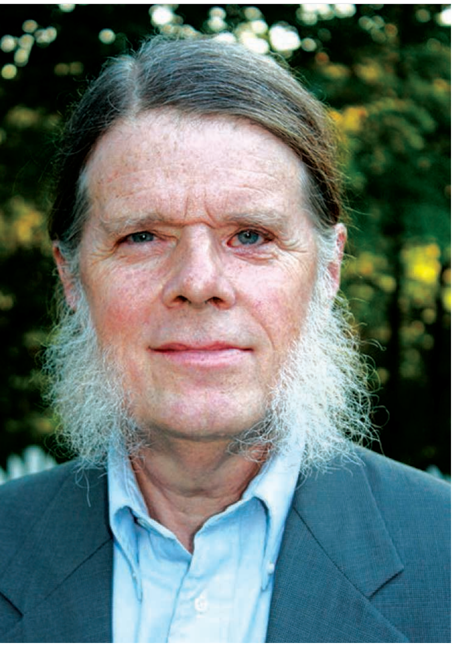

Daniel E. Geer, Jr.
In-Q-Tel

Security Theater, the Beat Goes On

My colleague Bruce Schneier created the neologism "security theater." Everyone reading *IEEE Security & Privacy* knows the phrase. Everyone has examples, the most ready of which are soft targets—criticizing the TSA's more embarrassing moments, say.

But many more are theater-in-truth even if thought of as progress(ive). Take pervasive encryption of public information in transit. Measured by the test of the greater good for the greater number, transmitting public information in encrypted form doesn't cut it. It's theater for the sophisticated commentator who is virtue signaling, and theatrically so. Nobody who receives public information in encrypted form learns anything extra because that information came to them disguised as white noise. Nobody who sends public information in encrypted form increases the utility of that information by disguising it as white noise. This leads to the framing question: "Whose connection is it?"

Yes, yes, yes, the argument in favor of encrypting everything in transit is not entirely fallacious. It is fundamentally correct that, if everything is encrypted, then special messages you most care about look like the great mass of messages you don't care a fig about, and some single, special (to you) message can hide in plain sight. Putting aside that this encrypted message almost surely came to you on a handheld device that is geolocated to a fare-thee-well at all times and in all jurisdictions, a fact that has evidently not dissuaded you from being so tracked, and/or that the JavaScript you accepted is beaconing scores, if not hundreds, of entities, only some of which have plausible recognizability, we are back to "Whose connection is it?"

Even if you believe that you are doing the world a service by using TLS 1.2, there are a lot of old people with old computers, people who can't update to a browser that plays the TLS 1.2 game. (Your own relatives, perhaps?) Wikipedia is used in a number of African countries in place of textbooks because they can't afford them, and, even if they could afford them, there's no way to get them to where they're needed. But since 1 January of this year, it's TLS 1.2 or no service—this for Wikipedia's public information, mind you. Locking out the old and, poignantly, the poorest of the poor who desperately need it for education purposes just to suit some ideological agenda is about as theatrical security as you can get.

To be sure, it's not as if Wikipedia is somehow the only Bad Boy; the style is spreading because virtue signaling is a contagious disease. AOL, Yahoo, and Verizon look close to catching it, requiring TLS 1.2 for mail transport. Consider *.gov, where encryption, including a TLS 1.2 floor, is now all but pervasive. You are protecting yourself from government snooping by encrypting your download of government information from the government? Is that your virtue signaling or theirs? By contrast and counterexample, the *Encyclopedia Britannica*, the BBC, Amazon, *The Washington Post*, and Google Project Zero know better than to require TLS 1.2, perhaps because they recall Shamir's law: "cryptography is typically bypassed, not penetrated"—meaning that if I want to perform an integrity attack on someone's Wikipedia reading, then I do it by editing the page to say what I want it to say, not by performing some nation–state-level attack on their TLS 1.0 browser session. These are not nuclear weapons launch codes being protected, they're public web pages informing you about the founding of the United States by the Bavarian Illuminati and the 1969 Soviet moon landings—disinformation delivered

continued on p. 75

Digital Object Identifier 10.1109/MSEC.2020.2992210
Date of current version: 9 July 2020

Last Word

continued from p. 76

"securely" is still disinformation, however much it was preceded by a TLS 1.2 negotiation.

In the middle days of C and Unix, programs would crash on null pointer dereferences, and this was seen as a possible security problem. So, for a while, a demand-zero page was mapped at the zero address. Programs whose null pointer dereferences were for strings would find empty strings, and this was somehow seen as safer. Later, the community learned that a null pointer dereference was a sign of an undefined program state and was the gateway to all kinds of hellfire. Today, Unix programs uniformly crash upon a null pointer dereference, because that's what nontheatrical security looks like.

Nation–state actors are usually patriotic and often well resourced. If the encryption-everywhere movement reaches everywhere it can possibly reach, then these nation–state actors will simply move out of reach, into the supply chain of all of the invisible hardware and firmware and software dependencies a local or foreign citizen needs to access their electronic life, or the nation–state can just dictate what can be accessed and make VPN use a punishable crime. Nation–state actors exist for reasons and have powers; nothing that comes out of the Internet or web standards and technology communities will banish that condition, and to speak or act otherwise is security theater. We should learn to recognize security theater in honest, heart-felt, good-will efforts, such as encrypted SNI, certificate pinning, DNS over HTTPS, and HTTP/3 over QUIC/TLS. The world's nation–states understand these issues, and they will not sit by to be disintermediated like other Silicon Valley targets.

Security theater demonstrates that, whereas, in commerce, the customer is always right, on the Internet, you're not the customer, you're the product. For the third time: Whose connection is it? ■

Daniel E. Geer, Jr. is the chief information security officer of In-Q-Tel. Contact him at dan@geer.org.

Digital Object Identifier 10.1109/MSEC.2020.3002088