ADDENDUM TO ACCESS SECURITY ALERT: SSL MAN-IN-THE-MIDDLE ATTACKS[1]

# TRANSPARENT MAN-IN-THE-MIDDLE ATTACKS ON SSL ARISING FROM COMPROMISES AT DIGINOTAR AND OTHER CERTIFICATE AUTHORITIES

## Introduction

The recent compromise of the DigiNotar SSL Certificate Authority (and possibly others) has been seen as transparent MitM attacks being perpetrated in Iran. This addendum to the ACCESS SECURITY ALERT: SSL MAN-IN-THE-MIDDLE ATTACKS sets out how the DigiNotar breach affects MitM attacks in Iran and potentially elsewhere.

The previous alert concentrated on clumsy MitM attacks, where fake certificates were generated for popular domains such as Facebook and Gmail. The recent issue is significantly more difficult to detect for end users, as it allows for transparent MitM. In these attacks, the end user does not know they are in danger of being compromised because it does not raise any error,warning or other detectable event.

The hacker or hackers in this event broke into the DigiNotar CA (Certificate Authority) and generated valid SSL certificates for both a very large number of domains as well as very broad TLDs (Top Level Domains) such as “*.com” and “*.org.” Because these hacker-generated certificates were signed by the valid root certificate of DigiNotar, the web browsers in use at the time trusted the certificates implicitly and thus generated no errors or warnings.

An investigation of the DigiNotar breach was conducted by Fox-IT and further details of what occurred and the potential magnitude of the damage for the SSL cryptosystem can be read in their interim report.[2]

## Mitigating Transparent MitM Attacks

The Fox-IT report presents some evidence that suggests a large number of users in Iran were compromised by a transparent MitM attack using the certificates generated in the DigiNotar breach. The report advises Iranians to "logout and log back in again". It is our view that while following this advice will get users a new session key, it actually does not help users in Iran

[1] https://www.accessnow.org/page/-/docs/Access_Security_Alert_SSL_MITM_v16.pdf
[2] DigiNotar Certificate Authority Breach "Operation Black Tulip"; Fox-IT Interim Report, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf, Fox-IT, September 2011.


solve their problem or get back to a state of personal security. Following the Fox-IT advice may only serve to lull users into a false sense of security.

Iranian users now face a serious problem: It is difficult for them to be able to trust anything because transparent MitM attacks could be in place for anything they attempt to reach. For example, users cannot be ensured a new version of a downloaded browser is actually from the browser vendor. They cannot trust pages they go to in order to verify checksums of SSL certificates or to download new certificates. Users cannot even trust anything downloaded over Tor has not been tampered with, nor can they get new versions of Tor with 100% certainty. If their Tor version was downloaded and installed before June and they did not upgrade it, then they can have a reasonable degree of faith in it. Otherwise, their situation is problematic and nothing can be certain.

Ideally, Iranian users need to find someone a Tor client version for which the signatures can be independently verified. That can be achieved if they had previously received a genuine copy of the Tor Developers' public PGP key. Then get that person to download new versions of their browsers which can be put onto USB sticks (or any memory devices), passed around and installed on other users' computers. Users not in Iran, or in nations closely allied with Iran, are probably safe from the fallout of the DigiNotar breach. A simple upgrade of their browsers should put them back on a secure footing.