外文原文

Protecting the privacy of user data from unauthorized access is essential for business executives, policymakers, and users themselves. The pace of targeted attacks and massive data breaches is only increasing. Each new incident hurts organizations’ bottom lines, undermines users’ trust in the products they use every day, and can have dire consequences for public safety.

The problem is multifaceted. Technologists are rushing to fix software vulnerabilities. Regulators are trying to keep pace with the realities of a complex ecosystem. Market-based approaches, such as cybersecurity insurance, remain immature. In addition, consumers are still learning what options they have, and what options they should be asking for.

Currently, end users can use software that provides strong privacy protection with a high degree of certainty. Unfortunately, adoption rates for such software are low, largely because of how hard it is for nonexperts to use. This does not have to be the case. Software developers in the open-source community —who are generally the first to build encryption and privacy tools—need to improve the design of their tools to make them more user-friendly and useful. In turn, corporate and government purchasers should begin promoting the value of open-source software, particularly as it offers best- in-class security. These steps would go a long way toward improving privacy online.

BACKGROUND:CRYPTOGRAPHYANDUSEREXPERIENCE

Tools that provide strong privacy guarantees have historically been niche products, requiring a special understanding of the underlying security mechanisms in order to operate them. However, many of the basic concepts are straightforward. For example, encryption allows the contents of a message to be scrambled so that third parties cannot read it. Users apply an encryption key—similar to a long, complex password—to scramble data, and a decryption key to unscramble it. If the encryption of messages passing between users Alice and Bob occurs on their respective computers, and the decryption keys are under their sole control, it is called end-to-end encryption. This form of encryption is the gold standard in privacy preservation, because it prevents would-be eavesdroppers from intercepting the conversation.

Software tools for end-to-end encryption have been available to users since the early 1990s, when Phil Zimmerman created a program called Pretty Good Privacy (PGP) and released it to the public free of charge. However, nonexpert users have faced a number of challenges with these tools from the beginning. In a 1998 paper, “Why Johnny Can’t Encrypt,” Alma Whitten and J. D. Tygar documented problems facing users of PGP. The authors found that participants had difficulty performing even basic tasks like encrypting and decrypting messages. Further studies have replicated these results with a variety of software programs.

The integration of software into daily life—from workplace desks to phones tucked in pockets—

has led to tremendous professionalization of user-experience (UX) design. From big firms to small app developers, many software companies live and die on the quality of their UX and employ a host of designers and researchers to improve it. Not surprisingly, end-to-end encryption tools are derided when they are hard to use, whether these tools are for playing games or talking confidentially about sensitive material. Given this industry focus on UX design, it may seem odd that privacy tools still have a reputation for being hard to understand and use. Several factors contribute to these apparent shortcomings, which limit the development and adoption of user-friendly privacy tools.

CHALLENGES

One fundamental challenge to both the usability and adoption of privacy-preserving tools is that privacy is considered a secondary task, as demonstrated through user-experience research. A secondary task is always subservient in users’ minds to the primary task, which is whatever core activity the software is meant to enable: sending emails in an email client, exchanging instant messages in a chat program, or collaborating on documents in a file-sharing application. Many security features have this second-class status: users describe talking to their friend not as “secure messaging” but simply “messaging,” with the need for security as an ancillary requirement. This is problematic for software designers because users will readily abandon success on the secondary task if it becomes too onerous, or if they perceive it to be in conflict with the primary task.

Privacy-preserving tools seeking mass appeal face another significant challenge: nonexpert users have a hard time distinguishing strong security properties from their snake-oil alternatives. It is easy to call a tool “secure,” but it is hard to communicate the nuances without going into overwhelming details in an app-store listing. There have been efforts over the years to create a third-party seal of approval for secure tools, but these attempts have either foundered in obscurity or lacked credibility by allowing developers to purchase approval after a cursory self-evaluation.

Creating well-designed privacy-preserving tools with mass appeal also faces a variety of ecosystem hurdles. First, most tools in this space are developed as open-source products, which means that the authors publish the source code for anyone to read. This is good for security because the transparency of the open-source development model makes it possible to conduct independent reviews of the software (reducing the probability of critical vulnerabilities). It is bad for sustainability because few open-source projects are profitable, and many derive their funding from unsteady sources of income such as donations or grants.

Second, the majority of nonexpert users are unlikely to transfer their digital lives to niche security tools, and prefer to prioritize their primary tasks by choosing the convenience of popular cloud platforms. End-to-end encryption is in direct conflict with the business model most platforms have adopted, because it prevents the data mining and ad targeting that these services have monetized. A service provider such as Google cannot serve targeted ads if it cannot read the contents of an email. Finally, a recent resurgence of a decades-old debate around the propriety of encryption technologies—particularly as they relate to law-enforcement efforts to thwart terrorism or investigate crimes—is creating tremendous uncertainty for software developers. Apple and Google have both made upgrades to support user-controlled encryption by default in strategic products (iMessage’s encrypted chat, Android’s encrypted file system). However, these nascent investments are unlikely to be followed by large-scale integration of privacy-preserving technologies, given that a multitude of conflicting requirements around cryptography loom on the horizon in different jurisdictions. For the United States, it is especially unfortunate that this debate emerges at a time when confidence in technology companies’ ability to protect user data is still suffering from the fallout of the Edward Snowden revelations.

RECOMMENDATIONS

First and most urgent, the current debate over the use of encryption undermines the promotion of privacy tools. The U.S. government proposed a technological backdoor with the Clipper Chip in theearly 1990s, using the same arguments heard today. It failed spectacularly. Although technology has evolved since, the fundamentals of encryption have not. Policymakers in the United States and other countries should recognize that anything less than intact cryptography puts all users at risk. Developers cannot build software that allows law enforcement to access encrypted communications but prevents malicious actors from exploiting that access. Cryptography cannot distinguish good people from bad, so a backdoor for one is a backdoor for all. Undermining the encryption used by

U.S. companies would place the average consumer at risk of attack by malicious third parties, and merely motivate criminals and terrorists to use one of many alternative options. Powerful cryptography tools can easily be built outside the United States; as the self-declared Islamic State’s use of German messaging service Telegram demonstrates, software rarely respects borders.

In addition, technology decision-makers, including chief information security officers and others with purchasing power, need to promote the value of open-source tools throughout their organizations. This can be done by authorizing in-house engineers to contribute to open-source projects during work hours and explicitly seeking technology consultants experienced in the open- source world. Open-source development can span geopolitical barriers to create technologies that offer best-in-class security, but all too often such projects are viewed as half-baked or risky by decision-makers. The volunteer authorship of many projects contributes to this reputation, but the lack of polish in the user experience design does greater damage. Changing a company’s culture from one of client (“software is an expense, what do I get for my money?”) to one of community (“software is an investment, how can we contribute strategically for long-term benefit?”) can help organizations and projects find innovative, secure, and affordable solutions.

Open-source developers, in turn, need to prioritize user-experience research and design, as well as to optimize their tools for large organizations. The focus of too many projects has long been on users who resemble the developers themselves. It is time to professionalize the practice of open- source development, recruit designers and usability researchers to the cause, and take a human- centered approach to software design. In particular, project leaders should make the development process more accessible to new participants by including explicit instructions to user-experience experts in their documentation. Although this change in focus will require a cultural shift within the open-source community, it will allow projects to attract more users and more donations, and ultimately result in more useful tools.

To support these efforts, technology-focused foundations and software companies’ research and development wings should shift funding priorities toward more applied research on crafting and communicating about security-related features. Much of the work in this area examines the reasons a tool is hard to use—not ways to improve it—or focuses on toy refinements (e.g., “this custom interface is better than the standard”). As an example of such research, WhatsApp recently incorporated end-to-end encryption into its mobile messaging platform, without changing the user experience of its product. However, it accomplished this by hiding all privacy-specific features and tasks from its users, which in turn introduces vulnerability to certain kinds of attacks. Instead, researchers should work to identify factors that make privacy features successful across tools, and examine how such features might be added to popular products without harming user satisfaction.

Taken together, these recommendations would both incentivize and facilitate organizations and individuals in their efforts to adopt stronger protections of user data from unauthorized access. Easier-to-use privacy tools and greater consumer confidence, in turn, will support continued growth, innovation, and financial stability in the digital era.

About the Author

Sara “Scout” Sinclair Brody is the executive director of Simply Secure, an organization that seeks to make privacy-preserving technology usable and useful for all people. Sinclair Brody has long been interested in improving the usability of security tools. Her Dartmouth College computer science doctoral dissertation, “Access Control In and For the Real World,” focused on the misintegration of classic security mechanisms with modern human organizations. As a product manager at Google, she worked on projects such as two-step verification and the Android operating system. She has authored numerous scholarly articles on a variety of security topics, and coedited Insider Attack and Cyber Security: Beyond the Hacker. The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious eaders,

and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing Foreign Affairs, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org. The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors. The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the Net Politics blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services. For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.