Invisible Security: Protecting Users with No Time to Spare

Josiah Dykstra
Cybersecurity Collaboration Center
National Security Agency
Fort George G. Meade, Maryland 20755
Email: josiah.dykstra@cyber.nsa.gov

***Abstract*—For over 50 years, the cybersecurity community has sought to protect vulnerable systems and users from victimization. Despite ongoing and valiant work at adoption and usability, some users cannot or will not avail themselves of necessary cybersecurity measures such as patching. Average, non-expert users—particularly those in small businesses—cannot afford to devote time to cybersecurity. Instead of accepting the risk of no security, alternatives are possible which achieve both security outcomes and conservation of time.**

We explore the paradigm of invisible security focused on creating cyber defenses that occur automatically without end user intervention. Invisible security is the next evolutionary step to aid users, now that automation is robust and effective in supporting it. Even though some example implementations, such as automatic updates, have existed for years, dedicated focus on this emerging paradigm is required to develop, measure, and deploy new capabilities. We present examples consistent with this approach in existence today, including automatic software updates and protective DNS. We draw insight and comparisons to other domains, including automobile safety. Then we describe how invisible defenses may aid potential beneficiaries in health care, the defense industrial base, and the general public. Finally, we present benefits and limitations of the approach and propose areas of future research and innovation.

I. Introduction

Seeking online security today requires time, skill, and financial commitments that some individuals and small businesses are unwilling or unable to apply. The doctor in a single-provider private practice medical clinic may lack enough time outside seeing patients to update software or backup electronic health records. Users such as this commit insufficient resources to cybersecurity mitigations, even if they acknowledge that noncompliance is risky [1]. No degree of usability entices these individuals to put forth time towards cybersecurity tasks.

The demand on users related to cybersecurity takes many forms. One is awareness of contemporary cyber threats and products or techniques for avoiding them, such as data backups as resilience against ransomware. Another demand is the mental effort to gauge harm, such as deciding if an email or website is trustworthy or malicious. There is also demand on users to respond to choices posed by interactive security products, such as SSL warnings in a browser or antivirus alerts.

Usable security emerged as an academic and commercial pursuit in recognition that prior security was too difficult and cumbersome for users. Scientifically-validated advances have been made, including new user interfaces and default settings that achieve varying degrees of security effectiveness and user satisfaction [2]–[4]. Nevertheless, users and systems continue to be exploited in similar ways as they have for decades, such as by social engineering. This is due, at least in part, to the fact that humans have the same biological and mental limitations that they have had for thousands of years. Unaugmented human brains remain ill suited, for example, to remembering many strong passwords. Many users could be better protected with automated security while avoiding security choices, decisions, and actions altogether.

Significant time and money are spent on security education. Some organizations and business sectors, including U.S. federal agencies, require annual training for the entire workforce. More, better, or tailored education are among the top recommendations from experts about how to raise awareness and improve users' behavior [5]. The security outcomes of awareness training are mixed. Furthermore, in some cases users are knowledgeable about the secure action they should take, and yet do something else (or nothing at all).

Invisible security is a different paradigm of cybersecurity protections that involve no end user attention or action [6]. Even if users are aware that the security is present, they can be absolved from action—potentially including installation, configuration, updates, or maintenance—while simultaneously achieving benefits afforded by the safety mechanism. To an unwitting user, those components of security are out of sight and out of mind.

Invisible security is not a lofty utopian goal, nor the pinnacle of usable security. Instead, it is a different way of thinking about security which requires zero end user interaction and still provides meaningful security outcomes. Furthermore, invisible security is not an excuse for the lazy but an acknowledgment and accommodation for the limitations of human ability. Advances in automation allow machines to augment limitations on speed or accuracy. Human augmentation, though still nascent, will allow humans to do uniquely human work while capitalizing on the tasks machines can do on behalf of humans. Demanding that a human make decisions about passwords or software updates is, for many, unnecessary.

Unattended automation is the natural evolution from invasive security tasks to invisible ones. Similar advances have happened in other domains. In the past 40 years, automobile manufacturers have added automatic anti-lock brakes and

978-1-7281-4146-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CIC50333.2020.00031

collision avoidance. Those features aid human drivers and increase safety for drivers, passengers, and pedestrians [7]. Physical buildings similarly protect occupants transparently without the need for individual attention or action. Architects now incorporate passive and discrete features into building design that are simultaneously aesthetic or invisible and effectively secure [8]. Yet, these are highly regulated domains where, today, computer hardware and software are not.

A key motivation for this work is the intuition that time is precious to business owners [1], and that they might embrace some cybersecurity that can be attained without user interaction. Downtime is extremely detrimental to business, and given the choice between security with downtime or uptime with no security, owners will often choose the latter. We seek to bring better cybersecurity to those who cannot devote the time.

A. Target Audience for Invisible Security

Invisible security can help a wide audience of individual users and, by extension, groups and organizations. We focus specifically on the benefits to non-expert users and organizations who are "average" in a colloquial sense and have non-specialized needs. We presume that all users are at risk for victimization and thus derive risk-mitigating value from cybersecurity. The user may not acknowledge the need or may be in denial of it. The intended target audience is anyone who is either doing nothing about cybersecurity or is unhappy with the resources required for their current cybersecurity methods. In some circumstances, such as Google Chrome automatic updates, we see that vendors who offer invisible security measures provide no official mechanism to disable the feature because of its effectiveness to protect all users of the software [2].

Of course, with few exceptions, users have some degree of control over the decisions about how to use their time and money, including whether or not to devote resources to cybersecurity. There are circumstances, most acutely in small business, where people accept great risks because the market demands it. Slim profit margins required to win a contract can mean that spending time and money on cybersecurity could cause the business to fail. So, some business owners accept risks of cyber victimization. Unfortunately, it is difficult to establish fixed thresholds for income or expertise to define the target audience who will most benefit from invisible security. Research may more clearly reveal the individual characteristics of people who can and do devote time and money to cybersecurity.

Finally, invisible security is neither appropriate nor universally advantageous for every situation. It is not intended as a solution for users who have the means to practice good cybersecurity but choose not to. This unwillingness or disinclination is the definition of laziness. And yet, invisible security can be a public good. An analogy is the addition of fluoride to the public water supply to reduce tooth decay. Such practices offer a public benefit, even to users who might otherwise afford them, and also to anyone unaware or not actively seeking its protection.

B. Related Work

Previous work on usable security and user adoption are informative to the consideration of invisible security. Many researchers and practitioners have sought to optimize cybersecurity outcomes and maximize adoption and practice while accommodating user capability and disruption. Unfortunately, the dominant and recurring theme among these works is informed and improved *action*, which is what we seek to eliminate. Instead of asking "why Johnny can't encrypt," we should now ask how Johnny can have encryption without any action whatsoever [9].

Invisible security has appeared before as an unfulfilled idea. Garfinkel suggested it as one approach to make human computer interaction and security "just work" [10]. In 2015, a master's thesis based on a user survey proposed an enterprise security platform design where users are not expected to confront security decisions that require special training [11]. Position papers, including those from Dykstra and Spafford [6] and Bella [12], have advocated a movement towards invisibility without a thorough analysis of existing implementations or their beneficiaries. In Section V we consider reasons why invisible security has not been fully utilized.

Much research has endeavoured to understand and improve cybersecurity for average users. One goal has been education, and prioritizing advice or recommendations that are most impactful. In a 2017 survey, researchers asked 231 security experts to provide the top three pieces of advice they would give to non-tech-savvy users [13]. The top result was "keep systems and software up to date," an area where invisible security is already at work. The authors concluded that "these findings suggest a need to better communicate expert practices and advice to nonexperts." We agree that better communication will help some audiences, but that optimized communications will never lead to cybersecurity adoption for some other users. Prioritization of advice can be complementary to invisible security if it is used to endorse or explain corresponding protections, such as automatic software updates.

Herley has suggested that users are right to reject security advice. He says that, "users' rejection of the security advice they receive is entirely rational from an economic perspective. The advice offers to shield them from the direct costs of attacks, but burdens them with far greater indirect costs in the form of effort" [14]. Even if optimized advice is not the sole solution, Herley advises that researchers and designers must seek a clearer understanding of the actual harms faced by users and an honest understanding of users' constraints.

There is a body of multidisciplinary work that brings insight to invisible security, including economics, risk communication, and mental models. Cybersecurity is highly intertwined with economic consideration of the cost and value of choices and their impact on security outcomes [15]. Mental models are another way to understand how and why users make cybersecurity decisions, with researchers suggesting that richer mental models could improve risk communication and decisions [16]. Wash found that inaccurate mental models cause home users

to justify ignoring security advice [17]. Invisible security may be a resolution to the cognitive dissonance that exists between what people know and what they do. There is mixed evidence about whether perceived control is a positive predictor of perceived risk in cybersecurity; this warrants exploration when considering the degree of the communication of risk with invisible security [18].

For unknown reasons, there is little public data, analysis, and consideration for the actual time people spend on cybersecurity tasks. A 2008 paper at the New Security Paradigms Workshop acknowledged time as a constraint to security [19]. A participant responded to the authors' survey saying, "Anything that loses time is not good for the business." Despite 291 citations to this paper, little can be found related to ground-truth data on how users decide and allocate their time to cybersecurity. Such results would allow the research and development communities to identify and prioritize invisible security implementations that saves users the most time.

The cybersecurity community should look to related disciplines for insight and inspiration. The science of safety, for example, deals primarily with the prevention of bodily injuries. Injury prevention strategies are commonly classified by education, engineering modifications, and enforcement/enactment. For example, automobile safety includes cars with crash worthiness (engineering), anti-drunk driving campaigns (education), and seat belt laws (enforcement). Unlike injury prevention, cybersecurity must be additionally concerned with proactive and intentional adversaries doing harm.

The remainder of this paper is organized as follows. Section II presents three examples of invisible security in existence today. In Section III we look at how invisible security could benefit three exemplar beneficiaries. Section IV discusses key benefits of the paradigm in more depth. Finally, Section V concludes the paper and offers areas for future work.

II. Example Implementations of Invisible Security

The implementations of invisible security are nascent and fertile for innovation. In this section, we describe three interventions that are compatible with invisible security. Each has been adopted independently, though certainly with the shared intention of usability. Their independent success suggests the potential for even greater impact as a combined strategy. Further, while these are technical security measures for well-known tasks, invisible security should be explored for a broader scope of tasks including social engineering defenses.

These examples illustrate that invisible security is possible and effective, not that it is solved. They reveal that the minimum user interaction can be, in fact, zero. Further study may provide insights about the nature and limits of invisible cybersecurity, and where human interaction is desired or essential. Additional innovation will create and promulgate new implementations of invisible security.

Automatic updates, protective DNS, and facial recognition authentication each offer security protection without end user attention or action. This section describes their emergence and use today.

A. Automatic Updates

Automatic software updates have become increasingly prevalent in today's operating systems and end user software. The software is written and configured to regularly check for patches and updates, which are automatically retrieved and installed. This feature is valuable, since patching remains an effective defense to help guard users from exploitation. Prevalent vendors of operating systems and browsers—notably Microsoft, Apple, and Google—allow behind-the-scenes, hands-free software updates. Automatic updates are commonly enabled by default. Research shows that this approach keeps users more secure [2]. The goal is not to simply make software updates easy for users to take deliberate action, but instead to make updates invisible to users.

Microsoft Windows was among the first software to introduce automatic updates in the year 2000. Software could autonomously check for patches and automatically download and install them. The user experience, however, was not entirely hands-off. For many years, the operating system was notorious for nagging users to reboot their computer after updates were installed [20]. In 2019 in response to customer complaints about stability, Microsoft stopped automatic installation of bi-annual "feature updates" containing new functionality and capabilities [21]. Automatic monthly fixes and security updates remain active.

Automatic updates are unique among safety science. By comparison, when defects are discovered in automobiles which pose unreasonable safety risk, the fix has historically required manual intervention and the expense of time, money, and labor. Software is comparatively easier and faster to update. There is no need for humans to devote time and attention to monitoring and installing software updates, unless the risk of doing so is severe and unknown.

B. Protective DNS

Most users have never heard of or thought about the domain name system (DNS), even though it is a linchpin to the online experience. Modern networking that uses Dynamic Host Configuration Protocol (DHCP) automatically configures DNS for clients when they join networks at home and work. Users benefit from DNS without having to understand how it is configured, or even that it exists at all.

An enormous number of cyber attacks are enabled by functional domain name resolution. Phishing emails and websites attempt to trick users through brand impersonation of similar-looking domain names. Bad actors rely on DNS for many facets of malware installation and execution, including command and control. Users may also visit and become inadvertently infected from compromised websites, despite warnings offered by safe browsing services [22].

The DNS infrastructure is capable of automatically blocking or redirecting malicious DNS queries from all applications on a device and invisibly protecting users. A business or internet service provider (ISP) who provides DNS resolution for users is perfectly situated to offer protective DNS to its employees and customers. In this case, a DNS provider blocks or filters

domain lookups for malicious domains. When a user clicks the link in a phishing email, for instance, the protective DNS provider recognizes the domain name as malicious and sends a benign response to protect the user automatically. The work of defense is transferred from users to providers. Vendors recognize the value of calculating the reputation of domain names, and many sell threat feeds as a service. In the United Kingdom, the National Cyber Security Centre (NCSC) offers free protective DNS services for the entire public sector [23]. Protective DNS could be implemented on a global scale if users had trust in the service provider and its domain filtering.

C. Facial Recognition Authentication

Passwords are the bane of many users. Authentication is both highly visible and pervasive to users of smartphones and other devices. Apple reported in 2016 that their average users unlocks their phones 80 times a day [24]. Yet, users are troubled by the selection, management, protection, and use of passwords. Many academic proposals have emerged for improving the usability and even transparency of authentication, especially for mobile devices [25]–[28]. Yet, text-based passwords and pins remain commonplace given the equilibrium they provide between security and usability, and the inertia of status quo [29].

One example of nearly-invisible security is facial recognition now available for smartphones and desktop operating systems. Unlike fingerprint biometrics, which still require action from the user, facial recognition can quickly authenticate the user when she or he looks at the device to use it. Once configured, this technique offers security with no recurring action and almost no time or effort demanded from the user. Fully invisible authentication would require no discrete action, even looking at the screen to deliberately unlock the phone.

Other behavior-based authentication schemes can contribute to invisible security. Continuous authentication has emerged as a strategy to verify users' identities in real-time as they carry out everyday computing tasks. Implementations have been demonstrated with keystroke dynamics, mouse movements, and cardiac rhythm. These techniques date back as far as 1975 [30] and have only recently become more prevalent, such as in mobile banking apps.

III. Potential Beneficiaries of Invisible Security

Rigorous scientific evidence is lacking, but observational and experiential data suggest that security remains a burden today. In this section we report on users in three groups of potential beneficiaries who show a need where invisible security would have a meaningful impact. Individuals and small businesses make up a large portion of that group. These examples are not the exhaustive list of potential beneficiaries, but are intended to illustrate the value to diverse populations.

In the United States, 99.9% of businesses are considered "small businesses" as defined by the U.S. Code of Federal Regulations (13 CFR Part 121). The determination takes into account the number of employees or annual income. For example, offices of dentists who have annual receipts up to $8 million per year are categorized as a "small business." In all, there were 30.7 million small businesses in 2019 and 59.9 million small business employees [31].

A common characteristic among small businesses, especially those with a very small number of employees, is the challenge of expertise and time for cybersecurity. According to one report, 62% of small businesses report that they lack the skills in-house to properly deal with security issues [32]. Deloitte found that small business owners spend no more than two hours per week on tasks unrelated to day-to-day tasks core to the business [33]. This leaves little time for continuing education, business development, and cybersecurity.

A. Health Care

The health care industry has a large number of small businesses and single providers. According to the U.S Small Business Administration, "Health Care and Social Assistance" is the top small business category with 44.7% [31]. These offices are heavy users of technology for business administration, such as scheduling and billing, and in the practice of health care. Gartner reports that health providers spent about 5% of their information technology budgets on security in 2018 [34]. Yet, data breaches of health care data continue and contribute to identity theft.

The delivery of health care also necessitates significant sensitive and personal information. In addition to medical results and diagnoses, health records include personal data such as date of birth and often include social security numbers, insurance details, and credit card numbers. As a result, they are a common target of data theft and ransomware. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) provides regulatory compliance, including security and privacy rules, for safeguarding personally identifying information. There are civil and criminal penalties for violations.

In 2017, the Health Care Industry Cybersecurity Task Force produced an analysis for Congress [35]. They reported that "No [health care] organization has all the financial resources it needs to employ enough personnel necessary to consistently and confidently protect its networks and data." Among their recommendations was "Identifying people and tools for addressing the small and medium-size health care organizations which cannot typically afford full-time technical resources." Such recommendations are noble but unlikely to succeed without external stimulus, and even so remain subject to human shortcomings.

Invisible security such as invisible authentication could be good for the health care workforce. Information technology is a powerful enabler to providing effective care, and both providers and staff continuously alternate between working with people and technology. Furthermore, many employees may share digital devices in clinic settings, and may share or eliminate passwords for convenience. Invisible authentication could allow both security and usability.

B. Defense Industrial Base

The Defense Industrial Base (DIB) is the worldwide collection of more than 100,000 businesses who design, produce,

deliver, and maintain military systems based on government requirements. In the United States, a small number of big prime contractors are supported by thousands of subcontractors in the supply chain. For example, a large contract to build an aircraft requires many subcontractors, down to basic components such as the manufacturing of bolts.

While prime contracts may bring tens of billions of dollars of annual revenue, small subcontractors make narrow profits. Out of necessity, the Department of Defense shares sensitive data with contractors in the defense industrial base and that data must be protected. The supply chain is also intertwined by necessity with business-to-business relationships and connections. Criminals and nation-states are targeting the DIB for access to sensitive information, or to exploit trust relationships between contractors, and seek more lucrative information. In recent years, high-profile cyber attacks against the DIB have been reported and the trend is likely to continue [36].

Employees at small DIB subcontractors have a need for cybersecurity but may be unable to devote the appropriate resources to protect data and survive as businesses. Invisible security, such as protective DNS or secure email, would be especially impactful to them and the U.S. government. Adopting this approach would relieve pressures of time and expertise from the contractor. The government could provide the services or cover the cost in the contract.

C. The General Public

Individual consumers of commercial technology represent a significant percentage of online activity. This population typically manages their own technology purchases, configurations, updates, and issues. Their understanding and adoption of cybersecurity practices varies widely, but a great percentage are not technical experts. Nevertheless, in sum they represent a rich target for victimization given the value of money they possess and financial potential (such as actual or potential financial credit).

Users in the general public need invisible security. They do not have an informed grasp about the threats facing them, and it would be burdensome to keep abreast of it. These users do not want the responsibility of updating their software, nor the inconvenience of rebooting their device, even though known vulnerabilities in software are a common initial access tactic and open the opportunity for hackers to access private and financial data. Given the size of the total population, individual compromises in the general public are a danger to others. For example, a hacker who compromises one email account may exploit trust relationships using contact information of that victim's friends and family to propagate malware or financial scams.

Invisible security would greatly aid the general public. Transparent authentication with strong security and little-to-no interaction, for example, could relieve a burden for users while protecting them and the community. More than ten years ago, Ryan West wrote in "The Psychology of Security" that "The ideal security user experience for most users would be none at all" [37]. Nowhere is this more fitting than with the general public.

IV. Discussion

In this section, we delve deeper into various aspects of invisible security that make it unique and potentially attractive for better cybersecurity.

More than Marketing. In Section II, we described three existing technologies that exemplify the attributes of invisible security. Labeling these approaches as invisible security may or may not increase their adoption, but it distinguishes them from usable security. Giving them a name and categorizing them may also inspire more implementations that deliberately eliminate user interaction. In their 2014 book, Garfinkel and Lipford trace the origins of usable security to 1975 when Saltzer and Schroeder proposed "psychological acceptability" as a key design principle for secure software systems [38]. Invisible security is a distinctly different goal and should be pursued in its own right.

Further research is necessary to more precisely understand which users and communities most desire and accept invisible security. Evidence suggests that a lack of time and knowledge constrain the deployment of cybersecurity generally, as hypothesized about resource-limited small businesses [39]. Research also highlights decision fatigue among users' security experiences and may suggest they are a willing beneficiary of invisible security [40].

Transfer of Trust. Invisible security is built on technology and trust is a keystone. Users of invisible security are outsourcing their security and some decisions to software or a third party, such as their ISP for protective DNS. It will be necessary to create and foster trust in the systems, processes, and providers of invisible security. One reason that users may be reluctant to embrace invisible security is their existing distrust of it. Past negative experiences with an automatic update crashing a computer can leave a lasting impression on users. Trust must also extend to the possibility that invisible security mechanisms are resilient to commandeering by malicious actors.

User trust is tied to the reputation and security of the invisible security providers, who become possible aggregated points of vulnerability and targets of attack. In April 2020, for example, an elevation of privilege vulnerability was discovered in Microsoft AutoUpdate for Mac [41]. Bugs in Microsoft's distribution of automatic updates could erode trust from end users. Trust can be an asset and and a vulnerability.

Public Good. Some instances of invisible security are a public good. In economics, a public good is both non-excludable and non-rivalrous, in that individuals cannot be excluded from use or could benefit from without paying for it, and where use by one consumer does not reduce availability to others, or the good can be used simultaneously by more than one person. Cybersecurity inherently demands effort at some level, and invisible security is not necessarily free (*gratis*) to users or service providers. For example, effort is required from internet service providers to curate and implement protective

DNS for customers. As a result, users might incur a small cost increase. As an analogy, all consumers of telephone service in the United States pay a telecommunications relay surcharge that funds services which allow people with hearing or speech disabilities to place and receive telephone calls. There is no charge to users of the Telecommunications Relay Service.

Other economic models for creating invisible security solutions are also tenable even when financial cost is a barrier. Vendors of operating systems and web browsers have already decided that automatic updates are a valuable feature, even in free software. In commercial software, vendors may see it as a brand differentiation or reputation value. In the future, invisible security could be subsidized or provided by the government, as with protective DNS in the United Kingdom.

Conservation of Time. The practice of cybersecurity requires time, which is a valuable resources that invisible security helps recover for end users. Task completion time is a common metric for usable security. When security tasks disappear, it will be even more necessary to measure the time recovered and its value. Reallocating the conserved time to other purposes also shifts its economic value. Future work is necessary to compare the value of time spend in security tasks to the time spent when security is hands-off.

Economic Benefits. Invisible security offers at least three economic benefits. First, some implementations will offer economies of scale which are achieved when many users adopt a protection that would otherwise be more expensive individually. Protective DNS for all consumers of an ISP share the cost that may be prohibitively expensive for individuals otherwise. Second, invisible security provides outsized benefit to the user. Security measures that distinguish a company from competitors offer a competitive advantage in winning contracts, in addition to the primary benefit of cybersecurity. Third, invisible security offers positive externalities when other users derive benefit from others' use of invisible security. As discussed above, defenses for some cyber attacks emerge from the protection of third parties. Compromised machines and stolen credentials, for example, have a spillover cost and adverse consequences for other online users because hackers will use the victim to attack others. So, when one machine is protected by invisible security, it benefits other users.

Metrics and Measurement. As adoption grows, we will want to know if invisible security is working. That is, measurements are necessary to gauge the degree to which new proposals achieve both security and invisibility. Chief among these measurements is the time spent interacting with the security feature. The traditional goals of cybersecurity are confidentiality, integrity, and availability. In fact, these pursuits are useful only if they support users' primary objectives, such as business goals. For invisible security to be worthwhile, it must be measured against primary outcomes in addition to security outcomes. The success of invisible security should be measured by adoption and by decreased cyber incidents. Unlike usable security, user satisfaction is not particularly relevant since the intent is to eliminate user activity.

V. Conclusions and Future Work

Invisible security is a paradigm for improving defenses against online attacks. If successful, it will lessen the difficulty for those who struggle even with usable security. User-configurable and manual controls will always be available to those who require them, but most users do not.

Making security transparent is not about eliminating user responsibility or limiting their control. Despite the goal of decreased victimization, invisible security will not make users immune and invincible. Automobiles have numerous automatic safety features, but drivers still have to buckle their seat belt and perform regular maintenance. Furthermore, designers of invisible security should respect the appropriate needs and desires for user autonomy where appropriate.

There are limitations of invisible security. People sometimes feel safer when they see security, as has been shown with visible policing [42]. It may be possible to notify users that they have been protected without requiring their intervention; some antivirus products have this feature. Research continues to explore concerns about eroding the mental model when humans are kept out of the decision loop [43]. We can surmise that one reason effort is still placed on users today is that designers may assume that users want control, or that the software might do the "wrong" thing. Further study is necessary. Invisible security will not be appropriate in all situations. Users with special needs or those with sufficient skill may desire greater control. There are also critical systems for which instability or failure are catastrophic, and deliberate control is essential to ensure safety. Thankfully, these special cases are exceptions and beyond the scope of average users.

Future work will expand and improve invisible security. Since there are many sources of security recommendations, these lists offer potential areas that might be developed as invisible protections. Software updates appear on many lists and can already be invisible today. NSA's "Top Ten Cybersecurity Mitigation Strategies" include other recommendations, such as the assignment of privileges based on risk exposure [44]. It is possible that the mitigation may someday be done without user interaction. It is also critical that future work explore the potential for unintended consequences of invisible security so that cybersecurity outcomes are, in fact, improved.

Cybersecurity today is stronger and more usable than ever before. The continued state of poor security adoption and practice—combined with factors of human biology, psychology, and economics—requires consideration for the next evolution of automated, behind-the-scenes cybersecurity. Continued work is necessary to refine the balance of control between human and machine. We look forward to new implementations and outcomes achieved by invisible security.

Acknowledgment

We thank the anonymous reviewers and shepherd, Jay Jeong, for their helpful comments. The views and conclusions expressed in this paper are those of the authors, and do not necessarily represent those of the Department of Defense or U.S. Federal Government.

REFERENCES

[1] L. F. Selznick and C. LaMacchia, "Cybersecurity liability: How technically savvy can we expect small business owners to be," *J. Bus. & Tech. L.*, vol. 13, p. 217, 2017.

[2] T. Duebendorfer and S. Frei, "Why silent updates boost security," *TIK, ETH Zurich, Tech. Rep*, vol. 302, 2009.

[3] R. Wash, E. Rader, K. Vaniea, and M. Rizor, "Out of the loop: How automated software updates cause unintended security consequences," in *10th Symposium On Usable Privacy and Security (SOUPS)*, 2014, pp. 89–104.

[4] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo, "Experimenting at Scale with Google Chrome's SSL Warning," in *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, 2014, pp. 2667–2670.

[5] W. Newhouse, E. McDuffie, C. Paulsen, and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public," *IEEE Security & Privacy*, vol. 10, no. 03, pp. 76–79, May 2012.

[6] J. Dykstra and E. H. Spafford, "The Case for Disappearing Cyber Security," *Commun. ACM*, vol. 61, no. 7, pp. 40–42, 2018.

[7] M. Itoh, T. Horikome, and T. Inagaki, "Effectiveness and driver acceptance of a semi-autonomous forward obstacle collision avoidance system," *Applied Ergonomics*, vol. 44, no. 5, pp. 756 – 763, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0003687013000197

[8] Zahner. (2017, Aug.) Passive security in architecture. [Online]. Available: https://www.azahner.com/blog/passive-security-in-architecture/

[9] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." in *USENIX Security Symposium*, vol. 348, 1999, pp. 169–184.

[10] S. Garfinkel, "Invisible HCI-SEC: Ways of Re-Architecting the Operating System to Increase Usability and Security," in *5th Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: Association for Computing Machinery, 2009. [Online]. Available: https://doi.org/10.1145/1572532.1572593

[11] P. Grahn, "Invisible security," Master's thesis, Lund University, Lund, Sweden, 2015.

[12] G. Bella, "Cybersecurity's way forward: to get beautiful or invisible." in *ICTCS*, 2016, pp. 1–7.

[13] R. W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 55–64, 2017.

[14] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proc. 2009 New Security Paradigms Workshop*, 2009, pp. 133–144.

[15] L. J. Camp and S. Lewis, *Economics of information security*. Springer Science & Business Media, 2006, vol. 12.

[16] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[17] R. Wash, "Folk models of home computer security," in *6th Symposium on Usable Privacy and Security (SOUPS)*, 2010, pp. 1–16.

[18] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior*, vol. 75, pp. 547–559, 2017.

[19] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proc. 2008 New Security Paradigms Workshop*, 2008, pp. 47–58.

[20] J. Atwood. (2005) XP Automatic Update Nagging. [Online]. Available: https://blog.codinghorror.com/xp-automatic-update-nagging/

[21] Z. Bowden. (2019) Windows 10 will no longer auto install feature updates twice a year. [Online]. Available: https://www.windowscentral.com/microsoft-will-no-longer-force-windows-10-feature-updates-users

[22] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *22nd USENIX Security Symposium (USENIX Security 13)*. Washington, D.C.: USENIX Association, Aug. 2013, pp. 257–272. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe

[23] National Cyber Security Centre. (2017) Protective DNS (PDNS). [Online]. Available: https://www.ncsc.gov.uk/information/pdns

[24] K. Leswing. (2016, Apr.) The average iPhone is unlocked 80 times per day. [Online]. Available: https://www.businessinsider.com/the-average-iphone-is-unlocked-80-times-per-day-2016-4

[25] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch Me Once and I Know It's You! Implicit Authentication Based on Touch Screen Patterns," in *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, ser. CHI '12. New York, NY, USA: Association for Computing Machinery, 2012, p. 987–996. [Online]. Available: https://doi.org/10.1145/2207676.2208544

[26] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Computers & Security*, vol. 39, pp. 127–136, 2013.

[27] M. Conti, I. Zachia-Zlatea, and B. Crispo, "Mind How You Answer Me! Transparently Authenticating the User of a Smartphone When Answering or Placing a Call," in *Proc. 6th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 249–259. [Online]. Available: https://doi.org/10.1145/1966913.1966945

[28] N. Clarke, S. Karatzouni, and S. Furnell, "Transparent facial recognition for mobile devices," in *Proc. 7th Int. Info. Security Conf.*, 2008.

[29] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Commun. ACM*, vol. 58, no. 7, p. 78–87, June 2015. [Online]. Available: https://doi.org/10.1145/2699390

[30] R. Spillane, "Keyboard apparatus for personal identification," *IBM Technical Disclosure Bulletin*, vol. 17, p. 3346, 1975.

[31] U.S. Small Business Administration. (2019) United States Small Business Profile. [Online]. Available: https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142719/2019-Small-Business-Profiles-US.pdf

[32] V. Bourne. (2019) Underserved and Unprepared: The State of SMB Cyber Security in 2019. [Online]. Available: http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[33] Deloitte. (2018) Connecting Small Businesses in the US. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-connected-small-businesses-Jan2018.pdf

[34] L. Schencker, "Hospitals' spending lags on digital security," *Chicago Tribune*, Mar. 2019. [Online]. Available: https://digitaledition.chicagotribune.com/tribune/article_popover.aspx?guid=26110cdb-8cb2-4810-ad17-cfab501d08c8

[35] Health Care Industry Cybersecurity Task Force, "Report on improving cybersecurity in the health care industry," 2017. [Online]. Available: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

[36] E. Nakashima and P. Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare ," *The Washington Post*, June 2018. [Online]. Available: https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-subm2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html

[37] R. West, "The psychology of security," *Commun. ACM*, vol. 51, no. 4, pp. 34–40, 2008.

[38] S. Garfinkel and H. R. Lipford, *Usable security: History, themes, and challenges*. Morgan & Claypool Publishers, 2014.

[39] A. Demjaha11, S. Parkin21, and D. Pym, "You've left me no choices: Security economics to inform behaviour intervention support in organizations," in *Proc. 9th International Workshop on Socio-Technical Aspects in Security 2019*, ser. STAST 2019. Springer, 2019.

[40] B. Stanton, M. F. Theofanos, S. Prettyman, and S. Furman, "Security fatigue," *IT Professional*, vol. 18, no. 05, pp. 26–32, Sept. 2016.

[41] Microsoft. (2020, Apr.) CVE-2020-0984 — Microsoft (MAU) Office Elevation of Privilege Vulnerability. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0984

[42] A. Crawford, "Reassurance policing: feeling is believing," in *Transformations of policing*. Routledge, 2017, pp. 157–182.

[43] P. Rajivan, E. Aharonov-Majar, and C. Gonzalez, "Update now or later? Effects of experience, cost, and risk preference on update decisions," *Journal of Cybersecurity*, vol. 6, no. 1, Mar. 2020.

[44] National Security Agency. (2018) NSA's Top Ten Cybersecurity Mitigation Strategies. [Online]. Available: https://media.defense.gov/2019/Jul/16/2002158046/-1/-1/0/NSA