A reprint from
American Scientist
the magazine of Sigma Xi, The Scientific Research Society

Cybersecurity Is Harder Than Building Bridges

Protecting the Internet and online computerized systems from attack is a difficult, messy problem. Here's why.

Peter J. Denning and Dorothy E. Denning

With a steady stream of reports about new cyber attacks and the vulnerabilities they exploit, it is easy to conclude that the overall state of cybersecurity is a mess. The developers of other engineered systems—such as bridges—seem to have evolved methods of design that keep their products safe and reliable. Why hasn't this relative stability happened for networked computers? By examining a series of threats faced by computer systems engineers, and comparing them with those confronting bridge engineers, we can show significant differences that help explain why cybersecurity is more complex. But there are signs of hope for much better cybersecurity.

Severity of the Problem

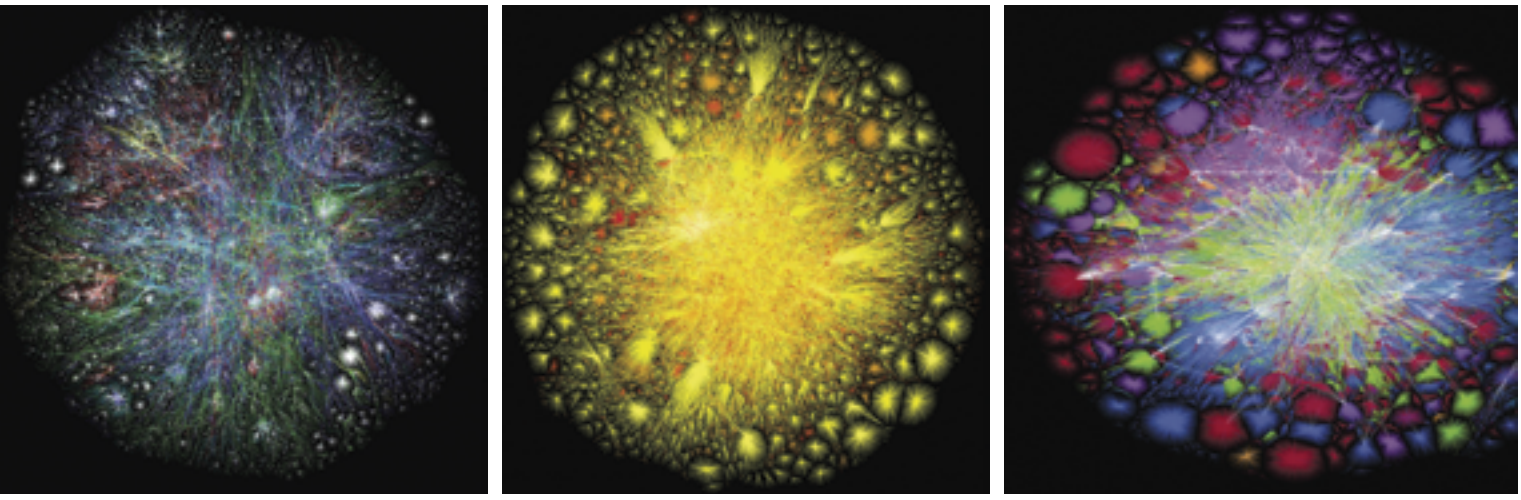
Cyber insecurity has become a growing public concern and top priority with governments. Recent headline-grabbers include the U.S. Office of Personnel Management data breach that compromised the confidential records of 22 million federal employees, the Anthem health insurance system breach that exposed personal data of 79 million people, the Target Corporation heist that harvested credit and debit card information of 40 million people, and the attack on Sony Pictures Entertainment that destroyed data and startup software on more than 3,000 computers, as well as disclosed prerelease films and embarrassing emails of executives. Public officials openly worry about cyber attacks on critical infrastructures such as power, water, communications, and transportation. Their concerns are well-founded. In December 2015, for instance, a cyber attack against Ukrainian power plants shut down electricity to 80,000 customers. Researchers have demonstrated numerous vulnerabilities in automobiles, airplanes, and medical devices that could be exploited with deadly consequences.

Reliable data on the extent and trends of cyber security incidents are surprisingly scarce. Security companies issue regular reports, but their findings are generally limited to data collected by surveys or through direct monitoring of their customers, and the reports seldom show trends beyond the fiscal quarter or year. David Shephard of software company NetIQ has extracted a list of 84 "most scary" facts and trends from multiple sources. Topping his list is a survey finding that 71 percent of organizations were victims of successful cyber attacks in 2014. His statistics show increases in detected cyber incidents, including a 517-percent increase for power and utility companies from 2013 to 2014. The average cost per incident for corporations was $3.5 million in 2013. The U.S. Computer Emergency Readiness Team has also seen a rise in cyber incidents reported to them, growing more than tenfold from about 5,500 in 2006 to more than 67,000 in 2014. The Center for Strategic and International Studies and McAfee put the annual cost of global cybercrime in the range of $375 billion to $575 billion.

The U.S. government maintains a national database of all reported software flaws that could be exploited in cyber attacks; it shows a steady increase from 1997 until about 2006, with a general leveling off at around 4,000 to 7,500 vulnerabilities per year after that. Although the leveling off sounds like good news, keep in mind that a single vulnerability can affect hundreds of millions of users. The majority of these vulnerabilities reside in top operating systems and applications software, including those from Apple (1,147 vulnerabilities in 2015), Microsoft (1,561), and Adobe (1,504). Considering that the desktop market share for Microsoft Windows and Apple Macintosh operating systems alone is greater than 95 percent, practically every desktop system is exposed.

This sorry state is not due to a lack of concern about cybersecurity. Computer and information security has been an ongoing worry of system designers and operators since the 1960s. By 1965, information protection was taken as one of six fundamental concerns of operating systems and has remained so for 50 years. These security technologies reflect a handful of basic themes: isolation, access control, encryption, authentication, and monitoring. But many cyber attacks are directed against the security technologies themselves—for example, guessing passwords or exploiting weaknesses in encryption protocols and antivirus software.

Peter J. Denning is Distinguished Professor of Computer Science and director of the Cebrowski Institute for information innovation at the Naval Postgraduate School in Monterey, California. He is also editor of ACM Ubiquity *and is a past president of the Association for Computing Machinery. Email: pjd@nps.edu. Dorothy E. Denning is Distinguished Professor of Defense Analysis at the Naval Postgraduate School. She is the author of* Cryptography and Data Security *(Addison-Wesley, 1982) and of* Information Warfare and Security *(Addison-Wesley, 1998) and is a member of the Cybersecurity Hall of Fame. The authors' views expressed here are not necessarily those of their employer or the U.S. Federal Government.*



Barrett Lyon / The Opte Project, opte.org

The vastness of the Internet has inspired artistic visualizations of its nodes and connections. These images (*from left to right*) were built from data in 2003, 2010, and 2015. The striking increase in visual complexity reflects the growth of the Internet over those dozen years. In 2003 there were 40 million websites, and in 2015, 1 billion. Any one of those sites could send you malware. How can you defend against an attack that could come from any of a billion directions?

Computer Systems and Bridges

Are other forms of infrastructure, such as bridges, as vulnerable to attack as cyber systems? Their physicality might make them seem easier to damage. But Wikipedia lists fewer than 100 bridge failures worldwide since 2000, and the American Society of Civil Engineers reports that 11 percent of 607,000 bridges in the United States contain deficiencies (known vulnerabilities determined by inspections). Both of these figures, either in absolute or relative terms, are dramatically lower than those for cyber incidents and vulnerabilities. Our bridges are in far better shape than our computers.

Computer systems and bridges have aspects in common. Both are engineered structures built from physical components. Their engineers work from specifications that give performance targets for critical functions. Both are concerned with moving traffic economically and efficiently—one with bits, the other with vehicles. Both are concerned with reliability, dependability, safety, and security. Both are susceptible, to varying degrees, to component and power failures, and external environmental factors such as earthquakes, floods, tornadoes, hurricanes, wind, aging, and traffic loads. Both deal with threats, although their nature differs. Looking at some main areas of threats to cyber versus bridge security reveals reasons why cybersecurity is hard and such a pervasive problem.

Restricted Access

Most bridges are open to the public. Although some require drivers pay a toll, they do not exclude most traffic. By contrast, most cyber systems are closed to the public, for the obvious reason that they are used to store and process sensitive information such as personal communications, financial data, health records, and trade secrets tied to individuals and organizations. To ensure that only authorized users have access, they require that users go through a login process that involves some means of authentication such as a password. All computer systems, whether open to public access (such as those in libraries) or closed, need to restrict what their users can do, so that they do not inadvertently or intentionally destroy system files, plant malicious code on the machines, or otherwise interfere with normal operations and other users.

To enforce these restrictions, computer systems employ a complex array of access controls that include not only login mechanisms, but also isolation techniques enforced by the operating system and hardware. These controls must ensure that users are only allowed to access digital objects such as files and database records for which they are authorized, and that they are only allowed to perform operations and transactions for which they have permission. Implementing these controls is vastly more complex than installing tollbooths and barbed wire on bridges.

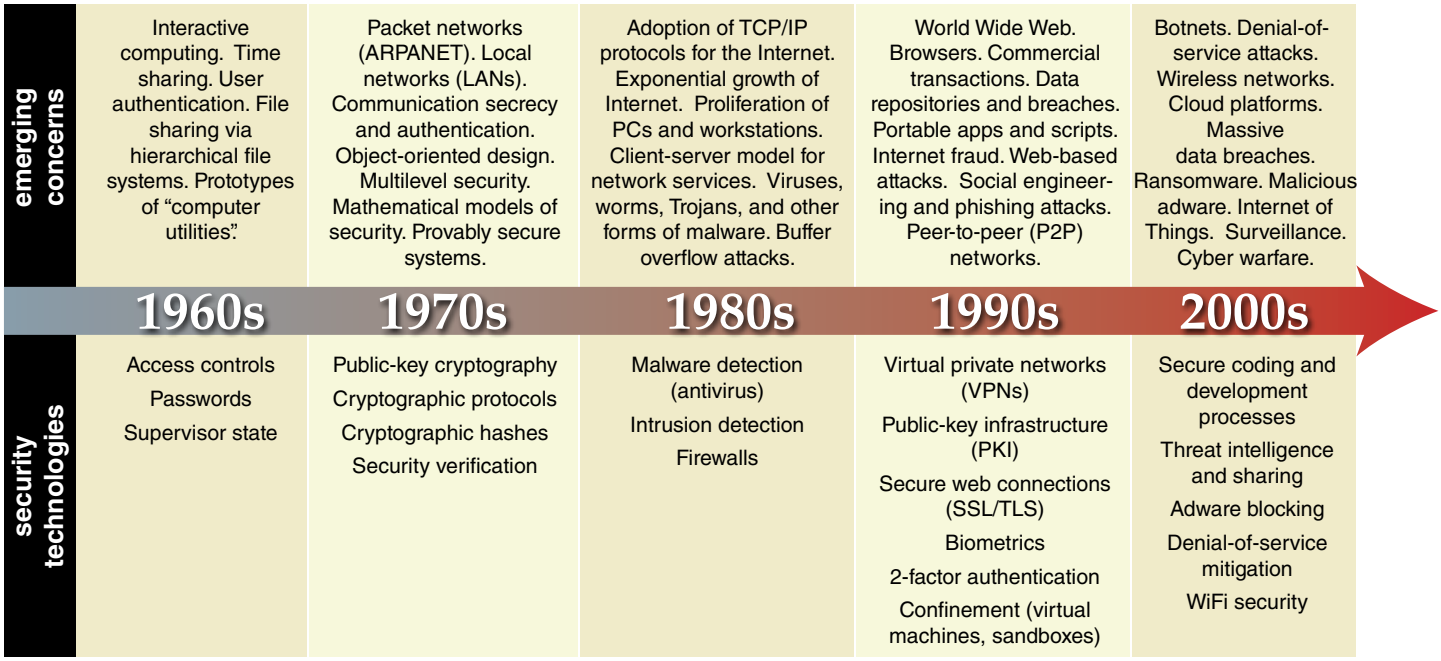
Although the access controls of operating systems go a long way toward securing data within a computer, they do nothing to protect data in transit over networks. Indeed, most network traffic is vulnerable to eavesdropping and corruption. Protecting these data requires a completely different set of security controls—notably cryptographic methods for encrypting and authenticating data—and traffic monitors watching for suspicious activity. Network security brings up the knotty problem of surveillance—less of a concern in a public location such as a bridge, where anyone is able to observe the flow of traffic.

Preventing Attacks

Except during times of war, bridges are rarely openly attacked. They may be vandalized with graffiti or blocked by protestors, but even these incidents are infrequent in comparison with the constant barrage of attacks against cyber systems, which must be monitored every second of every day with tools such as firewalls and programs for the detection of intrusion and malware (malicious software).

There are several reasons why cyberspace is a more attractive target of attack than bridges, but by far the most important is that cyber systems hold data of value. Intruders steal credit and debit card data, as in the Target breach. They raid bank accounts. They steal trade secrets and other data they can sell or use for competitive advantage. They download and disclose data to embarrass their victims. And they extort money from their victims by holding their data hostage or by threatening to disclose sensitive data acquired in a security breach. Even data you think has no value to anyone but yourself can be monetized with ransomware, which encrypts all your data and demands that you pay a hefty fee for the unlocking key. Nation-states commonly compromise the systems of adversaries and allies alike in order to acquire intelligence.

Timeline of Emergence of Security Technologies



China has been implicated in numerous breaches. North Korea objected to a movie depicting an assassination plot against its leader, and a group with ties to that country was blamed for the Sony attack.

In addition, cyber attacks are relatively cheap, easy to conduct, and of low risk to their perpetrators. Hacker tool kits are simple to acquire on the Internet. Young hackers have long been attracted to the thrill of invading someone else's system, whereas activist groups such as Anonymous have found cyber attacks to be a convenient means of protest. For criminals, cybercrime is a lower-risk alternative to traditional heists, such as bank robberies.

User Error

Cyber systems are much more prone to the weaknesses of their human users than are bridges, where careless drivers are unlikely to do more harm than tie up traffic or damage a guardrail.

Ignorant and careless users pose ongoing risks to cybersecurity. They pick weak passwords, open attachments with malicious software, click on links that lead to malicious sites, lose their laptops and other portable devices, and fall for phishing scams that harvest their usernames and passwords. Even careful users can be victimized by a "drive-by download" attack if they visit a legitimate site that has been compromised and are injected with malware that automatically infects their computer.

In addition to users, system administrators can be a source of vulnerabilities—for example, by failing to configure their systems for security, install patches, remove obsolete accounts, or respond to security alarms. Administrators need to install patches quickly for newly discovered vulnerabilities, but a speedy response does not always happen. Kenna Securities found that it takes companies on average 100 to 120 days to install patches, even though the probability of a vulnerability being exploited reaches 90 percent within 60 days.

Part of the reason that users fall short is that security is often inconvenient, interfering with their ability to accomplish their goals. Users do not like using 15-character passwords such as "7t$xKQ34(2@ad9#" or installing updates when they are busy with other things. They have difficulty using encryption and recognizing emails with malicious attachments and links. Some do not perceive the dangers and will bypass security protections and rules in their workplaces in order to get their jobs done more quickly.

Code Complexity

Cyber systems are enormously complex. The two major desktop operating systems, Windows 10 and Mac OS 10.4, use 50 million and 86 million lines of code, respectively. No bridge has so many components.

Each line of code in an operating system potentially contains errors that could be exploited to compromise security. Finding and removing vulnerabilities in 50 million lines of operating-system code is devilishly hard for developers, which is why thousands of new errors are revealed each year. Add in software applications—including browsers, email, database systems, and document processing tools—and the problem quickly becomes intractable. Further, even if software products are shipped with no known security flaws, backdoors and malicious code can be inserted somewhere along the supply chain. Rogue retailers, for example, have been reported to install data-collecting malware on Android phones made and largely sold in China.

To make matters worse, cyber systems are dynamic and constantly evolve. Whereas the American Society of Civil Engineers reports the average lifetime of bridges to be 42 years, software systems have much shorter lifetimes, measured in years rather than decades. Software systems are constantly upgraded—and the new and revised components often have novel vulnerabilities. In contrast, bridges are stable over their lifetimes, seldom require replacement parts, and need only periodic physical maintenance such as painting and inspections.

On top of all this, there are theoretical limits to cybersecurity. In the 1980s, security pioneer and computer scientist Frederick B. Cohen proved that it was impossible to develop an antivirus tool that would detect all

possible computer viruses. We are unaware of any theoretical limitations to constructing safe bridges.

Connectivity

Almost by definition, cyber systems are joined up with one another. Attacks can come from any direction and their sources can be made untraceable. Bridges are not so immediately interconnected; an attack or failure on one cannot spread to another.

Viruses and worms were some of the first lines of automated attacks enabled by network connectivity in the 1980s. The infamous Morris Worm of 1988 took down 10 percent of the Internet at the time in a few hours and stimulated the formation of the Computer Emergency Response Team at Carnegie Mellon University. Malware has become so ubiquitous that antivirus software has become a major industry. The Anti-Phishing Working Group reported that in the first quarter of 2015, the global malware infection rate was 36 percent. Norway had the lowest rate at 20 percent, and China the highest at 48 percent.

Attacks on bridges require some sort of physical presence such as a bomb, an aerial attack, or a mass protest. In contrast, remote attacks are common in cyberspace. The address from which you were directly attacked is probably not that of the perpetrator, because most attackers relay through multiple hosts to confound attribution.

Connectivity has also enabled attackers to assemble large networks of compromised computers, called *botnets,* and use them to conduct attacks and send out spam. They are particularly popular for conducting *distributed denial of service* (DDoS) attacks, which flood the chosen target with traffic and thus shut it down. Peak floods have reached hundreds of gigabits per second of traffic, causing major disruptions. In late 2012 and early 2013, an Iranian group shut off access to several bank sites with DDoS attacks reaching 120 gigabits per second, as a means of protest.

One of the biggest security concerns is the emergence of the Internet of Things, which has been enabled by cheap wireless technology. Another factor has been a change in the standard for Internet addresses to increase the number of digits from 32 to 128, which has expanded available addresses from about 4.3 billion to a basically unlimited number—more than 3.4×10^{38}. Now virtually every device and appliance can be connected to the Internet. The burgeoning Internet of Things is widely regarded as a potential security disaster because designers of individual things often pare down their operating system to bare essentials, such as wireless connections, and do not preserve security technologies. These devices contain many more vulnerabilities than do commercial operating systems.

Cyber systems are now an essential component of every infrastructure and are embedded in industrial controls systems. They are used to operate power grids, manage transportation systems, handle finances, move oil and gas, treat and distribute water, operate dams, and much more. Thus, an attack on a cyber system can have consequences that go well beyond computers and the data that they store, and can be a means of damaging many physical systems. Public officials and security professionals are increasingly concerned that devastating cyber attacks against critical infrastructure could lead to loss of life and have a huge economic impact.

Market Forces

Absolved by licensing agreements, cyber software vendors are generally not legally liable for flaws in their products. We are forced to accept their products "as is." Bridge builders, by contrast, are subject to legal action in the event of failures owing to faulty construction.

In addition, software companies are under tremendous pressure to get their products to market. If they spend too much time in development, they will lose market share when other companies beat them to the consumer. One consequence is that vendors limit the amount of time they spend hunting for and fixing vulnerabilities. A survey by the security software company Prevoty found that 79 percent of companies release applications with known bugs; nearly half reported releasing apps with known vulnerabilities at least 80 percent of the time. More than 70 percent said that business pressures often overrode security concerns, whereas 85 percent said that vulnerability remediation significantly affected their ability to release software on schedule.

On the other hand, companies whose computer systems are attacked are more often being held liable for the harm it causes their customers. To settle a class-action lawsuit following its security breach, Target set up a fund of $10 million for customers whose card payment data were compromised.

Is There Hope?

Although the state of cybersecurity seems bleak, not all of the news is bad. Software developers now take security much more seriously than they did at the turn of the century. They heed their customers' calls for more security for the personal data entrusted to them, and they cringe at lawsuits that will surely follow a damaging attack. Microsoft, for example, uses Security Development Lifecycle (SDL), a software development management process they created to enforce secure coding practices. Adopting SDL has significantly reduced the number of vulnerabilities in their software. The software industry's greater emphasis on security is no doubt one reason that the number of reported vulnerabilities has flattened out in recent years. Even so, many see security not as the top priority but as a tradeoff with other objectives, such as functionality and performance.

The cyber security community has also responded to the growing threat with new technologies and guidelines for operating cyber systems securely. Although no single security technology can make a system secure, using them together with recognized security practices provides many impediments to intruders and malware. The federal government and industry have developed a list of 20 critical security controls, and if everyone adopted these protocols, we would see a dramatic drop in successful cyber attacks.

Moreover, with help from industry, governments are taking greater steps to go after those responsible for cyber attacks and to shut down botnets and sites used to distribute malware and support cyber attacks. Governments and industry are sharing more threat intelligence so that organizations can better protect their systems.

Although cyber attacks certainly have been on the rise, so too has the use of cyber systems. An interesting study by Eric Jardine of the Centre for International Governance Innovation in Canada finds that relative to the growth of the Internet, many measures of insecurity growth show it slowing down or even declining. Such results are encouraging; at the least, they suggest that the threat is not getting too far ahead of us.

(A reference list for this article is available at http://www.americanscientist.org.)