ACCESS SECURITY ALERT:

SSL MAN-IN-THE-MIDDLE ATTACKS

There have been reports that the authorities have been compromising the Facebook accounts of citizens in closed and semi-closed societies by perpetrating clumsy Man-In-The-Middle attacks on the SSL encryption used when a user 'securely' accesses those social networking sites.

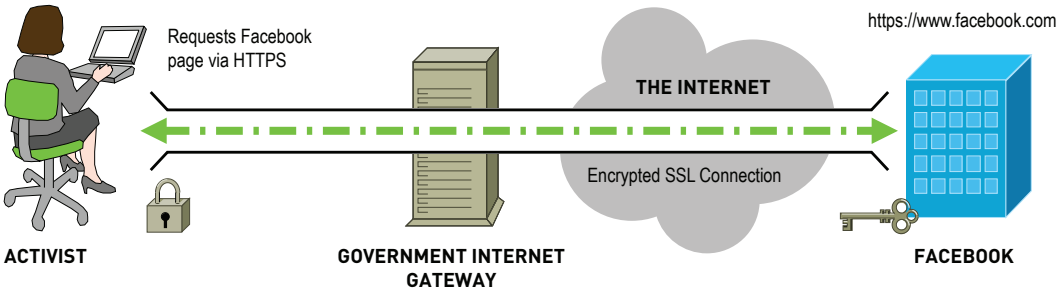
This guide is designed to offer a brief explanation of how Man-In-The-Middle (MITM) attacks are perpetrated by authorities on encrypted connections to websites and to help you take measures to protect yourself.

You need to be aware that any agency that owns or has access to the computer infrastructure within a nation which data must pass through to reach the internet can perpetrate a MITM attack on any connection, SSL encrypted or otherwise, to sites external to that nation.

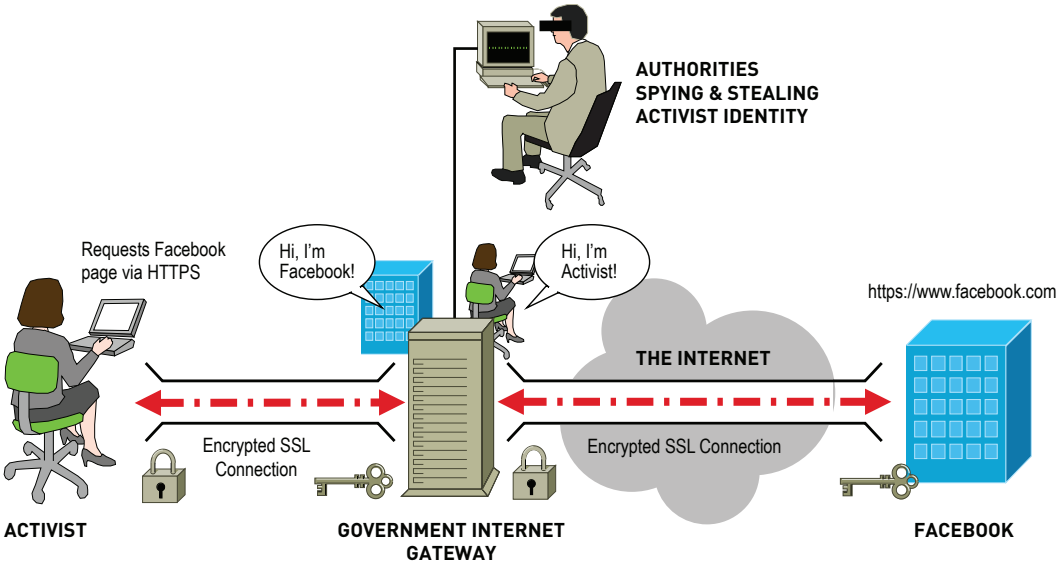
Normally, when you connect to a remote web site using the "https" protocol, the connection is encrypted end-to-end between you and the remote site using SSL (Secure Sockets Layer). However there have been reports that authorities have been perpetrating what is known as a "Man-in-the-middle" (MITM) attack when people within those nations have been using SSL encrypted connections to Facebook[1]. The authorities are able to do this because they have access to computer infrastructure that the encrypted connections would normally pass through. While this guide uses Facebook as a point of reference, it is important to note that all users and all sites are vulnerable to such an attack and that the vulnerability exists not in the Facebook platform, but in the way internet traffic is routed and encrypted.

The MITM attack is carried out as follows:

Normal Scenario



Man-in-The-Middle Attack



Here is how this Man-In-The-Middle attack is perpetrated:

1) You request an encrypted connection to Facebook
2) The authorities intercept this request as it tries to pass through the computer they have control of
3) The authorities pretend to be Facebook and present you with a fake certificate which causes a self-signed certificate warning to appear
4) You accept the fake certificate as an exception and this completes the setup of the encrypted connection with you
5) The authorities also pretend to be you and request an encrypted connection with Facebook
6) Facebook completes the setup of the encrypted connection with the authorities pretending to be you
7) Facebook issues a challenge for you to login to your Facebook profile
8) The authorities pass this challenge on to you
9) You (or your computer if you have saved your login credentials) pass your login credentials to the authorities (still believing them to be the legitimate Facebook). Once they have the credentials they are able to gain unlimited access to your account
10) The authorities save your login credentials to disk and/or open another connection to the real Facebook and supply your credentials to access your Facebook profile as if they were you
11) The authorities pass your login credentials on to the real Facebook
11) Facebook confirms your authority to login to your Facebook profile and passes back your profile page
12) The authorities pass your profile page back to you (this continues for the remainder of your session on Facebook, with the authorities passing everything between you and the real Facebook, but able to "see" everything you do as they are sitting "in-the-middle" of the connection)

To summarize, the authorities who are "in-the-middle" are pretending to be Facebook to you, and pretending to be you to the real Facebook. The connection between you and the fake Facebook is encrypted, and the connection between the fake you and the real Facebook is also encrypted. However, since the authorities are the ones that have set up one end of each encrypted connection, they are able to decrypt the data from one connection before re-encrypting it to pass it over the other connection. In this way, as they are passing the data back and forth between you and the real Facebook, they have the data unencrypted and can thus see everything you are doing. In addition to this, they now have your login credentials and can pose as you to Facebook without having to have you there to pass data back and forth. This means the authorities can look through your Facebook account, see who your friends are, and view all of the messages you have exchanged with them. They can also impersonate you and lock you out of your own account.

Note that all SSL encrypted connections are vulnerable to these clumsy man-in-the-middle attacks so be aware that other sites providing HTTPS access to their content or services including, but not limited to, Twitter, Google, Gmail, YouTube, etc may also be compromised by the authorities. Please be vigilant.

What to Do

There are a few important steps you can take in order to protect yourself from such attacks.

Step One: You should delete all the SSL certificates saved in your browser. Below are instructions for doing so for several popular browsers [Please note that menu and icon names and locations may vary slightly across different operating systems and versions].

Firefox:
Click on the 'Edit' menu item located at the top left corner of your browser. Select 'Preferences'. In the preferences dialog click on the 'Advanced' icon and then choose the 'Encryption' tab. In that tab space click on the button named 'View Certificates'. Select the 'Others' tab and select all the certificates listed by clicking on the first one and then scrolling down to the bottom of the list and Shift-click on the last entry. Then click on the 'Delete' button.

Chrome:
Click on the spanner icon in the top right corner of the browser. When the 'Preferences' page loads in the browser click on the 'Under the Hood' link on the left hand side, then at the bottom of the page loaded in the main area of the browser you should see the section titled 'HTTPS/SSL' with a button named 'Manage Certificates'. Click on that button. Select the certificate/s under 'Your Certificates' and then hit the 'Delete' button.

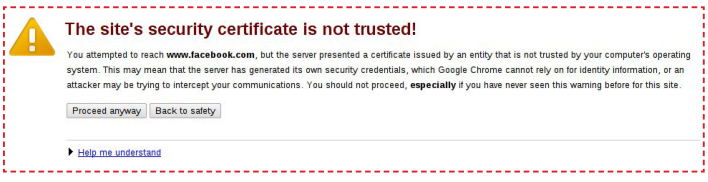
Safari:
Open the Finder application and click on 'Applications', then 'Utilities'. Execute the 'Keychain Access' application and select the 'Certificate' category on the left-hand side. Select the certificates by clicking on the first one, scrolling down, holding the 'shift' key and clicking on the last certificate. Then go to the menu at the top of the screen and select 'Edit' and 'Delete'.

Internet Explorer:
Click on 'Start' and open the 'Control Panel'. From there select 'Network and Internet Connections' and 'Internet Options'. Under the 'Content' tab you will find the 'Certificates' button. Click on that and then select the 'Trusted Root Certification Authorities' tab. Select the certificates you want to delete and click on the 'Remove' button, then 'Yes' in the dialog that appears, then 'Ok' and 'Ok' to finish.

Step Two: Restart the browser, return to sites using HTTPS and watch for errors.

For all browsers:
Now visit the sites again by typing the URL into your browser's location bar. Be sure to specify the protocol as "https://" for SSL encryption (e.g., https://www.example.com). If you get no warning you can be reasonably sure that the certificate is from the legitimate site and has been properly verified by your browser [Please note that a more sophisticated attack may not trigger a warning. We therefore always encourage at-risk users to connect through the Tor Network].

If you get an error message on your screen warning you that the certificate is self-signed or not verifiable DO NOT accept the certificate and DO NOT create an "Exception." The error dialog may look like the one below.



To proceed any further you will need to use an additional technology to communicate to Facebook without interference from the authorities. Note that using one of the following technologies is a great idea even if your SSL certificates for Facebook and Twitter are verified as being legitimate, as they further protect your identity and actions.

For further instructions on how to remove untrusted certificates, including a step-by-step visual guide for each browser, go to https://www.accessnow.org/policy-activism/press-blog/removing-untrusted-certificates.

Use Tor to Connect to Social Networking Sites

The most secure way to access social networking sites is to connect via the Tor system. Please refer to the "Protecting Your Security Online" guide for information on installing and using Tor. Note, connections via Tor can be slow, but it is by far the most secure way of connecting to social networking sites.

Use an HTTPS Proxy Outside the Region of Risk to Connect Through

If Tor is too slow, you can use an HTTPS proxy to connect through. This method is not safe from Government MITM attacks. It relies on the authorities not intercepting the encrypted connection on the basis they don't realize it is an interaction they are interested in. They will not see you connecting to Facebook, rather they will see you connecting to just an IP address or unfamiliar domain. Once you have an encrypted connection to the proxy you then request to login to Facebook, but since the authorities are unlikely to have seen the connection as something they want to perpetrate a MITM attack on the request to Facebook may go unseen by the authorities. The proxy will forward the request on to Facebook on your behalf, and forward the responses from Facebook back to you over the encrypted connection. Also be aware that any proxy you use can monitor your traffic, so pick proxies you trust or that are unlikely to have any interest in your communications.

Use Best Security Settings on Facebook

Tightening your privacy settings on Facebook will reduce the chance of your communications via the site being viewed by the authorities if they compromise the account of someone else two steps removed from you. Please read and utilize the guide "How to Organize on Facebook Securely" available at: http://www.movements.org/how-to/entry/organize-on-facebook-securely/

Risks of Using Facebook and other Social Networking Sites

Even if you verify the SSL certificates in your browser for Facebook, you need to be aware that the site should still be considered a risk to use. If the authorities compromise the account of another individual that you communicate with they may see your postings from that individual's perspective. Please remember that while you may have taken appropriate steps to ensure your communications are not spied upon when you post, your intentions may still be revealed by the insecure practices of the individuals or groups you have conversed with. We have also heard reports of cases where individuals have been detained and tortured by the authorities with the aim of obtaining the Facebook , Twitter and other social platform login credentials of activists[2][3][4]. You should be aware that the Facebook and Twitter accounts of other activists you interact with may have been compromised and therefore any of your past and future activity via these social platforms may be known by the authorities.

Alternatives

There is currently no fully functional secure social networking site ideally suitable for activist use. However, at least three social networking systems are currently in development and may be increasingly useful for coordination and mobilization activities in the near future.

- **Crabgrass**
  http://tiny.booki.cc/?crabgrass
  Crabgrass is a collaboration platform and social networking site being build by activists for activists. Crabgrass is being developed by RiseUp, a well-known technical activist collective.
- **Diaspora**
  https://joindiaspora.com/
  Diaspora is a decentralized social networking platform build around concepts of greater control and privacy for the users. It is currently being developed by students at the NYU Courant Institute of Mathematical Sciences.
- **Google+**
  https://plus.google.com/
  Google+ is the new social networking platform from Google. It offers more granular control than Facebook in its privacy settings. It also appears to allow for profiles not associated with an individual's real identity. Currently Google+ is in limited release and although rumored to be a better platform for activist use, it is too early to tell how appropriate it will be for that use.

References

[1] A Syrian Man-In-The-Middle Attack against Facebook, EFF, May 2011.
[2] Syria Torturing Activists for Facebook Passwords, Newser, May 2011.
[3] Syria 'tortures activists to access their Facebook pages', The Telegraph, May 2011.
[4] How Sudan used the Internet to crush protest movement, McClatchy Newspapers, April 2011.

Access (https://www.accessnow.org) is an international human rights organization working to promote and protect digital rights through technology, policy and advocacy.