Computer Security as Civil Defense

Marilyn Wolf, Georgia Tech

Given the prevalence of computer systems, we must change our approaches by ensuring that civilians and companies can become responsible for much of their own cyberdefense.

It is time for us to treat computer and information security and safety as civil defense issues. I use the term *civil defense* here in its classic sense: the protection of civilians against military attack and natural disasters. Computer systems, both IT and cyberphysical (CPS), or the Internet of Things (IoT) can wreak widespread and long-lasting damage to civilian lives and property. Given the huge attack surface presented by civilian systems, we have no choice but to rely on civilians for a great deal of their own cyberdefense. Ensuring that civilians are prepared for cyberattacks and mishaps will require changes in our approaches to both technology and policy.

THE STAKES ARE HIGH

Let's keep in mind the huge stakes involved by reviewing a few recent incidents.

- The Target retail chain was the victim of a large data breach in 2013.[5] The attackers gained access to 11 GB of data. As a result, Target sent notices to 110 million credit and debit card holders.
- The Notpetya attack of 2017[3] targeted data and system configurations at several companies and resulted in extensive interruptions of company operations as well as a lengthy recovery process.
- A 2015 cyberphysical attack on Ukrainian electric power facilities resulted in a temporary loss of electrical service to more than 100,000 customers.[2]
- A cyberattack took down the computer systems of the Erie County Medical Center for six weeks in 2017.[1] Medical staff relied on paper documentation during the outage.

These serious examples of the damage that can be caused by computational attacks may, in fact, not provide us with a sufficiently bleak picture of worst-case damage. Reasonable people may be concerned that we could see much worse in the future at the hands of a capable and determined adversary.

Embedded computers are now in an astonishing variety of physical objects. Although computers have improved physical systems in many ways, these innovations also mean that we can no longer treat computer security and physical safety as separate topics. Safe and secure cyberphysical and IoT systems were the subjects of a special

Digital Object Identifier 10.1109/MC.2019.2891980
Date of publication: 11 March 2019

 Published by the IEEE Computer Society

EDITOR **DIMITRIOS SERPANOS**
ISI/ATHENA and University of Patras; serpanos@computer.org

issue of *Proceedings of the IEEE* edited by Dimitrios Serpanos (this column's editor) and myself.[9] Security clearly affects safety; safety also influences our approach to computer security.

All nations need to be concerned about their cyber civil defense and readiness. Beyond nation-to-nation strife, nonstate actors could also carry out attacks, the effects of which give them a much broader reach. The 9/11 attacks showed that physical attacks with large effects can be planned and carried out by small groups;[6] we should be similarly concerned about the potential for large-scale computational attacks carried out by relatively small groups from well within their own safe havens.

CYBER AND CYPERPHYSICAL THREATS

Several types of threats are posed by cyber and cyberphysical attacks.

- Disruptions of service can affect both information systems and physical systems. The lines between IT and CPS/the IoT are often blurry. As one example, IT failures at three U. S. airlines caused flight delays and cancelations.[4,7,8]
- Identity theft enables follow-on crimes. Beyond credit card fraud, attackers could use stolen credentials for improper access to facilities or data.
- Cyberphysical attacks can damage equipment. The Ukrainian power grid attack targeted power control devices but operated nondestructively, allowing workers to manually reset the equipment. A variation of the attack could have resulted in permanent damage. Industrial equipment often has replacement lead times measured in weeks or months, resulting in extended outages. A large-scale attack damaging an unusually large amount of equipment could further increase these backlogs, as could attacks on the facilities that manufacture such equipment.

DEFENDING AGAINST CIVIL CYBERTHREATS

Broadly speaking, we can identify several goals of computer civil defense: 1) protect the integrity of data, 2) protect the timely transfer of data, and 3) protect physical equipment. These goals are challenging in themselves. Computer civil defense is made even harder because of the wide variation in equipment and configuration and computer system operators' relative lack of expertise.

We can identify technical steps, ranging from known best practices to research topics, that can reduce cyberthreats. Some of these methods should be practiced by manufacturers. Root-of-trust design, which ensures that critical software can be traced back to a trusted source, is employed in practice but not universally. Root-of-trust design uses a combination of hardware and software methods: digital signatures for software are checked, access privileges for trusted versus nontrusted software are enforced, and digital signatures may be applied at several levels of deployment.

More controversial is a move toward lessened reliance on software updates. This is one example of physical safety influencing our approach to computer security. Updating controllers for physical systems is difficult for several reasons. Shutting down equipment for updates and then returning the equipment to operation depend not only on the computers but also on the equipment. Power-generating equipment may take several hours to come online. Chemical plants may require hours or days for a shutdown/restart cycle. Moreover, software for safety-critical systems is held to a high standard; fast updates to correct security-related bugs may not be possible while also ensuring that the updates do not cause further problems. We need software-engineering methods that result in fewer bug-fix distributions.

Design techniques for graceful degradation have received extensive attention over many decades. However, these methods are applied primarily in certain types of high-reliability systems. Attacks that disrupt operations on IT systems suggest that more types of systems should be designed to provide some functionality in the face of failures to other parts of the system. Defense-in-depth methods are not consistently applied. The Target attack, for example, came through a cybersecurity weakness of a refrigeration contractor. System design should also take into account the time required to recover from attacks. The six weeks required to recover from the attack at the Erie County Medical Center is not an isolated example. Long recovery times amplify the damage caused by an attack.

> Security clearly affects safety; safety also influences our approach to computer security.

Cyberphysical systems are sensitive not just to data values but also to timing—we can disrupt many control systems merely by delaying critical data without changing a single bit of information. Research has developed some architectures that preserve timing properties. *Timing resilience*—the

detection of timing problems and responses to preserve system function—deserves more study. IT-oriented approaches to CPS and IoT security tend to treat these systems as collections of input–output devices to reduce the safety and security problems of traditional IT approaches. In fact, cyberphysical and IoT systems perform distributed real-time computations that require new security and safety methodologies.

Some quasi-technical factors also contribute to cybersecurity threats. Some IT personnel have received relatively little formal training in IT after promotion from technician or support roles. Training in cybersecurity is relatively new and may not have reached all practitioners. Personnel with training and experience in cyberphysical or IoT security are even harder to find.

Computer people pride themselves on the generality of computers. The result is that we see a huge variation in deployment configurations for devices and networks. Such variation makes security holes more likely and security properties harder to monitor. The use of more typical configurations for devices and networks would help to reduce problems and simplify fixes when problems are identified.

POLICIES TO RAISE AWARENESS

Policy will need to reinforce our understanding of risks and how we can best prepare ourselves. Organizations can help to educate the citizenry and encourage cybersecurity efforts. Such organizations will need to operate locally and provide a personal touch—ad campaigns won't cause enough people to change their ways. Organizations could be independent nonprofits, supported by local or state government, or national government organizations. We should expect that these organizations will cooperate to provide service—national or international organizations may provide expertise on specialized topics that smaller organizations cannot afford.

An important role of cybercivil defense organizations can be to disseminate useful information and provide training. The 21st century equivalents to pamphlets on bomb shelter construction could provide useful information to individuals and companies on how to prepare for cyberattacks. The cyber equivalent of duck-and-cover drills could educate citizens on the nature of threats and appropriate responses to unexpected events. Consider, for example, an attack on automobiles that interferes with their operation while on the road—a little preparation and practice could drivers them how to react to minimize risk.

A code-centric view of security minimizes the importance of system architecture and procedures followed by personnel.

Governments should consider encouraging or requiring reporting. Cyberattacks are not always reported by companies because of concerns about bad publicity or reliability. In contrast, accidents in several domains, such as transportation, are required by law to be reported. Information gleaned from attacks can be used to learn about attackers' methods and develop responses. Reporting systems can be designed to protect confidential data while providing useful public knowledge—patent litigation regularly uses protection orders for confidential data while conducting the main business of the case in public.

The U.S. National Transportation Board keeps public databases of aviation accidents (https://www.ntsb.gov/_layouts/ntsb.aviation/index.aspx) and railroad accidents (https://www.ntsb.gov/investigations/AccidentReports/Pages/railroad.aspx) that serve as examples of incident reporting and analysis. In some cases, safety recommendations or maintenance alerts may be made as a result of accidents.

In contrast, the National Vulnerability Database (NVD) maintained by the U.S. National Institute for Standards and Technology (https://nvd.nist.gov/) concentrates on code. The NVD defines *vulnerability* as "a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability" (https://nvd.nist.gov/vuln). A code-centric view of security minimizes the importance of system architecture and procedures followed by personnel.

Mandatory standards may be appropriate in some cases—for example, aircraft certification takes into account some aspects of cybersecurity and software safety. Mandates may help to overcome manufacturer inertia, with air bag regulations providing a classic example.

REGULATIONS AND STANDARDS

We need to be sure that export regulations do not unnecessarily restrict technologies that promote cybersecurity and safety. Some technologies will always be closely guarded. Regulators should take into account both risks and rewards when designing protections. Global supply chains mean that export controls have a broad reach that may keep important technologies from being adopted. Also, Internet attacks can be conducted by devices that have never entered the country.

Regulators need to treat cybersecurity and safety as top-of-the-list concerns. Electric power utilities put a great deal of effort into traditional reliability in case of storms and natural disasters; regulators require utilities

to be prepared for such events and impose fines for certain types of power outages. Cyberthreats are arguably a lower priority at some utilities because their regulators do not place high importance on such threats. Cyberattacks have been much less frequent than, for example, weather-caused outages. Unfortunately, the consequences of a cyberattack could be huge and long lasting. Regulators need to find ways to encourage utilities of all types—for example, electric, natural gas, water, sewage, and transportation—to plan for these new threats.

Voluntary standards have proven useful in other domains. The Energy Star ratings used in the United States were created by the federal government and are voluntary. A wide range of consumer products advertise their Energy Star ratings. Manufacturers can employ voluntary systems to advertise their security capabilities and allow consumers to vote with their wallets.

Cyberthreats to our data and our physical world are real, and they will not go away. The pervasive adoption of computer technology has given us huge benefits but also new types of risk. A civil defense approach to cybersecurity and safety can help the citizenry protect itself against attacks and effectively respond to the inevitable attempts by bad actors to interfere with daily life.

REFERENCES

1. CBS News, "Inside the New York hospital hackers took down for 6 weeks," Aug. 18, 2017. [Online]. Available: https://www.cbsnews.com/news/cbsn-on-assignment-hackers-targeting-medical-industry-hospitals/
2. D. Goodin, "First known hacker-caused power outage signals troubling escalation," *ArsTechnia*, Jan. 14, 2016. [Online]. Available: http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/
3. A. Greenberg, "The untold story of Notpetya, the most devastating cyberattack in history," *Wired*, Aug. 22, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
4. A. Halsey III, "Delta computers crash, causing delays and cancellations. Experts say it shouldn't have happened," *The Washington Post*, Aug. 8, 2016. [Online]. Available: https://www.washingtonpost.com/local/trafficandcommuting/delta-airlines-computer-systems-crash-causing-flight-delays-and-cancellations/2016/08/08/7d5e8fa0-5d72-11e6-af8e-54aa2e849447_story.html?utm_term=.cb218d77d206
5. M. Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet, Feb. 2, 2015. [Online]. Available: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/
6. National Commission on Terrorist Attacks Upon the United States, "The 9/11 report," July 22, 2004. [Online]. Available: https://www.9-11commission.gov/report/
7. J. W. Moyer, D. Hedgpeth, and F. Siddiqui, "Southwest Airlines computer glitch causes cancellations, delays for third day," *The Washington Post*, July 22, 2016. [Online]. Available: https://www.washingtonpost.com/news/dr-gridlock/wp/2016/07/21/long-lines-for-southwest-airlines-passengers-at-area-airports/
8. E. Ortiz, J. Shamlian, and T. Costello, "United Airlines flights no longer grounded, delays remain," NBC News, July 8, 2015. [Online]. Available: http://www.nbcnews.com/business/travel/united-airlines-passengers-say-flights-grounded-nationwide-n388536
9. M. Wolf and D. Serpanos, "Safety and *Security in Cyber-Physical Systems* and Internet-of-Things systems," *Proc. IEEE*, vol. 106, no. 1, pp. 9–20, Jan. 2018. doi: 10.1109/JPROC.2017.2781198.

MARILYN WOLF is the Rhesa "Ray" S. Farmer, Jr., distinguished chair in Embedded Computing Systems and Georgia Research Alliance Eminent Scholar at the Georgia Institute of Technology. She is a Fellow of the IEEE and ACM. Contact her at wolf@ece.gatech.edu.

This article originally appeared in Computer, *vol. 52, no. 1, 2019.*