A Survey of Security Analysis in Federated Identity Management

Sean Simpson and Thomas Groß(✉)

Newcastle University, Newcastle upon Tyne, UK
thomas.gross@newcastle.ac.uk

Abstract. We conduct a systematic survey of security analysis in Federated Identity Management (FIM). We use a categorisation system based off the Malicious and Accidental Fault Tolerance framework (MAFTIA) to categorise security incidents in FIM. When security incidents are categorised, we can paint a picture of the landscape of problems that have been studied in FIM. We outline the security incidents that are happening across FIM protocols and present solutions to those security incidents as proposed by others.

Keywords: FIM · Survey · Dependability · MAFTIA · Microsoft Passport · OAuth · OpenID · Facebook Connect · SAML · Liberty Alliance

1 Introduction

Federated Identity Management (FIM) aims to alleviate the problem of a user having to remember too many credentials by allowing the user to sign into multiple Service Providers (SP) using the same credentials which are provided by an Identity Provider (IdP). Typically in FIM, the user will attempt to access a SP which will then redirect the user to authenticate with the IdP which will vouch for the user, communicating with the SP to say that the user is who they say they are. FIM solutions are seeing increasing use and numerous attacks on protocols used in FIM have been found, which is motivation to do a survey in the area.

Protocols in FIM have been analysed by others in an attempt to find security problems. The issue is that there is a lot of different information on the analysis of security protocols in FIM that remains uncompiled. Our goal is to create a survey paper for security analysis in FIM. We review existing peer reviewed academic publications that perform security analysis on FIM protocols to establish a common ground and collect knowledge. In addition, we want to create a unified way of looking at security incidents in FIM and offer a framework to do that. We do this to provide insight on attacks that are seen on multiple protocol suites and state the solutions to security incidents as provided by the authors of the surveyed papers.

© IFIP International Federation for Information Processing 2016
Published by Springer International Publishing AG 2016. All Rights Reserved
A. Lehmann et al. (Eds.): Privacy and Identity 2016, IFIP AICT 498, pp. 231–247, 2016.
DOI: 10.1007/978-3-319-55783-0_16

2 Related Work

Delft & Oostdijk presented a paper which collects the security issues that exist in OpenID [5]. There is an additional need to examine security issues across FIM which is what we aim to do. There have been attempts to survey FIM in general. For instance, Ghazizadeh et al. [2] survey issues within OAuth, OpenID and SAML. The FIM standards surveyed is somewhat limited because Liberty Alliance and WS-Federation are not considered. In addition, analysis on FIM implementations—such as Microsoft Passport—are not considered in the survey which also provide information on security issues in FIM.

3 Method

3.1 Aim

RQ1: Understanding the Security Landscape in FIM. What is the landscape of the security analysis in FIM? We investigate to what extent FIM vulnerabilities, attacks and intrusions can be modelled systematically in a fault-tolerance formalization to understand security issues in FIM. What areas in this landscape might be missing research attention?
RQ2: Common Attack Classes. Which attack classes are prevalent across protocol suites? Do these attack classes apply to protocol specifications or implementations? Which papers go a step further and find a flaw in the specification and test it on implementations.
RQ3: Solutions/Mitigations. What solutions have been proposed to mitigate attack classes?

3.2 Search Methodology

We have done a systematic literature review based on the foundations described by Kitchenham [4]. We used two search engines to perform the literature search: Scopus and Google Scholar. Figure 1 contains the overall search term, in the Scopus format.

We observed a number of key words being used and used synonyms. We based the protocols searched off of surveys done in the area of FIM protocols [6]. We needed a logically equivalent search in Google Scholar. Below is a part of the resulting search term. We executed the search term with the "search by relevance" radio option selected and the "where the words appear anywhere in the article" radio button selected. *Protocol* as can be seen in the template search below is substituted with the twelve FIM protocol terms that can be seen in the Scopus search (Fig. 2).

3.3 Inclusion and Exclusion

Inclusion. We included papers returned from the search based on the following criteria:

```
TITLE-ABS-KEY((Analysis OR Evaluation OR Examine OR Proof OR
    Attack OR Intrusion OR Vulnerability OR Risk) AND
Security AND Identity AND
(OAuth OR OpenID OR ``Liberty Alliance'' OR SAML OR ``Security
     Assertion Markup Language'' OR WS-Federation OR ``
    Microsoft Passport'' OR (Passport AND Protocol) OR
    Cardspace OR ``Facebook Connect'' OR ``Google Accounts''
    OR Shibboleth)) AND
(LIMIT-TO(SUBJAREA, ``COMP''))
```

Fig. 1. Overall search term used in Scopus, modulo plural forms.

```
Protocol Security Identity Analysis OR Evaluation OR Examine
    OR Proof OR Attack OR Intrusion OR Vulnerability OR Risk
```

Fig. 2. Overall search term in Google Scholar, modulo plural forms.

- Be in the subject area of computer science.
- Reference FIM protocols.
- Be published as part of a peer-reviewed venue (i.e., workshop, conference or journal).
- Be unique: some papers are published somewhere, and then a very similar version of that paper can appear from the same authors at other venues.

Exclusion. After the inclusion phase, we excluded papers based on the following criteria:

- We exclude secondary sources (hence, constrain the SLR to original research).
- We exclude papers that do not offer a combination of vulnerabilities and anticipated exploits thereof. Claiming a vulnerability is not sufficient.
- We exclude hypothetical analyses, which modify a standardized FIM protocol to conduct a "what-if" analysis. We want to collect security incidents for real FIM systems and not for proposed extensions which may or may not be acted upon.
- We exclude security incidents that are put forward for FIM in general. The security incident has to be specific to a certain FIM protocol. The reason for this is to ensure that we get a representation of security incidents possible on real FIM systems.

3.4 Data Collection

After the inclusion/exclusion refinement we have a sample of 31 papers. From those papers, we manually code parts that describe security incidents and weaknesses (e.g., vulnerabilities or attacks). These observations are classified using our categorisation system described in Sect. 3.6.

3.5 Malicious and Accidental Fault Tolerance (MAFTIA)

We categorised security incidents based on Malicious and Accidental Fault Tolerance (MAFTIA) principles [3]. MAFTIA is built upon the foundation of dependability [1]. The dependability area is concerned with understanding what happens when a system fails in order to apply fault tolerance to avoid a failure. While dependability focuses on accidental failures, MAFTIA adapts the founding notions of dependability for use in understanding how systems fail under the influence of a malicious adversary. We use the notions founded by the dependability community to understand and thereby categorise security incidents in FIM. We introduce a number of key terms from MAFTIA which we use to build our categorisation system.

Definition 1. Adversary *Malicious person or organizations at the origin of attacks.*

Vulnerability *A fault that is created during the development or operation of the system that if exploited causes an intrusion.*

Attack *A malicious interaction fault that attempts to exploit a vulnerability. Can be thought of as an intrusion attempt.*

Intrusion *An adversary-introduced fault. An intrusion is created as the product from an attack successfully exploiting a vulnerability by an adversary.*

Failure *When the system is adjudged to not be offering correct service.*

3.6 Our Categorisation System

While MAFTIA terms help us understand a security incident, they are too low level to be used for categorisation. In addition, there are some additional aspects to a security incident in FIM that are desirable to capture which are not considered by the MAFTIA framework. We therefore introduce our categorisation system for use in categorising security incidents in FIM. The categorisation system has six dimensions *Vulnerability, Attack Class, CIA Failure, Target Protocol, Incident Type,* and *Solution Presented.* The term *Vulnerability* has already been defined in Sect. 3.5. We will go on to define what the rest of these terms mean.

Definition 2. Attack Class *A collection of attacks, intrusions and resultant errors in a system that form casual chains from vulnerabilities to a security failure if the errors are not dealt with.*

Considering a casual MAFTIA fault-error-failure tree for vulnerabilities, attacks, intrusions, errors and ultimately security failures, the attack class contains the trunk of the tree. An attack class is an abstraction of the adversary attack which attempts to exploit a vulnerability—therefore it is separate from the vulnerability—and all of the resulting intrusion states and further attacks (which sometimes can be trivial, like entering a user password) that produce errors in a system—up until the point at which a failure occurs. The purpose of the attack class is to capture the essence of what an adversary does and abstract away from the unimportant details. The unimportant details being the order of attack events, intrusions and errors occur in and slight variations in what errors, intrusions and errors actually occur. There is always a critical attack event which the attack class derives it's handle from and the surrounding details can vary. It is often the case that certain vulnerabilities lead to certain attack classes (i.e., Weak DNS leading to DNS Poisoning) but that is not always the case (i.e., a replay attack class can be caused by unencrypted communications or from a lack of binding)—which is why we distinguish between the vulnerability and attack class.

Definition 3. Confidentiality, Integrity, Availability (CIA) Failure *We view a system to have failed when the confidentiality, integrity or availability of a service is violated for a user.*

In essence we translate what a failure would mean in a FIM system. We want to know how a user is affected by a security incident in order to discern the impact of intrusions. Also of note is that an account can be compromised by a security incident, in this case, the confidentiality, integrity and availability of the service can all be affected.

We also consider the target FIM protocol, the incident type—was the security incident found at the protocol level, the implementation level, or found at the protocol level and tested on the implementation—and whether a solution was proposed—sometimes that solution is implemented before the publishing of the paper and this will be stated when it happens. The introduced terms have evolved to capture six different dimensions in a surveyed security incident: What is the weakness in the system (*Vulnerability*)? What does the adversary do to attack the system (*Attack Class*)?) How does the security incident affect the user (*CIA Failure*)? What FIM protocol is the subject of the attack (*Target Protocol*)? Is the incident due to an implementation or design flaw (*Incident Type*)? Was a solution put forward by the author (*Solution Presented*)? We use all of these terms to describe surveyed security incidents in FIM in subsequent sections.

3.7 Limitations of Survey

We performed a systematic literature review on Scopus and Google Scholar. The limitations of this is that we might miss things. We are aware of one notable paper which did not appear from our search in Microsoft Passport by Kormann and Rubin [7]. We included this paper in the survey as an exception. This is the only paper we made this exception for and the reason we did this for this one paper is because we consider it a cornerstone in analysis of FIM systems. A number of other security analysis papers cite the paper by Kormann and Rubin and it was the first paper, to the best of our knowledge, to bring security issues in FIM to light.

We do not attempt to discern the quality of the reviewed papers. This introduces the fact that security incidents, which some may deem to be trivial, are represented in the survey. In addition, we cannot guarantee that every security incident is correct because if we begin to use our judgement to discriminate what we perceive as incorrect results we risk compromising the survey.

4 Surveyed Papers

In this section we briefly outline the landscape of what we have seen, sorted by targeted FIM protocols that we have considered in the survey in order to address RQ1. We can see if attack classes are occurring at the protocol or implementation level which relates to RQ2. Some solutions proposed by the authors are also presented which relates to RQ3. The various protocols considered can have a number of different versions—to keep the survey into the protocols simple, we ignore this complication.

4.1 Microsoft

We are considering the papers that are concerned with the numerous attempts made by Microsoft to implement the concept of FIM (Passport .NET, Microsoft Accounts and Cardspace). We found four papers in this category [7–10] and all four papers proposed security incidents effective at the protocol level but did not test them on implementations. Three papers [7,9,10] reported on the vulnerability of weak DNS being exploited by a DNS poisoning attack class which would force an unknowing user onto a malicious domain that is supposed to look familiar to them, in order to trick the user into logging on. The adversary will steal these credentials since the adversary owns the malicious domain and will then compromise the account of the user—leading to a myriad of CIA problems. Alrodhan & Mitchell proposed a solution, which is the uptake of DNSSEC [9].

Two of these papers point out a bogus merchant attack class capitalising on the FIM no trust infrastructure vulnerability (there is no safe infrastructure list, meaning a user does not know who to trust) which would lead to compromised user accounts [7,10].

Alrodhan & Mitchell [9] brings up the possibility of a malicious provider—which is a provider that wants to track the actions of a user—exploiting the centralised infrastructure vulnerability that FIM suffers from (IdP at the center of FIM system being able to track user actions). The malicious provider in control of the IdP will observe the SPs a user visits and build a profile. No solution was proposed by the author for this security incident. Kormann & Rubin also state that the centralised infrastructure vulnerability can lead to a Denial of Service (DDoS) attack.

4.2 OAuth

The papers that we found to have security incidents in this category [11–17] widely report on a Cross-Site-Request-Forgery (CSRF) attack that capitalises on a weak SP vulnerability. The OAuth specification outlines things the SP must do to resist CSRF attacks, which some SPs do not do. In fact, five of the seven OAuth papers analysed reported this vulnerability [11,13–16] on the implementations of OAuth. It was found that these security incidents were possible because of the implementations of the protocol themselves rather than fundamental problems with the OAuth protocol. All five papers suggested solutions to be implemented by the relevant providers—such as proposals to attempt to bind authorisation requests to browsers—and Ferry et al. [13] reported that the CSRF attack had been addressed immediately upon the report.

Two papers [12,17] both point out the same security incident, which is the idea that a weak user credential vulnerability can be exploited by a brute force attack. Alotaibi & Mahmmod suggested a solution to this attack, which was to implement a biometric authentication system [12].

Sun & Beznosov pointed out a large number of security incidents for OAuth [11], which included the already mentioned CSRF incident. Additional vulnerability-attack class relationships that are pointed out by this paper: Unencrypted communications (HTTP being used) leading to message modification (can tailor a message from an existing base message), automatic authorisation (if the user has granted a privilege it is automatically granted again) leading to Cross-Site-Scripting (XSS), a lack of binding (vulnerability where a sent message is not sufficiently tied to the sender) allowing a message to be modified with a public URL which is used to authenticate a user, a lack of binding vulnerability leading to session swapping (an honest user is logged in to an adversary account—potentially divulging confidential information). All of the security incidents relating to these vulnerability-attack class relationships were possible at the implementation level.

4.3 OpenID

The first notable thing about the surveyed OpenID papers [17–26] is how the message formatting (a parameter or part of the message is not signed properly—common in OpenID) vulnerability is exploited by the message modification (possible because the message is not protected properly) attack class for the purposes of compromising a user account. For instance, an adversary could modify parameters such as Openid.ext1.value.email as shown by Wang et al. [37]. Oh & Jin [18] exploit this and note an issue with the protocol specification that allows for this security incident to take place and tests it on a real implementation—but no solution is offered. Sovis et al. [19] only goes as far to note the possibility of the attack at the protocol level without appearing to test it on a real system. Sun et al. [21] formally analyses the specification to find flaws and then exploits those flaws on real implementations to make the incident type tested—in addition, a solution is suggested for this security incident which is to further cryptographically protect the message.

Another notable vulnerability-attack class combination is observed. The no-trust-infrastructure being exploited by a bogus merchant to compromise user accounts—three papers put forward this idea [20,22,23] on the protocol level. Feld & Pohlmann [20] put forward an identity card solution to counter the bogus merchant. Abbas et al. [22] proposes a challenge-response scheme based on public key cryptography. Hsu et al. [23] leverages mobile phones to provide a physical token.

Mainka et al. [26] pointed out two security incidents at the implementation level which compromised user accounts. The first exploited a lack of binding by launching a MITM attack and had a suggested solution. The second incident (described as three incidents, but can be broadly boiled down) involves a lack of binding vulnerability which can be exploited by a message modification attack.

Two papers listed a large number of attacks too numerous to list here. Krolo et al. [24] puts forward five security incidents at the protocol level with suggested solutions and one affected the availability of the service while the others compromised user accounts. Li & Mitchell [25] introduces seven security incidents at the implementation level with suggested solutions and two incidents affected user confidentiality and the other five resulted in a compromised user account.

Sun et al. [21] also provides two more security incidents that were tested on real implementations: a lack of binding leading to a replay attack and a vulnerable SP leading to a CSRF attack—recommendations for the SP to follow were suggested to counter these attack classes.

4.4 SAML

Out of the five SAML analysis papers we found [27–31], three show how a lack of binding can be exploited by a MITM attack class to compromise a user account. Armando et al. [27] pointed out the discovered incident at the protocol level and that that by the time the paper is published Google implemented a fix. Groß [28] described a protocol level incident—which also exploited a weak DNS vulnerability with a DNS poisoning attack class to progress to the MITM attack which a solution was presented for. Mainka et al. [31] shows that when the adversary has access to a valid access token several MITM style scenarios are possible that were fixed upon publication.

Two more security incidents are introduced by Groß [28] at the protocol level: an unencrypted message vulnerability is stated to be exploitable by a message modification attack class which sniffs the message and then modifies a part of it to send to a SP which will compromise the account of a user; and a lack of binding vulnerability exploitable by a replay attack to compromise a user account. A countermeasure to the replay attack class was proposed to check the IP address of the sender. A countermeasure was also proposed for the message modification attack class, it is suggested that the referrer tag is dropped by browsers.

Mayer et al. [30] put forward two unique security incidents. The first exploits a vulnerable IdP and is referred to as an ACS Spoofing attack class which is similar to a bogus merchant attack class but the bogus merchant in the ACS Spoofing variant steals the user credentials and logs into many SPs—rather than requiring the user to manually enter credentials. A vulnerable IdP is exploited again by a UI redressing attack class, which involves tricking a user into clicking a malicious web element through a transparent web element. Both of these incidents were said to be because of poor implementations and compromise the user account. The paper also reviews several countermeasures.

4.5 Liberty Alliance

We found two papers describing security incidents in Liberty Alliance [32,33]. Pfitzmann & Waidner [32] exploits the vulnerability lack of binding by launching a MITM attack of which the aim is to compromise the user account. The security incident was shown to be possible on the protocol level but was not tested on real implementations. A fix was implemented before the paper was published because Liberty Alliance acknowledged the issue and acted quickly although it was not stated which solution of the list of possible solutions outlined in the paper Liberty Alliance chose.

Ahmad et al. [33] outlined that a centralised infrastructure can be exploited by a malicious provider who wants to breach user confidentiality. The incident was proposed at the protocol level and no solution was presented.

4.6 Facebook Connect

We are considering the papers that claim to find security incidents [35–37] for Facebook's FIM protocol—Facebook Connect. Two papers that we found to have security incidents in this category [35,36] were found to have the unencrypted communications vulnerability. The unencrypted communications vulnerability was exploited by two different attack classes: the replay attack class [35] and communications sniffing (being able to read a message, but not being able to modify it or replay it) attack class [36]. The replay attack class was proposed as possible on the protocol level but the communications sniffing attack class was tested in practice. Miculan & Caterina [35], suggests a solution where a Diffie-Hellman key exchange is added to the protocol. Urueña et al. [36] suggests forcing HTTPS.

A centralised infrastructure vulnerability pointed out by Urueña et al. [36] was exploited by a malicious provider attack class which would affect the confidentiality of the user. The attack class was proposed at the protocol level and no solution suggested.

Wang et al. [37] states a message formatting vulnerability which can be exploited by a message modification attack class which aims to compromise the account of the user. The attack class was tested in practice, reported to Facebook, who fixed the issue before the publishing of the paper. This same kind of security incident was also found to be possible on Google Accounts.

4.7 Google Accounts

There were two papers [27,37] with security incidents in Google Accounts but we discuss these in the SAML and Facebook section.

4.8 Shibboleth

Chadwick [38] points out that Shibboleth can be exploited by a bogus merchant attack class with the aim of compromising a user account. The author

Table 1. Coded Vulnerabilities & Attack Classes in FIM

(a) Coded Vulnerabilities

Vulnerabilities
Unencrypted Communications
Centralised Infrastructure
Lack of Binding
No Trust Infrastructure
Weak DNS
Vulnerable SP
Vulnerable IdP
Automatic Authorisation
Message Formatting
Automatic Authorisation
Weak User Credentials

(b) Coded Attacks

Attacks
Replay Attack
Communications Sniffing
Malicious Provider
MITM
Message Modification
Bogus Merchant
Brute Force
XSS
Session Swapping
DNS Poisoning
DDoS
CSRF
ACS Spoofing
UI Redressing

notes that this is because there is no trusted infrastructure list for Shibboleth (unlike Microsoft Cardspace, which the author advocates). The security incident is stated at the protocol level and no solution is presented.

5 Results

5.1 Vulnerabilities and Attack Classes in FIM

We found 11 unique vulnerabilities and 14 unique attack classes from our survey which can be seen in Table 1. We consider attacks and vulnerabilities the main raw output from our categorisation system. Where it might not be clear what a vulnerability or attack class is, we define them in their first appearance in Sect. 4.

5.2 Cross-Protocol Issues

This answers RQ2. We identify 14 different cross protocol issues (cf. Table 2). We identify a cross-protocol issue when the same vulnerability, is exploited by the same attack class and creates the same CIA failure across at least one additional protocol.

5.3 The Numbers

Sample Size: When we conducted our SLR search of security analysis of FIM protocols initially we included **145 papers**. We excluded papers that did not

Table 2. Cross-protocol issues in FIM

ID	Vulnerability	Attack Class	CIA Failure	Affected Protocols
1	Message Format	Message Modification	Compromised Account	Facebook, Google, OpenID
2	Centralised Infrastructure	Malicious Provider	Confidentiality	Facebook, Liberty, Microsoft, OpenID
3	Unencrypted Communication	Replay	Compromised Account	Facebook, Microsoft
4	Weak User Credentials	Brute Force	Compromised Account	OpenID, OAuth
5	Unencrypted Communications	Message Modification	Compromised Account	OAuth, OpenID, SAML
6	No trust infrastructure	Bogus Merchant	Compromised Account	Microsoft, OpenID, Shibboleth
7	Vulnerable SP	CSRF	Compromised Account	OpenID, OAuth, SAML
8	Lack of Binding	MITM	Compromised Account	Liberty, SAML
9	Lack of Binding	Replay	Compromised Account	OpenID, SAML
10	Weak DNS	DNS poisoning	Compromised Account	Microsoft, SAML
11	Unencrypted Communications	Communications Sniffing	Confidentiality	Facebook, OpenID
12	Lack of Binding	Session Swapping	Confidentiality	OAuth, OpenID
13	Vulnerable SP, Automatic Authorisation	XSS	Compromised Account	OAuth, OpenID
14	Lack of Binding	Message Modification	Compromised Account	OAuth, OpenID, SAML

present security incidents until we had **31** papers left and **60** security incidents were found from the papers.

CIA: The proportion of security incidents which had a CIA failure listed as "Compromised Account" was **83.3%**. Confidentiality breaches accounted for **13.3%** and availability denials **13.3%**.

Solution Offered: Of the incidents proposed by authors, **16.6%** of those authors provided evidence that the protocol was fixed before the paper was even published. **66.6%** of authors at least suggested a solution while **16.6%** offered no solution.

6 Discussion

6.1 The Landscape of Security Analysis of FIM

We discuss this to address RQ1. In the majority of security incidents we survey, the "Compromised Account" was the most common CIA failure. This also happens to be the CIA failure with the most impact, seeing as an adversary can potentially compromise any CIA property from a compromised user account. In addition, we do not observe many security incidents that exploit solely integrity or availability (without first compromising an account).

We have seen a fair balance between security incidents at the protocol, implementation, and tested (where a protocol flaw is found and then tested on real implementations) level. It is important to continue to evaluate both Protocols and the implementations in FIM because one can not succeed without the other.

Some protocols have received more attention from analysts than others (such as OpenID, OAuth) and we can therefore paint a clear history of the security issues for those protocols. Other protocols have not received such wide spread attention, especially WS-Federation which our survey did not turn up a security analysis that presented a security incident. There is work in the area, such as work done by Groß [28] that demonstrates the protocol is secure under certain assumptions, but work investigating the flaws in WS-Federation seems to be missing. Other low attendance protocols are Shibboleth and Google Accounts. Are these low-attention protocols more secure or are researchers turning a blind eye to them for one reason or another i.e., perception of less people using these protocols?

A positive story is that the majority of security analysis are not only pointing out vulnerabilities and attack classes which can be used to exploit those vulnerabilities, solutions are attached also with only **16.6%** of authors not claiming a solution.

6.2 Cross-Protocol Issues

We discuss this to further answer RQ2. There were 14 security incidents we found that were cross protocol. Of these 14, some were not surprising as they capitalise on well known FIM weaknesses. Cross-protocol incident **2**, happens across FIM protocols because if an IdP is malicious, they can easily track a user. Cross-protocol incident **4** is also not a surprising find, it is well known that user credentials suffer from low entropy and in addition user credentials will generally be more valuable for an IdP in a FIM system because of the potential to more deeply compromise a single user. In a FIM system, the burden of authenticating a user is merely shifted to the IdP and so the cross-protocol incident **6**, which involves a bogus merchant attack class, is still a menace.

In fact, it could be argued that it's made worse because of the interconnected nature of FIM systems. In a similar vein, **10** involves a DNS poisoning attack which is also arguably more effective on a FIM system. All of the aforementioned cross-protocol issues are not surprising to be found to be happening cross-protocol.

Liberty Alliance is built on SAML and we can also see that the same security issue **8** has been reported for both of these protocols. OpenID and OAuth also have this relationship and the same issue is also reported in **13**.

What is surprising is that vulnerabilities such as "unencrypted communications" are not just seen on one protocol but across Facebook and Microsoft as can be seen by this cross-protocol issue **3**. It is worrying that such large ubiquitous organisations harbour these sorts of vulnerabilities. Cross-protocol issue **11** is also observed on Facebook and in this case confidential information is sent without protection and can therefore be intercepted and used by an adversary.

One creative issue is issue **12** where an adversary gets a user to sign into the attacker's account. The attacker hopes that the user will divulge confidential information because the user thinks they are safely using their own account. This highlights the importance of an in-depth security analysis because without it, unexpected issues like this would likely be overlooked.

Another worrying sign is brought to light by **7**, where vulnerable SPs have been exploited by CSRF attack classes on OAuth, OpenID and SAML. What we observed is that even though the protocol itself is thought of as secure, a bad implementation can create risks for users. This is worrying because not only is OAuth, OpenID and SAML ubiquitous on the web, but a single bad implementation could spell trouble for a user as shown by the numerous papers presented by our survey that demonstrate the CSRF attack class on real implementations.

6.3 Solutions/Mitigations

We concentrate on the solutions for dealing with the vulnerabilities and attack classes shown to occur cross protocol in order to address RQ3. This is in no way a survey of how these attack classes can be mitigated, we simply use a solution provided in the already surveyed literature.

Cross-Protocol issue 1: The basis of this attack class lies in the fact that the OpenID message (which is used in Facebook and Google implementations) can be modified by an adversary. Sun et al. [21] present a Diffie-Hellman key exchange to mitigate the attack class. The IdP also has to sign an assertion for the Diffie-Hellman key exchange to be secure.

Cross-Protocol issue 2: The malicious provider profiling a user is difficult to stop so most of the papers do not present a solution for it. There is one exception, Feld & Pohlmann [20] reference a German identity card called nPA where a person attests to another person who they are using biometrics.

Cross-Protocol issue 3: The solution to the replay attack as put by Miculan & Caterina [35] is to ensure SSL/TLS is used.

Cross-Protocol issue 4: Alotaibi & Ausif Mahmmod [12] state that biometrics can be used as a solution to weak user credentials.

Cross-Protocol issue 5: Messages can be modified if they are not properly protected. Sovis et al. [19] suggest ensuring all relevant message parameters are protected by a MAC code.

Cross-Protocol issue 6: According to Feld & Pohlmann [20], the German based identity card nPA can address bogus merchants by introducing a higher level of authentication.

Cross-Protocol issue 7: Sun et al. [21] suggest binding requests to the session taking place by hashing a secret together with a session id and appending that token into a hidden field in the login form as a solution to CSRF.

Cross-Protocol issue 8: When access tokens are not explicit to single SPs a MITM attack class can be launched. Pfitzmann & Waidner [6] propose (amongst other methods) a way of binding the token to the SP it is intended for.

Cross-Protocol issue 9: Groß [28] suggests binding the IP address to a request to stop Replay attacks.

Cross-Protocol issue 10: Alrodhan & Mitchell [9] point out that the widespread use of DNSSEC could mitigate the difficult to address DNS Poisoning attack.

Cross-Protocol issue 11: Manuel Urueña et al. [36] suggest disabling the HTTP referrer tag which is known to leak information.

Cross-Protocol issue 12: Lie & Mitchell [25] suggest adding a state value to bind a message in order to mitigate Session Swapping.

Cross-Protocol issue 13: We have observed that an XSS attack which results in an account being compromised requires two vulnerabilities: a Vulnerable SP and Automatic Authorisation. Sun et al. [11] state that inputs should be properly sanitized in order to prevent an injection.

Cross-Protocol issue 14: Sun et al. [11] note that SPs do not actually check some credentials which allow an attacker to engineer fake credentials, so the SP checking those credentials is a mitigation to the problem.

7 Conclusion

We put forward three research questions RQ1–RQ3 and these have been answered. We emphasise the contribution of providing a landscape of security incidents (RQ1) and common attack classes across protocols (RQ2). These contributions together provide overall insight into security issues in FIM on the whole but also particular issues that are affecting different FIM systems.

References

1. Avizienis, A., Laprie, J.-C., Randell, B., et al.: Fundamental concepts of dependability. Computing Science, University of Newcastle upon Tyne (2001)
2. Ghazizadeh, E., Zamani, M., Pashang, A., et al.: A survey on security issues of federated identity in the cloud computing. In: 2012 IEEE 4th International Conference on Cloud Computing technology and Science (CloudCom 2012), pp. 532–565. IEEE (2012)
3. Powell, D., Stroud, R., et al.: Conceptual model and architecture of maftia. Technical report Series, University of Newcastle Upon Tyne Computing Science (2003)
4. Kitchenham, B.: Procedures for performing systematic reviews. Keele University (2004)
5. Delft, B., Oostdijk, M.: A security analysis of OpenID. In: Leeuw, E., Fischer-Hübner, S., Fritsch, L. (eds.) IDMAN 2010. IAICT, vol. 343, pp. 73–84. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17303-5_6
6. Pfitzmann, B., Waidner, M.: Federated identity-management protocols. In: Christianson, B., Crispo, B., Malcolm, J.A., Roe, M. (eds.) Security Protocols 2003. LNCS, vol. 3364, pp. 153–174. Springer, Heidelberg (2005). doi:10.1007/11542322_20
7. Kormann, D.P., Rubin, A.D.: Risks of the passport single signon protocol. Comput. Netw. **33**, 51–58 (2000). Elsevier
8. Oppliger, R.: Microsoft.net passport and identity management. Inf. Secur. Tech. Rep. **9**, 26–34 (2004). Elsevier
9. Alrodhan, W., Mitchell, C.: Improving the security of cardspace. EURASIP J. Inf. Secur. 1 (2009). Springer
10. Gajek, S., Schwenk, J., Steiner, M., Xuan, C.: Risks of the CardSpace protocol. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 278–293. Springer, Heidelberg (2009). doi:10.1007/978-3-642-04474-8_23
11. Sun, S.-T., Beznosov, K.: The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 378–390. Springer (2012)
12. Alotaibi, A., Mahmmod, A.: Enhancing OAuth services security by an authentication service with face recognition. In: Systems, Applications and Technology Conference (LISAT), pp. 1–6. IEEE (2015)
13. Ferry, E., Raw, J.O., Curran, K.: Security evaluation of the OAuth 2.0 framework. Inf. Comput. Secur. **23**, 73–101 (2015). Emerald Group Publishing Limited
14. Li, W., Mitchell, C.J.: Security issues in OAuth 2.0 SSO implementations. In: Chow, S.S.M., Camenisch, J., Hui, L.C.K., Yiu, S.M. (eds.) ISC 2014. LNCS, vol. 8783, pp. 529–541. Springer, Cham (2014). doi:10.1007/978-3-319-13257-0_34
15. Shernan, E., Carter, H., Tian, D., Traynor, P., Butler, K.: More guidelines than rules: CSRF vulnerabilities from noncompliant OAuth 2.0 implementations. In: Almgren, M., Gulisano, V., Maggi, F. (eds.) DIMVA 2015. LNCS, vol. 9148, pp. 239–260. Springer, Cham (2015). doi:10.1007/978-3-319-20550-2_13
16. Yang, R., Li, G., Lau, W., et al.: Model-based security testing: an empirical study on OAuth 2.0 implementations. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp. 651–662. ACM (2016)
17. Grzonkowski, S., Corcoran, P.M., Coughlin, T.: Security analysis of authentication protocols for next-generation mobile and CE cloud services. In: 2011 IEEE International Conference on Consumer Electronics-Berlin (ICCE-Berlin), pp. 83–87. IEEE (2011)

18. Oh, H.-K., Jin, S.-H.: The security limitations of sso in openid. In: Advanced Communication Technology, pp. 1608–1611. IEEE (2008)
19. Sovis, P., Kohlar, F., Schwenk, J.: Security analysis of OpenID, pp. 329–340. Sicherheit (2010)
20. Feld, S., Pohlmann, N.: Security analysis of OpenID, followed by a reference implementation of an nPA-based OpenID provider. In: Pohlmann, N., Reimer, H., Schneider, W. (eds.) ISSE 2010 Securing Electronic Business Processes, pp. 13–25. Springer, Heidelberg (2011)
21. Sun, S.-T., Hawkey, K., Beznosov, K.: Systematically breaking and fixing OpenID security: formal analysis, semi-automated empirical evaluation, and practical countermeasures. Comput. Secur. **31**, 465–483 (2012). Elsevier
22. Abbas, H., Qaemi, M.M., Kahn, F.A., et al.: Systematically breaking and fixing OpenID security: formal analysis, semi-automated empirical evaluation, and practical countermeasures. Secur. Commun. Netw. (2014). Wiley Online Library
23. Hsu, F., Chen, H., Machiraju, S.: WebCallerID: leveraging cellular networks for web authentication. J. Comput. Secur. **19**, 869–893 (2011). IOS Press
24. Krolo, J., Marin, Š., Siniša, S.: Security of web level user identity management. In: 32nd International Convention MIPRO 2009 (2009)
25. Li, W., Mitchell, C.J.: Analysing the security of Google's implementation of OpenID connect. arXiv preprint arXiv:1508.01707 (2015)
26. Mainka, C., Mladenov, V., Schwenk, J.: Do not trust me: using malicious IdPs for analyzing and attacking single sign-on. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 321–336. IEEE (2016)
27. Armando, A., Carbone, R., Compagna, L., Cuellar, J., Tobarra, L.: Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps. In: Proceedings of the 6th ACM Workshop on Formal Methods in Security Engineering, pp. 1–10. ACM (2008)
28. Groß, T.: Security analysis of the SAML single sign-on browser/artifact profile. In: Computer Security Applications Conference, pp. 298–307. IEEE (2003)
29. Kumar, A.: A lightweight formal approach for analyzing security of web protocols. In: Stavrou, A., Bos, H., Portokalidis, G. (eds.) RAID 2014. LNCS, vol. 8688, pp. 192–211. Springer, Cham (2014). doi:10.1007/978-3-319-11379-1_10
30. Mayer, A., Niemietz, M., Mladenov, V., et al.: Guardians of the clouds: when identity providers fail. In: Proceedings of the 6th edition of the ACM Workshop on Cloud Computing Security, pp. 105–116. ACM (2014)
31. Mainka, C., Mladenov, V., Feldmann, F., et al.: Your software at my service: security analysis of saas single sign-on solutions in the cloud. In: Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security, pp. 93–104. ACM (2014)
32. Pfitzmann, B., Waidner, M.: Analysis of liberty single-sign-on with enabled clients. In: IEEE Internet Computing, pp. 38–44. IEEE (2003)
33. Ahmad, Z., Ab Manan, J.-L., Sulaiman, S.: Trusted computing based open environment user authentication model. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. V6–487. IEEE (2010)
34. Groß, T., Pfitzmann, B., Sadeghi, A.-R.: Browser model for security analysis of browser-based protocols. In: Vimercati, S.C., Syverson, P., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 489–508. Springer, Heidelberg (2005). doi:10.1007/11555827_28
35. Miculan, M., Caterina, U.: Formal analysis of Facebook Connect single sign-on authentication protocol. In: SOFSEM, pp. 22–28 (2009)

36. Urueña, M., Muñoz, A., Larrabeiti, D.: Formal analysis of Facebook Connect single sign-on authentication protocol. In: Multimedia Tools and Applications, pp. 159–176. Springer (2014)
37. Wang, R., Chen, S., Wang, X.F.: Signing me onto your accounts through facebook and google: a traffic-guided security study of commercially deployed single-sign-on web services. In: 2012 IEEE Symposium on Security and Privacy, pp. 365–379 (2012)
38. Chadwick, D.W.: Federated identity management. In: Aldini, A., Barthe, G., Gorrieri, R. (eds.) FOSAD 2007-2009. LNCS, vol. 5705, pp. 96–120. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03829-7_3