Cybersecurity and the Future

Sven Dietrich, City University of New York

We need our computing systems to perform as intended, unaffected by adversaries big or small.

As the world becomes increasingly interconnected, with more devices from our daily lives becoming part of the Internet of Things (IoT), one issue will certainly prevail: cybersecurity. We care about our security and privacy, and this undoubtedly won't change over the next 50 years. There will be shades of gray—based on cultural perceptions, needs, and trends—but privacy is part of human nature and affirmed as such in the Universal Declaration of Human Rights. We need our computing systems to perform as instructed or intended, unaffected by adversaries big or small.

Computing devices exist in our businesses, homes, pockets, bodies (in the form of medical devices), hospitals and medical offices, transportation systems, industrial production and energy generation systems, financial and payment systems, voting systems, and even in the dams that protect our land from rising sea levels. These devices all have one thing in common: they execute code on one or more silicon chips. Code can be flawed or vulnerable to exploits, which can compromise the aforementioned massively proliferated systems with various degrees of impact on our world and lives.

While we continue to promote secure coding practices for existing and upcoming programming languages and microchips and to educate stakeholders about better cybersecurity practices, we need to think about legacy problems with devices that can't easily be changed and form an integral part of a critical infrastructure. We're also creating secure ways of verifying, patching, and updating our devices to maintain their functionality, integrity, and health at both the software and hardware level, as well as ways to let devices communicate securely.

We'll face new challenges when quantum computers become commonly available. As current computational, algorithmic, and distributed techniques allow us to bypass, crack, and compromise security protocols and cryptographic primitives using conventional computing (for example, the recent Google-led effort to find collisions in the cryptographic hash function SHA-1), we'll face even tougher obstacles when quantum computing techniques threaten to undermine our security and privacy safeguards (for instance, allowing for the factoring of RSA moduli or breaking other public-key cryptography mechanisms). Quantum computing in the hands of a few powerful actors would create an even greater imbalance. The security challenges that could arise from a quantum computing environment itself are yet to be seen, compared to the conventional containment challenges that exist now and in some cases can be mitigated (by secure enclaves in recent Intel chips, for example).

Interconnections pose a continued risk. We're developing novel ways of connecting old and new devices, vulnerable or not. We're using new Internet architectures and next-generation networks and protocols, potentially using software-defined components, and looking to ameliorate underlying flaws by incorporating lessons learned from the past. We'll likely fix a few mistakes but also introduce new attack vectors that we can't imagine yet.

Harnessing vulnerable devices into maliciously behaving networks such as botnets or as a source of exfiltrating private or sensitive information (such as email or health and financial data) will continue as long as devices remain connected and always on, vulnerable to flaws, improperly configured due to human error, or intentionally sabotaged by insiders. Just as bots migrated from government and university lab systems to home computers and mobile devices, and distributed denial-of-service attacks turned IoT devices (such as cameras, DVRs, home automation, and broadband routers) into botnets, we can only imagine what the next target will be, from smartwatches to connected toothbrushes and pacemakers.

As we add more devices to our lives and connect them to the somewhat fragile Internet (by cable, Wi-Fi, or some method yet to be discovered), it's important to remember that information can flow both ways, maliciously or not.

SVEN DIETRICH is an associate professor in the Mathematics and Computer Science Department at the City University of New York's (CUNY's) John Jay College of Criminal Justice, is on the doctoral faculty of the Computer Science department at the CUNY Graduate Center, and is on the IEEE Cybersecurity Initiative Steering Committee. Contact him at spock@ieee.org.