DOI:10.1145/2184319.2184330

Simson L. Garfinkel

Inside Risks
The Cybersecurity Risk

Increased attention to cybersecurity has not resulted in improved cybersecurity.

THE RISK OF being "hacked"—whatever that expression actually means—is at the heart of our civilization's chronic cybersecurity problem. Despite decades of computer security research, billions spent on secure operations, and growing training requirements, we seem incapable of operating computers securely.

There are weekly reports of penetrations and data thefts at some of the world's most sensitive, important, and heavily guarded computer systems. There is good evidence that global interconnectedness combined with the proliferation of hacker tools means that today's computer systems are actually *less secure* than equivalent systems a decade ago. Numerous breakthroughs in cryptography, secure coding, and formal methods notwithstanding, cybersecurity is getting worse as we watch.

So why the downward spiral? One reason is that cybersecurity's goal of reducing successful hacks creates a large target to defend. Attackers have the luxury of choice. They can focus their efforts on the way our computers represent data, the applications that process the data, the operating systems on which those applications run, the networks by which those applications communicate, or any other area that is possibly subverted. And faced with a system that is beyond one's technical hacking skills, an attacker can go around the security perimeter and use a range of other techniques, including social engineering, supply-chain insertion, or even kidnapping and extortion.

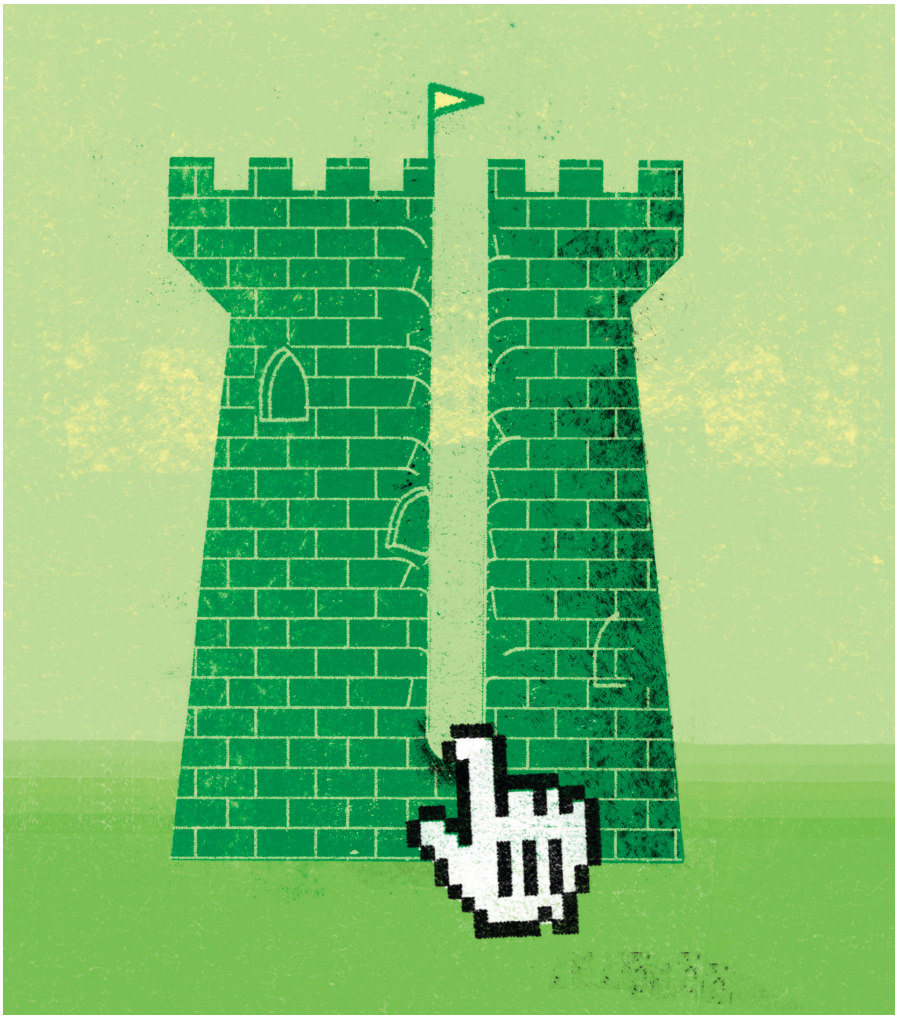

ILLUSTRATION BY YAREK WASZUL

It may be that cybersecurity appears to be getting worse simply because society as a whole is becoming much more dependent upon computers. Even if the vulnerability were not increasing, the successful hacks can have significantly more reach today than a decade ago.

Views of Cybersecurity

The breadth of the domain means many different approaches are being proposed for solving the cybersecurity problem:

- Cybersecurity can be viewed solely as an *insider problem*. What is needed, say advocates, are systems that prevent

The possibility of an active, malicious adversary is what distinguishes security from other computer science problems.

authorized users from acting improperly. Such technology would simultaneously prevent attacks from nonmalicious (but improperly trained) insiders, disgruntled employees, and malware that had compromised the accounts of the loyalists. The problem with this approach is that we fundamentally do not know how to address the insider threat.

▸ Given that operating systems have become too complicated to make any assurances about their correct or intended operation, many cybersecurity practitioners focus on the promise of network security as a kind of silver-bullet solution. But as Iran's experience with the Stuxnet computer worm demonstrated, even systems that are thought to be isolated can be compromised by outside adversaries. Even if network security were perfect—and it is not—we would still need to secure the hosts.

▸ Recently, there has been an effort to frame cybersecurity as an economic problem—convincing companies to spend resources on defense and training consistent with the risk they face. This formulation assumes spending more money actually increases security, but there is no evidence to support the assumption. Indeed, one of the persistent problems with framing security as an economic problem is that there are no reliable techniques that can be used to examine a system and measure the size of its vulnerabilities and the likelihood of compromise. Such attempts to measure security inherently risk focusing attention on what can be measured, instead of what matters.

▸ Others see security as a holistic process that encompasses all elements of an organization's IT and HR operations. Such a broad formulation seems to have some benefits—Microsoft's Security Initiative, started in 2002, dramatically improved the security of the company's products. But most organizations lack both the technical and financial ability to make information assurance a primary goal, and even an effort the size of Microsoft's did not create unhackable software.

The possibility of an active, malicious adversary is what distinguishes security from other computer science problems. A compiler designer worries that an optimizer bug might result in an incorrect calculation or undefined behavior. A security professional knows an adversary can analyze the compiler, the buggy output, and large amounts of code to find that single instance where the buggy executable and a specific input can be used to exploit a system.[1]

The adversary makes security more difficult than other computer science problems, because the adversary adapts to our best defenses and finds ways around them. Fortunately, adversaries are *not* all-powerful: they too are governed by economics, attention spans, and other external factors. There may be limits on the adversary's knowledge of the target systems. In many cases we can decrease the risk of a successful attack.

Making progress on cybersecurity requires that we address a myriad of both technical and nontechnical factors that work to prevent governments, corporations, and even individuals from securing their systems. We have real solutions to many security problems, but many are unwilling to adopt them.

Technical factors that comprise the cybersecurity problem dominate the discussion among both technologists and policymakers. These factors include language and operating system choices, security architectures, usability, and training. What is frustrating is that many of the techniques and technologies for developing secure systems that have been shown to reduce security-critical defects, such as Microsoft's Security Development Lifecycle (http://microsoft.com/sdl), have not been widely adopted. There is a huge gap between general practice and best practice.

Nontechnical factors impacting cybersecurity reflect deep political, social, and economic divisions within our society. These problems include shortened development cycles; the inability to attract and retain the best workers; and the general failure of our schools at early science, technology, engineering, and math (STEM) education. While it is certainly possible that the need to secure our computers will force us to find solution to these other problems, such Pollyannaish hopes seem unlikely to be realized.

In recent years there has been an effort to liken cybersecurity to a public health problem. Just as hand washing and coughing on our sleeves can help halt the spread of influenza, advocates say, good "cyber hygiene" such as running up-to-date anti-virus software and only going to clean Web sites run by reputable organizations can help stop the spread of malware and the growth of malicious botnets.

A more accurate public health metaphor might be obesity. Just as there are companies in the U.S. that benefit from the production and consumption of excess calories, while others make money treating the medical conditions that result, there are companies in the U.S. that benefit from poor security practices, while others are benefiting from mitigating the resulting problems.

Preventing security snafus is difficult and frequently thankless. It is commonly reported that chief security officers are denied resources by management because they cannot quantify the risk their organizations face or how the requested expenditures will improve the security posture. We would like to demonstrate that security has a significant return-on-investment, but security is frequently just a cost. Chief security officers that deploy technology are sometimes criticized for wasting money when new systems are purchased and no attack materializes. For senior managers, the risk to one's career of being innovative is frequently higher than the risk of maintaining the same poor practices of one's peers.

It frequently feels like many organizations are implicitly relying on hackers for their security testing.

Most companies see information security as a *cost* or a *product* rather than as an enabling technology.

The Isolation Fallacy

One of the simplest solutions proposed for the cybersecurity problem is to run systems in secure enclaves that are disconnected from the Internet. While the idea may sound attractive, execution is impossible in practice.

Even a so-called "stand-alone computer" has a bidirectional connection to the Internet. All of the software on these machines is typically downloaded from the Internet (or from media created on machines that were connected to the Internet). The documents produced on stand-alone machines are either burned to DVD or printed—after which they are often scanned and sent by email or fax to their final destination. A completely isolated system would have very limited utility.

Just as all computers are connected, so too are all humans connected to computers. Human activities as disparate as genetic engineering and subsistence farming rely on computers and communications systems to manipulate data and send it vast distances. An attacker can cause a lot of damage by modifying a message, no matter if the data is a genetic code or a coded SMS message. Millions of people live downstream from dams with floodgates that are controlled by computers.

Over the past 30 years security researchers have developed a toolbox of techniques for mitigating many kinds of cyber attacks. Those techniques include workable public key cryptography (RSA with certificates to distribute public keys); fast symmetric cryptography (AES); fast public key cryptography (elliptic curves); easy-to-use cryptography (SSL/TLS); sandboxing (Java, C#, and virtualization); firewalls; BAN logic; and fuzzing. These breakthroughs have resulted in countless papers, successful tenure cases, billions of dollars in created wealth, and several Turing awards. In spite of all this progress, cyberspace is not secure.

Some have argued that because today's cyber infrastructure was designed without attention to security, the proper solution is redesign. Such proposals, when realized, frequently result in systems having the same kinds of problems we experience today. For example, some have proposed adding a kind of "authentication layer" to the Internet.[3] Such a layer would increase the value of stolen credentials, proxy-based attacks, and implanted malware—problems that already bedevil today's authentication layers.

We frequently discover that what was once regarded as a breakthrough security technology is really nothing more than an incremental advance. For example, considerable effort was expended over the past decade to deploy non-executable stacks and address space layout randomization on consumer operating systems. As a result, Microsoft's 64-bit Windows 7 is not vulnerable to much of the malware that can infect 32-bit Windows XP systems. Yet even without an executable stack, Windows 7 applications can still fall victim to so-called "return-oriented programming"[5] in which the attacker's malicious code is created from the exploited program and a series of specially constructed stack frames, each frame executing a few instructions in the program before "returning" to the next sequence.

The Fault is Both in Our Bytes, and in Our Selves

While it is tempting to focus on technical factors impacting the cybersecurity problem, I believe nontechnical fac-

tors dominate the variety of risks we face today. Shortened development cycles and increased competition mean much of the software and configurations that are deployed have not been adequately validated. It frequently feels like many organizations are implicitly relying on hackers for their security testing.

At the same time, obsolete, bug-ridden vulnerable systems never seem to get retired. In February 2012 approximately 30% of the computers on the Internet were still running Windows XP (down from 31% the previous month), according to W3Schools.[4] Yes, Windows 7 has vulnerabilities, but Windows XP is dramatically less secure: it should be banned from today's cyber infrastructure.

Other factors increasing the cybersecurity risk include our difficulty attracting and retaining enough software engineers, and the failure of our schools to promote technology education from an early age.

It is important to realize that cybersecurity, despite its importance, represents only a tiny part of computer science research as a whole. Security professionals rightfully point out that a single flaw in practically any program can result in a devastating security compromise. This is troubling, because most computer professionals receive little if any training in security, most CS professors and software engineers try to ignore it, and there are few security specialists. This argues for better training and the creation of a licensing or certification process.

Some people blame pay scales. While science and engineering jobs pay better than average jobs in the U.S., they do not pay better than careers in medicine, law, and business, says Lindsay Lowell, director of policy studies at Georgetown University's Institute for the Study of International Migration. Testifying in 2011 before the House Subcommittee on Immigration Policy and Enforcement, Lowell said it is the lower salary paid to science and technology professionals that is responsible for the large number of non-U.S. students enrolled in U.S. graduate science and engineering programs.[6]

While we depend on our computers, we seem incapable of making or operating them in a trustworthy manner.

For generations educators have recognized that one of the primary purposes of schooling is to teach students how to write. As a result today's high school graduates have had at least 10 year's worth of writing instruction (and many say their writing still leaves much to be desired).

The situation is worse when it comes to technology education. Think what you want about so-called "digital natives," but experience with Facebook and video games does not translate into algorithmic thinking. Computers are part of early education in many communities, but the courses invariably teach how to be users, and not how to understand the underlying technology. Most college graduates have essentially no ability to perform even simple office automation tasks, and the typical CS graduate has less than six years' experience writing software. A real risk of our current educational system is that most graduates simply lack the experience to write security-critical software because they did not start programming in middle school.

We may be increasingly an information society, but most companies see information technology, and especially information security, as a *cost* or a *product* rather than as an enabling technology. Organizations balance their security against other competing requirements. A 2011 Bloomberg Government Survey of 172 Fortune 500 companies found they were collectively spending $5.3 billion per year on cybersecurity and stopping just 69% of all attacks. The organizations told Bloomberg they could increase the effectiveness of their defenses over the next 12 to 18 months such that they could stop 84% of cyber attacks; to do so they would need to increase their annual spending to $10.2 billion. Stopping 95% of cyber attacks, which Bloomberg claimed would be the "highest attainable level" of security, would increase spending to $46.6 billion per year.[2]

Stopping 95% of cyber attacks means one in 20 still gets through—far too many when the result of even a single successful attack can be devastating. The situation is similar to cancer treatment: if chemotherapy leaves a single surviving cancer cell, the patient frequently dies. With cybersecurity it is clear we cannot cure the patient. We must learn to live with the disease.

Live with Cyberinsecurity

There is no obvious solution to the problem of cybersecurity. While we depend on our computers, we seem incapable of making or operating them in a trustworthy manner. Much is known about how to build secure systems, but few of the people building and deploying systems today are versed in the literature or the techniques. We should be designing society so that we can survive the failure of our machines, but it is more cost-effective to create systems without redundancy or resiliency.

Reducing our cyber risk requires progress on both technical and political fronts. But despite the newfound attention that cybersecurity increasingly commands, our systems seem to be growing more vulnerable every year. C

References

1. C compilers may silently discard some wraparound checks. US-CERT Vulnerability Note VU#162289, April 4, 2008.
2. Domenici, H. and Bari, A. The Price of Cybersecurity: Big Investments, Small Improvements. A. Holmes, Ed., Bloomberg Government Survey (Jan. 31, 2012).
3. Landwehr, C. A national goal for cyberspace: Create an open, accountable Internet. *IEEE Security and Privacy 7*, 3 (May 2009).
4. OS Platform Statistics, w3schools.com; http://www.w3schools.com/browsers/browsers_os.asp.
5. Roemer, R. Buchanan, E., Shacham, H., and Savage, S. Return-oriented programming: Systems, languages, and applications. *ACM Trans. Info. Syst. Secur. 5*, 1, Article 2 (Mar. 2012).
6. "STEM" The Tide: Should America Try to Prevent and Exodus of Foreign Graduates of U.S. Universities with Advanced Science Degrees. Hearing Before the Subcommittee on Immigration Policy and Enforcement of the Committee on the Judiciary of House of Representatives (Oct. 5, 2011), 112–164.

Simson L. Garfinkel (slgarfin@nps.edu) is an associate professor at the U.S. Naval Postgraduate School in Monterey, CA.