The New York Times

Every Part of the Supply Chain Can Be Attacked

When it comes to 5G technology, we have to build a trustworthy system out of untrustworthy parts.

By Bruce Schneier
Mr. Schneier is a fellow and lecturer at the Harvard Kennedy School.

Sept. 25, 2019

The United States government's continuing disagreement with the Chinese company Huawei underscores a much larger problem with computer technologies in general: We have no choice but to trust them completely, and it's impossible to verify that they're trustworthy. Solving this problem — which is increasingly a national security issue — will require us to both make major policy changes and invent new technologies.

The Huawei problem is simple to explain. The company is based in China and subject to the rules and dictates of the Chinese government. The government could require Huawei to install back doors into the 5G routers it sells abroad, allowing the government to eavesdrop on communications or — even worse — take control of the routers during wartime. Since the United States will rely on those routers for all of its communications, we become vulnerable by building our 5G backbone on Huawei equipment.

It's obvious that we can't trust computer equipment from a country we don't trust, but the problem is much more pervasive than that. The computers and smartphones you use are not built in the United States. Their chips aren't made in the United States. The engineers who design and program them come from over a hundred countries. Thousands of people have the opportunity, acting alone, to slip a back door into the final product.

There's more. Open-source software packages are increasingly targeted by groups installing back doors. Fake apps in the Google Play store illustrate vulnerabilities in our software distribution systems. The NotPetya worm was distributed by a fraudulent update to a popular Ukranian accounting package, illustrating vulnerabilities in our update systems. Hardware chips can be back-doored at the point of fabrication, even if the design is secure. The National Security Agency exploited the shipping process to subvert Cisco routers intended for the Syrian telephone company. The overall problem is that of supply-chain security, because every part of the supply chain can be attacked.

And while nation-state threats like China and Huawei — or Russia and the antivirus company Kaspersky a couple of years earlier — make the news, many of the vulnerabilities I described above are being exploited by cybercriminals.

Policy solutions involve forcing companies to open their technical details to inspection, including the source code of their products and the designs of their hardware. Huawei and Kaspersky have offered this sort of openness as a way to demonstrate that they are trustworthy. This is not a worthless gesture, and it helps, but it's not nearly enough. Too many back doors can evade this kind of inspection.

Technical solutions fall into two basic categories, both currently beyond our reach. One is to improve the technical inspection processes for products whose designers provide source code and hardware design specifications, and for products that arrive without any transparency information at all. In both cases, we want to verify that the end product is secure and free of back doors. Sometimes we can do this for some classes of back doors: We can inspect source code — this is how a Linux back door was discovered and removed in 2003 — or the hardware design, which becomes a cleverness battle between attacker and defender.

This is an area that needs more research. Today, the advantage goes to the attacker. It's hard to ensure that the hardware and software you examine is the same as what you get, and it's too easy to create back doors that slip past inspection. And while we can find and correct some of these supply-chain attacks, we won't find them all. It's a needle-in-a-haystack problem, except we don't know what a needle looks like. We need technologies, possibly based on artificial intelligence, that can inspect systems more thoroughly and faster than humans can do. We need them quickly.

The other solution is to build a secure system, even though any of its parts can be subverted. This is what the former Deputy Director of National Intelligence Sue Gordon meant in April when she said about 5G, "You have to presume a dirty network." Or more precisely, can we solve this by building trustworthy systems out of untrustworthy parts?

It sounds ridiculous on its face, but the internet itself was a solution to a similar problem: a reliable network built out of unreliable parts. This was the result of decades of research. That research continues today, and it's how we can have highly resilient distributed systems like Google's network even though none of the individual components are particularly good. It's also the philosophy behind much of the

cybersecurity industry today: systems watching one another, looking for vulnerabilities and signs of attack.

Security is a lot harder than reliability. We don't even really know how to build secure systems out of secure parts, let alone out of parts and processes that we can't trust and that are almost certainly being subverted by governments and criminals around the world. Current security technologies are nowhere near good enough, though, to defend against these increasingly sophisticated attacks. So while this is an important part of the solution, and something we need to focus research on, it's not going to solve our near-term problems.

At the same time, all of these problems are getting worse as computers and networks become more critical to personal and national security. The value of 5G isn't for you to watch videos faster; it's for things talking to things without bothering you. These things — cars, appliances, power plants, smart cities — increasingly affect the world in a direct physical manner. They're increasingly autonomous, using A.I. and other technologies to make decisions without human intervention. The risk from Chinese back doors into our networks and computers isn't that their government will listen in on our conversations; it's that they'll turn the power off or make all the cars crash into one another.

RELATED

Opinion | Thomas L. Friedman: Huawei Has a Plan to Help End Its War With Trump Sept. 10, 2019

Senators Urge F.C.C. to Review Licenses of 2 Chinese Telecom Companies Sept. 15, 2019

U.S. Gives Companies More Time to Cease Doing Business With Huawei Aug. 19, 2019

All of this doesn't leave us with many options for today's supply-chain problems. We still have to presume a dirty network — as well as back-doored computers and phones — and we can clean up only a fraction of the vulnerabilities. Citing the lack of non-Chinese alternatives for some of the communications hardware, already some are calling to abandon attempts to secure 5G from Chinese back doors and work on having secure American or European alternatives for 6G networks. It's not nearly enough to solve the problem, but it's a start.

Perhaps these half-solutions are the best we can do. Live with the problem today, and accelerate research to solve the problem for the future. These are research projects on a par with the internet itself. They need government funding, like the internet itself. And, also like the internet, they're critical to national security.

Critically, these systems must be as secure as we can make them. As former FCC Commissioner Tom Wheeler has explained, there's a lot more to securing 5G than keeping Chinese equipment out of the network. This means we have to give up the fantasy that law enforcement can have back doors to aid criminal investigations without also weakening these systems. The world uses one network, and there can only be one answer: Either everyone gets to spy, or no one gets to spy. And as these systems become more critical to national security, a network secure from all eavesdroppers becomes more important.

Bruce Schneier, a fellow and lecturer at the Harvard Kennedy School, is the author, most recently, of "Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World."

The Times is committed to publishing a diversity of letters to the editor. We'd like to hear what you think about this or any of our articles. Here are some tips. And here's our email: letters@nytimes.com.

Follow The New York Times Opinion section on Facebook, Twitter (@NYTopinion) and Instagram.