Introduction

Hello. Firstly, I want to welcome everyone listening to my presentation. I am here to discuss my research proposal on “the security risks associated with the OpenID Connect protocol in cloud-based applications”. Robust security protocols are essential as cloud-based applications become increasingly integral to various sectors. OpenID Connect, or short OIDC, is widely adopted for user authentication and authorisation, offering a standardised method for managing identities for the Web (Primbs, J. and Menth, M., 2024). However, with the growing reliance on OIDC, understanding its security risks is crucial to protect sensitive data and ensure system integrity. This research proposal aims to analyse the security risks associated with the OpenID Connect protocol in cloud-based applications and propose mitigation strategies.

Significance/Contribution to the Discipline/Research Problem

Now, I would like to introduce the significance of this research. To put it into context, OIDC plays a critical role in user authentication and authorisation in cloud-based applications. With the increasing adoption of cloud services, organisations need a secure and scalable way to manage user identities and access controls. OIDC facilitates this by providing a standardised method for identity management, reducing the complexity and enhancing the security of cloud deployments (Pöhn, D. and Hommel, W., 2020).

As OpenID Connect is an identity layer built on the OAuth 2.0 protocol (Li, W. and Mitchell, C.J., 2020). It allows clients to verify the identity of end-users based on the authentication performed by an authorisation server or an OpenID provider (Li, W., Mitchell, C.J. and Chen, T., 2019). However, despite its advantages, OIDC has security risks. If not properly understood and mitigated, these risks can lead to unauthorised access, data breaches, and other cyber threats, potentially causing significant harm to individuals and organisations. This research will explore these risks in-depth and provide actionable insights for securing OIDC implementations in cloud environments. Primarily, two main topics focused on in this research are scalability demands in the cloud concerning authorisation and general security risks associated with the Open ID Connect protocol. This will help strengthen the security of cloud-based applications using OpenID Connect and provide developers with practical strategies and guidelines to implement this protocol in a cloud environment.

Moving next to the slide, it shows how vital cloud computing is getting, as we can see the increase in the use of cloud-based applications over the years and for 2023, it is estimated to be worth 197 Billion US dollars, according to Statista (Vailshery, L.S., 2024). Such growth in the cyber-space also makes it susceptible as more attackers choose to take advantage of the vulnerabilities for their gain and potentially get valuable user data.

Research Question

In this slide, I would like to discuss the research question for this proposal and the question that revolves around the different security vulnerabilities of OpenID Connect when implemented in a cloud-based application. As mentioned, a robust authentication mechanism to secure access to user data is a must. With the boom of digitalisation, many applications like shopping, renting cars, and even critical infrastructures like health sectors using cloud-based services are creating a large influx of users, making services and daily tasks much more accessible and more effortless. Despite its benefits, several security challenges can arise due to misconfigurations, inherent protocol flaws, or inadequate security practices. Addressing these vulnerabilities is crucial for maintaining the integrity and confidentiality of user data, ensuring secure authentication processes, and preventing culprits who would take advantage of open vulnerabilities.

Aims

This research explores the security risks of deploying the OpenID authentication protocol within cloud-based systems. While OpenID facilitates simplified logins across multiple services, it introduces unique vulnerabilities in a cloud setting. The main aim is to research a few critical risks shadowing this protocol in a cloud environment. To give an example of some risks, I would like to mention a few of them in order to give an overview.

The first and foremost critical risk of deploying OpenID authentication is its reliance on a single point of failure (Navas, J. and Beltrán, M., 2019). If an attacker compromises this single authentication point, they potentially gain access to all connected services and data. The distributed nature of cloud services amplifies this risk, as it can lead to widespread data breaches across multiple platforms.

Next, we address phishing attacks. OpenID relies on redirecting users to an identity provider to log in. For example, phishers can exploit this by creating fake login pages to capture user credentials. In a cloud environment, where services and data are remotely hosted, such attacks can swiftly compromise vast amounts of sensitive data (Bilal et al., 2023).

Also, session hijacking is one of the issues that is very concerning. An attacker can intercept a user session post-authentication and impersonate the user within the cloud environment.

The research scope is not limited to these risks, but these risks will definitely be analysed due to their severity of damage, the necessity of determining how to mitigate them, and the damages caused if left alone.

Objectives

So, the three main objectives of this research would be to analyse potential vulnerabilities when scaling these protocols for millions of users. This could lead to issues like token leakage, improper session management, endpoint security flaws and other problems that will be identified. Secondly, after analysing the different risks and their severity, a system design for incorporating OIDC protocol in a cloud environment will be produced. Lastly, a prototype containing the main significant findings and important features from the investigations will also be implemented.

Key Literature

The main key literature that seems initially important for the research proposal are as follows, An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm, Oauth documentation, Cloud Computing Security Risks, Cloud Security Service for Identifying Unauthorized User Behaviour, Analyzing Privacy Implications and Security Vulnerabilities in Single Sign-On Systems.

Some literature, such as “An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm” from 2016 and Oauth documentation from 2013, are older than five years old. However, I have still chosen this literature as it still has significant importance in understanding OpenID connect protocol and its vulnerabilities and also its usage in cloud computing. Although older, these resources will provide a deeper analysis to contribute more understanding to the research that will be carried out.

Methodology/Development Strategy/Research Design

The research design will begin with a comprehensive literature review based on three primary areas: the Current Implementation of OIDC in Cloud Environments, an in-depth examination of documented vulnerabilities and known attack vectors associated with OIDC, and Existing Security Measures and their Effectiveness.

The literature review on these areas will aid the research by exploring various existing implementations of OIDC. If available, implementing the protocol in a cloud environment will help understand the critical areas, such as integration processes, configuration settings, and the overall architecture adopted by leading cloud service providers. This step is the basis of understanding the issues and would help in the next step, data collection.

As mentioned, the literature review will provide a solid basis for understanding the present issues and prioritising the current essential risks and problems. The data collection will be executed by employing two methods. The first is finding case studies of cloud-based applications that utilise OIDC. This step will involve selecting various applications to understand how different systems implement and manage OIDC security.

Secondly, conducting interviews with industry experts, including cloud service providers, security professionals, and developers. These interviews will provide valuable insights into practical challenges and best practices related to OIDC security.

### Risk Analysis

In addition, a risk analysis will also be carried out to estimate the amount of risk that was detected during the investigations and order the vulnerabilities according to the risk. The risk analysis will be divided into qualitative and quantitative components to provide a holistic view using qualitative and quantitative methods.

Using the data collected from literature review, case studies, and expert interviews, we will perform a qualitative analysis to identify common themes, patterns, and insights regarding OIDC vulnerabilities and security measures.

Furthermore, statistical methods will be applied to quantify the frequency, severity, and impact of identified vulnerabilities and attack vectors. This analysis will help in prioritising risks based on their potential effects on cloud-based applications using analysis methods like Monte Carlo simulations (Wang, J., Neil, M. and Fenton, N., 2020).

Prototype Design and Implementation

Finally, we will design and implement a prototype to validate our findings and proposed solutions. Based on the insights gained from our research, a design tool or application with listed configurations will be produced to enhance the security of OIDC implementations in cloud environments. This design phase will incorporate best practices and innovative approaches to mitigate identified risks.

Ethical considerations

Given the sensitivity of Personally Identifiable Information (PII) handled in the context of authentication, the research will strictly adhere to data privacy laws, particularly the GDPR (Intersoft Consulting, 2024). This includes obtaining explicit consent from individuals before collecting any PII and mentioning their identity in the research, ensuring data minimisation, and implementing robust data protection measures by redacting names and PII data.

A critical aspect of the research will be exploring if users are adequately informed about data sharing, authentication risks, and their implications. By prioritising explicit consent, data minimisation, robust protection measures, user awareness, and transparent communication, the research aims to be conducted with the highest ethical standards.

Description of Artefacts

As part of the research, the methodology will produce some artefacts.

This research will include the visual representations of the threat models developed for OIDC implementations. These diagrams will map the system architecture, identify entry points, and highlight potential attack vectors. This artefact will help prioritise vulnerabilities, guiding the focus of mitigation efforts.

Complementing the risk assessment, a diagram illustrating the interaction between these components within cloud environments and a report on how OIDC is integrated with various cloud platforms, examining configuration settings, authentication flows, and security mechanisms. This report will highlight best practices and common pitfalls.

Using the system design, a prototype application using OIDC protocol will be used to authenticate and authorise, outlining the architecture and features of the prototype application.

In the end, to test whether the analysis and prototype produced reduce the security risks found during the investigation, a penetration test will be conducted using tools like Micro-Id-Gym, Metasploit, and OWASP Zap. Micro-Id-Gym is a specialised tool that conducts penetration testing for Identity Management solutions (Bisegna et al. 2020). As a result, a document outlining the structured methodology used for penetration testing, including phases such as reconnaissance, scanning, exploitation, and post-exploitation, will be produced.

Timeline

Now, I will briefly discuss the research timeline shown by the Gantt chart in this slide, and for simplicity, it will start in June 2024. The whole research project is expected to be completed in 7 months, where Documenting and writing the thesis begins from the first day, running parallel to other tasks. The thesis writing is estimated to start in June and end in December, around six months. At the same time, the literature review and OIDC Cloud analysis are expected to be completed within the first month, as seen in the chart, by the end of June. After the initial investigation of the literature, the data collection phase will start, which will span over a month, parallelly from the middle of the month in June also with the available data the threat modelling will also be initiated.

As a result of threat modelling, a risk assessment will now be carried out, which will help us identify the vulnerabilities from critical to non-critical. This is estimated to take about 15 days, from the beginning to mid-August. Using the mitigations, a prototype design for the application will be made, which is estimated to be completed in fifteen days by the end of August. Afterwards, the prototype implementation and the penetration testing with documentation will be done, and it is estimated to be done by mid-November. Lastly, the thesis revision will be done to find any errors and prepare for submission. After the submission, the preparation for the defence will commence in mid-December.

This is the rough timeline with estimations in mind of how long each step will need.

This concludes my presentation on the security risk analysis of the OpenID Connect protocol in cloud-based applications. I hope you found the information valuable and insightful. Thank you very much.

## 

## References

Bilal, M., Shongwe, S., Bashir, A. and Ghadi, Y., 2023. Assessing secure OpenID-based EAAA protocol to prevent MITM and phishing attacks in web apps.

Bisegna, A., Carbone, R., Pellizzari, G. and Ranise, S., 2020, September. Micro-Id-Gym: a flexible tool for pentesting identity management protocols in the wild and in the laboratory. In International Workshop on Emerging Technologies for Authorization and Authentication (pp. 71-89). Cham: Springer International Publishing.

Intersoft Consulting (2024) Legal text, General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ (Accessed: 18 May 2024).

Li, W., Mitchell, C.J. and Chen, T., 2019, November. Oauthguard: Protecting user security and privacy with oauth 2.0 and openid connect. In Proceedings of the 5th ACM workshop on security standardisation research workshop (pp. 35-44).

Li, W. and Mitchell, C.J., 2020, September. User access privacy in OAuth 2.0 and OpenID connect. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 664-6732). IEEE.

Navas, J. and Beltrán, M., 2019. Understanding and mitigating OpenID Connect threats. Computers & Security, 84, pp.1-16.

Primbs, J. and Menth, M., 2024. OIDC2: Open Identity Certification With OpenID Connect. IEEE Open Journal of the Communications Society.

Pöhn, D. and Hommel, W., 2020, August. An overview of limitations and approaches in identity management. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-10).

Vailshery, L.S. (2024) SAAS market size worldwide 2024, Statista. Available from: https://www.statista.com/statistics/505243/worldwide-software-as-a-service-revenue/ (Accessed: 14 May 2024).

Wang, J., Neil, M. and Fenton, N., 2020. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security, 89, p.101659.