chapter 3, the concept of possession is a crucial part in many security oriented domains, but its application within existing information security models remains lacking. To test this hypothesis, we incorporated the concept into a number information security models and discuss its implication on the models, to show how the adoption can improve on the existing landscape of models.

This chapter explores the extension how the concept of possession might be integrated into frameworks, examining potential benefits implications. By discussing its impact, we try to better understand whether and how possession can enhance current modeling approaches.

5.1 Proposing a Possession-Aware Security Model

Taking possession explicitly into consideration, can improve security solutions in organizations. In this section we want propose a possession aware information security model that showcases the implications for the current information security landscape. Basically, the concept follows the idea of identifying critical assets that shall be monitored using possession-aware tracking, allowing to step in in case there are unauthorized possession changes. The proposed model consists of four steps that ensure that an organization can assess and classify assets, implement possession monitoring, and appropriate responses to possession-violations (*e.g.,* when a ressource has changed possession without explicit authorization).

1. **Possession Based Asset Classification** Identify critical assets that require possession tracking (*e.g.,* credentials, encryption keys, sensitive data *etc.*). Each identi-

fied asset must then be classified, resulting in a set of conditions under which a user may be allowed to gain possession of the asset in question.

2. **Possession Verification Tools** Implement device-based authentication to explicitly (*e.g.,* hardware tokens, TPM-based identity verification). Geofencing and biometric authentication may be used to enforce physical possession constraints identified in step 1.

3. **Monitoring and Detecting Possession Violations** Deploy real-time monitoring solutions such as Security Information and Event Management (SIEM)[1][2] that flag unexpected possession transfers. Behavioral analytics may be used to detect unusual access and usage patterns to identify possession shifts (*e.g.,* an employee accessing files from a foreign data center they usually don't need).

4. **Automating Possession-Based Responses** Implement automated possession reclamation (*e.g.,* revoking stolen admin keys or certificated on detection). Enable smart quarantine—suspicious possession events trigger containment (*e.g.,* locking a laptop with leaked credentials remotely).

Identifying critical assets should not be a big change when other security frameworks have already been applied and implemented. Thus, this step should be relatively easy to incorporate in the already existing frameworks. What changes though is the classification step, where assets now not only have to be classified according to their security level, but also by how easily they can change possession without prior authorization. It is relatively easy to gain unauthorized possession of a small portable device such as a smartphone or a notebook, but gaining physical possession to a server positioned in a high-security facility is much more difficult. This has to be taken into consideration.

Implementing possession verification tools and methods allows an organization to authenticate who can – and does – gain possession of an asset or where an asset is currently positioned. Using Trusted Platform Modules and hardware tokens for this is by itself already a possession based approach that allows to cryptographically verify who gains possession of an asset. This is especially useful for smaller digital assets that change possession frequently – but can also be added to saves or such devices that contain an asset by itself. Applying the idea of Zero-Trust, for example, could accomplish this as

[1] https://www.ibm.com/think/topics/siem

[2] https://www.microsoft.com/en-gb/security/business/security-101/what-is-siem

well, requiring users and systems to authorize each time they access any assets. Geofencing on the other hand could be used to check the possession of very large mobile assets (*e.g.,* trucks, airplanes, or ships) that change possession when changing position.

After identification, classification, and the implementation of verification tools, the now accessible possession information must be monitored. Here, Monitoring solutions must be implemented that enable the continuous monitoring of the classified assets, issuing notifications about unauthorized or unexpected changes of possession. This might be triggered by explicit- (*e.g.,* a smartphone that changed possession) or implicit changes of possession (*e.g.,* a container was moved out of its geofenced area). Any such change must be recognized to be able to act accordingly, by triggering explicit counter-measures.

Any such counter-measures that can be triggered must be well-defined in advance and allow to mitigate any (further) damage that may result from the unauthorized change in possession. In case certificates, encryption-keys and the-like have been leaked, revocation mechanisms have to be triggered to render the leaked assets useless for anyone that currently possesses them. Unauthorized possession changes to assets located on cloud-infrastructures may be countered by locking the assets (if even only for the current user). This could even be done temporarily or proactively to delay any attacker in its steps. These counter-measures are very much dependent on the type of the asset and must be identified in accordance to the asset itself to ensure an appropriate reaction to any such situation.

5.2 Applying Possession to Existing Security Models

We now want to take a step back and try to apply these ideas to the three most commonly used frameworks from Section 4.3 STRIDE, MITRE ATT&CK, and NIST CSF 2.0. Both models aim to proactively identify threats and assess them following predefined terminology and rules. By explicitly considering possession in these frameworks we extend and show how these could be improved upon using such extension.

5.2.1 STRIDE

The STRIDE model aims to identify and assess threats that occur through violating a set of existing security objectives. It currently does not however, explicitly consider possession as an objective that has to be taken into consideration, leaving gaps in the resulting security assessment. Introducing possession to the model could be done by introducing a new threat category “Possession Violation” or (P) – moving from STRIDE to STRI**P**ED, resulting in a more holistic assessment. This explicit extension of the framework could improve the three STRIDE categories: (*i*) spoofing, (*ii*) information disclosure, and (*iii*) Elevation of Privilege.

Both spoofing and elevation of privilege are currently considered by STRIDE, addressing unauthorized access of assets. Cases where an attacker legitimately appears to have access even if they don’t, are unconsidered risks that result in gaps that could be exploited. Taken the case that Multi-Factor-Authentication (MFA) [24] is implemented and enforced as a countermeasure for spoofing, there still is the risk of stolen or leaked credentials that are currently not considered or uncovered by the framework. By explicitly considering possession, such an incident could be recognized and appropriate countermeasures could be rolled out, *i.e.,* by introducing mechanisms for revoking such leaked credentials or passwords.

Information Disclosure focuses on the unauthorized reading of data, but possession would address cases where attackers obtain data they are not cleared to access, even without immediate disclosure. For example, in a ransomware attack [9], assets could have been exfiltrated, and not yet published, since the overall goal would be to extort the attacked organization. By considering possession explicitly, any such asset could be prepared for this case by applying encryption to them, rendering the exfiltrated assets unusable without the possession of the decryption key. In this case, the attacker may have been successful in obtaining the assets, but extortion is off the table since the exfiltrated data poses no immediate risk.

5.2.2 MITRE ATT&CK

Applying Possession to the MITRE ATT&CK framework, aligns closely with techniques involving data exfiltration, credential dumping, and ransomware deployment. Key tactics and techniques that impact possession include: (*i*) Exfiltration (TA0010), (*ii*) Credential Access (TA0006), (*iii*) Impact (TA0040), or (*iv*) Collection (TA0009). Techniques like automated exfiltration directly affect possession because data is moved to an external attacker-controlled system. OS credential dumping affects possession by allowing attackers to take control of authentication secrets, enabling unauthorized access without immediately violating confidentiality. Data encrypted for impact is a good example where an attacker disrupts possession by encrypting data, making it unusable for the rightful owner, even if confidentiality isn't breached.

This shows that the MITRE ATT&CK framework does consider attacks that are leverage-, or are based on the concept of possession – but it does so implicitly. Taking the concept into consideration explicitly, could significantly improve upon the proposed countermeasures.

For example, exfiltration attacks allow an attacker to gain access to confidential data. The framework proposes solutions such as network monitoring, endpoint security and data controls, or access management as mitigation strategies for this class of attacks. If the concept of possession would be explicitly addressed, more holistic approaches to this could be proposed – for example, encrypting the owned asset, in combination with regular backups. In case an attacker gains access to the secured access through an exfiltration attack, the contained information would stay in possession of the owner, who could simply close the gap and recover the systems from a previous backup.

Credential access refers to adversary techniques used to steal authentication credentials such as passwords, hashes, or tokens. For this, techniques such as OS credential dumping, brute force, and stealing password stores enable attackers to gain unauthorized access to systems. Applying the concept of possession would allow maintaining control over credentials even if they are stolen. Enforcing multi-factor authentication would ensure that stolen credentials alone are not sufficient for access, while hardware security modules (HSMs) and secure enclaves allow storing credentials in a way that prevents exfiltration alltogether. Thus, integrating possession-based security measures can limit the impact of credential theft, ensuring that even if credentials are compromised, they cannot be easily used by attackers.

Impact refers to adversary techniques that disrupt, degrade, or manipulate data and system availability. Techniques like data destruction or data encryption for impact (ransomware attacks) enable attackers to render systems unusable or compromise data integrity. Possession can be applied to strengthen defenses against these impact attacks. For example, immutable backups and air-gapped storage can be solutions that ensure that data remains recoverable even if ransomware encrypts live systems (*i.e.,* the control of the data is retained). Endpoint and server rollback capabilities (*e.g.,* snapshot-based recovery) help organizations maintain possession of their data even after a destructive attack. Strict access controls and just-in-time privileges prevent adversaries from obtaining the permissions necessary to alter or delete critical data. Additionally, write-protected configurations and hardware security features (*e.g.,* Trusted Platform Modules) can prevent unauthorized system modifications.

Collection refers to adversary techniques used to gather sensitive information before exfiltration. Screen capture, input capture (keylogging), and email collection enable attackers to harvest valuable data from compromised systems. Applying possession can strengthen the defenses against Collection by implementing Data Loss Prevention (DLP) tools that can prevent unauthorized processes from copying or modifying sensitive data. Again, hardware-based security solutions, such as Trusted Platform Modules (TPMs) and secure enclaves, can ensure that certain data remains inaccessible even if an attacker gains system access. Finally, encrypting stored files and disabling clipboard/screenshot capabilities for sensitive applications can prevent attackers from easily capturing data.

5.2.3 NIST CSF 2.0

The NIST CSF 2.0 is designed around six core functions, of which possession is none. Explicitly considering possession could improve the framework by improving detection for the existing functions.

The identify, and govern functions, for example currently deal with asset management and governance but do not explicitly consider who has possession of any asset at a given moment. Assets protection is often achieved by implementing a secure perimeter without granular management of who should and is allowed to hold an asset. By introducing the concept of possession to this, tracking mechanisms could be implemented that continuously verify who has control over these assets, improving both responsibility and accountability. Tracking who owns an asset and who physically or logically controls it at any given time, enables monitoring any potential security risk that is associated with it. As an example: implementing such possession based monitoring for encryption keys would allow registering any unauthorized access, allowing to trigger a revocation mechanism of the key.

The protect function currently secures assets via access control, identity management, and data security to ensure any data is protected. By extending this function with a possession based access model, data could not only be secured against unauthorized access, but – depending on the implementation – also against disclosure in case the asset has been leaked. For example, by implementing strong encryption and managing the possession of keys using the govern functionality, asset protection could be improved, even beyond the currently typical level.

The recover function focusses on ensuring business continuity and restoring normal operations. This function could be strengthened by introducing an asset repossession strategy that handles plans for repossession of assets after they have been lost. Particularly in cloud-based or ransomware scenarios assets have to be recovered (*e.g.,* from backups) or the systems have to gain control of backup databases to restore the typical operation of the system. Any exfiltrated assets such as sensitive trade secrets, legal or contractual documents, or user data should be invalidated during this step as well, which could be achieved by a proper possession function.

5.3 Discussion

In this chapter we proposed a new possession-aware security model that considers possession explicitly to achieve a holistic approach to information security. We also revisited three information security models – STRIDE, MITRE ATT&CK, and NIST CSF 2.0 and applied the concept of possession to them, aiming to close some gaps in the models.

The proposed possession-aware model shows that taking possession explicitly into consideration can improve both the achieved security of the resulting implementation, as well as the mechanisms to uncover ongoing or planned attacks. By monitoring who currently has possession of assets, counter-measures can be implemented that ensure the security of information and secured assets, while allowing to simplify existing measures.

Revisiting the three information security models has shown twofold: (*i*) there are gaps in these models, and (*ii*) it does not require extensive shifts in existing information security implementations. The gaps result from a strict emphasis on the traditional CIA model, which has gaps in its view of information security. Especially that narrow scope and the resulting generalization of the three objectives results in an incomplete picture of the security situation that is to be determined. By applying possession as an objective to the models, allows to broaden the scope of the models and to address security vulnerabilities more holistically. Additionally, the extension has shown that applying this additional objective from the Parkerian Hexad to the CIA-based models is simple. This is due to the close relation of both models, rendering the application of the objective straightforward. Thus, applying the objective of possession to existing security models is a clear must for a holistic approach, that does not lead to problems during the process.

6 Counterarguments and Limitations

While Possession-Aware information security can improve upon the existing landscape of information security models, it is not without challenges and potential drawbacks. In this chapter we want to discuss possible counterarguments to the possession-aware extension, as well as possible limitations of the approach.

6.1 Counterarguments

In this section we propose several counterarguments arguing against the adoption of possession-aware security. The resulting collection of arguments will then then be discussed later in this chapter.

Increased Complexity and Cost While possession-aware modeling may improve security, it also requires additional tracking, verification mechanisms, and infrastructure changes. These could introduce additional complexity during planning, implementation and operation phases, accompanied by higher costs. Especially the introduction of additional required hardware can be a high cost-factor that might speak against the adoption – this cannot be decided without knowledge of the environment the concept shall be applied to.

Privacy Concerns Continuously tracking possession *i.e.,* by monitoring device locations or user behavior, can be seen as privacy violation and be too intrusive for organisations to implement. Particularly the GDPR discussed in Section 3.3.1, but other regulations as-well may be stopping the adoption of such monitoring approaches, favoring the privacy of the individual more than the improved security. At its core, this is a trade-off that must be evaluated before the concept can be applied.

False Positives Possession of assets may change legitimately – and this may happen frequently without any malicious intent. Users change devices, travel, or access data in different contexts, which could trigger unnecessary false alarms and access denials. This can result in vastly degraded service quality and velocity of processes, leading to a serious reduction of profitability.

Possession Controls Can Still be Bypassed Possession is not a solution to all problems – information security (even if following possession awareness) is not a standalone solution. Attackers could still compromise both credential- and possession verification, for example by stealing a notebook with a hardware security module. Breaking into a location, gaining access to the ressource directly, leads to a comparable outcome. Both will enable attackers to bypass defenses that are possession aware, rendering them useless even if thoroughly implemented.

Possession Monitoring May not be Feasible Not all assets are important enough to justify possession-based approaches, especially in cases where the currently adopted approach of following the CIA TRIAD results in good overall security. Due to the added cost and performance impacts of the approach, standard, off-the-shelve solutions might be enough. Especially organizations that rely heavily on legacy infrastructure that does not support real-time possession monitoring (such as banks, for example), makes the adoption of the approach difficult if not infeasible.

Access Control Bottlenecks By implementing yet another information security concept, users are again, being restricted from accessing assets they are not authorized to access. This may be impeding with the overall productivity of an organization, leading to overall productivity degradation and in the worst case, loss of revenue.

6.2 Discussion

Following the counterarguments and limitations of the approach, we also found downsides of using the possession-based approach. Most prevalent was the argument that the new approach is infeasible to adapt for the use-case of an organization – be it because of increased complexity or cost, or the added overhead that may not be justifyable by the benefits. These are all valid arguments that point to correct observations, however, they can be applied to any of the existing models and frameworks as well. No added benefit in information security comes free of cost, be it because it costs money or time, is risky due to inherent dependencies, or because it adds overhead to possibly already blown out processes.

Feasibility or achievability are two other concerns that address the concern of the addition being unnecessary, due to missing benefits or the infeasibility resulting from legacy systems that may not be up for the new task. In case no assets could be identified that would benefit from the approach, this is valid – if no assets need securing, we don't need to do anything about it. The case of legacy systems however, is one that uncovers a more serious problem in our eyes: Such systems may have been outgrown by the moving requirements that are required from them. This is not a problem of the possession-based approach, but rather a problem of inactivity or missed updates of the infrastructure.

Privacy Concerns are posing a challenge that aims at the legislative duties of organizations. Regulative requirements such as the GDPR are in our eyes there for a reason and must not be ignored – privacy is a valuable asset that each individual should be able to keep. While this is on one side a hindering aspect, storing, safeguarding and managing the resulting data is again a hard task that adds to the already existing problem of information security. So this is a point where it must be weighed up against its benefits, which should be outweighing this added overhead again.

Finally, the aspect of finding false-positives is one that does not really stand up against the threats that may not be found if no monitoring would have been in place. Having to deal with such false-positive notifications is necessary in our eyes, outweighing the negative aspects of not monitoring at all.

Thus, leaving us with a strong argument for the approach in our eyes. All but one argument are outweighed by the added benefits of the approach, while only a single aspect – the privacy – is a given legislative duty that must be followed anyways. We think that applying possession-aware information security models makes the original approaches to information security more holistic and better suited for securing assets in the long run.

6.3 Discussion and Recommendation

In this chapter we have presented counterarguments against the approach of applying possession-aware security, but were able to invalidate the majority of them in the discussion. Most counterarguments – while valid in general – must be taken into consideration during the planning and implementation phase, since they are trade-offs that need to be evaluated specifically for the field of application. Since every system, organization, or solution is different, it also poses different requirements and edge-cases that may cover one or multiple of these counterarguments. Identifying and addressing all valid ones, again, will result in a more holistic result that leaves less gaps in the security of assets.

Adopting possession-aware security in security models will pose many benefits in our opinion. Added drawbacks and disadvantages of the approach are easily circumvented or plain invalidated by the added benefits that we could already present in Chapters 5 and 6. The inclusion can thus leverage benefits of the concept of possession to increase the security of assets in an organizations significantly. While this does not come without cost, the impact can either be limited by cleverly applying the concept in different ways to different problems, or be circumvented completely by rethinking the problem with possession in mind.

To conclude, we want to propose a set of recommendations that can be followed when possession-aware security shall be adopted. This can aid information owners and software designers alike during the planning phase of information security in their organization.

1. **Collect, review, and assess all related requirements.** With every adoption of information security mechanisms, requirements have to be collected beforehand, so that the resulting security model that is applied meets the needs of the organization. This step is no different from the adoption of any other information security model, but has to be done also with possession-aware security, to rule out problems with the resulting framework. Possession-aware security can be applied in many facettes, that have to be tailored specifically to the needs of the organization as well.

2. **Combine multiple information security concepts to achieve a holistic solution.** For a holistic approach it is very important to apply not only a single concept to secure assets, since this will leave gaps in the resulting information security framework. Rather, it is important to leverage the benefits of as many key elements as possible, to ensure a holistic assessment of risks, vulnerabilities

*etc.*This allows to close gaps left by other concepts, while addressing more attack vectors and vulnerabilities.

3. **Address legacy systems and components.** Legacy Systems are a problem when applying new concepts, due to them often lacking extensibility and exchangeability of systems parts. In case of applying possession-aware security, it may be beneficial to only monitor the legacy systems that don't already explicitly consider possession-aware information security modelling. This ensures that the overall overhead introduced by monitoring is limited to those parts that cannot be easily exchanged or extended, while still enabling the explicit adoption of possession in the approach.

7 Conclusion and Future Work

The current landscape of information security frameworks and models is based on ideas dating back to the beginning of information security from 1970's. Most of the existing landscape and even newly developed models derive their ideas from the CIA TRIAD to explicitly address only three core security concerns – forming the de-facto standard. Other models have emerged over the years, one of them being the Parkerian Hexad, which was proposed in the 1990s because of this strong coupling to outdated ideas. The Hexad proposed – besides others – the explicit consideration of possession to achieve a more holistic and modern approach to information security that is up to its task.

Possession as a concept is the idea of physically holding or controlling an asset at any given time and is achieved by controlling the asset physically (*i.e.,* through safeguarding a phone, HDD, *etc.*), or by digital means (*i.e.,* through encryption, position monitoring, *etc.*). This concept has not yet gained much attention in the landscape of information security and was not yet considered by any of the widely accepted frameworks. Therefore, we applied the concept of possession and both introduced a new approach to information security, as well as extended existing frameworks with this additional concern.

With this thesis we provided an overview of the foundation of information security and its evolution up to now, exploring the current landscape. We discussed and motivated the concept of possession and considered its benefits and implications. We then explored frameworks that applied or should have applied the concept of possession to provide additional information on the field. Then, we explored and discussed the current information security landscape beginning with CIA and Parkerian Hexad, and ending with very specific authentication based models. We could apply this new knowledge and insights to propose both a possession-aware framework that leverages the concept, as well as discuss possible additions to existing frameworks and their benefits and implications.

Based on this work, we could demonstrate that possession has not been considered adequately within the security landscape. This lead to serious gaps in the current information security solutions. The frameworks which we extended with the concept of possession could assess and prepare for threats in a much more holistic fashion, while still achieving the already known level of safetly and security. All in all, we could show that considering possession in the security landscape results in benefits across the board with very minor drawbacks. This makes it especially useful in the increasingly distributed world we currently live in to address security concerns which are present in all organizations.

7.1 Future Work

While this thesis has explored the role of possession in information security, several areas remain open for further research. We want to collect these unexplored fields for future work, to enable readers to revisit the field.

1. The number of frameworks that are extended by the concept of possession could be expanded on. This could improve upon the existing security landscape by adopting the concept more broadly and possibly emphasize the importance while simultaneously showing the lack of adoption.
2. Finding more missing concepts that have been proposed by other frameworks and researchers. Since in this thesis only the concept of possession has been addressed, the resulting view of the landscape is limited and could be expanded upon. For example, Parker also proposed the concept of utility in his Hexad, aiming at the usability of Assets during and after reacting to threats. This concept has also not been considered widely, while it could pose a valuable addition to existing security models. Other researchers may have proposed new concepts as well, which are not considered in this thesis either, leaving room for further research.

Future research could build upon this list and expand upon our findings. Expanding on these areas could contribute to understanding and finding more comprehensive solutions in information security.

References

[1] Abomhara, Mohamed ; Gerdes, Martin ; Køien, Geir M.: A stride-based threat model for telehealth systems. In: *Norsk informasjonssikkerhetskonferanse (NISK)* 8 (2015), Nr. 1, S. 82–96

[2] Albert, Cecilia ; Dorofee, Audrey J.: OCTAVE criteria, version 2.0. (2001)

[3] Anderson, James P.: Computer Security Technology Planning Study. (1972)

[4] Anwar, Malik N. ; Nazir, Mohammed ; Ansari, Adeeb M.: Modeling security threats for smart cities: A stride-based approach. In: *Smart Cities—Opportunities and Challenges: Select Proceedings of ICSC 2019* Springer (Veranst.), 2020, S. 387–396

[5] Barkadehi, Mohammadreza H. ; Nilashi, Mehrbaksh ; Ibrahim, Othman ; Fardi, Ali Z. ; Samad, Sarminah: Authentication systems: A literature review and classification. In: *Telematics and Informatics* 35 (2018), Nr. 5, S. 1491–1511

[6] Bell, D E. ; LaPadula, Leonard J. u. a.: *Secure computer systems: Mathematical foundations*. The MITRE Corporation, nov 1973

[7] Biba, Ken: Integrity considerations for secure computing systems. In: *Mitre Report MTR-3153, Mitre Corporation, Bedford, MA* (1975)

[8] Brenner, Joel: ISO 27001 risk management and compliance. In: *Risk management* 54 (2007), Nr. 1, S. 24–29

[9] Brewer, Ross: Ransomware attacks: detection, prevention and cure. In: *Network security* 2016 (2016), Nr. 9, S. 5–9

[10] Burke, Peter J. ; Stets, Jan E.: Identity verification and the social order. In: *Order on the edge of chaos: Social psychology and the problem of social order* (2015), S. 145–164

[11] Culot, Giovanna ; Nassimbeni, Guido ; Podrecca, Matteo ; Sartor, Marco: The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In: *The TQM Journal* 33 (2021), Nr. 7, S. 76–105

[12] Diepenbroek, Martine: The Spartan Scytale and Developments in Ancient and Modern Cryptography. (2023)

[13] Gaj, Kris ; Orłowski, Arkadiusz: Facts and myths of enigma: Breaking stereotypes. In: *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22* Springer (Veranst.), 2003, S. 106–122

[14] Groš, Stjepan: A critical view on CIS controls. In: *2021 16th International Conference on Telecommunications (ConTEL)* IEEE (Veranst.), 2021, S. 122–128

[15] Jakobsson, Markus ; Ratkiewicz, Jacob: Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In: *Proceedings of the 15th international conference on World Wide Web*, 2006, S. 513–522

[16] Jiang, Li ; Chen, Hao ; Deng, Fei: A Security Evaluation Method Based on STRIDE Model for Web Service. In: *2010 2nd International Workshop on Intelligent Systems and Applications*, 2010, S. 1–5

[17] Kang, Myong H. ; Park, Joon S. ; Froscher, Judith N.: Access control mechanisms for inter-organizational workflow. In: *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*. New York, NY, USA : Association for Computing Machinery, 2001 (SACMAT '01), S. 66–74. – URL https://doi.org/10.1145/373256.373266. – ISBN 1581133502

[18] Khan, Rafiullah ; McLaughlin, Kieran ; Laverty, David ; Sezer, Sakir: STRIDE-based threat modeling for cyber-physical systems. In: *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, S. 1–6

[19] Kindervag, John: Applying zero trust to the extended enterprise. In: *Forrester Research, Cambridge, MA, Rep. E-RES60253* (2011), S. 1–8

[20] Klein, Dave: Micro-segmentation: securing complex cloud environments. In: *Network Security* 2019 (2019), Nr. 3, S. 6–10

[21] Luciano, Dennis ; Prichett, Gordon: Cryptology: From Caesar ciphers to public-key cryptosystems. In: *The College Mathematics Journal* 18 (1987), Nr. 1, S. 2–17

[22] Mendelsohn, Charles J.: Blaise de Vigenère and the "Chiffre Carré". In: *Proceedings of the American Philosophical Society* 82 (1940), Nr. 2, S. 103–129. – URL http://www.jstor.org/stable/985011. – Zugriffsdatum: 2025-03-04. – ISSN 0003049X

[23] The NIST Cybersecurity Framework 2.0 / National Institute of Standards and Technology. Februar 2024. – Standard

[24] Ometov, Aleksandr ; Bezzateev, Sergey ; Mäkitalo, Niko ; Andreev, Sergey ; Mikkonen, Tommi ; Koucheryavy, Yevgeni: Multi-factor authentication: A survey. In: *Cryptography* 2 (2018), Nr. 1, S. 1

[25] Parker, Donn B.: *Fighting computer crime: A new framework for protecting information.* John Wiley & Sons, Inc., 1998

[26] Rajesh, P ; Alam, Mansoor ; Tahernezhadi, Mansour ; Monika, A ; Chanakya, Gm: Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework. In: *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*, 2022, S. 4–12

[27] Samonas, Spyridon ; Coss, David: The CIA strikes back: Redefining confidentiality, integrity and availability in security. In: *Journal of Information System Security* 10 (2014), Nr. 3

[28] Schneider, Fred B.: Least privilege and more. In: *IEEE Security & Privacy* 1 (2003), Nr. 5, S. 55–59

[29] Sheikh, Nabeel ; Pawar, Mayur ; Lawrence, Victor: Zero trust using network micro segmentation. In: *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* IEEE (Veranst.), 2021, S. 1–6

[30] Shore, Malcolm ; Zeadally, Sherali ; Keshariya, Astha: Zero trust: the what, how, why, and when. In: *Computer* 54 (2021), Nr. 11, S. 26–35

[31] Strom, Blake E. ; Applebaum, Andy ; Miller, Doug P. ; Nickels, Kathryn C. ; Pennington, Adam G. ; Thomas, Cody B.: Mitre att&ck: Design and philosophy. In: *Technical report.* The MITRE Corporation, 2018

Erklärung zur selbstständigen Bearbeitung

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort Datum Unterschrift im Original