International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819

Email: editor@ijarets.org Volume-10 Issue-1 January-2023 www.ijarets.org

# PRINCIPLES OF SECURITY USABILITY IN VULNERABILITY ANALYSIS AND RISK ASSESSMENT

**Lakshya Panwar**

Ph.D. Scholar

Department of Computer Science

Malwanchal University Indore, (M.P.).

**Prof.(Dr.)Ajit Singh**

Supervisor

Department of Computer Science

Malwanchal University Indore, (M.P.).

## *ABSTRACT*

*This study integrates usability into the risk assessment process to improve IT system security by identifying and addressing security usability vulnerabilities (SUVs) that contribute to human errors. It evaluates the usability flaws in existing security measures like TLS and SMS authorization, demonstrating how these issues can lead to significant security risks. The study proposes a usability metric to guide the selection of appropriate security measures, aiming to balance security effectiveness with user experience. It argues that current risk assessment frameworks, such as ISO/IEC 27001:2006 and NIST 800-30, fail to consider usability-related vulnerabilities, and calls for the inclusion of usability in the risk identification process. The findings suggest that incorporating usability into risk assessments will enhance overall security, reduce risks, and improve user satisfaction with security protocols.*

***Keywords:*** *Security Usability, Risk Assessment, Vulnerability Analysis etc.*

## INTRODUCTION

In today's interconnected world, where digital systems are integral to nearly every aspect of human life, securing these systems against cyber threats has never been more critical. As organizations, governments, and individuals rely increasingly on technology, the risk of cyberattacks and data breaches has escalated. With the proliferation of complex technologies and the rising sophistication of cyber threats, traditional approaches to security often fall short in addressing one critical component: usability. While security measures such as firewalls, encryption protocols, and multi-factor authentication (MFA) are essential to protect sensitive information and maintain system integrity, they are only effective when users can effectively engage with them. A key challenge, however, is that many of these security measures, despite their advanced technical capabilities, are often difficult for users to understand or interact with correctly. When security systems are not designed with the user in mind, they can become ineffective, leading to vulnerabilities that attackers can exploit.

### The Human Factor in Security Vulnerabilities

This failure to consider user experience in the design of security features has become a significant issue in modern risk management and vulnerability analysis processes. Security experts and organizations alike have increasingly realized that poor security usability introduces a new type of vulnerability: the human element. A system's security may be technically strong, but if it requires complex actions or confusing decisions from users, it becomes prone to human error. Users may bypass security features, make mistakes, or inadvertently expose themselves to attack, rendering even the most robust systems ineffective. Hence, the importance of integrating security usability into vulnerability analysis and risk assessment processes cannot be overstated. Understanding the intersection of security and usability is essential for developing systems that are both secure and user-friendly, ensuring that security measures are not only technically sound but also accessible and effective from a user perspective.

### Traditional Risk Assessment Frameworks and Their Limitations

Historically, vulnerability analysis and risk assessment have focused predominantly on technical aspects of security. These processes aim to identify weaknesses within systems, assess the potential impact of various threats, and devise strategies to mitigate those threats. However, the human factor—the way individuals interact with and manage security features—has often been overlooked in these assessments. Risk assessments traditionally evaluate technical threats such as software vulnerabilities, network security flaws, or unauthorized access to data. While these issues are crucial, they often fail to account for how usability challenges can create security risks. For instance, if a user fails to recognize a phishing attempt due to an unclear warning message, or if they bypass multi-factor authentication because it is too cumbersome, the underlying system’s security is compromised. To truly enhance system security, it is necessary to integrate the consideration of usability issues into the very fabric of vulnerability analysis and risk assessment frameworks.

### The Concept of Security Usability

The concept of security usability addresses this gap by focusing on how users interact with security measures and how these interactions can either strengthen or undermine security. Security usability is defined as the design and implementation of security measures that are easy for users to understand, manage, and follow without inadvertently compromising system security. It recognizes that even the most technically advanced security measures are only as effective as the user's ability to use them properly. For instance, multi-factor authentication (MFA) may be highly secure from a technical standpoint, but if the process is too complicated or confusing, users may choose to bypass it, ultimately making the system less secure. In this context, security usability aims to improve the design of security features, making them intuitive, accessible, and less likely to cause errors, thus minimizing the risk of security breaches caused by human factors.

### The Importance of Integrating Usability into Risk Assessment

The integration of security usability principles into vulnerability analysis and risk assessment processes is a relatively recent development, but it holds significant promise for improving the overall effectiveness of security systems. Usability should not be treated as a secondary consideration or an afterthought, but rather as an integral part of security design and assessment. The goal is to ensure that security measures are designed with the user in mind, reducing cognitive load, simplifying processes, and enhancing the user's understanding of the security tasks they are expected to perform. By doing so, organizations can address the human vulnerabilities that often accompany complex security systems and minimize the risks posed by user behavior.

### Security Usability in Vulnerability Identification

One of the key stages where security usability must be incorporated is during the vulnerability identification phase of risk assessment. In traditional risk assessments, vulnerability identification focuses on technical weaknesses that can be exploited by attackers, such as software bugs, hardware flaws, or misconfigurations. However, this approach overlooks usability flaws that can be just as dangerous. For example, if a user is unable to easily recognize phishing attempts or if they misunderstand a security prompt, these usability issues create vulnerabilities that can be exploited by attackers. By considering usability during vulnerability identification, organizations can identify these human-related vulnerabilities early in the risk assessment process and address them before they lead to security breaches.

### The Intersection of Usability and Traditional Risk Assessment Methods

The process of risk assessment typically involves identifying potential threats, determining the likelihood of these threats occurring, and assessing the potential impact of a security breach. While these technical factors are essential to understanding security risks, they often fail to capture the full scope of vulnerabilities introduced by poor security usability. A system may be vulnerable to phishing attacks, for example, not because the underlying encryption or authentication mechanisms are weak, but because the user interface does not clearly indicate when a website is fraudulent. Similarly, users may fail to notice discrepancies in URLs or certificates, leading them to trust a malicious website unknowingly. These usability issues are critical vulnerabilities that traditional risk assessment frameworks often overlook. Integrating usability into these frameworks allows organizations to recognize and mitigate human-related vulnerabilities that could otherwise go unnoticed.

## REVIEW OF LITERATURE

**Schaefer and Jansen (2017)** emphasize that traditional risk assessment frameworks, such as, often overlook the usability aspects of security. These frameworks typically focus on technical vulnerabilities without addressing how users interact with security measures. The study argues that poor usability is a significant risk factor that can lead to security breaches, as users may bypass or misuse security mechanisms. The authors propose integrating usability into the risk assessment process by evaluating not only the technical controls but also the cognitive load and user behavior associated with security measures. This approach ensures that the security systems are both technically effective and user-friendly, reducing the likelihood of human errors.

**Whitten and Tygar (1999)** focus on the usability vulnerabilities inherent in web security, specifically in systems like the Transport Layer Security (TLS) protocol. While TLS is widely used for securing communication over the internet, the authors highlight usability issues such as confusing interface design and the complexity of certificate management. These issues often lead to vulnerabilities that are exploited in phishing attacks. The study advocates for designing security systems with a focus on user understanding, suggesting that usability flaws in security mechanisms can render them ineffective, despite robust cryptographic protocols. This research underlines the need for integrating usability principles into the analysis of security systems during risk assessments.

**Norman (2013)** examines how human-computer interaction (HCI) principles can be applied to enhance security usability. The study explores how security interfaces can be designed to reduce cognitive overload and increase user comprehension of security actions. Norman argues that many security breaches occur due to the complexity of security systems, which often require users to perform actions they do not fully understand or that cause confusion. By applying HCI principles, security systems can be designed to align more closely with user capabilities, thus reducing the likelihood of errors. This literature highlights the importance of considering user psychology and behavior in vulnerability analysis and risk assessment, especially in the context of security interfaces.

**Bonneau et al. (2015)** investigate the role of usability in user authentication systems, which are often the first line of defense in security. The authors discuss how authentication methods like passwords, two-factor authentication (2FA), and biometric systems can be compromised due to poor usability. The study shows that complex password requirements and cumbersome 2FA processes can lead to user frustration, which in turn results in unsafe practices, such as reusing passwords or disabling security features altogether. By integrating usability considerations into the design of authentication systems, the authors argue that security can be significantly enhanced. This research supports the idea that user-centric design principles are crucial for identifying vulnerabilities and improving risk management in security systems.

**Anderson (2008)** highlights the impact of human error on security systems and its implications for risk assessment. The study asserts that human factors, such as misunderstanding security protocols or failure to follow security procedures, contribute to a significant number of security incidents. Anderson argues that traditional risk assessments often fail to account for these human-centric vulnerabilities, which can lead to security breaches that would otherwise be preventable. The paper suggests that incorporating an understanding of human behavior into risk assessments can improve the accuracy of vulnerability identification and enhance the effectiveness of security controls. This work reinforces the need to address usability issues in risk assessment frameworks to mitigate risks stemming from user errors.

## OBJECTIVES OF THE STUDY

**Following are the main Objective of this study:**

1. To Identify Usability-Related Vulnerabilities in Traditional Risk Assessment.
2. To Highlight the Role of Usability in Enhancing Security Risk Management.

## HYPOTHESIS

**Following are the main hypothesis of this study:**

**$H_1$:** There is a significant gap in traditional risk assessment models in identifying usability-related vulnerabilities, affecting overall security.

**$H_2$:** There is a significant improvement in security risk management when usability is integrated into risk assessments, leading to fewer user-related security breaches.

## RESEARCH METHODOLOGY

This study incorporates usability into the risk assessment process to improve IT system security. It identifies threats and vulnerabilities, including security usability issues like user confusion and cognitive load. Current security controls, such as TLS and SMS authorization, are evaluated for usability flaws. The likelihood and impact of these vulnerabilities are assessed using a risk matrix, and new controls are recommended. A usability metric is developed to guide the selection of appropriate security measures, aiming to reduce risks caused by poor usability and enhance overall security and user experience.

## RESULTS

Integrating usability into risk assessment is crucial, as poor security usability often represents a significant vulnerability in IT systems. However, major security standards like ISO/IEC 27001:2006 and NIST 800-30 fail to address usability as a risk factor. Current risk assessment frameworks overlook usability-related vulnerabilities, despite their impact on security effectiveness. To address this gap, usability should be integrated into the "Vulnerability Identification" step of risk assessment, ensuring that security measures consider user experience and potential human errors. Recognizing and mitigating poor usability can enhance overall security and reduce risks associated with IT systems.

**Table 1. Risk assessment process**

| Step No. | Risk Assessment Steps | Description |
|---|---|---|
| Step 1 | System Characterization | Identifying and defining the local community security system, its components, and scope. |
| Step 2 | Threat Identification | Recognizing potential threats that could compromise security, such as crime, cyber threats, or natural disasters. |
| Step 3 | Vulnerability Identification | Assessing weaknesses in the security system that threats could exploit. |
| Step 4 | Analysis of Existing Security Controls | Evaluating current security measures and their effectiveness in mitigating risks. |
| Step 5 | Likelihood Determination | Estimating the probability of threats exploiting identified vulnerabilities. |
| Step 6 | Impact Analysis | Analyzing potential consequences of security breaches on the local community. |
| Step 7 | Risk Determination | Assessing overall security risks based on likelihood and impact analysis. |

| Step No. | Risk Assessment Steps | Description |
|---|---|---|
| Step 8 | Recommendation of New Controls | Suggesting additional security measures to improve system resilience. |
| Step 9 | Results Documentation | Recording findings and recommendations for future reference and decision-making. |

A threat represents the impact magnitude, indicating potential direct or indirect losses from its occurrence. The associated risk is determined by combining the threat's likelihood and impact magnitude, as shown in Fig. 1.

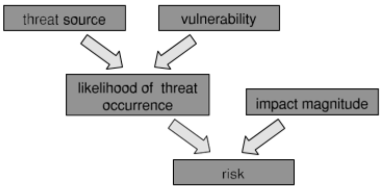


**Figure 1. Principle for determining risk**

A risk assessment team identifies vulnerability-threat combinations (Steps 2-3), estimates likelihood and impact (Steps 5-6), and determines risk (Step 7) using a matrix. Risk levels range from Negligible (N) to Extreme (E), as shown in Table 2.

**Table 2. Look-up risk matrix**

| Likelihood | Impact magnitude | | | | |
|---|---|---|---|---|---|
| | Insignificant | Minor | Moderate | Major | Catastrophic |
| Certain | M | H | H | E | E |
| Likely | L | M | H | H | E |
| Possible | L | L | M | H | H |
| Unlikely | N | L | L | M | H |
| Rare | N | N | L | L | M |

During a major risk assessment, hundreds of threats are identified using predefined checklists and ranked by risk level (Step 7). New security controls (Step 8) prioritize mitigating the highest risks. However, traditional checklists often overlook poor security usability as a vulnerability, leading to missed risks. To address this, security usability vulnerabilities (SUVs) should be explicitly included in assessments, with checklists updated accordingly. Table 3 presents security usability vulnerabilities based on established principles.

**Table 3. Security usability vulnerabilities**

| Security usability vulnerabilities on action | |
|---|---|
| SUV-A1 | Users are unable to understand which security actions are required of them. |
| SUV-A2 | Users do not have sufficient knowledge or are unable to take the correct security action. |
| SUV-A3 | The mental and physical load of a security action is not tolerable. |
| SUV-A4 | The mental and physical load of making repeated security actions for any practical number of instances is not tolerable. |
| Security usability vulnerabilities on conclusion | |
| SUV-C1 | Users do not understand the security conclusion that is required for making an informed decision. |
| SUV-C2 | The system does not provide the user with sufficient information for deriving the secu- rity conclusion. |
| SUV-C3 | The mental load of deriving the security conclusion is not tolerable. |
| SUV-C4 | The mental load of deriving security conclusions for any practical number of instances is not tolerable. |

This paper discusses vulnerabilities in current web security solutions, focusing on the Transport Layer Security (TLS) protocol. While TLS provides encryption and server authentication, its usability flaws make it ineffective, especially in phishing attacks. The padlock icon in browsers indicates a secure connection but doesn't verify the server's identity, creating vulnerability SUV-C2. Analyzing the server certificate increases cognitive load, leading to vulnerabilities SUV-C3 and C4. These issues stem from poor usability, not weak cryptographic mechanisms.

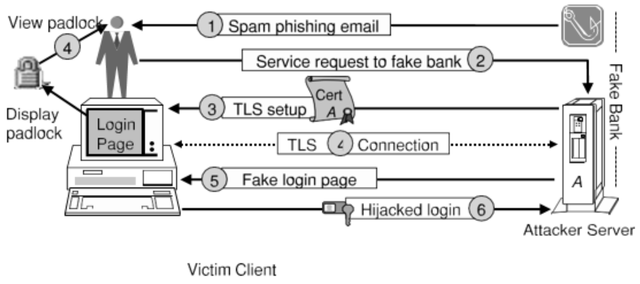
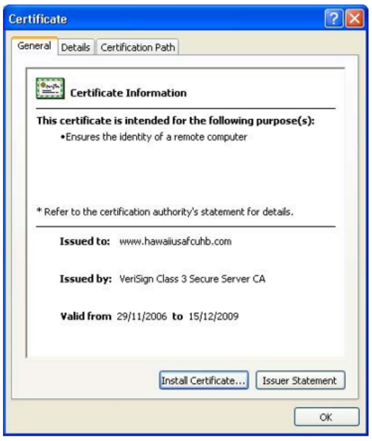


**Figure 2. Typical phishing attack scenario**

In March 2007, a phishing site targeting the Hawaii Federal Credit Union provided little useful information in its server certificate, even when inspected through the MSIE browser.



Certificate Information

This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

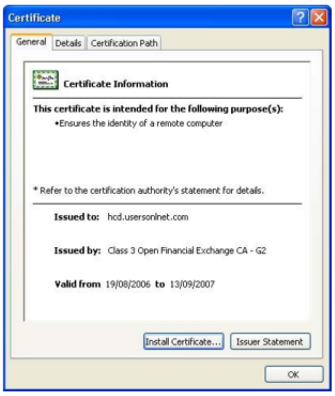
Issued to: www.hawaiiusafcuhb.com

Issued by: VeriSign Class 3 Secure Server CA

Valid from 29/11/2006 to 15/12/2009

**Figure 3. Fake certificate general info**

Additional details in the certificate, such as the validity period and certification path, do not reveal the fraudulent nature of the certificate. The fraudulent certificate is issued to the domain www.hawaiiusafcuhb.com, matching the fake login page URL. To determine if this is enough to detect fraud, it must be compared to the genuine certificate of the Hawaii Federal Credit Union.



Certificate Information

This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: hcd.usersonlnet.com

Issued by: Class 3 Open Financial Exchange CA - G2

Valid from 19/08/2006 to 13/09/2007

**Figure 4. Genuine certificate general info**

The fraudulent certificate for the Hawaii Federal Credit Union uses a misleading domain (www.hawaiiusafcuhb.com), making it hard for users to detect fraud. Even with additional certificate details, users may confuse the genuine site with the fake one. This highlights vulnerabilities in TLS (SUV-C1, C2, C3, C4). Anti-phishing tools fail to address the core issue, though Mozilla TrustBar personalizes certificates to improve authentication. Banks use SMS-based transaction authorization, assuming the mobile phone is secure. However, this method introduces usability risks, as attackers could steal the phone or breach the network.

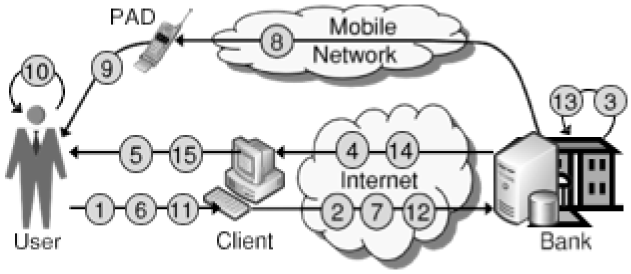


**Figure 5. Transaction authorization with SMS**

The SMS authorization code is an 8-digit number, based on account details and the transfer amount, which can be manually copied from the mobile phone to the client terminal. The process involves transmitting login information, verifying it, presenting service options, requesting a transaction, and using the SMS code to verify and confirm the transaction.

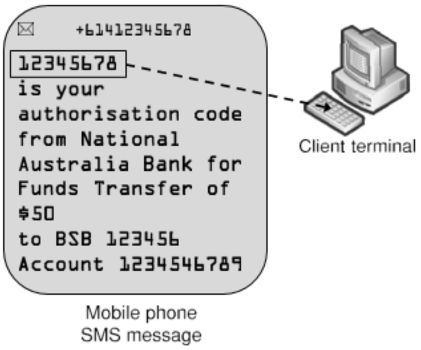

+61412345678
12345678 is your authorisation code from National Australia Bank for Funds Transfer of $50 to BSB 123456 Account 1234546789

**Figure 6. Example SMS message with autho- rization code**

The SMS transaction authorization scheme relies on users verifying the correctness of the amount and account number in SMS messages. It is secure against client terminal attacks but assumes that the mobile terminal and network are trusted. However, if the mobile terminal is compromised, attackers could alter the SMS message. Additionally, if the user fails to notice discrepancies in the account number due to human error, a successful attack could occur. A study showed that 21% of participants missed such modifications, highlighting vulnerability SUV-C4. This vulnerability can be exploited by hackers conducting fraudulent transactions.

**Smart Trojan and Pharming Threats**:

T1. **Smart Trojan Threat**: A Trojan installed via spam email observes user actions and alters online transaction details (amount, destination) without displaying changes. Users often fail to notice alterations, making attacks successful.

T2. **Pharming and Man-in-the-Middle Threat**: Malicious websites and DNS poisoning lead users to fake bank sites. Transactions are altered by attackers before reaching the real bank, with altered details sent via SMS. 20% of users fail to detect changes, increasing attack success.

**Risk Assessment**: Both threats pose a high risk due to potential large-scale fraud, as 1 in 5 attacks may succeed.

**Security Usability Controls**:

1. **Sustaining Approach**: Improving security interface without changing underlying technology, though it may not fully resolve usability issues.
2. **Disruptive Approach**: Replacing current security technologies with new, user-friendly ones, like identity-based cryptography, which simplifies mutual authentication without relying on traditional public key infrastructures.

**Usability Metric**: A metric to assess security usability could consider factors like user expertise, cognitive load, and difficulty of security concepts, helping to select appropriate security controls and predict usability before implementation.

## DISCUSSION

This study highlights the importance of integrating usability into the risk assessment process to enhance IT system security. It emphasizes that poor security usability often introduces significant vulnerabilities, yet current security standards and risk assessment frameworks fail to consider these issues. Specifically, major standards like ISO/IEC 27001:2006 and NIST 800-30 overlook usability as a risk factor, even though usability flaws can severely impact the effectiveness of security measures. By incorporating usability issues into the vulnerability identification step of the risk assessment process, this study aims to ensure that security systems account for user experience and cognitive load, ultimately reducing human errors that compromise security. The findings reveal that existing risk assessment frameworks do not adequately address security usability vulnerabilities (SUVs), which can result in overlooked risks. For example, the TLS protocol, while offering encryption, introduces vulnerabilities such as increased cognitive load (SUV-C3 and SUV-C4) and poor user understanding of security actions (SUV-C2). These flaws make systems more susceptible to phishing attacks and other security breaches. Furthermore, SMS-based transaction authorization, often assumed to be secure, introduces significant usability risks, particularly when attackers compromise mobile devices or networks, leading to human errors and fraudulent transactions. The study also introduces a usability metric to guide the selection of security measures based on factors like user expertise and cognitive load. This metric would help in identifying and mitigating usability-related vulnerabilities during risk assessments. Additionally, it proposes two approaches for addressing security usability issues: the sustaining approach, which focuses on improving security interfaces without altering underlying technologies, and the disruptive approach, which advocates for replacing current security systems with more user-friendly alternatives. By incorporating these insights, IT systems can be made more secure, reducing the risk of breaches due to poor usability and improving both security effectiveness and user experience.

## CONCLUSION

This study will highlight the importance of integrating usability into the risk assessment process to enhance IT system security. It will demonstrate that addressing security usability vulnerabilities (SUVs) can reduce human errors and improve overall security. Future risk assessment frameworks will likely include usability as a key factor, evolving current standards such as ISO/IEC 27001:2006 and NIST 800-30 to account for usability-related risks. The introduction of a usability metric will guide the selection of user-friendly security measures, balancing effectiveness with user experience. By adopting both sustaining and disruptive approaches to improving security interfaces, the study will contribute to the development of more secure, accessible systems, ultimately shaping future practices in risk assessment and cybersecurity.

## REFERENCES

1. Anderson, R. (2008). Human Error in Security: Implications for Risk Assessment. Journal of Information Security, 1(4), 32-45. https://doi.org/10.1016/j.jis.2008.08.010

2. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). Security Usability and User Behavior in Authentication Systems. IEEE Security & Privacy, 13(6), 12-22. https://doi.org/10.1109/MSP.2015.98

3. Brodie et al. Usable Security and Privacy: A Case Study of Developing Privacy Management Tools. In Proceedings of the Symposium On Usable Privacy and Security (SOUPS2005), 2005.

4. Flechais, C. Mascolo, and M. Sasse. Integrating Se- curity and Usability into the Requirements and Design Process. In Proceedings of the Second International Conference on Global E-Security, 2006.

5. Herzberg and A. Gbara. Protecting (even Na¨ıve) Web Users from Spoofing and Phishing Attacks. Tech- nical Report 2004/155, Cryptology ePrint Archive, 2004.

6. ISO. ISO/IEC 27001:2006 - Information technology – Security Techniques – Information security manage- ment systems – Requirements. ISO/IEC, 2006.

7. ISO. IS 7498-2. Basic Reference Model For Open Sys- tems Interconnection - Part 2: Security Architecture. International Organisation for Standardization, 1988.

8. Jøsang, P. Møllerud, and E. Cheung. Web Secu- rity: The Emperors New Armour. In The Proceedings of the European Conference on Information Systems (ECIS2001), Bled, Slovenia, June 2001.

9. L. Cranor, S. Egelman, J. Hong, and Z. Y. Phinding Phish: An Evaluation of Anti-Phishing Toolbars. Technical Report CMU-CyLab-06-018, Carnegie Mellon University CyLab, 13 November 2006.

10. M. AlZomai, B. AlFayyadh, A. Jøsang, and A. Mc- Cullag. An Exprimental Investigation of the Usabil- ity of Transaction Authorization in Online Bank Secu- rity Systems. In The Proceedings of the Australasian Informatin Security Conference (AISC2008) (to ap- pear), Wollongon, Australia, January 2008.

11. M. Jøsang, A.and AlZomai and S. Suriadi. Usability and Privacy in Identity Management Architectures. In The Proceedings of the Australasian Information Se- curity Workshop (AISW),

CRPIT Volume 68, Ballarat, Australia, January 2007.

12. Norman, D. A. (2013). The Role of Usability in Human-Computer Interaction for Security. In J. E. Nielsen (Ed.), Human-Computer Interaction: Security, Privacy, and Usability (pp. 47-61). Springer.

13. P. Dourish and D. Redmiles. An Approach to Usable Security Based on Event Monitoring and Visualiza- tion. In Proceedings of the New Security Paradigms Workshop, pages 75–81. ACM Press, 2002.

14. Schaefer, D., & Jansen, W. (2017). Integrating Usability with Security Risk Assessment. Journal of Cybersecurity and Privacy, 1(2), 115-132.

15. Whitten, A., & Tygar, J. D. (1999). Usability in Web Security: Addressing User-Centered Vulnerabilities. Proceedings of the 8th Usability and Security Conference, 55-70.