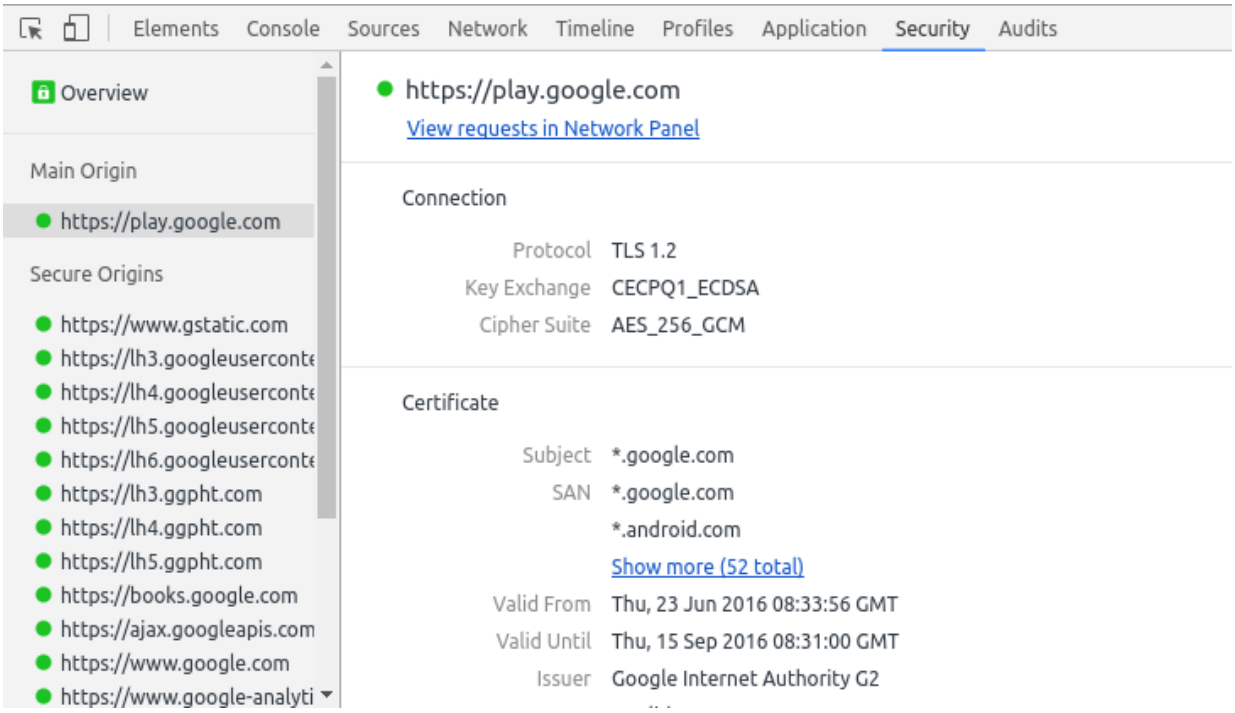
Software engineer announces experiment with post-quantum cryptography in Chrome

July 8 2016, by Nancy Owano



(Tech Xplore)—There are conventional computers and then there is another kind—quantum computers, different, designed to leverage aspects of quantum physics to solve certain sorts of problems dramatically faster than the first type of computer can.

A quantum computer can perform calculations on a far greater order of magnitude, which translates into serious concerns in cryptography and encryption, said science writer, Andrew Zimmerman Jones.

As if Google is unaware. From the Google security blog on Thursday came a posting from Matt Braithwaite, software engineer, who wrote that "if large quantum computers can be built then they may be able to break the asymmetric cryptographic primitives that are currently used in TLS, the security protocol behind HTTPS."

He went on to say that a hypothetical quantum computer could retrospectively decrypt any internet communication recorded today, and that is a problem, considering many types of information need to stay confidential, he said, "for decades."

So what to do? Although it's still very early days for quantum computers, said Braithwaite, "we're excited to begin preparing for them, and to help ensure our users' data will remain secure long into the future."

He had an announcement in this regard. "Today we're announcing an experiment in Chrome where a small fraction of connections between desktop Chrome and Google's servers will use a post-quantum key-exchange algorithm in addition to the elliptic-curve key-exchange algorithm that would typically be used."

Tom Brant in *PCMag* discussed "post-quantum cryptography" and the Chrome experiment. "It's an experiment that enables a small fraction of connections between desktop Chrome browsers and Google's servers to use post-quantum encryption key exchanges on top of the usual HTTPS encryption method, known as an elliptic-curve key exchange algorithm."

(Post-quantum cryptography, said *9to5Google*, "is the study of cryptographic primitives that remain secure against quantum

computers.")

Braithwaite said if the post-quantum algorithm were to turn out to be breakable, "the elliptic-curve algorithm will still provide the best security that today's technology can offer." On the other hand, if the post-quantum algorithm turns out to be secure then it will protect "the connection even against a future, quantum computer."

The post-quantum algorithm that Braithwaite and team selected for the experiment.are thanks to researchers Erdem Alkim, Léo Ducas, Thomas Pöppelmann and Peter Schwabe.

What's next: The Google security blog said they intend to end the experiment within two years, "hopefully by replacing it with something better."

Last year, Tom Simonite in *MIT Technology Review,* wrote about Physicist John Martinis in Santa Barbara, California, working on a quantum computer. Simonite said, "The difficulty of creating qubits that are stable enough is the reason we don't have quantum computers yet. But Martinis has been working on that for more than 11 years and thinks he's nearly there." There are others' projects as well.

Braithwaite said on Thursday that "Quantum computers exist today but, for the moment, they are small and experimental, containing only a handful of quantum bits. It's not even certain that large machines will ever be built, although Google, IBM, Microsoft, Intel and others are working on it."

More information: security.googleblog.com/2016/0 … th-post-quantum.html