

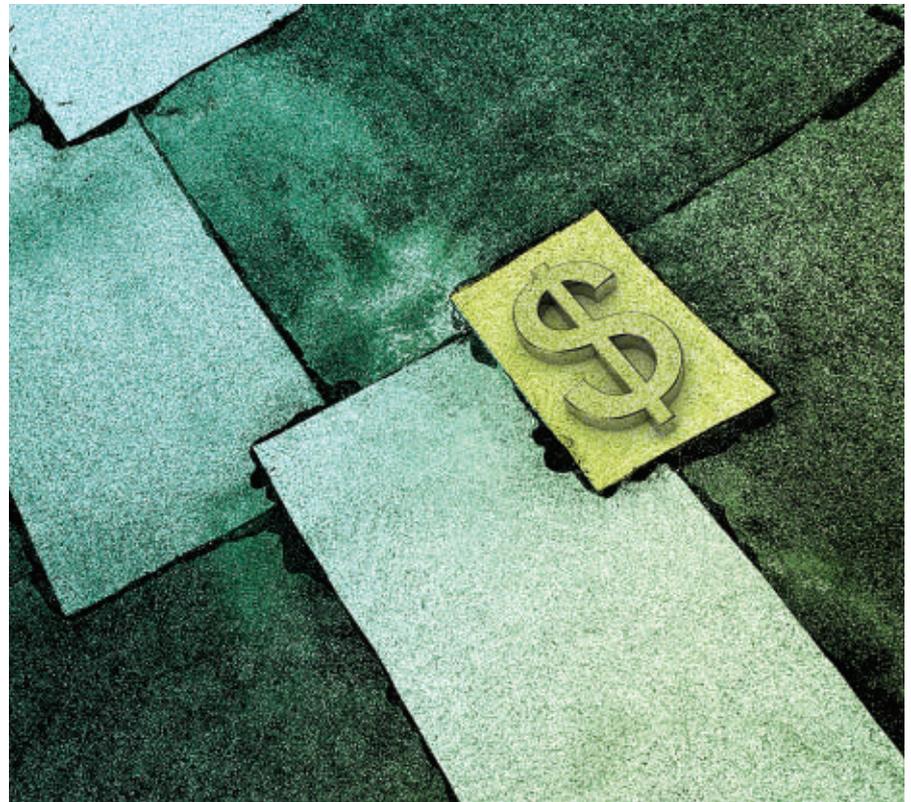
Viewpoint

Designing User Incentives for Cybersecurity

How to encourage better user security practices and behavior.

THE TRADITIONAL “PATCHING” approach to managing software vulnerabilities and cybersecurity risk has been less effective than desired. In theory, once a vulnerability is discovered, software patches should be quickly developed and released by producers and then expeditiously applied by users. Successful completion of this process would help to maintain secure systems. However, what has been consistently observed in practice is that this process instead breaks down.⁷ Of particular concern is the failure of the current approach to adequately address the economic incentives that underlie users’ decisions to patch their systems. We propose a simple adaptation to software producer offerings (“versions”) involving users’ patching rights and argue why this change would make a patching approach more effective.

In particular, we advocate that users should be charged for the *right* to control patching of their own individual copies of software. That is, a user’s ability to choose whether to install patches should no longer be an implicit right. Rather, a user who prefers to retain the ability to choose whether and when to patch would need to pay a certain price; one can think of this fee as the price to cause additional security risk (perhaps temporarily) which has negative consequences on other users and the software producer. A user who chooses



to forgo this right, and not pay the premium, has his or her system automatically updated with security patches as soon as they are released. Framed differently, a user can choose whether to purchase a “discounted,” default version that is automatically updated or a “premium” version that includes the right to patch at one’s convenience or even not at all.

Although on the surface this prescription is simple, the design of an incentives-based approach to improve cybersecurity is a difficult task because the level of risk that realizes on a given system or network is a complex outcome of the behaviors of many stakeholders: government, critical infrastructure providers, technology producers, malicious (“black hat”) hack-

ers, and users. With regard to users, how has the current approach failed? For more than 40 years, malware has posed a significant challenge to cybersecurity. The commercialization of the Internet in the 1990s exacerbated this situation tremendously as millions of users began connecting vulnerable devices to networks. Today, the situation is even more problematic. It is common to find an end user with a desktop computer, laptop, tablet, and smartphone running both system software and applications that are not secure. The problem is not limited to companies like Microsoft, who has released on the order of hundreds of security updates to its Windows 7 operating system. There are already one billion smartphones in the U.S. and this number is expected to double by 2015.¹² Many of these devices are running the Android operating system that is being modified by the carriers. These devices are so insecure the American Civil Liberties Union (ACLU) has filed a complaint with the Federal Trade Commission (FTC) requesting action be taken to require vendors to provide more frequent and timely updates to their systems.¹¹

But a patching approach to mitigate cybersecurity risk will only work if users actually apply the patches. Historically, many users have lacked sufficient incentives to properly maintain computing systems by applying these patches. As an example, Code Red is notorious malware that attacked instances of Microsoft's Internet Information Services (IIS) Web server software by exploiting a particular vulnerability. Microsoft had developed a security patch for this vulnerability and released it approximately three weeks before Code Red erupted. Yet, even with the technical fix being made publicly available, most users failed to patch their installations in time, and nearly 360,000 servers were struck by the worm.⁷ Code Red is not an exception. Similar patching windows existed in the cases of other high-profile attacks by SQL Slammer, Blaster, and Sasser. To effectively address the security problem, one must understand how to incentivize improved user behavior.

Users are heterogeneous in the total value they derive from deploying and protecting a system running a given

A patching approach to mitigate cybersecurity risk will only work if users actually apply the patches.

software product. For example, one can consider the differences between two users of enterprise application software: an organization that highly values a system enabled by the software and an organization that values the software just enough to purchase it. A prudent approach to patching involves costly activities including testing, staging, and a controlled roll-out of patches to production systems. Because of the higher value the former organization derives from the software (for example, perhaps the software supports an e-commerce website), it also possesses stronger economic incentives to incur these patching costs and protect its systems. In contrast, the organization that derives less value has much weaker incentives. Not only would such an organization likely not allocate resources to follow the extensive patching process described earlier, even potential inconvenience costs associated with a patch failure may sway it to not deploy patches in a cursory manner either. Although the example with two types of users described here is informative, in reality, there is a continuum of users varying in their patching preferences. But, the point remains: some users tend to have less incentive to patch while other users who utilize software for mission-critical purposes have stronger incentives to patch and protect their systems at the expense of time and resources.

Unfortunately, cybersecurity risk is characterized by detrimental network externalities. That is, when users behave insecurely on a network, they increase the risk faced by everyone else connected to the network.^{1,2} Nevertheless, users in the segment who choose not to patch can still be targeted by eco-

nommic incentives that align their protection decisions more closely with the objective of keeping systems secure. The approach we propose is for software producers to version their products based on users' patching rights. One can logically reason through how this approach would affect different types of users. Organizations and other high-value users will opt for premium versions and pay for the right to patch according to their own timeframes, thereby causing additional security risk on others while remaining unpatched. However, because of their inherent incentives for patching, most of these users will indeed patch at the end of their internal, systematic processes. For users who value the software enough to use it but not enough to protect their systems, they will now be forced to decide whether the right to remain unpatched in a network environment is worth paying the price. Because they may likely belong to the more price-sensitive segment, many of them will prefer not to pay the premium and instead have their systems automatically updated.

Considering that people make daily decisions on whether to install security updates for operating systems, Web browsers, productivity tools, antivirus software, and a long list of other application software, the impact of well-crafted incentives that target user behavior can be quite substantial. Will some consumers prefer discounted versions of popular products like Microsoft Windows and Microsoft Office that automatically update, no longer include the right to be unpatched, and remove the hassle of deploying patches? The answer is likely "yes," and if such a versioning strategy can convert a sizable percentage of unprotected systems from the status quo, then cybersecurity can improve considerably.

Given all of the stakeholders involved, our recommended approach to version based on patching rights also faces counterarguments. Users may contend they should be endowed with the right to choose whether to patch. By not having this right, they would be forced to incur inconvenience costs associated with loss of control, system rebooting, and even system instability due to poorly designed patches. These concerns are valid and underscored by

the not-so-distant memories of Windows XP Service Pack 2. However, we argue the social concern should tilt in favor of improved security. In fact, similar trade-offs exist in other settings where it is common for “users” of products and services to be required to protect others’ interests. For example, most states require that children be immunized before being permitted to attend school. Similarly, many states have requirements that vehicle owners regularly have their vehicles inspected and possibly corrected to meet emission standards. In our case, we are advocating an even milder approach. Users may always retain the ability to choose whether to patch—mandates are not necessary. What is important is that users internalize the cost of causing greater security risk as is reflected through a higher price for retaining patching rights.

Software producers may push back on our recommended approach because they will either lose customers at the low end due to these inconvenience costs or be forced to cut prices to keep them as paying users. While this may be true, producers may also

find versioning on patching rights to be beneficial for several reasons. First, organizations and other high end users will derive greater value from more secure software. If the unpatched population shrinks considerably, these organizations will bear less security risk during the time it takes them to undergo their patching processes. For this lower risk, software vendors can charge a higher price that helps make up for revenue losses associated with the user segment that forgoes patching rights. Second, the often employed argument by software producers that they should not be held liable for security vulnerabilities because they make patches available is somewhat fragile if patches are not being applied.⁵ By providing better economic incentives such that the patching approach they subscribe to actually leads to more secure outcomes, software producers can strengthen their arguments against governmental intervention through means such as liability. There is an opportunity for future research to formally examine these trade-offs using economic models of the decision problem faced by software producers;

such research can yield useful and important insights.

One noteworthy risk of our approach concerns the reaction of black hat hackers. Like other economic agents, black hats have typically found it more cost effective to reverse engineer security patches and develop attacks to exploit the vulnerabilities these patches aim to fix. In this sense, black hats are leveraging the fact that users’ lack of incentives to deploy patches leads to large exploitable populations. Our recommended approach would likely force black hats to redirect their efforts toward other endeavors such as finding unknown vulnerabilities and exploiting them with zero-day attacks. What is important to note is that by their revealed attack preferences, these endeavors appear to be costlier for the same economic return on effort. Hence, the extent of their efforts may be partially reduced. Nevertheless, zero-day attacks can cause considerable economic losses. In anticipation of how black hats respond, both organizations and end users will necessarily need to adjust their defense-in-depth strategies such



Your next job is waiting.

Many of today’s senior tech jobs go unfilled as candidates lack the advanced skills and training needed. Demonstrate your commitment to get ahead and earn CEUs by completing non-credit courses from **Georgia Tech’s Master of Science in Computer Science** online program.

Each course is just \$399.

For more information or to register, visit
pe.gatech.edu/omscs-acm

ACM
Transactions on
Reconfigurable
Technology and
Systems

ACM Transactions on Reconfigurable Technology and Systems

SPECIAL EDITION ON THE 15TH INTERNATIONAL SYMPOSIUM ON FPGAs

Articles 1-10 pages: M. Beaulieu, M. Loh, Introduction

Articles 11-15 pages: M. Beaulieu, M. Loh, Sparse Bitstream

Articles 16-20 pages: T. M. Shiple, M. J. Heule, Substitution of Static Data Patterns in FPGAs using Multiple Configurations

Articles 21-25 pages: S. Ghosh, S. Ghosh, Hardware Analysis and Programmatic Access Modeling and New Algorithms for FPGAs

Articles 26-30 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 31-35 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 36-40 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 41-45 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 46-50 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 51-55 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 56-60 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 61-65 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 66-70 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 71-75 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 76-80 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 81-85 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 86-90 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 91-95 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 96-100 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 101-105 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 106-110 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 111-115 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 116-120 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 121-125 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 126-130 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 131-135 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 136-140 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 141-145 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 146-150 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 151-155 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 156-160 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 161-165 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 166-170 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 171-175 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 176-180 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 181-185 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 186-190 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 191-195 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 196-200 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 201-205 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 206-210 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 211-215 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 216-220 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 221-225 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 226-230 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 231-235 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 236-240 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 241-245 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 246-250 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 251-255 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 256-260 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 261-265 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 266-270 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 271-275 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 276-280 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 281-285 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 286-290 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 291-295 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 296-300 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 301-305 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 306-310 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 311-315 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 316-320 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 321-325 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 326-330 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 331-335 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 336-340 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 341-345 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 346-350 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 351-355 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 356-360 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 361-365 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 366-370 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 371-375 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 376-380 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 381-385 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 386-390 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 391-395 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 396-400 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 401-405 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 406-410 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 411-415 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 416-420 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 421-425 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 426-430 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 431-435 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 436-440 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 441-445 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 446-450 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 451-455 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 456-460 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 461-465 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 466-470 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 471-475 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 476-480 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 481-485 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 486-490 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 491-495 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 496-500 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 501-505 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 506-510 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 511-515 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 516-520 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 521-525 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 526-530 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 531-535 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 536-540 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 541-545 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 546-550 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 551-555 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 556-560 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 561-565 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 566-570 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 571-575 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 576-580 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 581-585 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 586-590 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 591-595 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 596-600 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 601-605 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 606-610 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 611-615 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 616-620 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 621-625 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 626-630 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 631-635 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 636-640 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 641-645 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 646-650 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 651-655 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 656-660 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 661-665 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 666-670 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 671-675 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 676-680 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 681-685 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 686-690 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 691-695 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 696-700 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 701-705 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 706-710 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 711-715 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 716-720 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 721-725 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 726-730 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 731-735 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 736-740 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 741-745 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 746-750 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 751-755 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 756-760 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 761-765 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 766-770 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 771-775 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 776-780 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 781-785 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 786-790 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 791-795 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 796-800 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 801-805 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 806-810 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 811-815 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 816-820 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 821-825 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 826-830 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 831-835 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 836-840 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 841-845 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 846-850 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 851-855 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 856-860 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 861-865 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 866-870 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 871-875 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 876-880 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 881-885 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 886-890 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 891-895 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 896-900 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 901-905 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 906-910 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 911-915 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 916-920 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 921-925 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 926-930 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 931-935 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 936-940 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 941-945 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 946-950 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 951-955 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 956-960 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 961-965 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 966-970 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 971-975 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 976-980 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 981-985 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 986-990 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 991-995 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

Articles 996-1000 pages: S. Ghosh, S. Ghosh, Achieving Compactness with a Reconfigurable Network

www.acm.org/trets
www.acm.org/subscribe

acm Association for Computing Machinery

that the economic gains from a world with versioning on patching rights are not overshadowed by losses in the “equilibrium” state that arises. More research studies that endogenize black hat behavior can help to better predict the actual outcomes.

The U.S. government would likely be a strong advocate of the approach we outline. Several federal agencies including the National Science Foundation (NSF) have recognized that innovative policies are needed to help reduce security risks currently faced by the U.S.^{4,8} Along with President Obama’s executive order to develop a cybersecurity framework, the Department of Commerce was also directed to determine what types of economic incentives will cost-efficiently help facilitate adoption of the framework and whether additional legislation may be required.⁹ The government seems to implicitly favor a *voluntary* approach toward improving cybersecurity. For example, whether software producers should be held liable for the economic losses incurred by their users due to poor security has been heavily debated over the last decade, but with little legislative action taken by the government.^{6,10} In spirit, the idea is that holding a company like Microsoft liable will ultimately hurt its bottom line and thus finally provide incentives for greater investments in making its products more secure. This outcome may indeed be the case. But, other undesirable outcomes can certainly arise instead. In particular, Microsoft may make strategic choices to limit its liability. One way to do so is to serve fewer users because a smaller network of users corresponds to reduced security risk due to the network externality. Specifically, all software users benefit in terms of security when there are fewer users exhibiting insecure behaviors, such as not protecting their individual systems. Under a liability policy, Microsoft would, in turn, benefit by not paying out as much to cover users’ losses. If this latter effect of a liability policy is strong, Microsoft may in fact reduce its investments and/or raise its prices to achieve a smaller user population.³

Instead, an approach where software producers begin versioning their products based on patching rights

seems to strike a balance across the interests of government, software producers, and users. Unlike government-imposed liability, this approach is more consistent with how the government has thus far attempted to nudge stakeholders toward better cybersecurity outcomes. Furthermore, targeting user incentives to protect their machines can be a more direct and effective approach in comparison to liability schemes that software producers would prefer to avoid. In fact, if producers are able to charge higher prices from users who appreciate the increased security and it thereby leads to increased producer profitability, there is the potential for win/win outcomes that also substantially improve the economic value associated with software to society. **C**

References

- Anderson, R. and Moore, T. The economics of information security. *Science* 314, (2006), 610–613.
- August, T. and Tunca, T. Network software security and user incentives. *Management Science* 52 (2006), 1703–1720.
- August, T. and Tunca, T. Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science* 57 (2011), 934–959.
- Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (2011); <http://www.defense.gov/news/d20110714cyber.pdf>.
- Espinosa, T. EC wants software makers held liable for code. ZDNet (2009).
- Heckman, C. Two views on security software liability: Using the right legal tools. *IEEE Security & Privacy* 1, (2003), 73–75.
- Moore, D., Shannon, C., and Brown, J. Code-Red: A case study on the spread and victims of an Internet worm. In *Proceedings of the ACM SIGCOMM/USENIX Internet Measurement Workshop* (2002), 273–284.
- National Science Foundation. *Secure and Trustworthy Cyberspace (SaTC) Program Solicitation NSF 12-596* (2012); www.nsf.gov/pubs/2012/nsf12596/nsf12596.pdf.
- Obama, B. Executive Order—Improving Critical Infrastructure Cybersecurity. The White House, Office of the Press Secretary, Washington, D.C., 2013.
- Ryan, D. Two views on security software liability: Let the legal system decide. *IEEE Security & Privacy* 1, (2003), 70–72.
- Satter, R. ACLU: Slow smartphone updates are privacy threat. Associated Press (2013).
- Yang, J. Smartphones in use surpass 1 billion, will double by 2015. Bloomberg (2012).

Terrence August (taugust@ucsd.edu) is an associate professor in the Rady School of Management at the University of California, San Diego and a visiting Ijjin Professor at the Korea University Business School, Seoul, Korea.

Robert August (augur@lake.ollusa.edu) is an associate professor emeritus in the School of Business and Leadership at Our Lady of the Lake University, San Antonio, TX.

Hyoduk Shin (hdshin@ucsd.edu) is an assistant professor in the Rady School of Management at the University of California, San Diego.

This Viewpoint is based upon work supported by the National Science Foundation under Grant No. CNS-0954234.

Copyright held by authors.

Copyright of Communications of the ACM is the property of Association for Computing Machinery and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.