New Elliptic Curve X25519 Trips Up ProxySG

David Holmes, 2016-11-07

I happened to be with a customer in Oslo last month when Google threw them for loop by upgrading the main encryption cipher used between the Chrome browser and Google services such as Google.com and Gmail. I wrote with more specifics about this in my SecurityWeek article, but for those of you who somehow missed it, let me recap the salient points.

In 2005, Daniel J. Bernstein introduced a high-performance elliptic curve cipher, Curve 25519 (which we are calling X25519 now). X25519 avoids many side-channel attacks and weaknesses in deterministic random number generators. In the decade since, X25519 has withstood enough scrutiny and gained enough market share to be supported by many clients and is now OpenSSH's default cipher.

In May of 2016, Google switched X25519 on for their servers and their client software such as Chrome. Since this affected only communications between Google clients and Google services it should be no problem, right?

Wrong.

The Oslo customer, like many customers, must intercept outbound SSL connections from within their data centers and headquarters for scanning purposes. Specifically, this customer's security policy requires the scanning of email services. Their policy works to prevent:

- Phishing
- Malware infection
- Data loss prevention

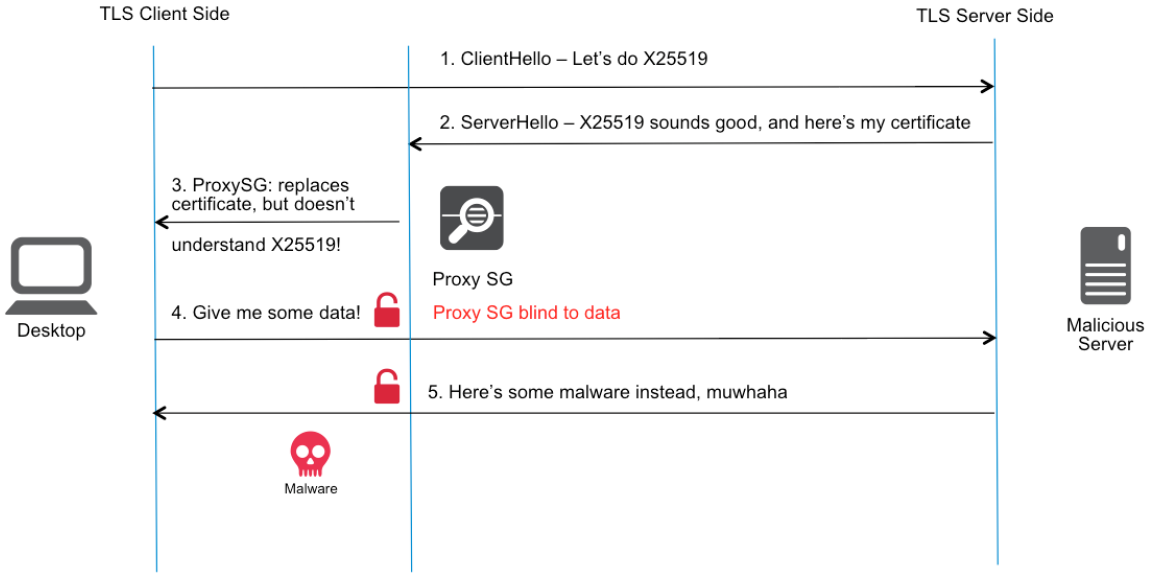
When Google switched on X25519, the customer's Blue Coat ProxySG solution was no longer able to "tap" the communications between Google client software and Google services, meaning the customer was no longer able to decrypt and scan Gmail.

Let me pause the conversation here to address this point. Perhaps you, dear reader, are thinking "Hey, maybe IT shouldn't be reading my Gmail in the first place!" That sentiment is understandable, but if you really feel that way, don't be checking your personal email at work. It's that simple. I try never to spread fear, uncertainty, or doubt, but let me be clear about this: the Internet is hard enough to secure even when everyone in the organization follows all the rules. When users go around the rules, creating holes in the security policy, it becomes impossible. How do you think ransomware, business email fraud attacks, and APT get into organizations? Because, users. IT departments are, as a whole, actually quite respectful of privacy where possible and go out of their way not to intercept your banking or healthcare information. But email? Yes, it must be scanned. Most corporate users understand that by using corporate equipment and corporate networks they are consenting to their email being scanned for malware for the protection of the organization.

So, back to our story. Once the ProxySG was blind to Google traffic, the Oslo customer was faced with a difficult choice: disable Google services or stop scanning. Their security policy dictated the former, but they were loath to do that.

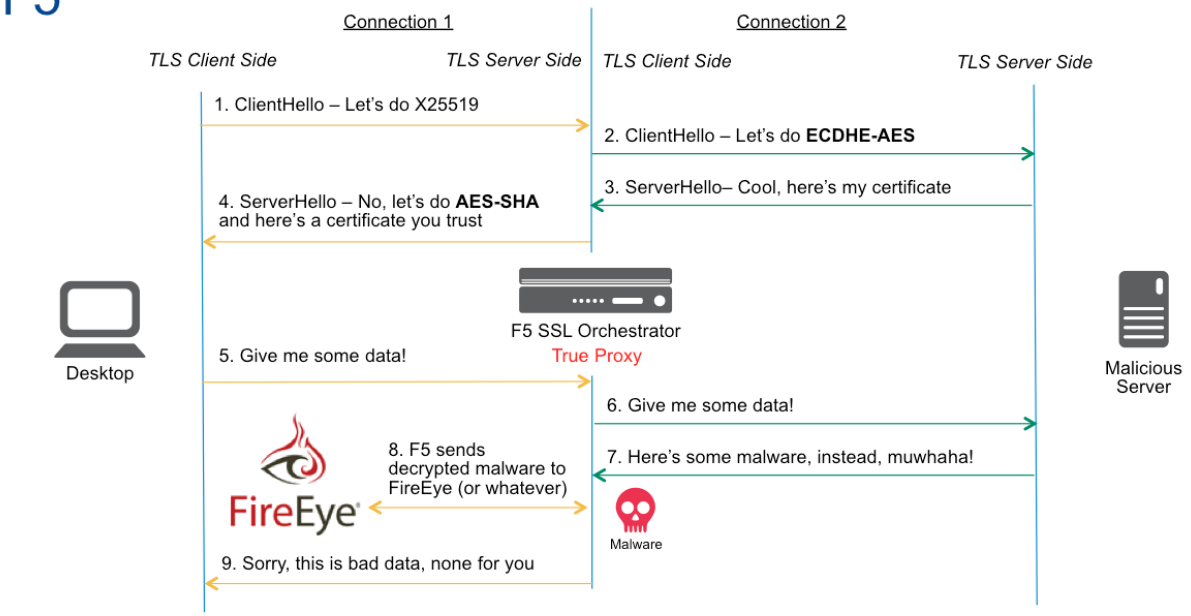
It didn't have to be this way. If ProxySG were a **full-proxy,** it could have survived the Google cipher upgrade. The problem with ProxySG is that it snoops *just enough* of the SSL connection to auto-generate an intercept certificate and retrieve the SSL session key that it will need to decrypt the session. It's more of a tap than a proxy. Since ProxySG didn't support X25519, it wasn't able to retrieve the session key and decrypt the session.

Proxy SG



A full-proxy, like F5's SSL Orchestrator, does not have this problem. A full-proxy establishes two connections: one from the client to the proxy, and a second from the proxy to the end-server. By using two connections, a true proxy can fully control the parameters of the conversation and enforce ciphers and policies that it understands.

F5



In this example, the SSL Orchestrator would have negotiated a cipher that it understood (such as AES256-SHA256) with the client and a different one with the server (perhaps ECDHE-AES256-GCM-SHA256). No X25519.

Lori MacVittie wrote an excellent piece, "Three things your proxy can't do unless it's a full-proxy," on DevCentral last year. In it, she explains the fundamental difference between half-proxies like ProxySG and full-proxies like the F5 SSL Orchestrator. She also (as telegraphed by the title) showcases three things you can't do with just a half-proxy. I won't spoil the whole article, but number three is **terminate SSL/TLS.** See, it's not just me saying this.

Getting back to our Oslo customer: if they had been using the F5 SSL Orchestrator when Google flipped on X25519, they would have been able to continue their scanning and not suffered from the SSL blind spot.

Ultimately, both Blue Coat ProxySG and the F5 SSL Orchestrator are being upgraded to support X25519, but F5 customers won't be blind to SSL traffic during the transition.

Remember that when something like this happens again.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com