DOI:10.1145/3213764

Josiah Dykstra and Eugene H. Spafford

# Viewpoint
# The Case for Disappearing Cyber Security

*A proposal for keeping cyber security both out of sight and out of mind for end users.*

In May 2017, WannaCry ransomware rapidly proliferated around the Internet, despite availability of a patch released by Microsoft in March. This is simply one of the most recent and notable attacks exploiting known flaws—there is a constant barrage of attacks, large and small. Although cyber security is more complicated than a simple failure to patch end systems, analysis of cyber security incidents has consistently shown that a failure to apply patches is one of the leading enablers of successful attacks.

We have reached a point in the evolution of cyber security where hands-off, behind-the-scenes cyber defense should be the norm. Clearly, the best solution would be to deploy less-vulnerable systems. This is a topic that has received great attention for approximately five decades, but developers continue to resist using tools and techniques that have been shown to be effective, such as code minimization, employing formal development methods, and using type-safe languages. Additionally, consumers are widely believed to be reluctant to accept the software limitations and increased costs that result from some of these more secure development practices. Those issues, coupled with the vast amount of legacy code in place and being reused, have meant that better security is often, at best, an "add-

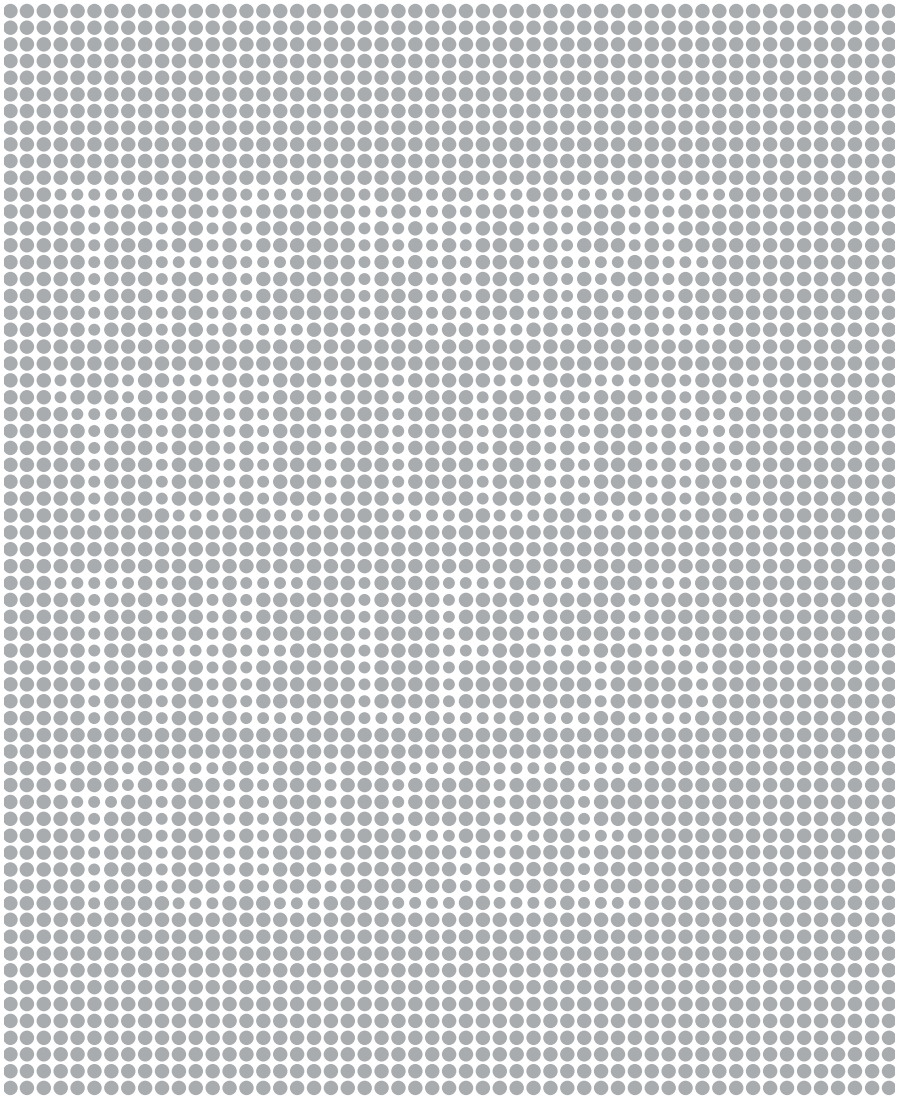

IMAGE FROM SHUTTERSTOCK.COM

on" rather than "built-in" function. Patching and configuration changes will be required indefinitely to keep the current infrastructure at least moderately secure.

Many end users today are not taking the deliberate actions required to protect themselves. For many decades, we have created increasingly effective tools and techniques for protecting users and systems, including limited automatic updates.[3] Despite active and valiant work at adoption and usability, it is apparent many users cannot or will not avail themselves of appropriate cyber security options. Many of today's systems were created with many low-level options by those who understood how they worked. Most end users today do not understand the underlying risks and results of their choices for those options. Those who are better informed may believe (sometimes, mistakenly) they understand all the issues and do not want to give up any options. In one study, even well-intentioned users with high engagement in security made choices leading to ineffective security.[2] In a 2008 *Communications* article, "The Psychology of Security," Ryan West concluded that "The ideal security user experience for most users would be none at all," but that users were, at that time, in the control loop by necessity.[10] It is time to reconsider the amount of control we require of users across the spectrum of experience.

We suggest an answer for a large percentage of end users would be to make the security aspects and interactions of today disappear from their view. That is, we ought to continue the pursuit of secure system development, patching, configuration, and operation as required, but do so without any explicit or necessary action of the users. Security should become transparent and all but "disappear" from those users' consciousness.

Users seem to be accepting one form of out-of-sight security already: automatic patch updates. Automatic software patches are now a common feature in desktop software, including Windows 10 and Google Chrome. It is certainly conceivable that other vendors and service providers could employ additional defenses needing updating without the express permission and awareness of users. It is commonplace now for users to agree to (but not read) end user license agreements (EULAs), some of which include language about limited out-of-sight changes.

**It is time to reconsider the amount of control we require of users across the spectrum of experience.**

Consider phishing as another example different from patching. Social engineering attacks executed by email have existed since the deployment of MIME-enabled email in the 1990s and remain a significant threat to this day. For decades, educational campaigns have attempted to raise awareness, with mixed success. In an ideal and sufficiently advanced world, phishing messages would never reach the end user and require the user's attention or judgment. Today, email providers such as Gmail employ machine learning and self-reporting in an attempt to flag suspicious messages and warn users. However, no matter how good those systems become there are false positives and users may still suffer consequences as they browse their "junk" folders looking for misclassified email messages. Incidents could be further reduced if the bad items known with extreme certainty were never even visible in the "junk" repositories of most users. This would make part of the protection "invisible" in the typical case.

An additional factor that supports more automated, invisible security is that online safety is closely tied to where users get their security information and advice. Too few users know where to obtain understandable, authoritative, and actionable advice. Furthermore, as threats (and systems) evolve, users need to update their security knowledge more often than they do. A 2016 research study examined reasons why subjects chose not to take a secure action even after receiving information recommending the behavior.[6] Among the 43% that rejected at least one action from the choices of installing antivirus, updating, and deploying two-factor authentication, the most common reasons were inconvenience and advice with "too much marketing material." Not only do people reject advice they think is unduly biased by vendors, but we have also seen far too many incidents with people who think they understand the risks and mechanisms better than they do. In both cases, the end users fail to follow best practices and good advice for patching, protections, firewalls, authentication, backups, and so forth. Security for both groups could be improved if the appropriate actions were executed automatically, without the need for user intervention or awareness.

Complexity for end users is an enemy of good security. The base case of applying security updates without delay or modification is all that a majority of end users need. Out-of-sight security could be simpler for the user if it reduced or eliminated complex security configurations and user interactions. If the security evolved along with the systems, users would not need to master the accompanying new terms and concepts.

While home and enterprise users will benefit from out-of-sight security by default, enterprises may continue to require more granular control. In many large environments, automatic, forced patching and control are already the norm for systems administered by organizations. Centralized control results in a more uniform application of necessary updates, and obviates the need for user involvement. It also simplifies issues of recovery from failures, and, when necessary, forensic analysis. Here, the same concept of automated, invisible security is applied, but at an organizational level, consistent with local needs.

Users may look for ways around automated security mechanisms.[7] A small population of technical users will be uncomfortable about surrendering control of their security options;

some of these users value theoretical considerations of control over practical security. Thus, it may be necessary to allow more control for those users with greater experience or special needs. The default start for these users would be the "invisible" security, with non-obvious options requiring explicit acknowledgment of risk, and perhaps a certain level of technical skill to access. This would be the cyber equivalent of "No user serviceable parts inside" warnings on many consumer electronics.

We acknowledge there are risks with invisible security that must be considered. Automated updates could interfere or break other software, or worse.[a] We will need mechanisms to verify that the invisible security is enabled and working as it should. We also recognize there are circumstances where patches must be certified in some way—including having patched systems meet performance and safety standards, such as those present for industrial controls, medical uses, and national security. In these cases, exceptions may need to be made to delay patching and support necessary testing. (This begs the questions of why those critical applications are using commodity software that may be prone to serious errors, and why they are configured in such a way that their safe operation would necessitate such patches.) Generally, these special cases make up a minority of deployed systems, and exempting them from automated patching would not negate the benefits of quickly fixing problems in all the rest. We also note the serious issue of securing legacy, unsupported, and unlicensed systems will remain a challenge, but it is made neither better nor worse by behind-the-scenes security.

Research will be necessary to determine whether or not users feel more secure—and if they actually are more secure—when cyber security defenses are invisible. That requires understanding what is meant by "security" in different contexts and with different types of security controls (such as patching, anti-malware, anti-phishing). It has been repeatedly noted that

**Complexity for end users is an enemy of good security.**

adequate security is relative to current environments and threats. For many end users, good security simply means their privacy is protected, even if nothing else is. Thus, security is often seen as both a reality and a feeling. Bruce Schneier, in particular, has criticized "security theater" but he acknowledges that "a bit of well-placed security theater might be exactly what we need to both be and feel more secure."[8] Cyber security professionals can learn from examples in other domains of visible versus non-visible security implementations. For instance, visible policing is an approach to security that places uniformed police officers in public to deter crime and reassure citizens. Research shows mixed results, including cases of increased crime and fear of crime after increasingly visible police presence.[4]

Clearly, those of us involved with equipping the world with advanced computation have some ethical obligations to make that computation safe.[1] The security community should strive for default security without explicit user interaction. The challenge is one of balance: How do we continue to provide appropriate autonomy and freedom to computer users while also protecting them? What is an appropriate level of residual risk to allow? We believe these (and related) questions should be considered and discussed, now, to enable development of a new climate for cyber security (and thus, privacy protection, which usually depends on good security) rather than continue to apply patchwork protections as marketing opportunities. We suggest that part of the solution is to move away from solutions that default to settings for the users who need the most options and choices, and instead automate security as the new default.

The cyber security community has succeeded in substantially advancing the field of resilient and trustworthy systems. Furthermore, research and development in security usability have made better security available to more users. The continued state of poor security adoption and practice, interacting with basic human nature, requires us to consider the next step of offering automated, behind-the-scenes cyber security as widely as possible. Continued work is necessary to refine the balance of control between human and machine, similar to the conversations around machine learning and artificial intelligence. If anything, those fields will require good cyber security to achieve their full promise. We believe it is time to consider a new approach, as we have outlined in this Viewpoint. C


**References**

1. ACM Committee on Professional Ethics. *2018 ACM Code of Ethics and Professional Conduct: Draft 2*; https://ethics.acm.org/2018-code-draft-2
2. Forget, A, Pearman, S., Thomas, J. et al. Do or do not, there is no try: User engagement may not improve security outcomes. In *Proceedings of the Symposium on Usable Privacy and Security* (SOUPS). (USENIX Association, Denver, CO), 2016, 97–111.
3. Frei, S., Duebendorfer, T. and Plattner, B. Firefox (in) security update dynamics exposed. *ACM SIGCOMM Comput. Commun. Rev. 39*, 1 (Jan. 2009), 16–22.
4. Millie, A. and Herrington, V. Bridging the gap: Understanding reassurance policing. *The Howard Journal 44*, 1 (Feb. 2005), 41–56.
5. Nachenberg, C. *The Florentine Deception*. Open Road Media Mystery & Thriller, 2015. http://florentinedeception.weebly.com
6. Redmiles, E., Malone, A. and Mazurek, M. I think they're trying to tell me something: Advice sources and selection for digital security. *IEEE Symposium on Security and Privacy*, 2016.
7. Sasse, M.A., Smith, M., Herley, C., Lipford, H., and Vaniea, K. Debunking security-usability tradeoff myths. *IEEE Security & Privacy 14*, 5 (May 2016), 33–39.
8. Schneier, B. The psychology of security. In *Proceedings of the Cryptology in Africa 1st International Conference on Progress in Cryptology* (AFRICACRYPT'08), Serge Vaudenay, Ed. Springer-Verlag, Berlin, Heidelberg, 2008, 50–79.
9. Wash, R., Rader E., Vaniea K. et al. Out of the loop: How automated software updates cause unintended security consequences. In *Proceedings of the Symposium on Usable Privacy and Security* (SOUPS). USENIX Association, Berkeley, CA, 2014, 89–104.
10. West, R. The psychology of security: Why do good users make bad decisions? *Commun. ACM 51*, 4 (Apr. 2008), 34–40.



**Josiah Dykstra** (josiahdykstra@acm.org) is a cyber security researcher with the U.S. Department of Defense in Baltimore, MD, USA.

**Eugene H. Spafford** (spaf@acm.org) is a professor of computer science at Purdue University, West LaFayette, IN, USA.


The views and opinions expressed in this Viewpoint are those of the authors and do not necessarily reflect those of the U.S. government, the U.S. Department of Defense, or Purdue University.



a This topic is explored in a recent work of fiction by a senior security professional.[5]