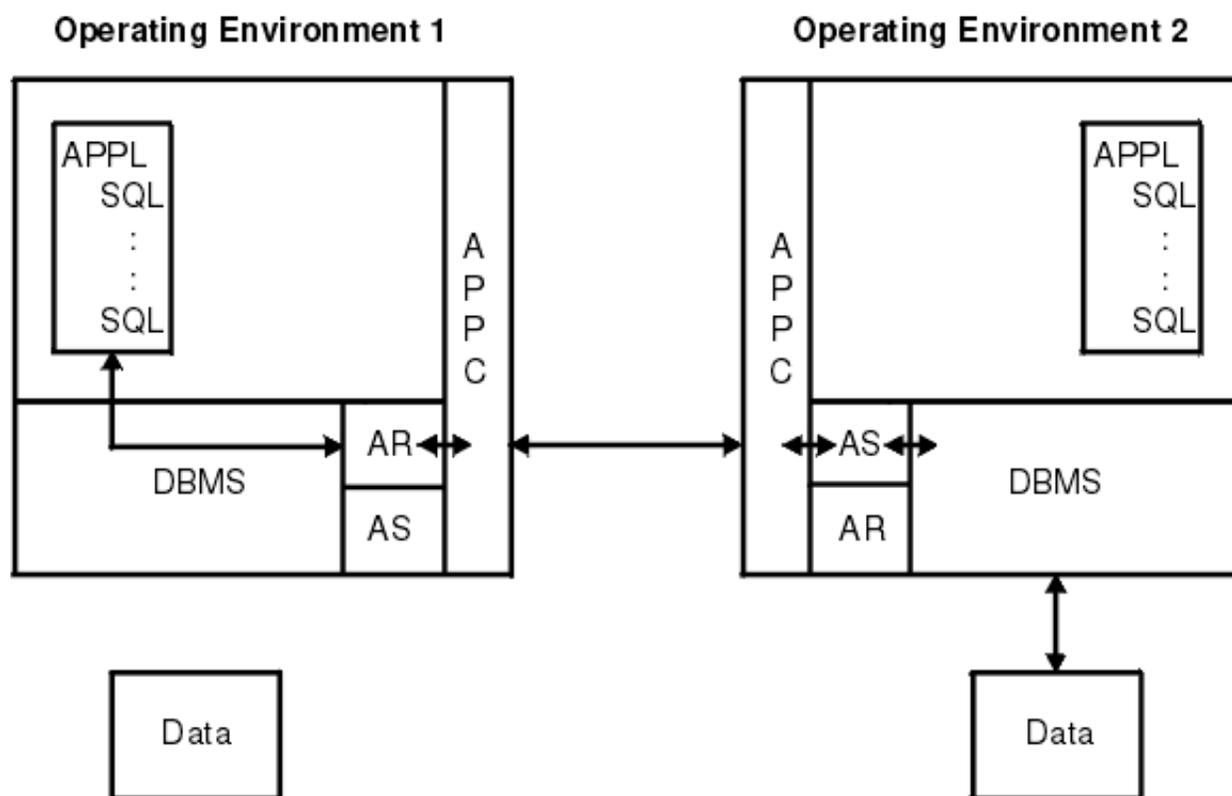


Remote Data

LUCA VENTURA | DVP 2
E: LAVENTURA@FULLSAIL.EDU

WHAT IS REMOTE DATA

Remote data is digital information that is already stored in a location that can be accessed. Open Database Connectivity (ODBC) is an interface that makes it possible to access data from a plethora of different database management systems (DBMSs). Because ODBC is independent of database systems and operating systems it can be ported to other platforms on both the client side and server side. When accessing remote data there are two parts: the system requesting the data (called the application requester) and the system that needs to handle that request and send the data back (known as the application server). Lets say your are using Facebook to log into a third party app, the application requester will send a request to verify the user credentials from Facebook and return the name, email address and profile picture of that user, the application server will process this request and send the requested data back to the application requester which returns the information back to the application program.



WHERE TO GET REMOTE DATA

THREE POSSIBLE PLACES AND USES

Remote data can be as simple as using an HTTP request to obtain search results from Google or as advanced as accessing a satellite in the sky. In both cases remote data is being accessed, because in both cases you are retrieving data that is already stored in a non-local database. Here are three specific examples of when remote data could be gathered and how that data could be used:

Weather App: When you check the weather on your phone, tablet, computer, whatever it may be, that weather report is not local. Remote data is being gathered from countless locations, ranging from weather databases to satellites (think about the Satellite view in a weather app) and more. That information is in-turn used to tell you the current, future and past weather reports.

Navigation App: Nowadays smartphones know where you (aka the phone) are at all times, and how they know this is by accessing and gathering remote data. When you use the “locate me” function of navigation apps your phone attempts the following three things in order to determine your location, and all of them involve remote data. Your phone either acquires a GPS satellite link, determines your location via a WiFi network or uses cell tower data.

Social Logins: Every time a user logs into an application via a social media account an API call is made to said social media platform. This call usually verifies your login credentials and then makes your profile image, name and email address available to the third-party app you are logging into. This information is used by that app to create a profile within their database, which is why your profile with that app will have the same profile image as your Facebook account.

TWO TYPES OF DATA FACEBOOK CAN USE AND WHY

Location Data: Facebook uses the location data that is gathered from your smartphone (which is acquired using remote data sources) to allow you to include a location in your posts and also let you check in at a specific location, such as a restaurant. The catch is that this information is only available to Facebook if you choose to let them have access to it. This is done through the Location settings for the Facebook app (on the iPhone). You can choose to not share your location with Facebook, but then you will not be able to include locations in your posts and some other features.

Browsing History: It should come as no surprise that Facebook tracks what you search and what websites you visit (among other things). They use this information for marketing purposes, such as displaying a product that relates to a search that user made earlier that day.

TWO TYPES OF DATA FACEBOOK CANNOT USE AND WHY

User Information: Over the years there have been many reports of Facebook selling user information, photos, browsing history and more to advertisers. While it is certainly true that Facebook stores and uses information such as your browsing habits, one thing that Facebook cannot sell to advertisers is data that can be used to directly identify you, such as your name or email address.

Disabled Data: Facebook can access a lot of information about you, more than you know they could, but there are some limitations. You have the ability to limit some things that Facebook is allowed to access. For example, on the iPhone you can turn off the Location Services and Photo access for Facebook. However, most, if not all, users will allow Facebook to access this data because it is an integral part of the "social" norm when it comes to sharing photos and location data.

TWO SECURITY ISSUES WITH REMOTE DATA

When accessing data remotely there is always a security concern, because this information is not housed locally and needs to be accessed from an outside source. Multiple security questions can arise in these situations, such as: is the remote data secure? Is the data confined within the remote database trustworthy? Can the request/call to this remote database be intercepted?

Issue #1: When accessing remote data over HTTP extra attention needs to be put on security because you don't know if the information you are retrieving is safe. Directory Traversal Attacks can be exploited with HTTP and allows for attackers to access restricted directories and execute commands outside of the root directory for that specific web server. This goes for all data, not just remote data obtained via HTTP. However, a Directory Traversal Attack is specific to HTTP.

Issue #2: The second issue that arises with remote data pertains to the request to access and gather the remote data. When your application requester sends out a request to an application server the call can be intercepted and/or rerouted before it reaches the application server. This is known as "API Hooking" and can leave your server vulnerable to DLL (Dynamic-Link-Library) injections and other attacks. Attackers can use DLL injections to inject code that can hook into function calls, read password textboxes and more.

REFERENCES

IBM Knowledge Center. (n.d.). Retrieved July 19, 2016, from https://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.13/gtpa3/rda.html

Microsoft Open Database Connectivity (ODBC). (n.d.). Retrieved July 19, 2016, from [https://msdn.microsoft.com/en-us/library/ms710252\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms710252(v=vs.85).aspx)

Understanding iOS Location Services. (n.d.). Retrieved July 19, 2016, from <http://www.quepublishing.com/articles/article.aspx?p=1927378>

Facebook and Location | Facebook Help Center | Facebook. (n.d.). Retrieved July 19, 2016, from <https://www.facebook.com/help/337244676357509/>

Do advertisers have access to my personal information? | Facebook Help Center | Facebook. (n.d.). Retrieved July 19, 2016, from <https://www.facebook.com/help/146156215456790>

Facebook. (n.d.). Retrieved July 19, 2016, from https://www.facebook.com/full_data_use_policy

What is a Directory Traversal Attack? (n.d.). Retrieved July 19, 2016, from <http://www.acunetix.com/websecurity/directory-traversal/>

API Hooking and DLL Injection on Windows - InfoSec Resources. (2013). Retrieved July 19, 2016, from <http://resources.infosecinstitute.com/api-hooking-and-dll-injection-on-windows/>

LUCA VENTURA
E: LAVENTURA@FULLSAIL.EDU