TDDD17 lab 1

Gustav Ahlberg gusah849
Claire Vacherot clava401

January 24, 2013

Exercise 1

When the user signs up for the website, he also has to download a specific app for his smart-phone and scan a QR-code that pairs with the phone to the newly created account to activate it. Then when the user wants to log in he has to supply his username to the website. He gets a response with a QR-code printed on the screen he has to scan with the app on his smart-phone. The application generates a one-time password based on the information in the QR-code. These information can only be interpreted by this specific application and not using other QR-code readers. The user then supplies the website with this one-time password to authenticate himself.

This is more secure than a ordinary password because it uses something that the user owns rather than what the user knows. To be able to get access to the account the attacker has to get physical access to the phone rather then just steal his password. That means that the attacker can't launch an attack on the user over the internet and the pool of possible attackers shrinks. The authenticated application can eventually be faked but this requires even more work to get to compromise it, and then after get access to the account. This can be avoided by authenticating the phone itself by logging its identity while accessing the website. The application can also be more secure if the user has to authenticate with an ordinary password before the QR-code can be scanned.

Figure 1: To be able to login the user has to first type in the username, generate a one-time password using the application and then use the one-time password to log in.

Figure 2: The sequence of actions to perform to authenticate with this method.

Exercise 2

2-1

OpenID

OpenID is used to authenticate a specific user by giving its identity, which is granted or not by the provider. The application has to know and verify using a certificate who you are to give the permission to access.

OAuth

OAuth is used to authenticate by using a key to get access given by the provider which has identified the user/process. This means that the application you log into doesn't need to know who you are, just that you have the permission (key) to access it on user's behalf.

2-2

1. OpenID delivers a certificate (the information needed to get access) whereas OAuth delivers a key (the means to access directly)
2. OAuth is about the user authorize the application to do things on the users behalf and OpenID authenticate the user so that the user can access the application.
3. OpenID only communicate with the user and OAuth allows the application the communicate with other applications that the user has authorized access to.
4. With OpenID the user can login to multiple websites using the same account information. With OAuth the user can share resources between applications.
5. With OpenID each application sees the user as a unique user and he has to specifically login to all the websites that uses OpenID. With OAuth the user only have to authenticate once to get access to several applications.

2-3

For both the application, being able to log in once extends the scope of the attacker (as you gain access to more than one account/application): For OpenID, getting the log in information for one means that you got them for everything. For OAuth being logged in to one application can mean you are logged in to a lot of them.

Exercise 3

3-1

Facebook.com IDP

Google.com IDP

YouTube.com RP

Yahoo.com IDP and RP

Baidu.com None

Wikipedia.org None

Live.com IDP

Amazon.com None

QQ.com None

Twitter.com IDP

Taobao.com None

Blogspot.com RP

Google.co.in IDP

LinkedIn.com RP

Yahoo.co.jp None

sina.com.cn None

Google.co.jp IDP

eBay.com None

Msn.com RP

yandex.ru RP

When we look at the login page of a webite we can see if we are provided with the option to log in using another account. Then we know that this website is a RP.

3-2

Computers

Most of the sites of this top are IDP or RP, related to Facebook or Google mainly.

Facebook IDP

Google IDP

Youtube RP (Google)

Gmail RP (Google)

Yahoo IDP and RP (Google and Facebook)

Wikipedia None

Yahoo Mail RP (Google and Facebook)

Windows Live Hotmail RP (Microsoft Account)

Twitter IDP

Linkedin RP (Facebook)

Shopping

From the top 10 of this section, only one is an RP (Groupon, on which you can login with your Facebook account). There is no IDP.

Almost no shopping site uses an IDP, we think that is is because the shopping sites want to have full control over the customer and not rely on any third parties to have a functional website. Most shopping sites also save a lot more information about the customers (such as payment information), so they will need some kind of customer database anyway.

3-3

France

Google France IDP

Facebook IDP

Google IDP

Youtube RP (Google)

Windows Live Hotmail RP (Microsoft Account)

Amazon.fr None

Leboncoin.fr None (no registration required)

Wikipedia None

Yahoo IDP and RP (Google and Facebook)

Orange RP

Sweden

Google IDP

Facebook IDP

Google IDP

Youtube RP (Google)

Aftonbladet RP (SPiD)

Wikipedia None

Windows Live Hotmail RP (Microsoft Account)

Yahoo IDP and RP (Google and Facebook)

Blocket None

Swedbank RP (BankID)

Between Sweden and France the number of IDPs and RPs are almost the same. The most common IDP is Google.