

11 August 2008

By: Lucian Constantin, Web News Editor



Gmail account hacking tool presented at Defcon
TECKH

[Gmail Account Automatic Hacking Tool Presented at Defcon](#)

Users are encouraged to enable the permanent https option in Gmail

A tool that automatically steals IDs of non-encrypted sessions and breaks into Google Mail accounts has been presented at the Defcon hackers' conference in Las Vegas. Last week Google [introduced a new feature](#) in Gmail that allows users to permanently switch on SSL and use it for every action involving Gmail, and not only, authentication. Users who did not turn it on now have a serious reason to do so as Mike Perry, the reverse engineer from San Francisco who developed the tool is planning to release it in two weeks. When you log in to Gmail the website sends a cookie (a text file) containing your session ID to the browser. This file makes it possible for the website to know that you are authenticated and keep you logged in for two weeks, unless you manually hit the sign out button. When you hit sign out this cookie is cleared. Even though when you log in, Gmail forces the authentication over SSL (Secure Socket Layer), you are not secure because it reverts back to a regular unencrypted connection after the authentication is done. According to Google this behavior was chosen because of low-bandwidth users, as SLL connections are slower. The problem lies with the fact that every time you access anything on Gmail, even an image, your browser also sends your cookie to the website. This makes it possible for an attacker sniffing traffic on the network to insert an image served from **http://mail.google.com** and force your browser to send the cookie file, thus getting your session ID. Once this happens the attacker can log in to the account without the need of a password. People checking their e-mail from public wireless hotspots are obviously more likely to get attacked than the ones using secure wired networks. Perry mentioned that he notified Google about this situation over a year ago and even though eventually it made this option available, he is not happy with the lack of information. "Google did not explain why using this new feature was so important" he said. He continued and explained the implications of not informing the users, "This gives people who routinely log in to Gmail beginning with an https:// session a false sense of security, because they think they're secure but they're really not." If you are logging in to your Gmail account from different locations and you would like to benefit from this option only when you are using unsecured networks, you can force it by manually typing **https://mail.google.com** before you log in. This will access the SSL version of Gmail and it will be persistent over your entire session and not only during authentication.