CLOUD

Gmail, Outlook.com and e-voting 'pwned' on stage in crypto-dodge hack

Once you enter, you can never ~~leave~~ logout

By John Leyden, 1st August 2013 Follow 1,738 followers

18

Black Hat 2013 Security researchers say they have developed an interesting trick to take over Gmail and Outlook.com email accounts - by shooting down victims' logout requests even over a supposedly encrypted connection.

And their classic man-in-the-middle attack could be used to compromise electronic ballot boxes to rig elections, we're told.

Ben Smyth and Alfredo Pironti of the French National Institute for Research in Computer Science and Control (INRIA) announced they found a way to exploit flaws in Google and Microsoft's web email services using an issue in the TLS (Transport Layer Security) technology, which encrypts and secures website connections.

Full details of the attack are yet to be widely disseminated - but it was outlined for the first time in a demonstration at this year's Black Hat hacking convention in Las Vegas on Wednesday.

In short, we're told, it uses a TLS truncation attack on a shared computer to block victims' account logout requests so that they unknowingly remain logged in: when the request to sign out is sent, the attacker injects an unencrypted TCP FIN message to close the connection. The server-side therefore doesn't get the request and is unaware of the abnormal termination.

The pair explained:

> **In essence, we block encrypted messages that are sent over the network to de-synchronize authorisation: we force Gmail and Hotmail [Outlook.com] to display on your browser the page that announces that you have successfully signed-out, whilst ensuring that your browser maintains authorisation with Gmail and Hotmail [Outlook.com].**
> **Given such an announcement, you should be assured that you are secure, in particular, a hacker should not be able to access your email, even if you [log out and] leave your computer unattended. However, we can violate this basic security premise and access your Gmail and Hotmail [Outlook.com] accounts just by reloading the web page.**

The attack does not rely on installing malware or similar shenanigans: the miscreant pulling off the trick must simply put herself between the victim and the network. That could be achieved, for example, by setting up a naughty wireless hotspot, or plugging a hacker-controlled router or other little box between the PC and the network.

The researchers warned that shared machines – even un-compromised computers – cannot guarantee secure access to systems operated by Helios (an electronic voting system), Microsoft (including Account, Hotmail, and MSN), nor Google (including Gmail, YouTube, and Search).

"This blocking can be accomplished by a so-called 'man in the middle'," Pironti told *El Reg*.

"Technically, whatever piece of hardware is relaying data between you and Google

RELATED STORIES

Bad timing: New HTML5 trickery lets hackers silently spy on browsers

Black Hat 2013 Step into the BREACH: HTTPS encrypted web cracked in 30 seconds

A simple SSL tweak could protect you from GCHQ/NSA snooping

HTTPS cookie crypto CRUMBLES AGAIN in hands of stats boffins

Yahoo! and! Microsoft! have! long! way! to! go! in! account! hijack! fight!

Like 50

Tweet 151

MORE READING

Hotmail

Gmail

Cryptography

Tls

Account Hacking

MOST READ MOST COMMENTED

Google goes dark for 2 minutes, kills 40% of world's net traffic

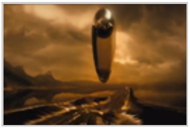
New blinged-up 'iPhone 5S' touted by Jobs FROM BEYOND THE GRAVE

iPhone 5S: 64-bit A7, 128GB storage, flashy ƒ/2.0 camera, and...

Nude swimmers warned of GONAD-GOBBLING FISH ON THE LOOSE

20 injured at LG phone giveaway as PR stunt turns into freetard riot

SPOTLIGHT



Speaking in Tech: Will Google's telly dongle dangle ding Apple?

Typical! Google's wonder-dongle is a solution looking for a problem

Cloud pricing begins to take hold inside the firewall

Salesforce and Oracle forge partnership to smash rivals

MORE

could decide to stop relaying at some point, and do the [logout] blocking.

"In practice, this is very easy to do: with wireless networks (e.g. setting up a rogue access point) or with wired networks (e.g. by adding a router between your cable and the wall plug - alternatively this could be done with custom-built hardware, which could be very small)."

Block and tackle

Several attacks might be possible as a result of the vulnerability, according to Pironti.

"In the context of voting, a single malicious poll station worker could do the attack, voting at his pleasure for any voter. He sets up his man-in-the-middle, then waits for a designated victim to enter the voting booth. The man-in-the-middle device blocks the relevant messages. Then the malicious worker enters the voting booth (e.g. with the excuse to check that the machine is operational) and votes on the victim's behalf."

Webmail attacks on shared computers in settings such as libraries are also possible. An attacker simply needs to access a computer after a mark incorrectly believes she has signed out.

Unbeknown to the user, the hacker's hardware will have blocked the relevant messages, yet the user must be shown what appears to be a "you've signed out" page - the core element of the con. After that, it's easy for an adversary to use the computer to access the user's email.

"We believe this [problem] is due to a poor understanding of the security guarantees that can be derived from TLS and the absence of robust web application design guidelines. In publishing our results, we hope to raise awareness of these issues before more advanced exploits, based upon our attack vector, are developed," the researchers concluded.

The attack developed by INRIA is apparently possible thanks to a de-synchronisation between the user’s and server’s perspective of the application state: the user receives feedback that her sign-out request has been successfully executed, whereas, the server is unaware of the user’s request.

"It follows intuitively that our attack vector could be exploited in other client-server state transitions," Smyth and Pironti explained.

Mitigating the attack could be achieved by reliably notifying the user of server-side state changes. "Unfortunately, the HTTP protocol is unsuited to this kind of notification", we're told, so the researchers advocate the use of technologies such as the SPDY networking protocol and AJAX (asynchronous JavaScript and XML, a web development framework).

The two researchers shared their findings with Google and Microsoft; the web advertising giant acknowledged the discovery in its application security hall of fame.

Smyth and Pironti's presentation of their research was titled *Truncating TLS connections to violate beliefs in web applications*. The researchers were seemingly able to exploit the Helios electronic voting system to cast ballots on behalf of voters, take full control of Microsoft Live accounts, and gain temporary access to Google accounts.

Subtle reasons make Microsoft's webmail service more exposed than its Google equivalent, Pironti explained.

"Google happens to be less exposed for two reasons," Pironti told *El Reg*. "First, our attack relies on a de-synchronisation at the server side: it happens that Google ensures synchronisation every five minutes, which makes our attack [only] work within this five minutes window. Second, Microsoft allows you to change your password without re-typing the old one, so once we access the user account, we can change its password and get full control."

Pironti said the research didn't look at other popular webmail systems, such as Yahoo!'s, so he can't say for sure whether they are vulnerable or not.

"We suspect many other services are broken, but we didn't look into details," he said. ®

18 Reader Comments

◀ Previous Story

Next Story ▶

WHITEPAPERS

Lowering costs and cutting complexity through consolidation

Consolidating on SAP, Linux, and System z

The end user security jigsaw

End user security is about much more than technology level protection. This report looks at the nature of the end user security challenge.

European IT migration survey

Discover the key issues facing organisations undertaking IT migrations.

2013 Cost of data breach study: United Kingdom

In This whitepaper Symantec Corporation and Ponemon Institute present a study concerning the cost of data breach incidents for companies located in the UK.

MORE FROM THE REGISTER

Microsoft SkyDrive, Outlook stricken by cloud outage

Redmond forgets how to give people email, storage

'Database failure ate my data' – Salesforce customer

We're working on it, says cloudy services pusher

Google follows Amazon with auto-encryption of cloud data

Free security service streaks ahead of Microsoft

MORE FROM THE REGISTER

Send us News Tips Week's Headlines Reg Archive Top 20 Stories eBooks Webcasts

The Channel

Privacy Advertise with Us Company Info