An Evaluation of Potential Attack Surfaces Based on Attack Tree Modelling and Risk Matrix Applied to Self-Sovereign Identity

Nitin Naik, Paul Grace, Paul Jenkins, Kshirasagar Naik, Jingping Song

PII: S0167-4048(22)00202-4
DOI: https://doi.org/10.1016/j.cose.2022.102808
Reference: COSE 102808

To appear in: *Computers & Security*

Received date: 8 September 2021
Revised date: 23 April 2022
Accepted date: 17 June 2022

Please cite this article as: Nitin Naik, Paul Grace, Paul Jenkins, Kshirasagar Naik, Jingping Song, An Evaluation of Potential Attack Surfaces Based on Attack Tree Modelling and Risk Matrix Applied to Self-Sovereign Identity, *Computers & Security* (2022), doi: https://doi.org/10.1016/j.cose.2022.102808

An Evaluation of Potential Attack Surfaces Based on Attack Tree Modelling and Risk Matrix Applied to Self-Sovereign Identity

Nitin Naik[a,*], Paul Grace[a], Paul Jenkins[b], Kshirasagar Naik[c] and Jingping Song[d]

[a] School of Informatics and Digital Engineering, Aston University, Birmingham, United Kingdom
[b] Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, United Kingdom
[c] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
[d] Software College, Northeastern University, Shenyang, China

ARTICLE INFO

Keywords:
Attack Tree Model
Risk Matrix Model
Digital Identity
Self-Sovereign Identity
SSI
Identity Management System
Decentralized IDentifier
DID
Verifiable Credential
Distributed Ledger Technology
Blockchain
Faking Identity
Identity Theft
Distributed Denial of Service
Lockheed Martin's Cyber Kill Chain
MITRE ATT&CK Framework
Diamond Model of Intrusion Analysis

ABSTRACT

Self-Sovereign Identity (SSI) empowers users to govern their digital identity and personal data. This approach has changed the identity paradigm where users become the central governor of their identity; hence the rapid growth of the SSI model. Utilizing the security and privacy properties of blockchain, together with other security technologies, SSI purports to provide a robust security and privacy service. However, this governing power for users comes with a greater accountability and security risk, as not all users are capable or trained in its use and therefore in its efficient application. This trade-off requires a systematic evaluation of potential attacks on the SSI system and their security risks. Hitherto, there have been no noteworthy research studies performed to evaluate potential attacks on the SSI system and their security risks. This paper proposes an easy, efficient and economical approach to perform an evaluation of potential attacks on the SSI system and their security risks. This approach utilises a combination of an attack tree and risk matrix models to perform this evaluation of potential attacks and their security risks, in addition to outlining a systematic approach including describing the system architecture and determining its assets in order to perform this evaluation of potential attacks and their security risks. This evaluation work has identified three potential attacks on the SSI system: faking identity, identity theft and distributed denial of service attacks, and performed their security risk evaluation utilising the proposed approach. Finally, this paper has proposed several mitigation strategies for the three evaluated attacks on the SSI system. This proposed evaluation approach is a systematic and generalised approach for evaluating attacks and their security risks, and can be applied to any other IT system.

1. Introduction

1.1. Research Motivations

An Identity Management (IDM) model combines policies and technologies to enable the governance of digital identity (Moyle, 2021). Most IDM models were developed based on the necessity of organisations rather than users. However, Self-Sovereign Identity (SSI) is an emerging IDM, which is a user-centric and user-governed approach to digital identity that empowers users to govern their digital identity and personal data in a decentralized manner (Allen, 2016). This SSI approach is developed around the user who is the sole governor of their own identity and accountable for all identity related operations and decisions (Allen, 2016). However, this governing power to users comes with a greater accountability and security risk, as not all users are able to manage their identity efficiently (Naik and Jenkins, 2020b). This trade-off requires a systematic evaluation of potential attacks to the SSI system and their security risks to determine the possible mitigation strategies for preventing those attacks.

1.2. Principle of the Proposed Approach

Evaluating potential attacks on any IT system and their security risks is crucial to understand its vulnerabilities and determine the mitigation strategies to provide robust security for preventing those attacks. Several attack modelling techniques have been utilised when evaluating potential attacks and their risks such as Lockheed Martin's Cyber Kill Chain (LockheedMartin.com, 2011), MITRE ATT&CK Framework (MITRE.org, 2021), Diamond Model (Caltagirone, Pendergast and Betz, 2013), Attack Tree (Weiss, 1991; Salter, Saydjari, Schneier and Wallner, 1998; Schneier, 1999) and Attack Graph (Dacier, 1994; Dacier and Deswarte, 1994; Dacier, Deswarte and Kaâniche, 1996; Swiler, Phillips and Gaylor, 1998). All these attack modelling techniques have their own strengths and limitations and suitable for different types of attack analysis. Additionally, most of these techniques are focused on attackers' goals, actions, and methods for exploiting vulnerabilities; however, very little focus is given to the risk analysis and assessment aspect of an investigation (Korolov and Myers, 2018, November 15; CyCraftTechnology, 2020, July 1). Risk analysis is an important process in project management, and several risk management models are utilised for it such as Delphi Schedule Risk Assessment (Campanis, 1997), Decision Tree Analysis (Hulett, 2006), SWIFT Analysis, Bow-Tie Analysis and Risk Matrix; notwithstanding this, the majority of these models are developed for an organisational or business risk analysis, and not specifically for the attack risk analysis purpose (Cox Jr(2008), Tony). Though some models can be easily adapted for conducting an attack risk analysis (Julian, 2011).

Based on the comparative analysis of these two categories

[*] Corresponding author
n.naik1@aston.ac.uk (N. Naik)
ORCID(s): 0000-0002-0659-9646 (N. Naik)

of attack models and risk models, an attack tree modelling technique is selected for attack analysis and a risk matrix model is selected for attack risk analysis. Both selected methods are easy, efficient and economical methods and more importantly, they can be combined to apply as an integrated approach in the evaluation of potential attacks on any IT system and their security risks. An attack tree is a systematic and illustrative method for describing an attack on a system for analysing its various aspects. Where potential attacks against a system are represented in a tree structure, with the attack goal is being represented as the root node and different methods or actions of achieving the attack goal as leaf nodes (Schneier, 1999). An attack tree method is a graphical, efficient and economical method used to perform an analysis of potential attacks on any IT system as it does not require significant resources and expertise. This attack tree analysis outcome can be further utilised for the security risk analysis of attacks utilising the risk matrix model to evaluate the potential security risk of each attack. This combination of an attack tree model and risk matrix model offers a simple and efficient way of performing an analysis of attacks on any IT system and their security risks.

1.3. Main Contributions

The paper has several significant contributions in the field of evaluating attacks and their risks on an IT system and identity management system, and in particular the SSI system. The main contributions of the research work performed in the paper are as follows:

- This paper has proposed an approach for evaluating potential attacks on the SSI system and their security risks utilising a combination of an attack tree model and risk matrix model.
- The proposed attack risk evaluation approach outlines the step-by-step procedure to perform an attack illustration and risk analysis for the SSI system.
- This attack risk evaluation work has identified three potential attacks on the SSI system: the faking identity, identity theft and distributed denial of service attacks, and carried out the security risk evaluation utilising the proposed approach.
- Based on the evaluation of the three potential attacks on the SSI system and their security risks, several mitigation strategies are proposed for preventing these three evaluated attacks on the SSI system.
- The proposed attack risk evaluation approach is easy, efficient and economical approach due to the benefits of its underlying attack tree model and risk matrix model.
- The proposed attack risk evaluation approach is a systematic and generalised approach for evaluating attacks and their security risks, and can be applied to any other IT system.

1.4. Content Organisation

The rest of the paper is structured as follows. Section 2 describes the self-sovereign identity model, attack tree model and risk matrix model. Section 3 proposes the attack risk evaluation approach for evaluating potential attacks on the SSI system and their security risks, and proposing their mitigations. Section 4 presents an application of the propose attack tree based risk analysis method and comparative analysis with other attack modelling techniques. Section 5 concludes the proposed attack risk evaluation approach and highlights the outcomes of the evaluation of potential attacks on the SSI system and their risks for facilitating their mitigations.

2. Technical Background

2.1. Self-Sovereign Identity (SSI)

Self-sovereign identity (SSI) is a standard framework used in digital identity for providing sovereignty with respect to the digital identity and personal data (Naik and Jenkins, 2020a; Sovrin.org, 2018b). In other words, self-sovereign identity is a sovereign, enduring, decentralized, and portable digital identity for any real world entity, that enables its owner to obtain various services in the digital world in a secure, privacy-protected, trusted and self-governed way (Naik and Jenkins, 2020c). SSI is enhancing the internet ideology of greater sovereignty in identity management and access control arenas, by offering greater freedom and personal autonomy to identity owners (Naik and Jenkins, 2021a). This sovereignty includes all aspects and activities related to their identity and personal data, wherein identity owners store their personal data in digital wallets at their own devices. This decentralization process is implemented through the use of blockchain technology, which enables the SSI system to permit users to perform operations independently through the use of technology without requiring the need or approval from any central authority or service provider. Every individual holding an identity in the SSI system, is in complete control of this identity, thus, it is named as *self-sovereign* identity (Sovrin.org, 2018b).

SSI not only empowers identity owners, but also makes the identity management process very efficient and less onerous for organisations. It accomplishes this by permitting identity owners to store personal data on their own device, allowing organisations to minimise their various data management issues related to storage, cost, security, privacy and bureaucracy (Tykn.tech, 2021). For example, any breach, loss or theft of personal data may result in significant lawsuits and fines for an organisation (Tykn.tech, 2021). Therefore, minimising data management activities and focusing on the essential identity management tasks, increases the efficiency of overall processes of issuing and verifying identity.

There are three key roles in the SSI ecosystem *Issuer, Holder* and *Verifier* as shown in Fig. 1. An issuer is a trusted entity who issues credentials to holders. A holder owns an identity and obtains desired credentials from the issuer, holds in their digital wallet and presents it to the verifier for its

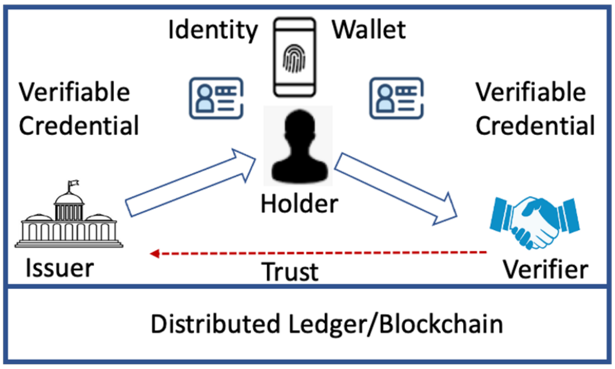


Figure 1: Self-Sovereign Identity Ecosystem

verification as and when required. A verifier is normally a service provider who requests credentials from a holder and verifies this through a blockchain enabled trust relationship between the issuer and verifier. There are three main pillars of SSI: a blockchain, Decentralized IDentifier (DID) and Verifiable Credential (VC).

A blockchain or distributed ledger is used to establish a trust relationship in the identity management process without requiring any trusted third party to establish the trust relationship as was the case in previous identity management systems. A Decentralized IDentifier (DID) is the core component of the SSI framework, which is a permanent, universally unique identifier linked to an identity that can be created independently of any organisation or service provider with full control given to its owner (W3C, 2019; Sovrin.org, 2018a). A Verifiable Credential (VC) is a tamper-evident and privacy-preserving credential made by an issuer (Tykn.tech, 2021). This verifiable credential is linked with the DID of an identity owner (W3C, 2019). The validity of the issuer can be verified by their digital signature and the authenticity of the issuer's digital signature can further be verified through the issuer's public DID on the blockchain (Tykn.tech, 2021).

2.2. Attack Tree Model

An attack tree is a systematic and illustrative method of describing an attack on a system and analysing its various aspects. Where potential attacks against a system are represented in a tree structure, with the attack goal is being represented as the root node and different methods or actions of achieving the attack goal as leaf nodes (Schneier, 1999). An attack tree method is an efficient and economical method to perform an analysis for potential attacks on any IT system, as it does not require significant resources and a fully implemented IT system (Jhawar, Kordy, Mauw, Radomirović and Trujillo-Rasua, 2015). In this research work, the attack tree structure is designed in such a way where each attack tree comprises a root node representing the attack goal, with several levels of sub-nodes representing attack vectors to perform that attack, and finally, leaf nodes representing an atomic action exploiting a vulnerability to achieve the attack goal as shown in Fig. 2. The different levels of the tree are structured and connected using two main operators: conjunction (denoted as AND) and disjunction (denoted as OR). The AND relationship represents that all child nodes must need to perform their actions in order to achieve the action of the parent node; and the OR relationship represents that any one child node needs to perform their action in order to achieve the action of the parent node. The attack vector and vulnerability can have multiple levels depending on the specific attack scenario. In attack tree diagrams, the AND relationship should be indicated, whereas OR relationship is normally a default relationship and does not require explicit indication.

The attack tree enables security analysts to implement a process where different stakeholders with different backgrounds and skills provide their feedback to help analyse potential attacks and facilitate their mitigations. The attack tree method can be used to perform various types of attack analysis depending on the types of attack trees and their connecting operators. For example, an attack tree utilising sequential AND operator (denoted as SAND) can be used to analyse time-dependent attacks by describing sequential nodes as conjunctive nodes with a notion of progress of time (Arnold, Hermanns, Pulungan and Stoelinga, 2014). Similarly, an attack tree utilising sequential AND operator can also be used to perform risk analysis with conditional probabilities (Jhawar et al., 2015; Jiang, Luo and Wang, 2012). Another attack tree utilising ordered AND operator (denoted as OAND) can be used to represent temporal dependencies between various attack components (Camtepe and Yener, 2007). This attack tree method offers several benefits over other attack analysis methods such as it is an illustrative, understandable, economical, efficient, customizable, scalable, reusable method and facilitates mitigations (Schneier, 1999; Amenaza.com, 2021).

2.3. Risk Matrix Model

A risk assessment matrix is a visual tool that depicts the potential risks affecting a system. The risk assessment matrix determines the risk based on two intersecting elements: the probability that the risk event (here, an attack) will occur, and the potential severity of harm that the risk event will have on the system (Auditboard.com, 2021). Depending on the probability of an attack and severity of an attack, the attack risk can be classified as low, medium and high as shown in Fig. 3, or in more granular level depending on the requirement of a specific risk analysis. A risk assessment matrix is a popular tool used in project management and also known as a probability matrix, or severity matrix (Markovic, 2019, November 8). In this research work, utilising the risk assessment matrix in Fig. 3 and Equation 1, security analysts can calculate and prioritise different attack risks.

$$Risk = Probability \quad X \quad Severity \tag{1}$$

2.4. Lockheed Martin's Cyber Kill Chain (CKC) and Its Limitations

The Cyber Kill Chain (CKC) is a phase-based attack model to assist security experts understand the breakdown

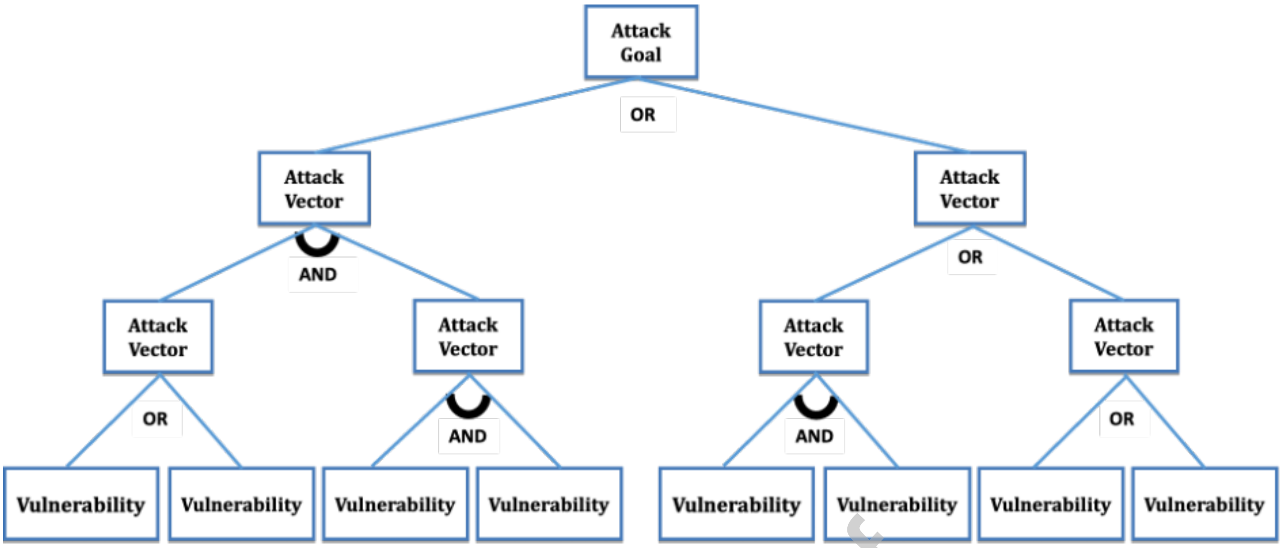
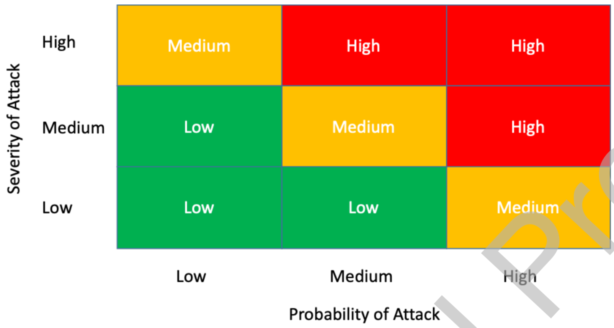


Figure 2: Template of an Attack Tree for an Attack Analysis



Severity of Attack	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

Probability of Attack

Figure 3: Risk Assessment Matrix for an Attack Analysis

of an externally originated attack into seven different steps (LockheedMartin.com, 2011). It identifies a sequence of attack stages: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives (see Fig. 4). It is developed by Lockheed-Martin, which is co-opted from the military term kill-chain used to break down the structure of an attack (CyCraftTechnology, 2020, July 1). The CKC concept is that a defender needs only to disrupt one attacking stage in the chain to stop that attack.

The CKC model applies the century-old military kill chain model to a cyberattack, however, it has several security gaps as it remains unmodified since its creation (Thecyphere.com, 2022). The CKC model works well to protect against malware and Advanced Persistent Threats (APTs) (Cybotsai.com, 2021). However, these are not the only security risks identified since its inception. Additionally, the cyber kill chain model does not account for sophisticated and modern methods that attackers currently use to attack an environment. Moreover, an analysis was conducted in 2013, wherein the US senate discovered that the different stages of the protocol could not detect an attacks' progression (Thecyphere.com, 2022). The CKC model does not account for iterative approaches or combinations of Tactics, Techniques and Procedures (TTP) that adapt according to the encountered environment (Idealintegrations.net, 2019).

2.5. MITRE ATT&CK Framework of Intrusion Analysis and Its Limitations

MITRE ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge, which is a framework created by MITRE in 2013 (MITRE.org, 2021). This model is a globally accessible knowledge base of adversarial tactics and techniques based on real-world observations, reflecting the various phases of an adversary's attack lifecycle (see Fig. 5) and the platforms they are known to target (Cybotsai.com, 2021). ATT&CK comprises a structured list of known adversary behaviours that have been compiled into tactics and techniques, expressed as a series of matrices (MITRE.org, 2021). The tactics and techniques abstraction in the model provide a common taxonomy of individual adversary actions understood by both offensive and defensive sides of cybersecurity (CyCraftTechnology, 2020, July 1). Furthermore, it provides an appropriate level of categorization for adversary action and specific mechanisms of defending against it (Cybotsai.com, 2021). 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 (MITRE.org, 2021).

The main problem with ATT&CK is that hierarchical structures are missing or inconsistent (Ruef and Schneider, 2021). The identifiers of both tactics and techniques are also not traceable, lacking linearity, grouping or hierarchy (Ruef and Schneider, 2021). This means that these techniques cannot be assigned exclusively to individual tactics and are often used by multiple tactics and across multiple phases of

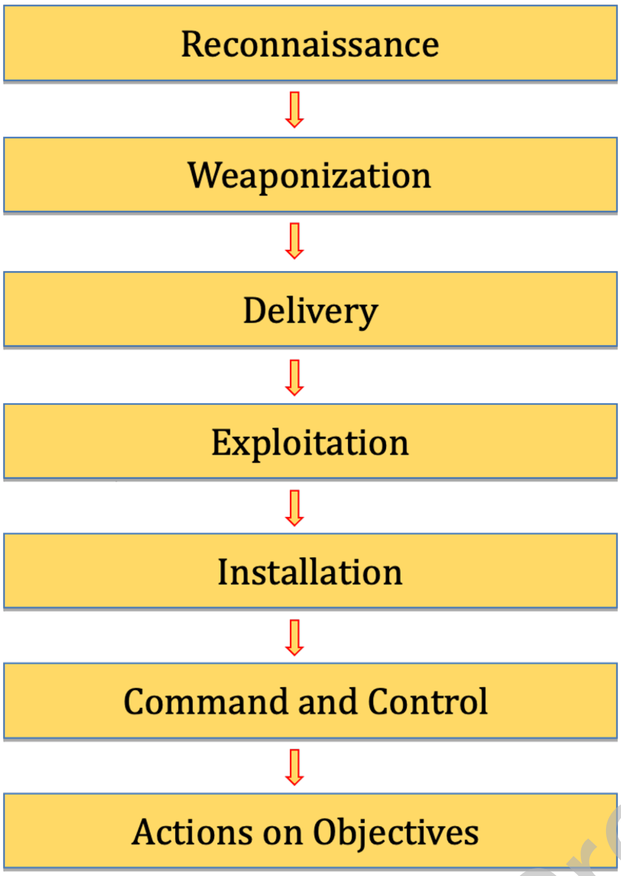


Figure 4: Stages of Lockheed Martin's Cyber Kill Chain (CKC) of Intrusion Analysis

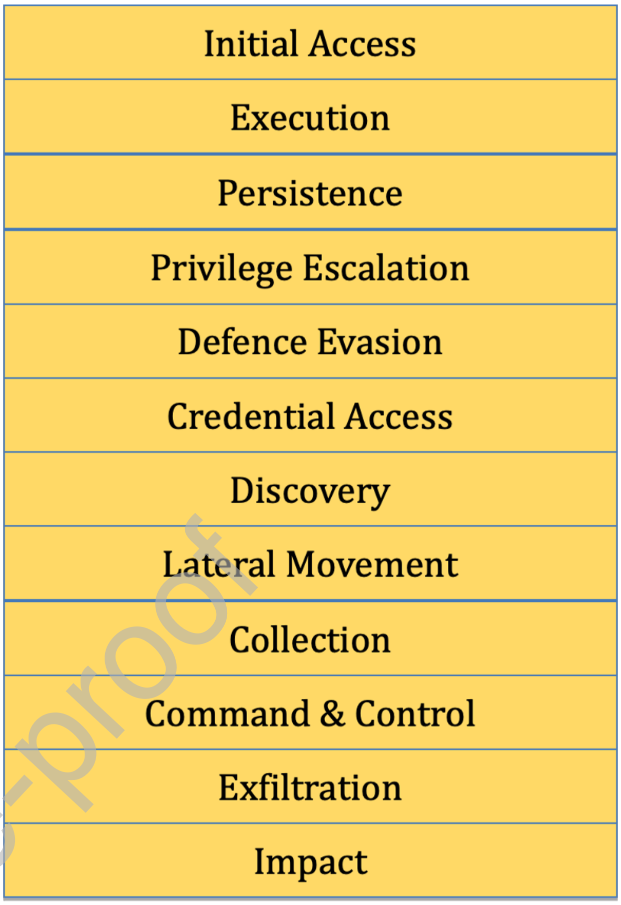


Figure 5: Various Tactics of MITRE ATT&CK Framework of Intrusion Analysis

an attack (Cybotsai.com, 2021). This method utilises some generic definitions of attacks, whereby some attacks are considered the same, as is the case of network DoS, which can be caused through bandwidth overload by excessive network connections, or by data overload; however, this is not distinguished by the method (Ruef and Schneider, 2021). Moreover, sub-techniques are specific, however, they are incomplete, inconsistent, and narrowly defined.

2.6. Diamond Model of Intrusion Analysis and Its Limitations

The Diamond model emphasizes the relationships and characteristics of an attack based on its four core components: adversary, infrastructure, capability, and victim (Caltagirone et al., 2013). This model explains how an *adversary* exploits a *capability* over an *infrastructure* against a *victim* (see Fig. 6) (Socradar.io, 2022). These four main components of an attack are the vertices of the diamond that gives this model its name. It further defines additional meta-features to support higher-level constructs and applies measurement, testability, and repeatability to provide a more comprehensive scientific method of analysis. This model was released by the US Department of Defense in 2013 (Caltagirone et al., 2013). The diamond model is a cognitive model as well as a set of mathematical techniques (Socradar.io, 2022). The cognitive model allows security experts to organize large amounts of interrelated logic, whereas a set of mathematical techniques enables them to enhance strategic decision-making and analytical workflow against the adversary (Socradar.io, 2022).

While the Diamond Model has a simple appearance, it can become very complicated and in-depth quite quickly. The diamond of a threat actor is not static but is in constant flux as attackers alter their infrastructure and/or capabilities frequently (CyCraftTechnology, 2020, July 1). An attacker's capabilities require significant effort to build and are relatively static, however, an attacker's infrastructure can be changed easily, which can be used to link different attack campaigns together and to a particular adversary (Poston, 2020, November 10). This infrastructure replacement can lead to higher false positives as several different actors can use the same infrastructure, meaning that as an attribution tool it is less than ideal, due to the cognitive and mathematical techniques involved in the model (Poston, 2020, November 10). Therefore, to maximise the efficiency of this technique, security experts are required to be highly skilled in these techniques (Cybotsai.com, 2021).

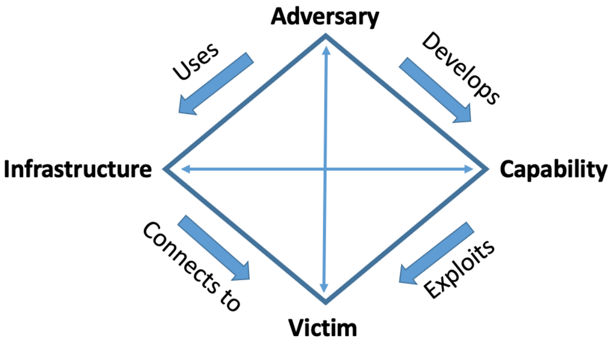


Figure 6: Diamond Model of Intrusion Analysis

Table 1
Entities and Assets in the SSI System

SSI Entity	SSI Asset	Description
SSI Network	Node	Multiple SSI network nodes.
	Agent	Same software agent on all the SSI network nodes.
	Data	Governance and regulatory data.
Blockchain	Node	Multiple blockchain nodes.
	Agent	Same software agent on all the blockchain nodes.
	Data	Same ledger data on all the nodes.
Issuer	Node	Multiple issuer nodes.
	Agent	Same software agent on all the issuer nodes.
	Data	Credential data on all the nodes.
Holder	Node	Individual holder nodes.
	Agent	Same software agent on all the individual holder nodes.
	Data	Personal data in wallet.
Verifier	Node	Multiple verifier nodes.
	Agent	Same software agent on all the verifier nodes.
	Data	Verification data on all the nodes.

Note: Above description is the generalization of the SSI system and basis of an evaluation of potential attacks on the SSI system and their security risks in the paper, however, it may differ for some SSI systems.

3. Proposed Attack Tree Based Risk Analysis Method for the SSI System

In this section, an attack risk evaluation approach is proposed to perform an evaluation of potential attacks on the SSI system and their risks for facilitating their mitigations. This proposed approach consists of several steps to perform the complete attack risk evaluation as shown in Fig. 7.

3.1. Describe the SSI System Architecture

In the preliminary step of this attack risk evaluation approach, the system architecture and functionality of the system should be described, this should include all the software components, hardware components, data stores, and the flow of data within the system. The SSI system architecture comprises a blockchain based decentralized SSI network; three key roles issuer, holder and verifier; data wallets; software agents and network nodes as shown in Fig. 8. The blockchain based decentralized SSI network comprises several nodes required to perform identity related operations and validation of transactions. These network nodes only store public data such as credential definitions, public decentralized identifiers (DIDs), schema definitions, and revocation registries; but not any personal and sensitive data (Naik and Jenkins, 2020d, 2021b). Software agents are used to perform specific functionalities on various network nodes based on specific roles and requirements. Data wallets are the main data stores in the SSI system, which store personal data and credentials for holders. There are two main data flow in the SSI system in addition to the data flow through the blockchain: first, between an issuer and holder for the issuance of credentials, and second, between a verifier and holder for the verification of credentials as shown in Fig. 8.

3.2. Determine Assets of the SSI System

Determining the important assets of the underlying system is the crucial step of the attack risk evaluation approach for identifying the possible target assets of attackers or requiring the utmost protection of these assets. Depending on the specific requirements of the system, the relevant assets can be determined as an asset set for the attack risk evaluation approach, which may include all the system assets or selected assets. The assets can also be classified into main categories for the purpose of an efficient analysis such as software assets, hardware assets and data assets.

The architecture diagram of the SSI system in Fig. 8 outlines the key assets that compose an SSI system. The first type of assets are software agents that perform the functionality of the SSI network and various network nodes to achieve decentralised identity management. Secondly, there are network nodes, i.e., computational devices that host the software agents; these are instrumented with network connections to allow software agents to run and data to be exchanged between remote nodes. Thirdly, data stores (here mainly wallets) that store the decentralised credential information and personal data of holders. These are the main assets of the SSI system which are considered as the prime target of attackers for this attack risk evaluation approach.

3.3. Identify Potential Attacks on the SSI System

Once all the necessary assets, stakeholders, and data flow activities are identified, then potential attacks on them can be

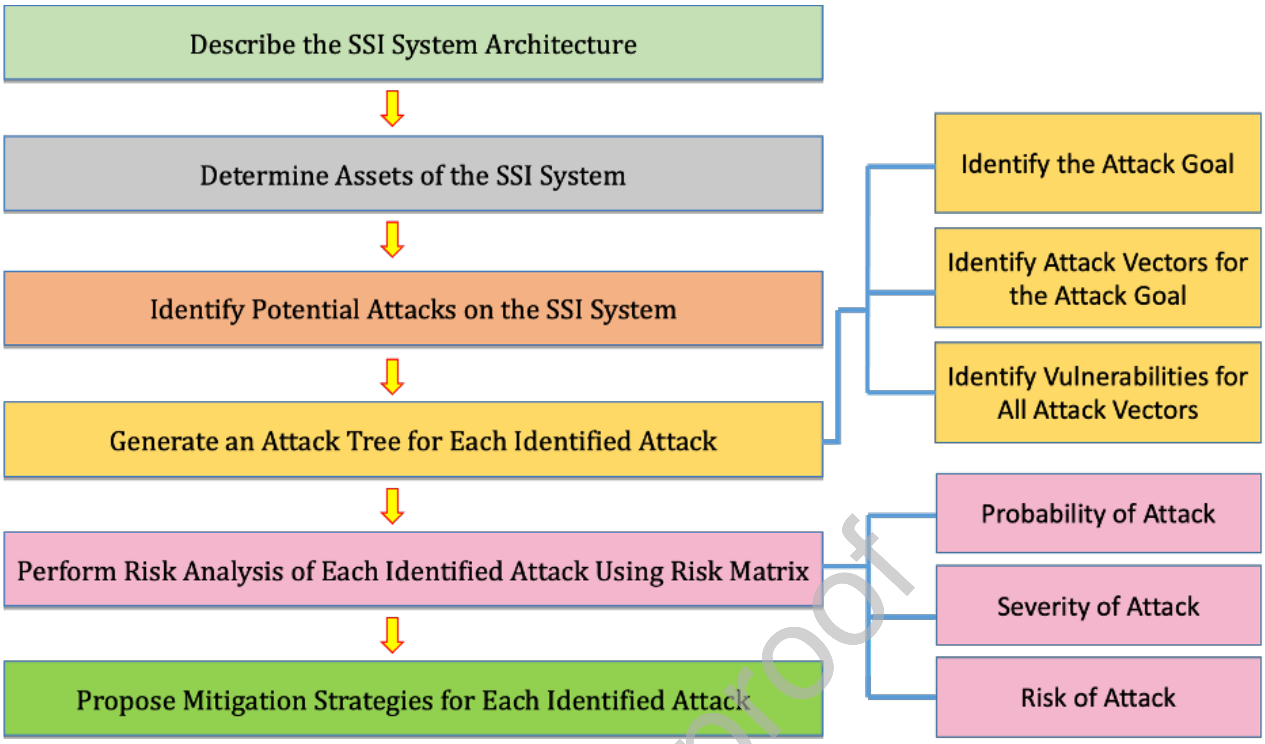

Describe the SSI System Architecture
Determine Assets of the SSI System
Identify Potential Attacks on the SSI System
Generate an Attack Tree for Each Identified Attack
Perform Risk Analysis of Each Identified Attack Using Risk Matrix
Propose Mitigation Strategies for Each Identified Attack
Identify the Attack Goal
Identify Attack Vectors for the Attack Goal
Identify Vulnerabilities for All Attack Vectors
Probability of Attack
Severity of Attack
Risk of Attack

Figure 7: Steps of the Proposed Attack Risk Evaluation Approach for the SSI System Based on Attack Tree Modelling and Risk Matrix

identified. The potential attacks can be selected for the attack risk evaluation approach based on the well-known attacks in the specific application area or available historical/existing data, and the specific security and privacy requirement of the specific system. The SSI system offers several security and privacy features based on blockchain, Zero Knowledge Proofs (ZKPs) and various regulations to resolve most privacy issues and protect from several security threats (Naik and Jenkins, 2020d; Naik, Grace and Jenkins, 2021); however, it is still vulnerable to several attacks due to the greater accountability of users. In this research work, based on the preliminary research, three attacks faking identity, identity theft and distributed denial of service are prioritised for the attack risk evaluation approach to demonstrate the successful development of the proposed approach (Naik and Jenkins, 2017; Naik et al., 2021; Kazarian, 2016, July 22; Cohen, 2019, October 29; Okta.com, 2021; Hayes, 2020, September 29). Nonetheless, other attacks can also be selected and prioritised depending on the specific analysis requirements, and this proposed method can be adapted for those identified attacks.

3.3.1. Faking Identity Attack

A malicious holder/user can exploit vulnerabilities in the SSI system to obtain fake credentials and thus gain unauthorised access to services within the SSI system.

3.3.2. Identity Theft Attack

An attacker can exploit vulnerabilities in the SSI system to access personal and confidential data in a wallet. A user may allow credentials to be given away without understanding the potential privacy threats. While the user may believe they are anonymous, linking attacks may collect data from credential presentations to re-identify individuals using background data. Common personal data may be collected across different pseudonyms (DIDs), e.g., matching sets of data in verifiable credentials may also be used to link pseudonyms.

3.3.3. Distributed Denial of Service Attack

An attacker can exploit vulnerabilities in the SSI system to reduce the availability of the identity services within the SSI system, for example, by disrupting the availability of hosts including issuer, holder or verifier hosts and agents, and distributed ledger hosts and agents.

3.4. Generate an Attack Tree for Each Identified Attack

Attack trees can be generated in different ways; here, the formalisation of attack trees is based on the attack tree generation approach initially described by Bruce Schneier in (Schneier, 1999) and explained in the previous section. This attack tree provides an opportunity from an attacker's viewpoint to analyse different possible ways (i.e., from each leaf node to the root node as shown in Fig. 2) to obtain a desired attack goal and the ease or difficulty of achieving this attack goal. Different ways may provide different levels of ease or difficulty in achieving the attack goal. Each way is analysed to assess the probability of the attack through that particular pathway, which may help to assess the risk of an attack based on each attack vector and propose its

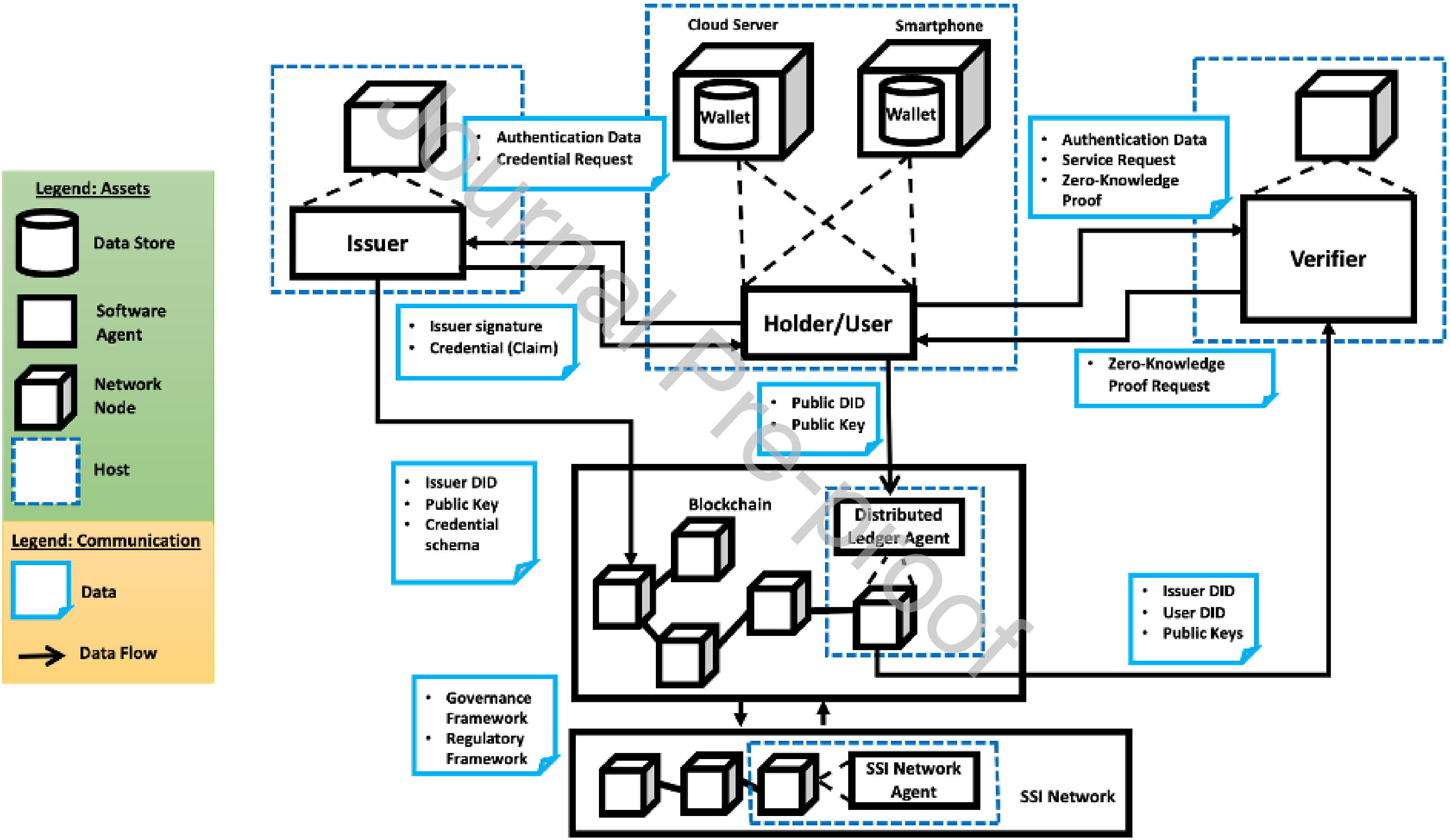


Figure 8: SSI System Architecture Illustrating its Various Entities, Assets and Data Flows

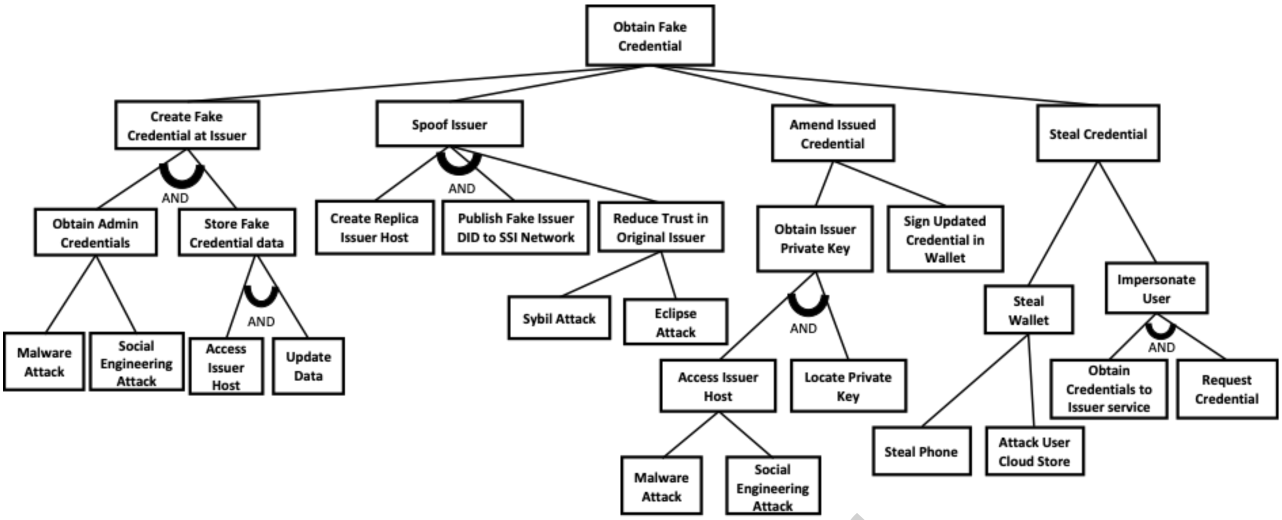


Figure 9: An Attack Tree to Evaluate Faking Identity Attack and its Associated Risks in the SSI System

mitigation strategies for preventing the attack. Attack trees can be generated manually or automatically using various available attack tree generation tools. In this evaluation, three potential attacks are already identified for the attack tree analysis: the fake identity, identity theft and denial of service attacks. Therefore, the three different attack trees will be generated and analysed for these three identified attacks.

3.4.1. *Attack Tree of Faking Identity Attack*

Fig. 9 illustrates a generated attack tree for the potential faking identity attack, where the goal of a malicious user is to obtain a fake credential using a number of different identified attack vectors that exploit specific vulnerabilities of assets within the SSI architecture. Here, each illustrated path (i.e., from each leaf node to the root node) to obtain a fake credential needs to be evaluated for its potential success and severity.

For example, an attacker can spoof the issuer, creating an issuer service and agent that behaves in the same way as the authentic service, e.g., a spoof government driving license issuer. This will publish its DID and public key to the SSI network but must mislead the network into trusting that this is the authentic issuer. One approach would be an eclipse attack, where malicious nodes are inserted into the SSI network and the peer-to-peer network is manipulated to ensure that all connections from the authentic issuer host are connected to malicious nodes. In this attack, any publication of the DID and public key is not stored in the ledger, and hence the spoof issuer data is accepted instead. Other attack vector exploits vulnerabilities in the deployment infrastructure, e.g., access to network machines to obtain administrative credentials or private keys which can then be used to update credentials within a wallet. The credential can be updated and re-signed using a stolen key. Similarly, all the possible ways to perform this attack should be evaluated in order to assess its risks and derive conclusions.

3.4.2. *Attack Tree of Identity Theft Attack*

Fig. 10 illustrates a generated attack tree for the potential identity theft attack, where the goal of a malicious user is to obtain personal data using a number of different identified attack vectors that exploit specific vulnerabilities of assets within the SSI architecture. Here, each illustrated path (i.e., from each leaf node to the root node) to obtain personal data needs to be evaluated for its potential success and severity.

For example, an attacker or another stakeholder can access personal data they are not permitted to access, or the user has not consented to them. Vulnerabilities in the infrastructure assets, e.g., authentication weaknesses in network host potentially allow threats that access a personal wallet directly to obtain the personal data or credentials stored in the wallet. The SSI architecture and functionality is a target to exploit in order to attack personal data and credentials. The mechanism to verify credential claims can be exploited in the form of credential creep in order to collate personal data. A verifier request for more additional information than is needed to verify a claim. Repeated verifier requests can also be used to collect personal data and link them to the targeted user. Similarly, all the possible ways to perform this attack should be evaluated in order to assess its risks and derive conclusions.

3.4.3. *Attack Tree of Distributed Denial of Service Attack*

Fig. 11 illustrates a generated attack tree for the potential distributed denial of service attack, where the goal of a malicious user is to disrupt services of the SSI system using a number of different identified attack vectors that exploit specific vulnerabilities of assets within the SSI architecture. Here, each illustrated path (i.e., from each leaf node to the root node) to disrupt services of the SSI system requires evaluation for its potential success and severity.

For example, an attacker can deny services to any of the three main roles the issuer, holder/user or verifier by flood-

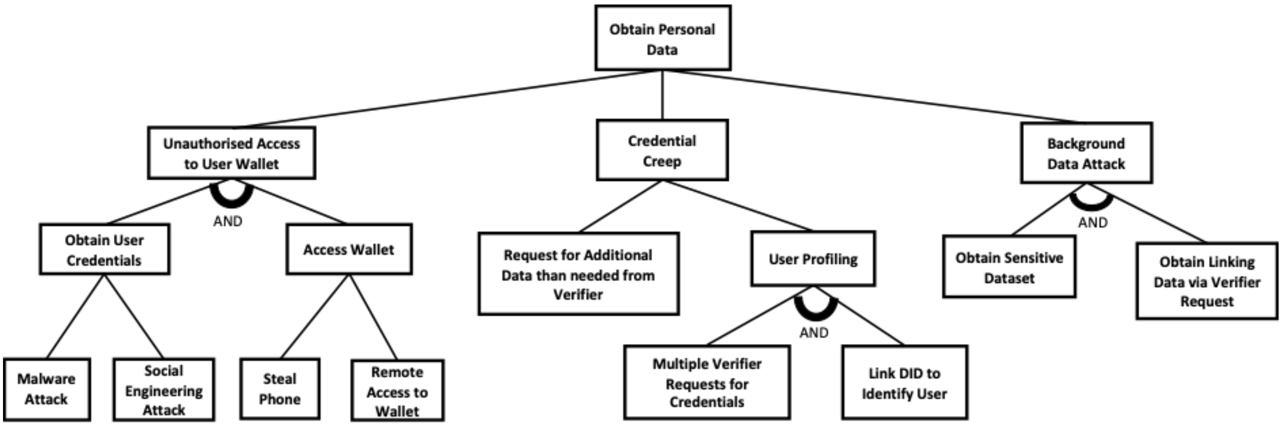

Obtain Personal Data
Unauthorised Access to User Wallet
AND
Credential Creep
Background Data Attack
AND
Obtain User Credentials
Access Wallet
Request for Additional Data than needed from Verifier
User Profiling
AND
Obtain Sensitive Dataset
Obtain Linking Data via Verifier Request
Malware Attack
Social Engineering Attack
Steal Phone
Remote Access to Wallet
Multiple Verifier Requests for Credentials
Link DID to Identify User

Figure 10: An Attack Tree to Evaluate Identity Theft Attack and its Associated Risks in the SSI System

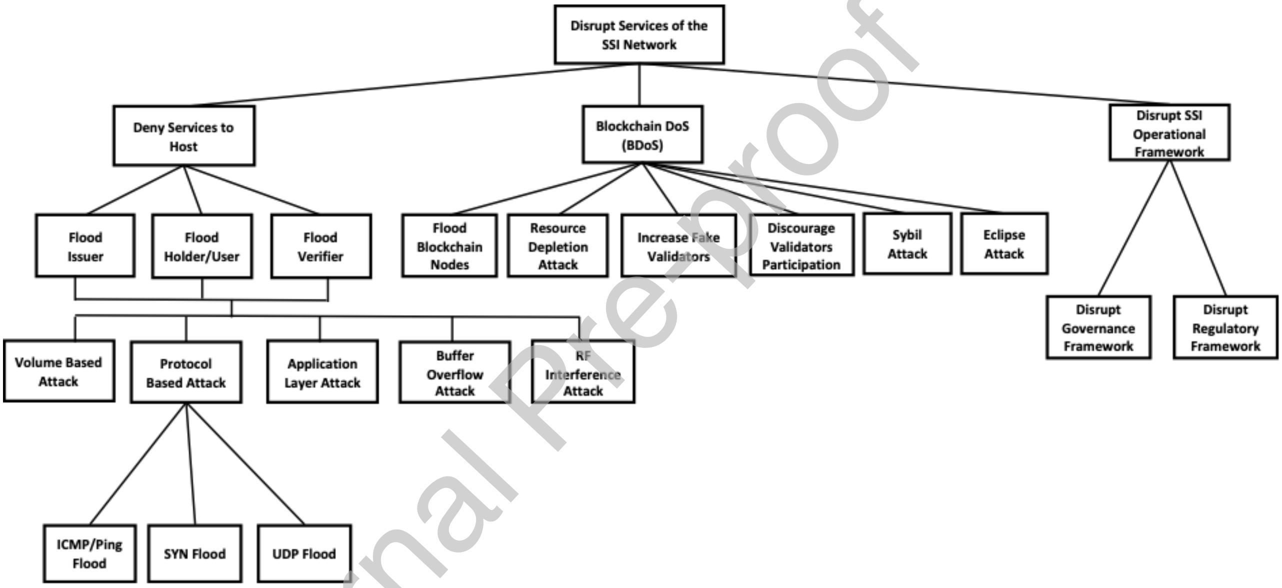


Figure 11: An Attack Tree to Evaluate Distributed Denial of Service Attack and its Associated Risks in the SSI System

ing network traffic towards them using different flooding methods. In particular, holders or users are more vulnerable than issuers and verifiers to this kind of attack due to their resource constrained devices and usually a lower level of protection from such attack. Another disruption of services is possible within the blockchain infrastructure using different attack vectors such as flooding blockchain nodes, resource depletion attack or disrupting its consensus process through fake validators or discouraging validators. Disruption of services in the SSI system is also possible by disrupting its operational framework either by disrupting its governance framework or regulatory framework. Similarly, all the possible ways to perform this attack should be evaluated in order to assess its risks and derive conclusions.

3.5. Risk Analysis of Each Identified Attack Using Risk Matrix

After generating an attack tree for each identified attack, the risk analysis of each attack is performed using a risk matrix model to analyse its potential attack risks with respect to various attack vectors and vulnerabilities to assess the various security aspects of the system. This attack risk analysis can be performed at an attack vector level or at a further granular level depending on the specific risk analysis requirement. In this attack risk analysis of the SSI system, based on the generated attack tree for each identified attack, the following questions can be answered for analysing the risk of each attack using a risk matrix model:

- What would be the probability of attack using each attack vector by an attacker?
- What would be the severity of attack using each attack vector?

- What would be the risk of attack based on its probability and severity using each attack vector?

The risk matrix model is required in answering the first two questions on the probability of attack and the severity of attack to automatically find the answer of the third question on the risk of attack. Answering the first two questions requires the selection of a specific evaluation criteria based on the chosen risk matrix model to determine the probability of attack, and severity of attack. In this attack risk analysis of the SSI system, a risk matrix comprising three levels *Low, Medium* and *High* is selected (see Fig. 3), therefore, all the attack risk assessment should be based these three levels. However, a different risk matrix comprising different levels can be chosen depending on the specific risk analysis requirement. Determining these three levels *Low, Medium* and *High* for the probability of attack and the severity of attack requires a thorough analysis of each corresponding attack tree and affected assets for each entity.

The probability of attack is based upon the difficulty of the attack being carried out successfully. This is dependent upon the ease of which the vulnerability can be exploited; for example, an attack exploiting an end-user is more likely to be successful than exploiting technical weaknesses in the SSI system, and would be considered as *High* probability of occurring. An attack requiring a technical exploit of a vulnerability of the issuer or verifier would be considered as *Medium* probability. An attack requiring multiple successful steps involving technical exploits of a vulnerability of the SSI system would be considered as *Low* probability.

The severity of attack is measured in terms of the amount of harm to the SSI system that occurs from the attack. For example, an attack that is a minor breach of a single user's privacy has much lower impact than a successful breach on an issuer or verifier that will impact many users and would be considered as *Low* severity. An attack that affected multiple individuals, issuers or verifiers would be considered as *Medium* severity. An attack that harmed the entire SSI network or blockchain would be considered as *High* severity.

Once both the probability of attack and severity of attack are calculated, the attack risk can be easily calculated based on the standard risk matrix model (see Fig. 3) and Equation 1 to assess the level of risk associated with each attack employing each attack vector. Here, the corresponding detailed analysis is performed for the probability of various attacks based on different assets corresponding to each entity, and their summary is presented in Table 2 to determine their specific levels. The similar detailed analysis is performed for the severity of various attacks based on different assets corresponding to each entity, and their summary is presented in Table 3 to determine their specific levels. Based on the corresponding probability and severity of each attack utilising each attack vectors, its risk is easily determined and illustrated as shown in Figs. 12 to 14.

3.5.1. *Risk Analysis of Faking Identity Attack*

Utilising the developed faking identity attack tree in Fig. 9, and generalised levels of the probability and severity of attacks related to each asset of each entity in Tables 2 and 3, a risk analysis is performed to determine the probability and severity of the faking identity attack based on each attack vector exploiting specific vulnerabilities, thus the risk of the faking identity attack which is shown in Fig. 12. For example, the create fake credential at issuer attack requires obtaining of administrative credentials, whose probability is medium; if successful, such an attack would impact many users associated with that particular issuer as trust in an issuer would be reduced, hence its severity is medium. This leads to a medium risk calculation result, and hence an important risk to mitigate.

3.5.2. *Risk Analysis of Identity Theft Attack*

Utilising the developed identity theft attack tree in Fig. 10, and generalised levels of the probability and severity of attacks related to each asset of each entity in Tables 2 and 3, a risk analysis is performed to determine the probability and severity of the identity theft attack based on each attack vector exploiting specific vulnerabilities, thus the risk of the identity theft attack which is shown in Fig. 13. For example, an attack such as credential creep requires a sophisticated manipulation of the use of Zero Knowledge Proof by the verifier/attacker, hence its probability is medium; if successful, it has the potential to collect personal data from a large number of individuals associated with that particular verifier, hence its severity is medium. This leads to a medium risk calculation result, and hence an important risk to mitigate.

3.5.3. *Risk Analysis of Distributed Denial of Service Attack*

Utilising the developed distributed denial of service attack tree in Fig. 11, and generalised levels of the probability and severity of attacks related to each asset of each entity in Tables 2 and 3, a risk analysis is performed to determine the probability and severity of the distributed denial of service attack based on each attack vector exploiting specific vulnerabilities, thus the risk of the distributed denial of service attack which is shown in Fig. 14. For example, an attack such as disrupting SSI operational framework requires to compromise nodes in the SSI network which is a difficult task for an attacker due to its robust security, hence its probability is low; however, if successful it will affect the entire SSI system and all of its stakeholders significantly, hence its severity is high. This leads to a medium risk calculation result, and hence an important risk to mitigate.

3.6. Propose Mitigation Strategies for Each Identified Attack

Table 4 shows the proposed mitigation strategies for the faking identity attack based on each individual attack vector and where its implementation is required. Here, the mitigations should be selected by developers according to their acceptance of the previously measured risk. For example, the steal credential attack is medium-risk and hence the developer of the SSI software agents and wallets should strongly consider deploying the multi-factor authentication control to remove this risk.

Table 2
Analysis of Probability of Attack on Different Assets of Entities in the SSI System

SSI Asset Category	Probability of Attack	Description	Justification
SSI Network (Agent, Node, Data)	Low	SSI network is the backbone of the SSI system, and it is expected that all necessary security techniques and technologies will be employed at the network to protect the SSI system against any attacks. Therefore, exploiting a vulnerability is very difficult.	Using the latest security standard in cryptography, blockchain and Zero Knowledge Proofs (ZKPs), the SSI Network allows for digital credentials to be securely and privately issued, controlled, managed, and shared. For example, in the Sovrin Network, users or identity owners requires credentials and biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data in a secure peer-to-peer model. It incorporates Privacy by Design and Privacy by Default practices such as pairwise-pseudonymous DIDs, off-chain private data, selective disclosure of data, minimising correlation of an identity owner, and Guardian and Delegate confidentiality. The Sovrin Network employs Zero-Knowledge Proof cryptography for credentials and its anonymous verification, therefore, identity owners are required to share only anonymous or minimum information for verification and maintain their anonymity. It employs a public permissioned blockchain, thus, inherits all the security properties of blockchain, and only trusted institutions known as Stewards can operate nodes. Sovrin Stewards are organizations that operate the network by running validator nodes which write to and read the Sovrin ledger.
Blockchain (Agent, Node, Data)	Low	Blockchain is used to established a trust relationship between stakeholders in the SSI system without relying on any central authority. It is inherently secure against many attacks due to its decentralized nature. Therefore, exploiting a vulnerability is very difficult.	Blockchain is based on principles of cryptography, decentralization and consensus, which produces a tamper-proof ledger of transactions to ensure trust in transactions. Blockchain technology enables decentralization through the participation of members across a distributed network. There is no single point of failure and a single user cannot change the record of transactions. The most suitable blockchain for SSI system is a public permissioned blockchain, which allows additional security measures for enhanced security. For example, the public permissioned blockchain Hyperledger Indy is the basis of the Sovrin Network, thus, only trusted institutions known as Stewards can operate nodes whilst partaking in the consensus process. It uses Hyperledger Ursa, a shared cryptographic library to provide secure and decentralized key management functionality. It employs a Plenum Byzantine Fault Tolerant Protocol which is a modified version of Redundant Byzantine Fault Tolerance (RBFT). The Indy Plenum consensus protocol uses Digitally Signed (DS) messages using CurveZMQ which differs from RBFT that uses Message Authentication Codes (MACs), this makes it a more secure protocol.
Issuer (Agent, Node, Data)	Medium	Issuer is a well-trusted organisation with necessary security arrangements in place. Therefore, exploiting a vulnerability is difficult.	Issuers are generally the established government organisations, banks, academic institutions, hospitals, who have already got a secured IT infrastructure in place with a team of security experts to ensure sufficient security measures for issuing credentials to a holder based on the definition provided by the W3C Verifiable Claims Working Group.
Holder (Agent, Node, Data)	High	Majority of holders are normally an ordinary identity user with minimum security arrangements in place. Therefore, exploiting a vulnerability is not difficult.	Each credential holder or identity owner has a digital wallet holding credentials containing certain information about that holder or identity owner, where the digital wallet is an app running on a smartphone, tablet, desktop, or other local device with minimum security arrangements in place on their personal device and may not be able to apply necessary security operations.
Verifier (Agent, Node, Data)	Medium	Verifier is a well-trusted organisation with necessary security arrangements in place. Therefore, exploiting a vulnerability is difficult.	Verifiers are generally the established government organisations, banks, academic institutions, hospitals, who have already got a secured IT infrastructure in place with a team of security experts to ensure sufficient security measures for verifying credentials from a holder based on the definition provided by the W3C Verifiable Claims Working Group.

Table 3
Analysis of Severity of Attack on Different Assets of Entities in the SSI System

SSI Asset	Severity of Attack	Description
SSI Network Node	Medium	SSI network is the backbone of the SSI system and responsible for its functioning, therefore, the severity of any attack on any node will be considered as high. However, depending on the decentralization of SSI network nodes and the number of nodes attacked, the severity will be considered from high to medium.
SSI Network Agent	High	It is mostly expected that the same software agent will be used on all the SSI network nodes, therefore, any attack on the SSI network agent will be considered as high.
SSI Network Data	High	SSI network data can exist in wide variety, however the SSI network does not store any personal data and credentials, and depending on the nature and amount of data affected by the attack will determine the severity of an attack. If the data is audit and historical data then the severity will be considered as medium, and if the data is related to the governance framework or regulatory framework then the severity will be considered as high.
Blockchain Node	Medium	An attack on a blockchain node may disrupt its service to the SSI system, however, its severity will be dependent on the nature of attack and number of node affected, therefore, the severity of an attack will be considered from high to medium.
Blockchain Agent	High	It is mostly expected that the same software agent will be used on all the nodes of the blockchain, therefore, any attack on the blockchain agent will be considered as high.
Blockchain Data	High	Blockchain is one of the most secure way to store and manage data, and any attack on blockchain data will affect the entire SSI system, therefore, the severity of the attack will be considered as high.
Issuer Node	Medium	An SSI network contains several issuers. Any issuer issues credentials to users, and an attack on it will affect to that issuer and its associated users, which will be significant, but it will not affect the entire SSI system, therefore the severity will be considered as medium.
Issuer Agent	High	If the same agent is used on all the issuers of the SSI system, then the severity will be considered as high. If separate issuer agents are used at different issuers then the attack may not affect all issuers and the severity will be considered as medium.
Issuer Data	Medium	An attack on any issuer data will affect to that issuer and its associated users, which will be significant, but it will not affect the entire SSI network, therefore the severity will be considered as medium.
Holder Node	Low	An SSI network contains numerous holders, and an attack on any holder node will not affect the entire SSI system significantly unless the attack targeted mass users, therefore, the severity of attack will be considered as low.
Holder Agent	High	As it is widely expected that the holder software agent is provided by the SSI system, and all holder nodes are using the same agent, therefore, the severity of an attack on the agent will be considered as high.
Holder Wallet	Low	If the attack on a wallet is due to any design and implementation vulnerability, then this will affect the entire SSI system, and the severity of this attack will be considered as high. If the attack on a wallet is due to any user-specific vulnerability, then this will only affect a specific user, and the severity will be considered as low.
Verifier Node	Medium	An SSI network contains several verifiers. Any verifier verifies credentials of users, and an attack on it will affect to that verifier and its associated users, which will be significant, but it will not affect entire SSI system, therefore the severity will be considered as medium.
Verifier Agent	High	If the same agent is used on all the verifiers of the SSI system, then the severity will be considered as high. If separate verifier agents are used at different verifiers, then the attack may not affect all verifiers and its severity will be considered as medium.
Verifier Data	Medium	An attack on any verifier data will affect to that verifier and its associated users, which will be significant, but it will not affect the entire SSI system, therefore the severity will be considered as medium.

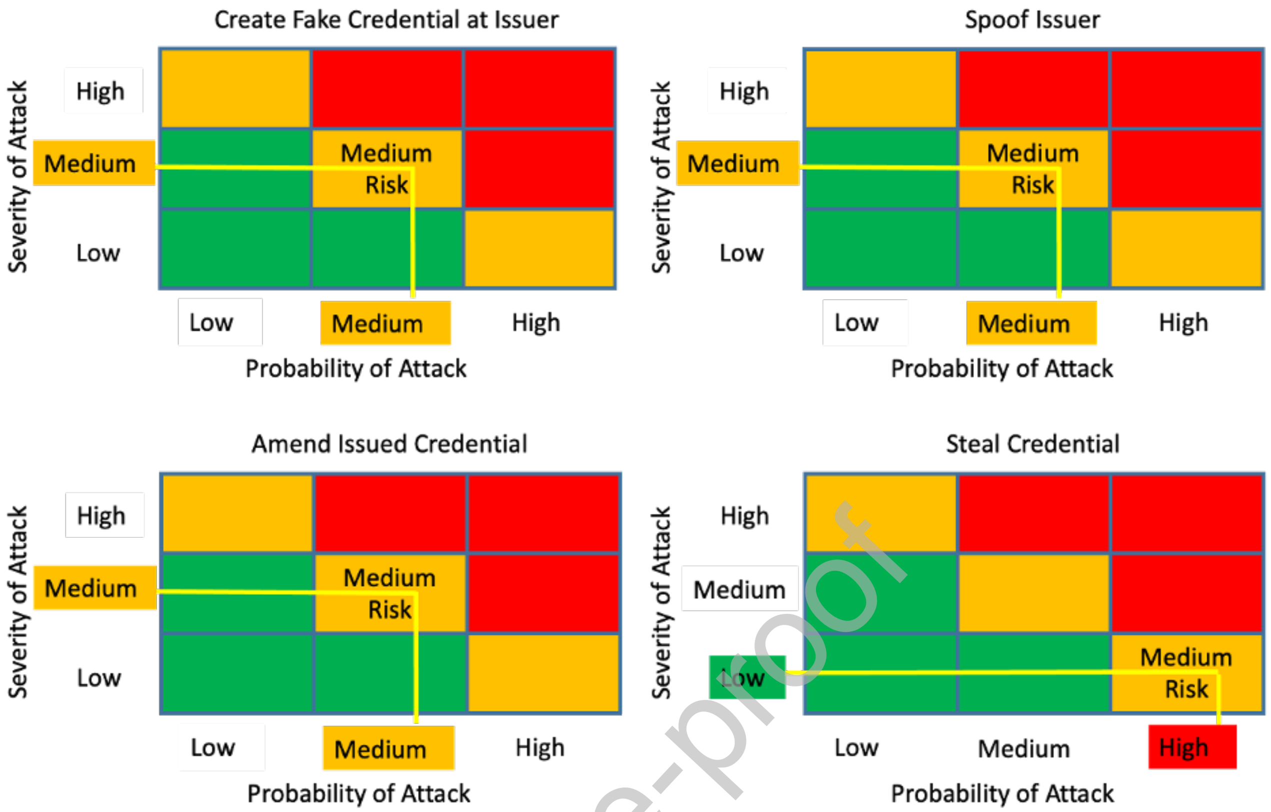


Figure 12: Risk Analysis of Faking Identity Attack Based on Various Attack Vectors Using Risk Matrix

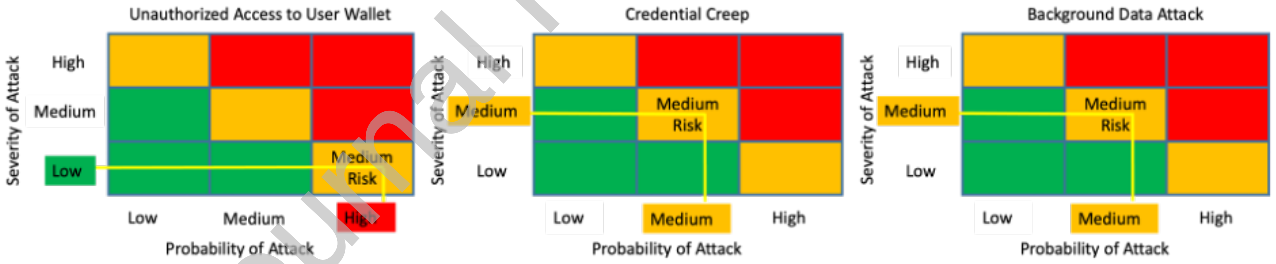


Figure 13: Risk Analysis of Identity Theft Attack Based on Various Attack Vectors Using Risk Matrix

Table 5 shows the proposed mitigation strategies for the identity theft attack based on each individual attack vector and where its implementation is required. Similarly, Table 6 shows the proposed mitigation strategies for the distributed denial of service attack based on each individual attack vector and where its implementation is required. For both tables, the developers of SSI must consider the risk acceptance and select which are the appropriate mitigations.

4. An Application of the Proposed Attack Tree Based Risk Analysis Method and Comparative Analysis with Other Attack Modelling Techniques

4.1. Application of the Proposed Attack Tree Based Risk Analysis Method for an Information Theft Attack on an Organisation

In the previous sections, the combination of attack trees model and risk matrix model has been proposed and described. It has been stated that the proposed method is a systematic and generalised approach for evaluating attacks and their security risks, and can be applied to any other IT system. Therefore, this section will present an application

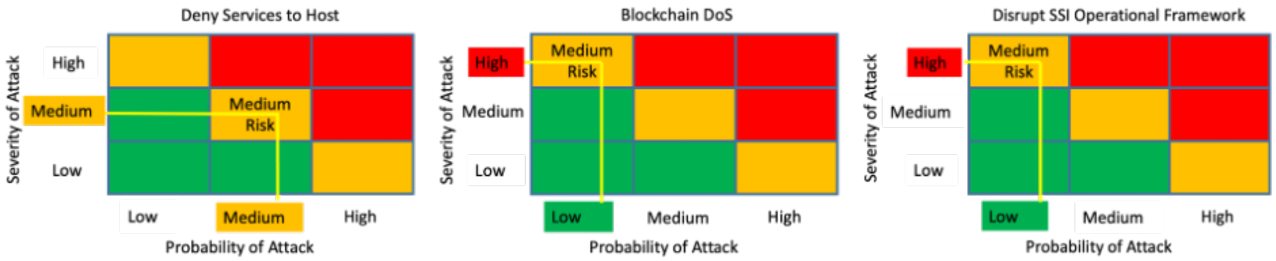


Figure 14: Risk Analysis of Distributed Denial of Service Attack Based on Various Attack Vectors Using Risk Matrix

Table 4
Mitigation Strategies for Faking Identity Attack in the SSI System

Obtain Fake Credential	Attack Mitigation Strategies
Create Fake Credential at Issuer	Use effective authentication and authorisation at issuer such as risk-based access control; Review and update access permissions at an issuer; Applying application controls and limiting use of third-party web scripts or plugins at an issuer; Applying service partitioning or workstation segmentation at an issuer.
Spoof Issuer	Applying data encryption tools at an issuer; Use a traffic monitoring and alerting mechanism at an issuer; Use a gateway firewall or IDS at an issuer; Use IPv6 for better security and avoid IP4 at an issuer.
Amend Issued Credential	Use effective authentication and authorisation at a user; The SSI app and wallet do not interact with unauthorised third-party web apps at a user; Applying service partitioning or workstation segmentation at a user.
Steal Credential	Use Multi-Factor Authentication (MFA) to limit the damage of a stolen/lost credential/device at a user; The SSI system should enforce Least User Access (LUA) policy at a user; The SSI app and wallet do not interact with unauthorised third-party web apps at a user; Applying service partitioning or workstation segmentation at a user.

Table 5
Mitigation Strategies for Identity Theft Attack in the SSI System

Obtain Personal Data	Attack Mitigation Strategies
Unauthorised Access to User Wallet	Implement Multi-Factor Authentication (MFA) and access control to restrict access permissions to wallet; Update security software regularly at the wallet host; Implement data encryption tools and endpoint security at the wallet host; The wallet does not interact with unauthorised third-party web apps at the wallet host; Limit privileges when accessing the SSI system from public networks.
Credential Creep	Implement SSI network policies limiting the access of verifiers to minimum information for verification process; Standardised the verification process and format for all verifiers for making user-understandable.
Background Data Attack	Applying service partitioning or workstation segmentation at a user; Implement SSI network policies limiting the access of verifiers to minimum information for verification process; Standardised the verification process and format for all verifiers for making user-understandable.

of the proposed method for a given scenario an information theft attack on an organisation, which is a very common attack and applicable to any IT system. This attack analysis of an information theft attack on an organisation follows the stages described in the proposed method to clearly demonstrate that how the method can be easily applied to any attack scenario.

4.1.1. Describe the System Architecture

In this application scenario, a general architecture of an organisation is considered, which includes various departments IT, HR, Research & Development, and Manufacturing as shown in Fig. 15. Therefore, it can be easily mapped to most of similar organisational structures to perform an attack analysis of an information theft attack.

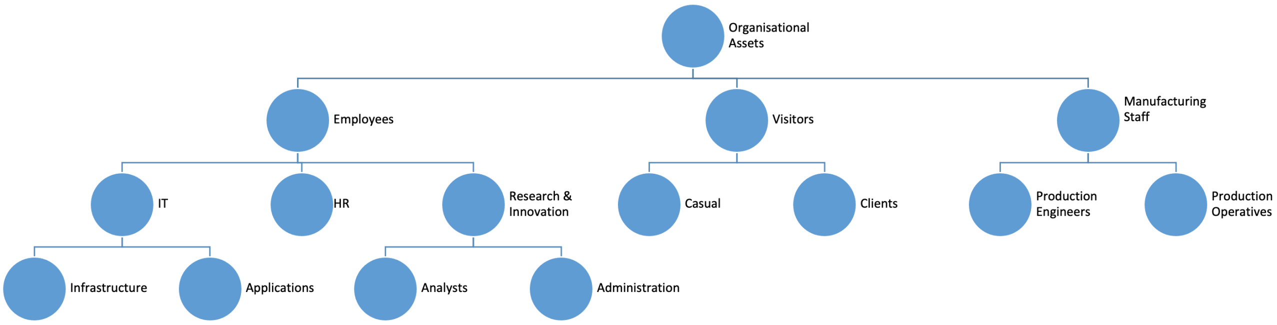


Figure 15: Identified Assets of an Organisation for an Application of the Proposed Method

Table 6
Mitigation Strategies for Distributed Denial of Service Attack in the SSI System

Disrupt Services of the SSI Network	Attack Mitigation Strategies
Deny Services to Host	DDoS alert and prevention services at the host; Blackhole routing; Rate limiting at the host; Deploy a web application firewall; Anycast network diffusion.
Blockchain DoS	Further decentralization of the SSI network and its administrative operations; Implement a blockchain which utilises uncle blocks, stale blocks, orphan blocks or similar blocks with rewards for producing blocks; Establishing a rigorous trust and reputation mechanism for validators to ensure their utmost credibility and responsibility in the consensus process.
Disrupt SSI Operational Framework	Mechanism to observe suspicious behaviour of nodes such as repetitive transactions for the same user; Establish response plan, response time and response team or utilise DDoS-as-a-Service at the SSI provider; Implement a strict authorization and access policy to the operational framework.

4.1.2. Determine the Assets of the System

The identified assets of an organisation are shown in Fig. 15, covering those entities which are relevant to an information theft attack. Again, these assets are very generic and can easily mapped to most of the similar assets in any organisation, however, the selected assets can be customised depending on the specific organisation.

4.1.3. Identify Potential Attacks on the System

As earlier mentioned that this application will cover only one attack scenario of an information theft attack on an organisation to demonstrate its applicability for any IT system. This attack has been selected as it is a very common attack type and applicable in most scenarios. However, the other attack analyses can also be performed in similar way.

4.1.4. Generate the Attack Tree for the Identified Attack Vectors

Fig. 16 illustrates a generated attack tree for the information theft attack, where the goal of a malicious user is to steal information using a number of different identified attack vectors that exploit specific vulnerabilities of assets within an organisation. Here, each illustrated path (i.e., from each leaf node to the root node) to steal information needs to be evaluated for its potential success and severity.

4.1.5. Perform Risk Analysis of Each Identified Attack Using Risk Matrix

Utilising the developed information theft attack tree in Fig. 16, a risk analysis is performed to determine the probability and severity of the information theft attack based on each attack vector exploiting specific vulnerabilities, thus the risk of the information theft attack which is shown in Fig. 17. Clearly these risks are subjective and for illustrative purposes only, as "physical" contains further attack surfaces which will have different risk levels attached to them. However, for simplicity and to demonstrate the ease of use of the combined method, these have been combined into a single risk factor for each of the three attack vectors.

4.1.6. Propose Mitigation Strategies for Each Identified Attack

Given that the attack tree has identified the different attack vectors, and risks have been assigned, it should be straightforward to implement well known mitigating strategies for these three types of attack. Here, the mitigations should be selected by developers according to their acceptance of the previously measured risk. For example, the technical attack vector is high-risk and hence the security experts must mitigate such risk in order to provide robust security.

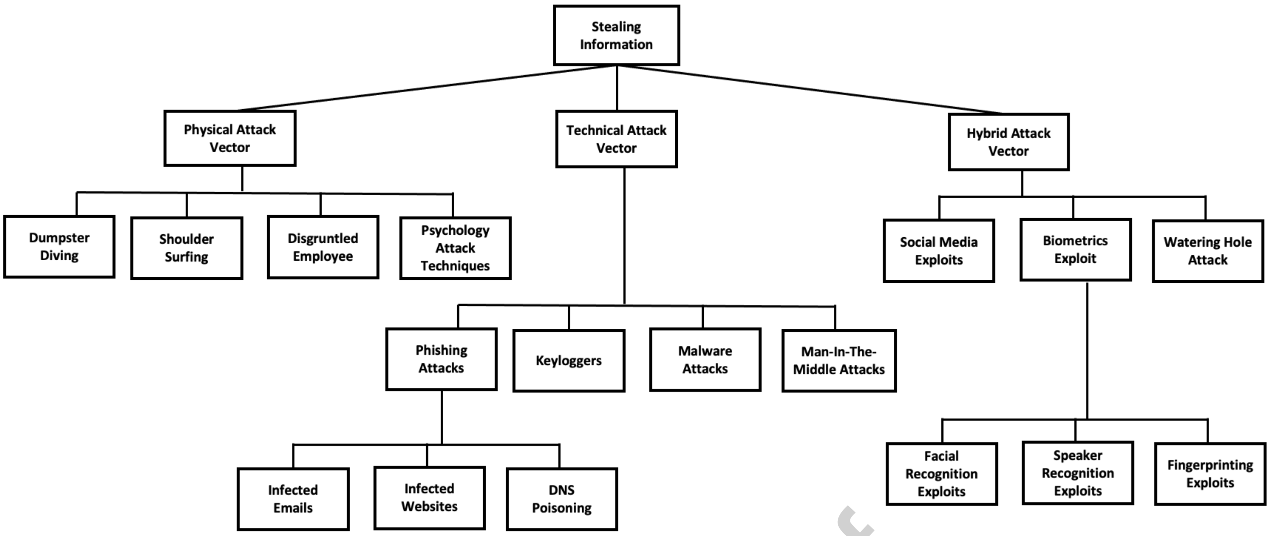


Figure 16: An Attack Tree to Evaluate Information Theft Attack and its Associated Risks in an Organisation

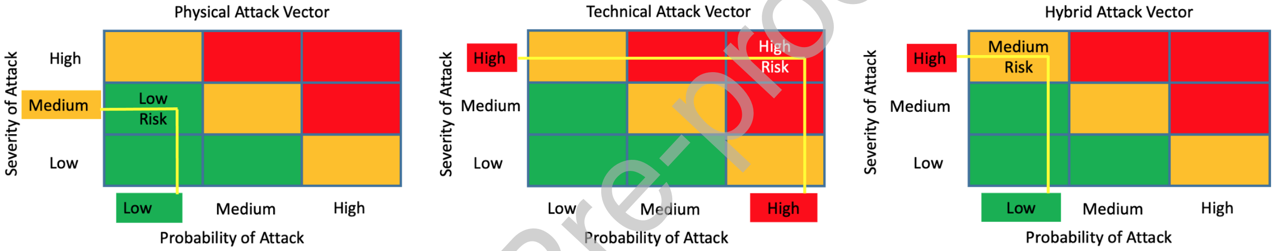


Figure 17: Risk Analysis of Information Theft Attack Based on Various Attack Vectors Using Risk Matrix

4.2. Application of the Lockheed Martin's Cyber Kill Chain for an Information Theft Attack on an Organisation

For the comparative analysis of the proposed method with the Lockheed Martin's Cyber Kill Chain, the same application scenario of an information theft attack on an organisation is considered to perform an attack analysis using the Lockheed Martin's Cyber Kill Chain, which is shown in Fig.18.

4.3. Application of the MITRE ATT&CK Framework for an Information Theft Attack on an Organisation

For the comparative analysis of the proposed method with the MITRE ATT&CK Framework, the same application scenario of an information theft attack on an organisation is considered to perform an attack analysis using the MITRE ATT&CK Framework, which is shown in Fig.19 . Here, all the examples of suggested techniques are based on *Standard Enterprise Techniques* (MITRE.org, 2022).

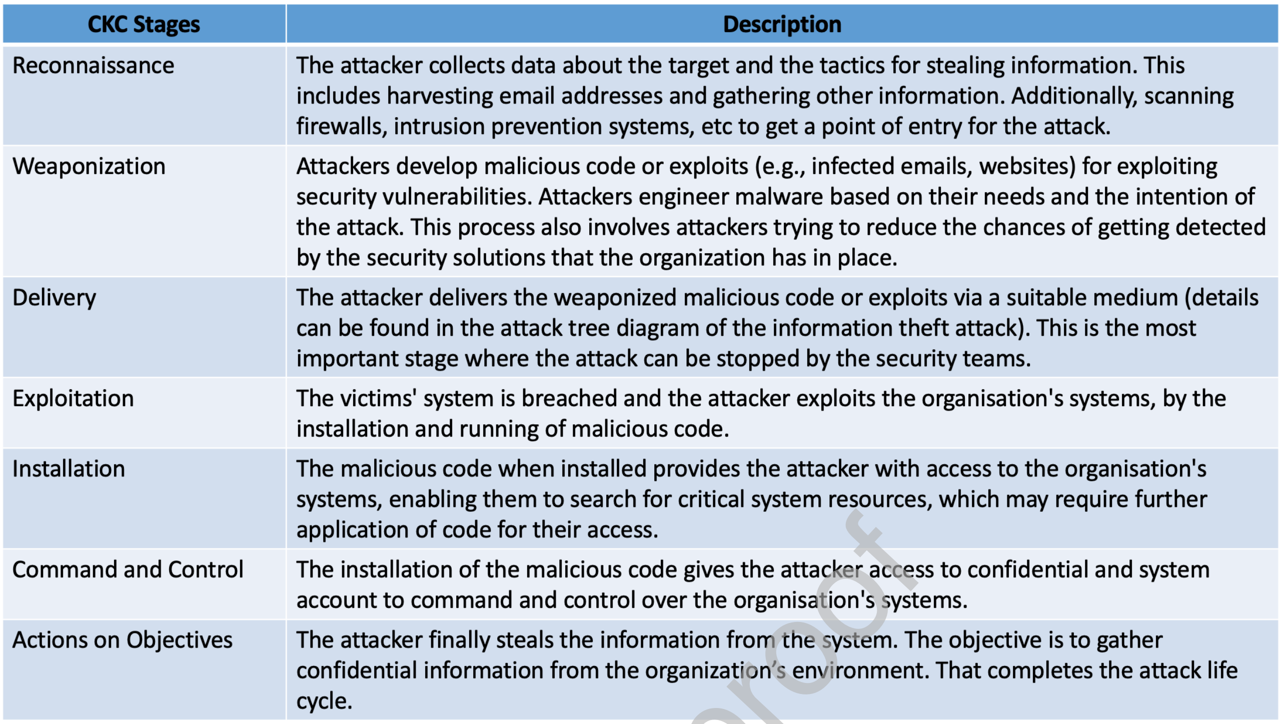
4.4. Application of the Diamond Model for an Information Theft Attack on an Organisation

For the comparative analysis of the proposed method with the Diamond Model, the same application scenario of an information theft attack on an organisation is considered to perform an attack analysis using the Diamond Model, which is shown in Fig.20.

4.5. The Rationale for Selecting the Attack Tree Model and Risk Matrix Model for the Proposed Method

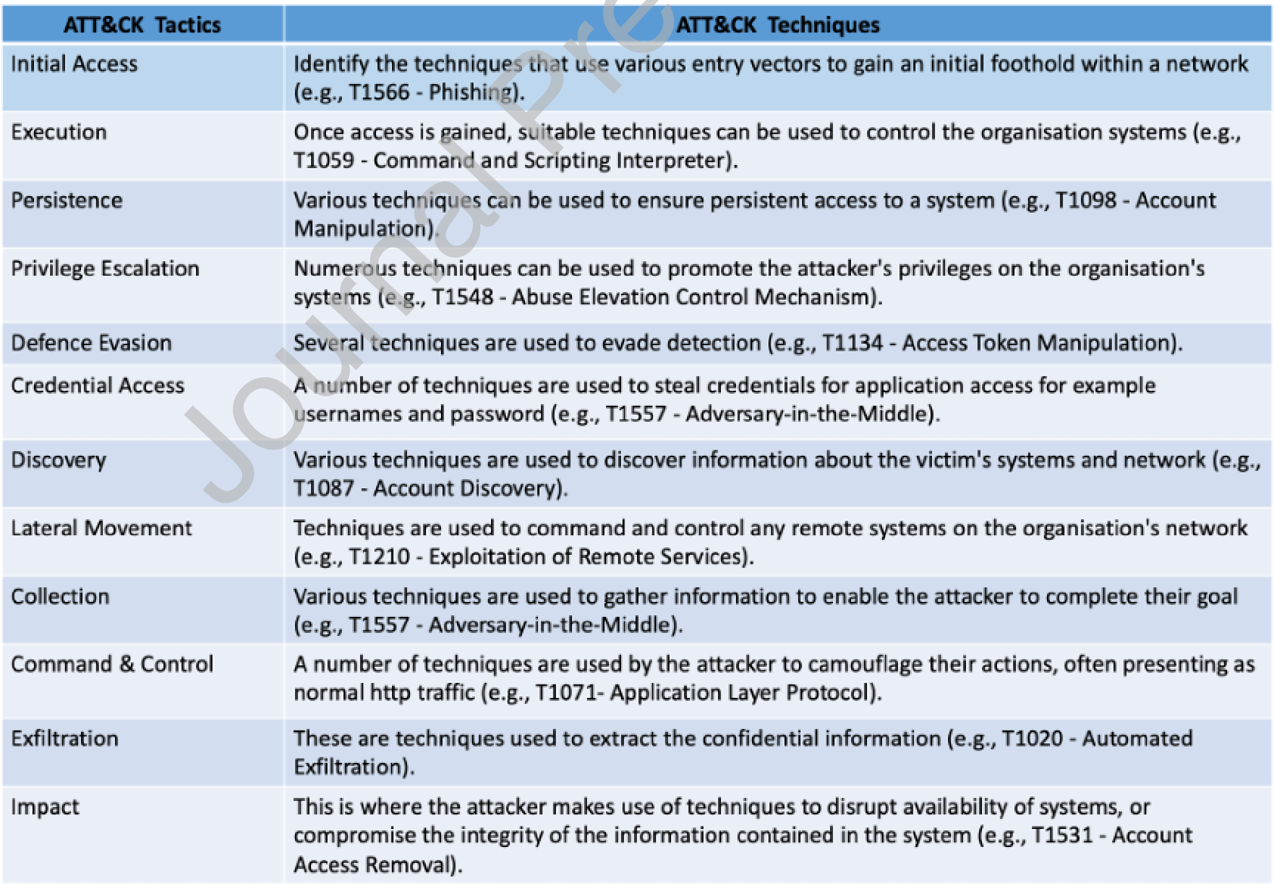
All the popular attack modelling techniques explained earlier have their strengths and weaknesses, with each of them being suitable for different types of attack analyses. It is commonly known that there is no single method which can be used as a silver bullet for all types of attack analyses. The limitations of each technique are highlighted previously, however, this subsection will summarise some common limitations which led to the development of this combinational technique of an attack tree model and risk matrix model.

Most of the prevalent attack modelling techniques are focused on the attackers' goals, capabilities, actions, and methods for exploiting vulnerabilities; however, very little focus is given to the risk analysis and assessment aspect of an investigation (Cybotsai.com, 2021). These attack modelling techniques include application of known threat types, or known attacks to a scenario, and seek to ensure that the analysis has considered the known domain of knowledge (in each of the phases) to some extent (Cybotsai.com, 2021).



CKC Stages	Description
Reconnaissance	The attacker collects data about the target and the tactics for stealing information. This includes harvesting email addresses and gathering other information. Additionally, scanning firewalls, intrusion prevention systems, etc to get a point of entry for the attack.
Weaponization	Attackers develop malicious code or exploits (e.g., infected emails, websites) for exploiting security vulnerabilities. Attackers engineer malware based on their needs and the intention of the attack. This process also involves attackers trying to reduce the chances of getting detected by the security solutions that the organization has in place.
Delivery	The attacker delivers the weaponized malicious code or exploits via a suitable medium (details can be found in the attack tree diagram of the information theft attack). This is the most important stage where the attack can be stopped by the security teams.
Exploitation	The victims' system is breached and the attacker exploits the organisation's systems, by the installation and running of malicious code.
Installation	The malicious code when installed provides the attacker with access to the organisation's systems, enabling them to search for critical system resources, which may require further application of code for their access.
Command and Control	The installation of the malicious code gives the attacker access to confidential and system account to command and control over the organisation's systems.
Actions on Objectives	The attacker finally steals the information from the system. The objective is to gather confidential information from the organization's environment. That completes the attack life cycle.

Figure 18: Lockheed Martin's Cyber Kill Chain to Evaluate Information Theft Attack and its Associated Risks in an Organisation



ATT&CK Tactics	ATT&CK Techniques
Initial Access	Identify the techniques that use various entry vectors to gain an initial foothold within a network (e.g., T1566 - Phishing).
Execution	Once access is gained, suitable techniques can be used to control the organisation systems (e.g., T1059 - Command and Scripting Interpreter).
Persistence	Various techniques can be used to ensure persistent access to a system (e.g., T1098 - Account Manipulation).
Privilege Escalation	Numerous techniques can be used to promote the attacker's privileges on the organisation's systems (e.g., T1548 - Abuse Elevation Control Mechanism).
Defence Evasion	Several techniques are used to evade detection (e.g., T1134 - Access Token Manipulation).
Credential Access	A number of techniques are used to steal credentials for application access for example usernames and password (e.g., T1557 - Adversary-in-the-Middle).
Discovery	Various techniques are used to discover information about the victim's systems and network (e.g., T1087 - Account Discovery).
Lateral Movement	Techniques are used to command and control any remote systems on the organisation's network (e.g., T1210 - Exploitation of Remote Services).
Collection	Various techniques are used to gather information to enable the attacker to complete their goal (e.g., T1557 - Adversary-in-the-Middle).
Command & Control	A number of techniques are used by the attacker to camouflage their actions, often presenting as normal http traffic (e.g., T1071- Application Layer Protocol).
Exfiltration	These are techniques used to extract the confidential information (e.g., T1020 - Automated Exfiltration).
Impact	This is where the attacker makes use of techniques to disrupt availability of systems, or compromise the integrity of the information contained in the system (e.g., T1531 - Account Access Removal).

Figure 19: MITRE ATT&CK Framework to Evaluate Information Theft Attack and its Associated Risks in an Organisation

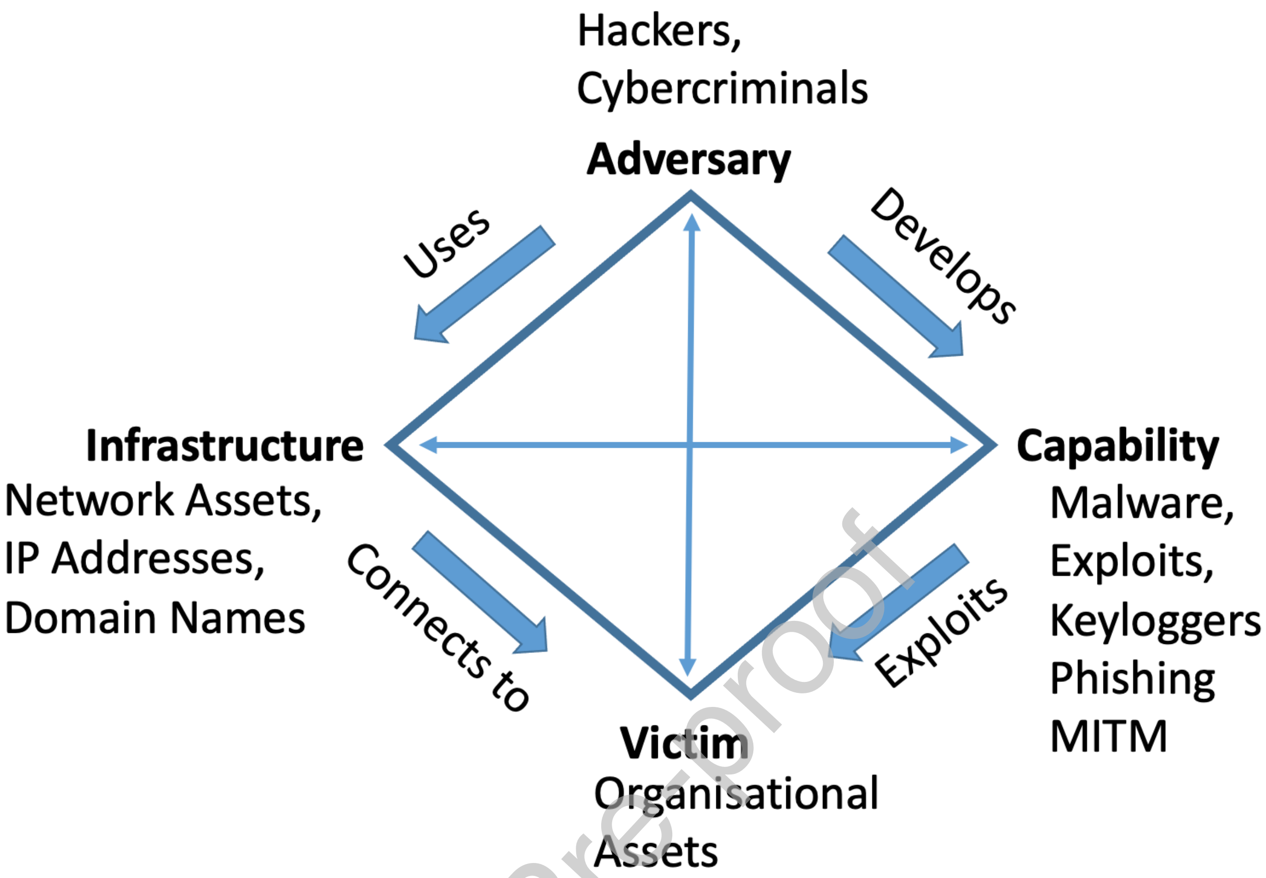


Figure 20: Diamond Model to Evaluate Information Theft Attack and its Associated Risks in an Organisation

Most attack modelling techniques are a comprehensive scientific methods of attack analysis, which requires significant expertise in the relevant area (Poston, 2020, November 10). Due to the verbose nature of these techniques with little or no graphical illustration they are rendered less understandable to various stakeholders and limits their participation in the attack analysis (CyCraftTechnology, 2020, July 1). In some cases, these techniques are long-standing and archaic and did not include all the dynamics of an attack in the current environment, in particular the distributed environment (Thecyphere.com, 2022). To overcome some of the limitations of these attack modelling techniques, some can be combined to provide an improved attack analysis (Poston, 2020, November 10), however, this may increase the complexity and overheads of the combined technique and its attack analysis.

The purpose of the proposed combinational technique of an attack tree model and risk matrix model is to identify novel attacks in an emerging distributed environment; in addition to identifying known attacks within the design and development of a typical information system. The attack tree model provides a graphical and granular relationship between the adversary and the victim, which is not possible in some of the most popular attack modelling techniques, enabling stakeholders to understand and participate in the attack analysis. The risk matrix model is complementary to the attack tree model to add the risk analysis and assessment aspect of an attack analysis. Both employed models are simple to understand and use making this proposed combinational technique easy to use and to perform attack analysis.

5. Conclusion

This paper proposed an attack risk evaluation approach to perform an evaluation of potential attacks on the SSI system and their security risks. This proposed approach utilised a combination of an attack tree model and risk matrix model to perform this evaluation of potential attacks and their security risks in an easy, efficient and economical manner. It outlined a systematic attack risk evaluation approach starting from describing the system architecture of the system, determining its assets, identify potential attacks on the assets of the system, generating an attack tree for each identified attack, perform risk analysis of each identified attack, and finally proposing mitigation strategies for it.

This evaluation work identified three potential attacks on the SSI system: the faking identity, identity theft and distributed denial of service attacks, and performed their security risk evaluation utilising the proposed approach and its systematic steps. It generated an attack tree for each identified attack on the SSI system, subsequently performed an attack risk analysis of it using a risk matrix model to analyse its potential attack risk with respect to various attack vectors and vulnerabilities to assess the various security aspects of the system. This attack risk evaluation was performed at an attack vector level; however, it can be customised at a further granular level depending on the specific risk analysis requirement. Finally, several mitigation strategies were proposed for each analysed attack on the SSI system. This proposed approach can be further extended and utilised for other identified attacks on the SSI system in the same manner utilising its systematic steps.

The proposed attack risk evaluation approach offers several benefits over other attack risk evaluation approaches such as it is an illustrative, understandable, economical, efficient, customizable, scalable, reusable approach. Additionally, this approach enables security analysts to implement a process where different stakeholders with different backgrounds and skills provide their feedback to help analyse potential attacks and risks. This approach is a systematic and generalised approach for evaluating attacks and their security risks, and can be applied to any other IT system.

The proposed approach has some limitations due to its underlying models attack tree model and risk matrix model. An attack tree is simply a hierarchical structure with only one root node, which is a trade-off as each attack requires an individual attack tree for its effective analysis; however, depending on the system and a significant number of attacks, this attack tree modelling may become very intensive (Ingoldsby, 2010). Similarly, a risk matrix can assign identical ratings to quantitatively different risks or higher qualitative ratings to quantitatively smaller risks and vice versa depending on the designed criteria (Anthony , Tony), (Julian, 2011). Therefore, in future, this proposed approach would be extended and evaluated to perform analysis of a wide range of attacks from completely different attack categories such as the temporal and spatial analysis of attacks in the SSI system and other systems.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Nitin Naik: Conceptualization, Investigation, Methodology, Writing - Original Draft. Paul Grace: Investigation, Methodology, Writing - Review & Editing. Paul Jenkins: Investigation, Methodology, Writing - Review & Editing. Kshirasagar Naik: Methodology, Writing - Review & Editing. Jingping Song: Methodology, Writing - Review & Editing.

References

Allen, C., 2016. Self-sovereign identity principles. URL: https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md.

Amenaza.com, 2021. The SecurITree advantage. URL: https://www.amenaza.com/SS-advantage.php.

Anthony (Tony) Cox Jr, L., 2008. What's Wrong with Risk Matrices? Risk Analysis: An International Journal 28, 497–512.

Arnold, F., Hermanns, H., Pulungan, R., Stoelinga, M., 2014. Time-dependent analysis of attacks, in: International Conference on Principles of Security and Trust, Springer. pp. 285–305.

Auditboard.com, 2021. What is a risk assessment matrix? and why is it important? URL: https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/.

Caltagirone, S., Pendergast, A., Betz, C., 2013. The diamond model of intrusion analysis. Technical Report. Center For Cyber Intelligence Analysis and Threat Research Hanover Md.

Campanis, N.A., 1997. Delphi: Not the greek oracle, but close. PM NETWORK 11, 46–49.

Camtepe, S.A., Yener, B., 2007. Modeling and detection of complex attacks, in: 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007, IEEE. pp. 234–243.

Cohen, Z., 2019, October 29. Spoooooky types of identity fraud. URL: https://www.finextra.com/blogposting/18077/spoooooky-types-of-identity-fraud.

Cybotsai.com, 2021. An introduction to MITRE ATT&CK. URL: https://cybotsai.com/introduction-mitre-attck/.

CyCraftTechnology, 2020, July 1. CyCraft Classroom: MITRE ATTCK vs. Cyber Kill Chain vs. Diamond Model. URL: https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f.

Dacier, M., 1994. Towards quantitative evaluation of computer security. Ph.D. thesis. PhD thesis, Institut National Polytechnique de Toulouse.

Dacier, M., Deswarte, Y., 1994. Privilege graph: an extension to the typed access matrix model, in: European Symposium on Research in Computer Security, Springer. pp. 319–334.

Dacier, M., Deswarte, Y., Kaâniche, M., 1996. Models and tools for quantitative assessment of operational security, in: IFIP International Conference on ICT Systems Security and Privacy Protection, Springer. pp. 177–186.

Hayes, M., 2020, September 29. The many different forms of identity theft. URL: https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/.

Hulett, D.T., 2006. Decision tree analysis for the risk averse organization, in: PMI EMEA Congress.

Idealintegrations.net, 2019. The Cyber Kill Chain Model is Obsolete. URL: https://www.idealintegrations.net/the-cyber-kill-chain-model-is-obsolete/.

Ingoldsby, T.R., 2010. Attack tree-based threat risk analysis. Amenaza Technologies Limited .

Jhawar, R., Kordy, B., Mauw, S., Radomirović, S., Trujillo-Rasua, R., 2015. Attack trees with sequential conjunction, in: IFIP International Information Security and Privacy Conference, Springer. pp. 339–353.

Jiang, R., Luo, J., Wang, X., 2012. An attack tree based risk assessment for location privacy in wireless sensor networks, in: 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE. pp. 1–4.

Julian, T., 2011. What's Right with Risk Matrices. Management Policy .

Kazarian, J.P., 2016, July 22. Why decentralized encryption key management for mobile is dangerous. URL: https://techbeacon.com/security/why-decentralized-encryption-key-management-mobile-dangerous.

Korolov, M., Myers, L., 2018, November 15. What is the cyber kill chain? Why it's not always the right approach to cyber attacks. URL: https://www.csoonline.com/article/2134037/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html.

LockheedMartin.com, 2011. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Markovic, I., 2019, November 8. How to use the risk assessment matrix to organize your project better. URL: https://tms-outsource.com/blog/posts/risk-assessment-matrix/.

MITRE.org, 2021. MITRE ATT&CK. URL: https://attack.mitre.org/.

MITRE.org, 2022. MITRE ATT&CK Enterprise Techniques. URL: https://attack.mitre.org/techniques/enterprise/.

Moyle, L., 2021. Identity Management Introduction. URL: https://www.nexusgroup.com/resources/identity-management-introduction/.

Naik, N., Grace, P., Jenkins, P., 2021. An attack tree based risk analysis method for investigating attacks and facilitating their mitigations in self-sovereign identity, in: IEEE Symposium Series on Computational Intelligence (SSCI), IEEE.

Naik, N., Jenkins, P., 2017. Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect, in: 11th International Conference on Research Challenges in Information Science (RCIS), IEEE. pp. 163–174. doi:10.1109/RCIS.2017.7956534.

Naik, N., Jenkins, P., 2020a. Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems, in: 2020 IEEE International Symposium on Systems Engineering (ISSE), IEEE.

Naik, N., Jenkins, P., 2020b. Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology, in: 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2020), IEEE.

Naik, N., Jenkins, P., 2020c. uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain, in: 2020 IEEE International Symposium on Systems Engineering (ISSE), IEEE.

Naik, N., Jenkins, P., 2020d. Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity, in: 7th International Conference on Behavioural and Social Computing (BESC2020), IEEE.

Naik, N., Jenkins, P., 2021a. Does Sovrin Network offer sovereign identity?, in: 2021 IEEE International Symposium on Systems Engineering (ISSE), IEEE.

Naik, N., Jenkins, P., 2021b. Sovrin Network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology, in: 2021 IEEE International Symposium on Systems Engineering (ISSE), IEEE.

Okta.com, 2021. 5 Identity attacks that exploit your broken authentication. URL: https://www.okta.com/resources/whitepaper/5-identity-attacks-that-exploit-your-broken-authentication/.

Poston, H., 2020, November 10. How to use the MITRE ATT&CK framework and Diamond model of intrusion analysis together. URL: https://resources.infosecinstitute.com/topic/how-to-use-the-mitre-attck-framework-and-diamond-model-of-intrusion-analysis-together/.

Ruef, M., Schneider, M., 2021. MITRE ATT&CK flaws of the standardization. URL: https://www.scip.ch/en/?labs.20210204#:~:text=The%20basic%20problem%20of%20ATT,techniques%20are%20also%20not%20traceable.

Salter, C., Saydjari, O.S., Schneier, B., Wallner, J., 1998. Toward a secure system engineering methodolgy, in: Proceedings of the 1998 workshop on New security paradigms, pp. 2–10.

Schneier, B., 1999. Attack Trees. Dr. Dobb's Journal 24, 21–29.

Socradar.io, 2022. What is the Diamond Model of Intrusion Analysis? URL: https://socradar.io/what-is-the-diamond-model-of-intrusion-analysis/.

Sovrin.org, 2018a. Sovrin: A protocol and token for self-sovereign identity and decentralized trust. URL: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.

Sovrin.org, 2018b. What is Self-Sovereign Identity? URL: https://sovrin.org/faq/what-is-self-sovereign-identity/.

Swiler, L.P., Phillips, C., Gaylor, T., 1998. A graph-based network-vulnerability analysis system. Technical Report. Sandia National Labs., Albuquerque, NM (United States).

Thecyphere.com, 2022. What is Cyber Kill Chain? URL: https://thecyphere.com/blog/cyber-kill-chain/.

Tykn.tech, 2021. Self-Sovereign Identity: The ultimate beginners guide! URL: https://tykn.tech/self-sovereign-identity/#The_Benefits_of_Self-Sovereign_Identity.

W3C, 2019. A primer for Decentralized Identifiers. URL: https://w3c-ccg.github.io/did-primer/.

Weiss, J.D., 1991. A system security engineering process, in: Proceedings of the 14th National Computer Security Conference, pp. 572–581.

Credit Author Statement

Nitin Naik: Conceptualization, Investigation, Methodology, Writing - original draft.
Paul Grace: Investigation, Methodology, Writing - review & editing.
Paul Jenkins: Investigation, Methodology, Writing - review & editing.
Kshirasagar Naik: Methodology, Writing - review & editing.
Jingping Song: Methodology, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors Biography

Nitin Naik
Nitin Naik received the Ph.D. degree in computer science from Aberystwyth University, Aberystwyth, U.K. He additionally holds several academic qualifications: M.Tech., M.Sc., MBA, MSW, B.Sc., and Polytechnic (Electrical Engineering). He has authored or coauthored more than 100 peer-reviewed papers in the areas of artificial intelligence, cybersecurity, big data, cloud computing, Internet of Things, and game based learning. He is currently a Senior Lecturer with the School of Informatics and Digital Engineering, Aston University, Birmingham, U.K.

Paul Grace
Paul Grace is a senior lecturer in Computer Science at Aston University in the UK. He has over 20 years research and development experience in the field of interoperability, middleware, distributed systems, security & privacy, and pervasive computing. He has published over 100 papers in these areas. He has previously held research fellow positions at Lancaster University, Katholieke Universiteit Leuven, and the University of Southampton. He received his PhD from Lancaster in 2004, an MSc from the same institution in 2000 and a BSc in Computer Science from the University of York in 1999.

Paul Jenkins
Paul Jenkins received the Ph.D. degree in applied mathematics and computing from Cardiff University, Cardiff, U.K. He has authored or coauthored more than 50 peer-reviewed papers in the areas of artificial intelligence, cybersecurity, big data, cloud computing, Internet of Things, and game based learning. He is currently a Senior Lecturer with the Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, U.K.

Kshirasagar Naik
Kshirasagar (Sagar) Naik is a Full Professor in the Department of Electrical and Computer Engineering at University of Waterloo. His research interests include energy performance of mobile devices and applications, detection of anomalous behaviour of wireless devices and physical systems, energy harvesting IoT (Internet of Things) devices for sustainable monitoring of physical systems, and communication security, and wireless sensor networks. He was an Associate Editor of IEEE Transactions on Parallel and Distributed

Systems and a guest editor of four special issues of IEEE Journal on Selected Areas in Communications and IEEE Transactions on Cloud Computing. He is a co-author of two textbooks, namely, Software Testing and Quality Assurance (Wiley, 2008)