OUT OF BAND

Bruce Schneier on Future Digital Threats

Hal Berghel, University of Nevada, Las Vegas

Computer security expert Bruce Schneier weighs in on a number of issues explored in this column.

Bruce Schneier is without question one of the leading computer security professionals alive today. A true renaissance man when it comes to IT security, he has been involved in the creation of a host of cryptographic algorithms (for example, Blowfish, Twofish, and Threefish); has written several books on cryptography and security topics, the most recent of which is *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton & Company, 2016); has extensive academic publications; is a prolific writer for magazines, newspapers, and his own blog (schneier.com); and serves the profession through his appointment as fellow at Harvard's Berkman Klein Center for Internet & Security and board membership to the Electronic Frontier Foundation. He's currently CTO for IBM Resilient. This "interview" resulted from our e-mail exchanges during November and December 2017.

STUXNET AND CYBER-PHYSICAL SYSTEMS

HAL: Welcome to Out of Band, Bruce. Let's begin modestly with arguably the most potent cyber-physical weapon in history: Stuxnet. What lessons should we have learned from the Stuxnet experience?

BRUCE: Stuxnet was one of the first cyberweapons fired by one country against another—in this case, the US and Israel against Iran. We've seen many cyberweapons since then: Iran against Saudi Arabia, Iran against the US, Russia against the Ukraine, North Korea against the US. These are damage-causing attacks, not espionage operations such as China hacking the US Office of Personal Management or the US hacking the Brazilian national oil company Petrobras. The lessons from all of these are (1) that the world's critical infrastructure is vulnerable to attack, (2) some countries are more vulnerable than others simply because of how critical the Internet is to their lives and economies, and (3) this isn't going to change anytime soon. On the Internet, attack is easier than defense.

HAL: What are the implications of Stuxnet on future cyber-physical systems designs?

0018-9162/18/$33.00 © 2018 IEEE

EDITOR HAL BERGHEL
University of Nevada, Las Vegas; hlb@computer.org

BRUCE: Again, I'll take all of the recent nation-state cyberattacks as a whole. For years now, the US has been working towards an insecure Internet because we believed we had an advantage. We pushed Internet-based espionage and surveillance as the new normal. We worked against securing Internet and telephone protocols. Even now, the FBI is pressuring Internet companies to make their devices less secure. The lesson of Stuxnet and related attacks is that we don't have an advantage; instead, we have a disadvantage. We might have the biggest stones, but we also live in the glassiest houses. In this world, we need to prioritize defense over offense, even if it means giving up espionage and attack capabilities.

DATA BREACHES

HAL: Sloppy security practices have produced a bewildering array of data breaches in recent years. Equifax, Yahoo (twice), MySpace, Heartland Payment Systems, the Sony PlayStation Network, CardSystems Solutions, and T.J. Maxx accounted for 1 billion accounts/records lost. It's getting to the point that any hack of less than 100 million records isn't considered newsworthy. What reasons, if any, are there to think that business is getting any better at protecting personally identifiable information?

BRUCE: There aren't any, at least not as long as we leave industry to invest or not in security as they see fit. What we have now is exactly what a market-based solution provides. Companies skimp on security because that's the rational thing for them to do. Customers don't demand security because the whole system is opaque, and it's hard to connect identity-theft harms to a particular data theft. In the case of companies like Equifax, the people whose data they lost aren't even their customers. Executives would rather save 10 percent on their security budget and take the chance of being hacked, because that's what Wall Street rewards. If we want security to improve, the only solution is for government to step in and set minimal standards.

SMART THINGS

HAL: These days, smart mattresses tell your smart thermostat, smart toaster, and smart coffee pot to anticipate your awakening, followed shortly thereafter by your smart wakeup alarm deactivation and remote starting of your car. Google now has an app for smart mobile devices that trigger merchants' smart devices to look for you as you pass their storefront. Call me a Luddite, but all of this "smartness" seems pretty unnecessary, and it exponentially increases the number of digital attack vectors we face. Do you see genuine value propositions in these smart devices for the consumer?

BRUCE: Okay: you're a Luddite. Our parents said the same thing about e-mail, and our children will say the same thing about whatever comes after all those Internet of Things examples you derided. All of these things have value, and in most cases the value comes from emergent properties that those of us—especially those of us already set in our ways—can't anticipate beforehand. Yes, there's genuine value in all of this. Yes, insecurity increases, but it did when people started connecting their computers to the Internet, connecting wireless access points to their networks, and when they put all their data in the cloud. We have to accept that technology will continue to progress, and we have to engineer our way to more security and not limit our way to more security.

In this world, we need to prioritize defense over offense, even if it means giving up espionage and attack capabilities.

SURVEILLANCE CAPITALISM

HAL: What is your long-term vision of who will ultimately control the identity layer of the IoT? I have three concerns that I'd like you to address: (1) that future IoT programs like burp suites will routinely harvest the sensory data on upon which the IoT is built and share it without our permission and to our disadvantage, (2) access to this data/metadata will further diminish any lingering hope that we have for a right to be left alone, and (3) the IoT will marginalize those who refuse to willingly share this information in much the same way that credit reporting agencies marginalize people who have never used credit.

BRUCE: This is an important question. Surveillance capitalism is the primary business model of the Internet, and a secondary business model of so many other industries. We're all under constant surveillance through our computers and smartphones, and increasingly through other means as well. The Internet of Things is the Internet of sensors, so the amount of surveillance data will increase exponentially.

As you point out, it's primarily used without our knowledge and consent—and against our interest. But here's the thing: our surveillance data is only worth so much. The more of it that gets collected, the less each piece of it is worth. Or, to put it more concretely, lots of companies are willing to buy the data about my willingness to buy a new car—but at the end of the day, I'm only going to buy one car. I think surveillance capitalism is going to crash hard; already our data is worth less and less. The question is what happens in the meantime. You're right that we're losing our last bits of privacy as the IoT infiltrates all corners of our lives, and you're right that there will be a digital divide between those of us who accept this surveillance and those of us who resist. Again, without government stepping in and declaring some of these invasive business practices illegal, we have no choice but to ride along and watch what happens.

I think surveillance capitalism is going to crash hard; already our data is worth less and less.

HAL: With regard to holding personal data of others, the neoliberal/corporatist promise to the public has always been "let us have access to all of your personal data, and we'll do great things with it." The recent Equifax hack illustrates the inherent risks of such covenants and their attendant risks.

BRUCE: Their promise is more along the lines of "Here's a bunch of free services and stuff, and please don't pay too much attention to the fact that we've got you under surveillance. We'll do great stuff with it, but much of that will be for our benefit and not yours." I'm not saying that companies like Google don't do great stuff for us with our data—but they primarily treat us as the product they sell to their actual customers. I see your example as the broken promise of Big Data. Big Data told everyone: "save everything, and you can figure out how to use it later." Because data storage and processing is so cheap, saving everything is possible. In fact, it's easier to save everything than to figure out what to save. The problem is that saving everything isn't really cheap. The cost is in the security risk, as companies like Equifax have found out. I think companies need to balance the costs of saving personal data on their customers/users against the risks. The best security against data theft is to delete the data before the theft occurs.

HAL: I see the IoT as an enormous moral hazard that creates a classical double whammy: misdirected incentives for the providers to abuse our personally identifiable information, and no accountability for any negative externalities to the consumers/users that might result. Do you agree?

BRUCE: Yes, but that's no different than what we already have. Internet service providers have the same moral hazard. As do data brokers. The IoT is a difference in degree, but not a difference in kind.

IOT SECURITY CHALLENGES

HAL: What are the most important security challenges for the IoT?

BRUCE: The traditional way of thinking about computer security is the CIA triad: confidentiality, integrity, and availability. Until now, threats have largely been about confidentiality. That's what we've mostly been talking about. The IoT isn't just the Internet of sensors, it's also an Internet that can affect the world in a direct physical manner. Once that happens, the integrity and availability threats matter more. Information manipulation is an increasing threat as systems become more capable and autonomous. Denial of service is an increasing threat as systems become more essential. Hacking is an increasing threat as systems have implications to life and property. This changes everything. There's a fundamental difference between crashing your computer and losing your spreadsheet data and crashing your pacemaker and losing your life, even though it might be the same computer chips, the same operating system, the same software, the same vulnerability, and the same attack software. I'm currently writing a new book about this, tentatively titled *Click Here to Kill Everybody: Perils of Life on a Hyper-Connected Planet*, to be published in September 2018.

HAL: What are your thoughts about the recent IoT Cybersecurity Act of 2017? Who are the winners and losers?

BRUCE: To be clear, this is a bill introduced by four US senators that has zero chance of ever becoming law. Not because it's a bad idea, but because Congress is too dysfunctional right now to pass any sensible legislation that might annoy well-funded lobbying groups. The bill is incredibly modest. It doesn't prescribe, regulate, or otherwise force any company to do anything. It imposes minimum security standards on IoT devices purchased by the US government. Those standards are all sensible and not very onerous. The bill also ensures that good-faith security research isn't criminalized, something essential to secure the IoT. Because the bill has no chance of passing, the winners are industry, who can continue to build and sell insecure stuff. The losers are all of us, who are stuck with the insecurity.

VOTING MACHINES

HAL: Let's conclude with some general questions on the ultimate cyber-physical system for democracies: voting machines. You've observed that unless we change the way we deploy technology in our elections, it's just a matter of time until a hack corrupts an outcome. Scholarly books and articles have been written about this vulnerability, yet the majority of politicians and election officials remain unfazed. What can be done to animate the public to demand intelligent oversight of election systems?

BRUCE: I don't think anything can. Election hacking is a risk that people don't worry about when it's theoretical. That is, before an election. But after an election, half of the electorate is happy with the result and doesn't want to investigate very much. (That might not be true in a rigged election.) This bias isn't in any particular party; it's general. Voting is infrastructure, and we don't generally want to spend money on securing our infrastructure.

HAL: Modern OCR scanners are simply amazing. The days of using #2B pencils to fill in ovals is way behind us. Do you see any clear path to the return to paper ballots (and vote recording that is less vulnerable to hacking)?

BRUCE: Using a particular type of pencil is obsolete. Modern optical-scan voting machines still require filling in ovals, but they're much easier to use. They're the most secure and accurate voting system we have, and they're not uncommon. I use them to vote in my home state of Minnesota. The system has several benefits. One, voters are able to clearly mark their choice on the ballot—and not via some intermediary machine. Two, the ballots can be quickly scanned and tallied by a computer and reader. And three, there's a paper record of the votes in case of a recount. More jurisdictions should be using them.

HAL: As I see it, Internet voting is dead not because it's a bad idea that opens voting systems to all Internet vulnerabilities (which it is), but rather because of its potential to expand the voting franchise, which is opposed by those who control Congress. What's the future of Internet voting?

BRUCE: Unfortunately, I think it has a strong future. People really want the convenience of being able to vote from their homes. In jurisdictions that don't actively engage in voter suppression measures, that's a popular policy goal. And just as we've seen a significant rise in mail-in ballots—there have been entire mail-in elections—even though there are security risks in that process, I think we'll see Internet voting within a decade. I don't think it's a good idea, and opens us up to much more serious election hacking, but that won't stop it.

This exchange highlights two features of the digital security debate: first, that in broad strokes computing security professionals agree in most respects, and second, that there's still room for serious debate. In my view, the acronym IoT would better describe an Internet of Trouble. Bruce is more positive about its future. Where I see Internet voting as a dead issue as long as there remains a neoliberal lock on our government—which I predict that special interest control of campaign finance, gerrymandering, and voter suppression will guarantee for the foreseeable future—Bruce sees it as a reality within the decade, neoliberal lock or not. These nuanced differences make the topic all the more exciting to watch. C

HAL BERGHEL is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.