Papering Over the Cracks: The Effects of Introducing Best Practices on the Web Security Ecosystem

Emil Larsson
Schibsted Media Group
Stockholm, Sweden
emil.larsson@schibsted.se

Johan Sigholm
Department of Military Studies
Swedish Defence University
Stockholm, Sweden
johan.sigholm@fhs.se

***Abstract*—Hypertext Transfer Protocol Secure (HTTPS) is the de facto standard for secure end-to-end web communication. However, numerous flaws discovered during recent years, such as Apple's "goto fail" bug, and cryptographic weaknesses as illustrated by the Poodlebleed vulnerability, have brought the efficiency of the mostly self-regulated web security market into question. In this cross-disciplinary paper, the authors survey some 160.000 HTTPS-enabled servers among popular web sites over a time period of three years. The research question is what effect the introduction of best practices and vulnerability publication have on web server security in the form of protocol support. Main findings include that (i) insecure configurations, although well known, can remain widespread for over a decade, (ii) the introduction of best practices affect the decline of insecure configurations only moderately, whereas highly publicized security flaws have a significant impact, and (iii) economic incentives for website owners to provide secure services are weak, motivating such other levers of influence as legislation or blocking of noncompliant sites.**

Keywords—Internet governance; network security; security economics; HTTPS

I. Introduction

Emerging Internet based economic systems are growing rapidly, both as a share of the global economy and when considering the innovation and diversity of online economic activity. Nevertheless, a number of studies have identified lack of trust and security concerns as main constraints on e-commerce growth, particularly in terms of consumer protection. As economic gain is also one of the prime motivators for cybercrime, safeguarding the products and services used for web transactions against antagonistic attacks is naturally of high importance for involved actors.

According to Symantec's 2015 Internet Security Threat Report [1], a current trend is attacks against the "Internet of Things," including such network connected devices as Point of Sales equipment, network routers and wireless access points. Although these systems may not contain sensitive information themselves, they commonly carry network traffic that may be intercepted. Another cause for concern is the growing use of smartphones, smartwatches and embedded systems integrated into our TVs, cars and personal health equipment, uplinked to cloud-based services [2]. End users generally have a poor understanding of what privileges they have granted their installed apps, and that their personal information, contacts, login names, and passwords are often sent over the network in plaintext, or with an unknown security configuration at best.

Flaws in the employed security protocols may be exploited by various actors, ranging from hacktivists to organized cyber criminals [3], but also by nation-backed hackers and intelligence services [4]. All in all, attacks on cyber infrastructure generate costs to the global economy in the hundreds of billions on a yearly basis [5]. The costs may be direct, e.g. through theft of information or financial resources, but they may also be indirect, such as loss of productivity or by requiring expensive risk mitigating products or services.

In spite of this, the costs associated with insecurity in cyber technology seldom affect the central stakeholders, such as the actors responsible for making decisions on what security protocols to employ. Customers also rarely have the option to "vote with their wallet" and thus favor secure products and services, due to challenges in determining the level of security, as well as vendor lock-in effects and de-facto monopolies generated by large commercial services. These effects result in low or no incentives for the responsible stakeholders to employ secure protocols. On the contrary, compatibility with legacy software and upgrade costs reward retaining old protocols even though they suffer from known vulnerabilities.

In order to uphold the confidentiality and integrity of web communications it is essential that connections are encrypted, and that the identity of the communicating parties can be ascertained. Hypertext Transfer Protocol Secure (HTTPS) is the de facto standard for establishing such secure end-to-end web sessions. It is not a protocol per se, but rather a result of layering the Hypertext Transfer Protocol (HTTP) on top of various versions of the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. Additionally, digital certificates based on the ITU X.509 standard are used to guarantee that the communicating parties on a channel are the ones they claim to be.

Almost immediately upon the 1995 release of the first version of HTTPS, based on SSL version 2, severe security issues were identified [6]. As a consequence, SSL version 3 was introduced in 1996, demonstrating the need for rapid protocol transition. However, this process was left to market

978-1-5090-1724-9/16/$31.00 ©2016 IEEE

forces, and after three more major protocol revisions during two decades, self-regulation had not yet sufficed to engender a full transition. In 2008 the Internet Engineering Task Force (IETF) thus published a recommendation on the discontinued use of SSL version 2, introducing cross-market best practices in an effort to speed up protocol conformity. In 2011 this recommendation was strengthened to a ban [7]. A remaining question is whether best practices are enough to reach an acceptable level of web security, or if other means are required. Although several serious flaws in the underlying authentication and encryption protocols of HTTPS have been discovered and gained wide media exposure, collected data shows that a significant portion of the most popular websites worldwide still support remarkably insecure configurations.

Some of the most highly publicized HTTPS security incidents during the past few years include the Comodo and DigiNotar [8] man-in-the-middle attacks targeting weaknesses in the digital certificate model, and rather trivial application programming mistakes, albeit with serious consequences, such as in the Apple "goto fail" bug [9] and the Heartbleed bug [10] in OpenSSL. We have also seen attacks targeting cryptographic weaknesses, such as the Poodlebleed vulnerability [11], and documents leaked by former NSA contractor Edward Snowden [12] have further confirmed that HTTPS is a prioritized target for government-backed cyber operations. While exploiting flaws in web security may be useful addition to the offensive cyber operation toolbox, employing such methods, especially if they involve compromising critical cyber security technologies, risks having detrimental effects on the level of global cyber security and to be ethically questionable [13].

Analysis of the rate of decay of old and insecure protocols in the most popular websites worldwide, along with adoption rates of new protocols, is of the essence. If they reveal that the web security ecosystem reacts very slowly, it would certainly generate negative externalities – unexpected consequences of an activity, affecting people external to the activity [14]. In the case of insecure web communications, negative externalities are caused by service providers commonly only taking into consideration what security costs them (such as the costs of upgrading servers) and overlooking the total costs of insecure products and services. A significant part of the costs must thus be borne by external parties, such as end users or society. Central questions are thus how responsible the commercial actors are, and if they can be made to take into account the side effects they generate, so that these may be reduced.

In this cross-disciplinary article we make use of engineering and economics methods to analyze the web security ecosystem. We study the effects of market intervention via best practices using numerical analysis, and investigate the responsibilities, incentives and actions of the central stakeholders, and their relationship network. Finally, we analyze the technical circumstances of the HTTPS rollout.

The rest of the article is structured as follows; Section 2 gives a background to the HTTPS ecosystem. Section 3 describes the central case study, presents the collected data, and models some behaviors of adoption of secure and decay of insecure configurations. Section 4 discusses the results, and Section 5 offers some implications and suggests ways forward.

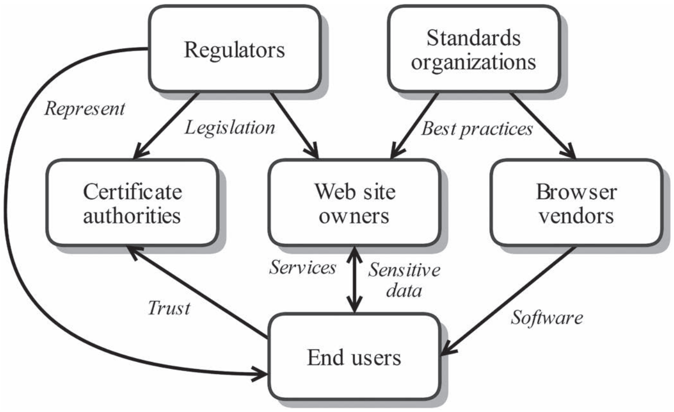

Fig. 1. Actors and relationships in the web security ecosystem.

II. The HTTPS Ecosystem

A. Background

The actors of the HTTPS ecosystem were essentially set in 1996 and have been unchanged to date. The introduction of TLS to replace SSL as the preferred method of encrypting web traffic occurred in January of 1999. The possibility to offer only secure configurations – at the cost of client compatibility – has thus been available for nearly two decades.

In 2011 the IETF confirmed the status of SSL 3.0 as "Historic" [15], and on October 15, 2014 a critical vulnerability dubbed "Poodlebleed" [11] was discovered, sounding the death knell of SSL 3.0 security. Poodlebleed relies upon the ability of an attacker to force version downgrades by garbling or interrupting packets, typically by acting from the position of man-in-the-middle. State actors have been known to prepare themselves to take such a position [16]. If the client and server agree to version downgrades, the attacker can thus cause communication to use the lowest common denominator – a so-called rollback attack. However, the Poodlebleed vulnerability cannot be used against correctly implemented TLS due to the requirement that padding bytes have a specific, predetermined value. It thus seems clear that introduction of newer and more secure protocol versions for web communication is not enough. Old ones must be deprecated and removed in a timely fashion, in order to prevent the exposure of sensitive communications.

Nevertheless, the current methodology preferred by the various actors in the HTTPS ecosystem is to preserve backwards compatibility, almost indefinitely. "Secure by default" has been considered to be secure enough, and the risk of cracking open security using rollback attacks has mostly been ignored.

B. Actors and relationships

The central actors within the HTTPS ecosystem were categorized by Arnbak et al. [17], describing four principal categories; web-site owners, web-browser vendors, certificate authorities and end users. To widen the analysis, we propose to include standards organizations and regulators as additional actors in the web security ecosystem, shown in Fig. 1.

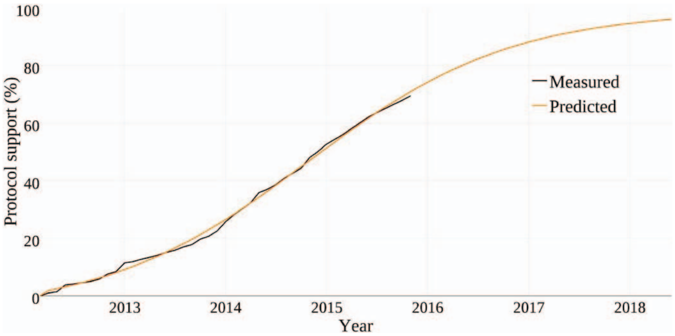

Fig. 2. TLS protocol adoption.

Web Site Owners: The owners and operators of web sites are in control of what security protocols and mechanisms are available to clients. Although the user is made aware that a connection with the server is secure (commonly illustrated by a padlock in the web browser) a connection using outdated protocols appears similar to that of an implementation using state of the art protocols. It was not until quite recently that large web services such as Google and Facebook started supporting secure web connections by default. The reason for this was likely not only the care for end users' sensitive data, but perhaps rather the fact that encryption costs processing power, resulting in increased server power consumption and slower connection establishment times. Connections over HTTPS may also prevent third party advertisements or the collection of user statistics. Security design decisions have thus been heavily influenced by factors other than best practices. In the case of Gmail, HTTPS was enabled as the default setting one day after it was revealed that accounts had been compromised in a series of Chinese cyber-attacks dubbed "Operation Aurora" [18].

Certificate Authorities: In order to establish a secure web session through SSL or TLS, a mechanism is required to let the web server prove its identity to the client. This is achieved through the exchange of digital certificates based on the ITU X.509 standard, which vouch for the ownership of a public key by the named subject of the certificate. Such certificates are issued and sold by Certificate Authorities (CAs). Security vulnerabilities in the HTTPS authentication model are discussed in depth by Arnbak et al. [17]

Browser Vendors: The companies that create web browsers play a key role in the HTTPS ecosystem. Like the web site operators they have the option to avoid or ban the use of certain protocols. They can also affect the end user by providing various messages intended to inform the users of web sites that have poor or insecure configurations. Although most users tend to ignore such warnings [19], web site owners may prefer to have their site "warning free" and thus take action to conform to higher security standards.

End Users: As much of the communication performed through web services can be categorized as sensitive, ranging from patient records to financial transactions, end users have a large stake in the security of the HTTPS ecosystem. Nevertheless, they are largely dependent on security design decisions made by other actors, having limited influence over the risks that their information is exposed to, and thus ultimately suffering from the resulting negative externalities.

Standards Organizations: The main standards organization concerned with regulating HTTP security is the Internet Engineering Task Force (IETF). Rather than being an organization in the traditional sense, the IETF is an activity or task force of the Internet Society, and relies entirely upon volunteers for all work [20]. Since 1986, the IETF has published a large numbers of Internet Standards using the Request For Comment (RFC) system, whereby drafts are publicly revised for an extended length of time. RFCs serve both to define many core Internet protocols and to provide community best practices. Certain commercial organizations, such as Cisco and Microsoft, also publish configuration guides and other best recommendations. Generally speaking, such publications serve as guidelines – but failure to adhere closely to them will virtually guarantee insecure configuration.

Regulators: Centralized legislation for the Internet as a whole is a problem on a gargantuan scale. Although each country attempts to regulate its users and enterprises, only a few actors have the potential to make a significant difference. The European Union provides central regulation of the Internet through the office of the High Representative of the Union for Foreign Affairs and Security Policy. This office is currently developing legislation to improve end-user security. In the United States, a similar role is filled by the "Cyber Czar", the White House cyber security coordinator.

C. Regulatory Background and Future

As seen in our lineup of actors and relationships, the cost of security is ultimately borne by society as each individual uses web technology. In a well-functioning market it seems likely that users would exercise their economic power to compel browser vendors and server operators to implement secure and up-to-date solutions. However, in practice this is not the case. A central concept in understanding any closed market such as the commercial HTTPS ecosystem is that of the externality [14]. When an externality is present there is a divergence between private cost and social cost – the market is unable to internalize certain costs or interactions. A common example of negative externalities is when pollution is discharged into a river, without cost to the polluter, while actors downstream must clean the water before it can be used, resulting in inefficient use of resources and the reduction of real wealth.

The field of Information Security is generally full of externalities, often caused by commercial actors who strive to be as profitable as possible by balancing the costs of more secure software (extra developers, fewer features, longer time to market) against the costs of insecure software (expense to patch, occasional bad press, potential loss of sales) [21]. Addressing such externalities, i.e. by forcing the cost into the market, can be done via outright legislation or via the establishment of new markets, like those created for greenhouse emissions. As end users have little direct influence upon server operators, and even less understanding of the collateral cost they are made to bear as a result of security deficiencies, we consider the transport layer security deficiency cost to be an externality to the closed, commercial HTTPS ecosystem.

A fundamental problem of regulation and legislative solutions is that they require consequences to be relevant. The Internet, however, is based on voluntary adherence to de facto standards and best practices. As the standards organizations have no mandate for punitive action, adherence is left to the free market. The 2013 Cybersecurity Strategy of the European Union [22] does contain "a proposal for legislation to [...] improve preparedness and engagement [...]. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors." It seems clear that the private sector has well developed cyber resilience capabilities outlined in best practices. The missing component is measures of enforcement – and the strategy does not contain forceful measures to rectify this shortcoming.

III. Case study: HTTPS adoption and decay

In order to understand the timeframes involved in adopting a new security protocol, as well as the external events impacting the adoption rate, real-world measurements must be taken, modeled and contrasted with known security disclosures and introductions of best practices. We propose that the various HTTPS protocols are suitable for such a case study, particularly TLS v1.2 for which full-lifecycle statistics are available, can be used to model protocol adoption.

A. Method

The SSL Pulse project [23] was started in April 2012 and collects statistical data to quantify the quality of SSL support, based on some 160.000 HTTPS-supporting web sites in the top one million most popular websites in the world. We utilize this data to understand the uptake of available web security protocols, and numerically analyze the rates of adoption and decay. The data includes the most recent TLS version, 1.2, currently under adoption, as well as the highly outdated SSL v2.0, still in decline. We also observe the transition from de facto standard to decay of SSL v3.0 following the highly publicized Poodlebleed vulnerability of October, 2014.

B. Modeling the Adoption of TLS v1.2

The TLS v1.2 protocol was standardized in August 2008 but first came into mainstream use in February 2012 when OpenSSL v1.0 was released, providing server side support. Most popular web browsers also started implementing it at this time. To understand what factors drive transition and whether specific events can accelerate it, it is useful to have a model of the uptake of this protocol. Adoption of new technologies typically follows an S- or sigmoid-shaped curve [24].

As previously shown [25], the adoption of TLS v1.2 can be accurately modeled by the function:

$$y = \frac{a}{1 + e^{-\frac{t-b}{c}}} + d \tag{1}$$

Using the newly fit coefficients a = 104.5821, b = 31.8343, c = 12.0790, d = -5.6651, the model describes adoption data, presented in Table 1, as a function of time t in months up to and including November 2015 with a low root-mean-square residual error of 1.007. Fig. 2 shows the measured data along with the model, and predicts that the protocol becomes near-ubiquitous in late 2017.

TABLE I. Observed adoption rates of TLS v1.2

Survey month	***Adoption rate***	***Survey month (cont.)***	***Adoption rate (cont.)***	***(cont.)***	***(cont.)***
2012-04	1.0 %	2013-07	15.8 %	2014-10	44.3 %
2012-05	1.4 %	2013-08	17.0 %	2014-11	48.1 %
2012-06	3.8 %	2013-09	17.8 %	2014-12	50.1 %
2012-07	4.1 %	2013-10	19.7 %	2015-01	52.7 %
2012-08	4.5 %	2013-11	20.7 %	2015-02	54.5 %
2012-09	5.0 %	2013-12	22.5 %	2015-03	56.0 %
2012-10	5.8 %	2014-01	25.7 %	2015-04	58.1 %
2012-11	7.6 %	2014-02	28.2 %	2015-05	60.0 %
2012-12	8.4 %	2014-03	30.2 %	2015-06	62.1 %
2013-01	11.4 %	2014-04	32.3 %	2015-07	63.6 %
2013-02	11.9 %	2014-05	35.8 %	2015-08	65.1 %
2013-03	12.7 %	2014-06	37.0 %	2015-09	66.5 %
2013-04	13.4 %	2014-07	38.5 %	2015-10	67.9 %
2013-05	14.1 %	2014-08	40.8 %	2015-11	69.5 %
2013-06	15.1 %	2014-09	42.6 %		

C. Decay of SSL v2.0

Although superseded in 1996, SSL v2.0 is still available for negotiation by tens of thousands of popular websites worldwide. This lingering support is unlikely to be caused by abandoned or misconfigured servers, but rather shows proof of knowing disregard of best practices. Considering all public HTTPS servers globally, including abandoned ones, SSL v2.0 support is likely even higher.

The decay of SSL v2.0 in the measured three-year period from April 2012 to April 2015 has been mostly linear and averages 0.55 % per month. The discovery of the Heartbleed bug had a limited effect on the decay, and despite the protocol being explicitly banned by best practices, it is still supported by some 10 % of sampled SSL servers.

D. Decay of SSL v3.0

Long considered the lowest common denominator of HTTPS, recent years have seen more and more care necessary to securely configure SSL v3.0. However, up until the discovery of the Poodlebleed vulnerability, it had been ubiquitous as a fallback option from TLS, with more than 98 % of servers supporting negotiation of that standard. This number, although high, represents the beginning of a slow decline from near-universal support. Immediately after Poodlebleed, the share dropped very significantly by more than a third, as seen in Table 2 and Fig. 3. We note that years of obsolescence and best practice recommendations against the use of SSL v3.0 did nothing to convince this group of operators, whereas a highly publicized security vulnerability had an immediate impact. In

Fig. 3 we project the continued support for the historic and insecure SSL v3.0 protocol in two scenarios. The more rapid decline is based upon the average of the immediate post-Poodlebleed development. The slower decline is based upon our measurement of the average decline of SSL v2.0.

IV. Discussion

A significant problem in the procurement of systems is information asymmetry. Web site owners, much like any other traders in a market, are only ready to pay for quality that they can measure [26]. The level of security of a system or its software components is generally very difficult to ascertain, with local customizations which require site-specific penetration testing being the norm. When security cannot be sufficiently determined beforehand, vendors have strong incentives to claim their systems and software is secure. The buyer, unable to verify this claim, will pay as much for actually-secure products as for insecure ones, driving vendors who invest into security out of the market.

The cost of shortcomings in web security, as a result of data theft, loss of privacy or the cost of investment in additional security solutions, must often be borne by end users or society as a whole. Whereas browser vendors appear to represent the market entity with interests closest aligned to those of the end user, web site owners commonly have limited incentives to go the extra mile for enhanced end user security, granted that they can refrain from doing so. As seen in the presented data, this actor category is also disinclined to adhere to market best practices in the same rapid manner as may be seen among browser vendors. Only discovery of major vulnerabilities, threatening the security of own infrastructure generates a rapid reaction (as for instance seen after the Poodlebleed vulnerability disclosure).

To some degree this is understandable, at least in a historical perspective. Costs inferred by server power consumption and slower connection establishment times have previously been significant, especially when transitioning from unencrypted HTTP to HTTPS. Moreover, the fact that HTTPS sessions may prevent third party advertisements or the collection of user statistics has additionally impeded the rollout of secure web protocols in popular, high-volume sites. However, as more and more web sites now support HTTPS, these arguments become increasingly moot.

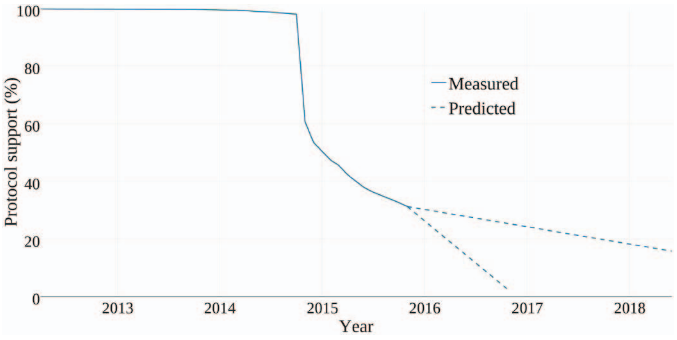

Fig. 3. SSL v3.0 support and linear predictions.

TABLE II. Observed global support of SSL v3.0

Survey month	*Support rate*	*Survey month (cont.)*	*Support rate (cont.)*	*(cont.)*	*(cont.)*
2012-04	99.9 %	2014-03	99.4 %	2015-02	47.3 %
2012-05	99.8 %	2014-04	99.3 %	2015-03	45.5 %
···	···	2014-05	99.0 %	2015-04	42.3 %
2013-07	99.8 %	2014-06	98.9 %	2015-05	40.0 %
2013-08	99.7 %	2014-07	98.7 %	2015-06	37.7 %
2013-09	99.7 %	2014-08	98.5 %	2015-07	36.2 %
2013-10	99.7 %	2014-09	98.3 %	2015-08	35.0 %
2013-11	99.6 %	2014-10	98.0 %	2015-09	33.8 %
2013-12	99.5 %	2014-11	60.6 %	2015-10	32.6 %
2014-01	99.5 %	2014-12	53.5 %	2015-11	31.2 %
2014-02	99.4 %	2015-01	50.4 %		

A comparison can be made with automotive safety. The perception during the 1960s was that drivers involved in a collision were generally themselves to blame, and the demand for stronger personal safety was limited enough that automakers could continue to focus on other areas of improvement. Only vigorous public discussion changed the awareness of safety as an externality in this domain [27].

Although end users are seldom aware of the technical specifics of web security, e.g. the difference between communicating over HTTP or HTTPS connections (let alone the implications negotiating SSL v3.0 versus TLS 1.2 when both result in a visible in-browser “padlock”) the negative externalities are becoming a societal concern. If web site owners cannot be made to internalize costs for web security, other options must be considered. These include market regulation, but may also entail, or be combined with, other incentives. While EU legislation is currently being developed to improve the dismal security situation, the wording does not strike the authors as being powerful enough to engender relevant change.

An alternative or complement to legislation could be to alert users to the practices of their business partners by making them aware of the security status of the web sites being accessed. Whereas attempting to access a web site with an incorrect certificate chain or a self-signed certificate will produce a large warning, requiring nontrivial user interaction to bypass, accessing a web site which permits the negotiation of SSL v2.0 commonly gives no warning at all. Implementing such warning schemes or ISP level blocking for insecure HTTPS configurations (including SSL v3.0) could incentivize web site owners to upgrade their servers. Although ISPs are neutral in relation to the traffic they carry, and are thus excluded from our web security ecosystem model, they are still in a position to influence protocol usage. In some European countries ISPs have introduced blocking of for instance software piracy sites through court orders. Although the effects of these blocks are debated [28], it provides an example of measures that lie between best practices and legislation.

V. Implications

In this article we have analyzed the economic incentives behind adoption and decay rates of some common protocols employed for web security, a critical contemporary cyber security technology. We have also studied the effects of best practices on the HTTPS ecosystem.

We can draw the conclusion that in a self-regulated web environment, insecure web site configurations can remain widespread for over a decade, even though their weaknesses are well-known and best practices oppose their use in the strongest possible terms. On the contrary, best practices appear to affect the decline of insecure configurations only moderately. Moreover, most discovered severe security flaws seem to have a limited effect on decay rates of vulnerable protocols, and an even smaller effect on the adoption rate of enhanced protocols.

Based on our model of adoption of TLS v1.2, we expect the protocol to be ubiquitous (reaching 95 % or more) at some point in late 2017. Since the use of SSL v3.0 is now in decline, it seems interesting to attempt to create a full life cycle model of the protocol and connect or compare it to the observed decline of SSL v2.0. If these follow the same late-stage decline curve, it would support generalizability of such a model. We can already note, however, that SSL v3.0 is likely to be with us for a long time despite being broken.

Stronger, possibly noneconomic incentives, such as client-side or ISP blocking of noncompliant sites or legislation, may be the most effective way to reduce the gap between security mechanisms and attack vectors. While best practices seem to be sufficient for browser vendors, other means are most likely required in order to properly internalize market costs for web site owners. More research is needed to determine exactly what they should be, so that the cracks in web security may be properly mended, rather than papered over.

References

[1] Symantec Corporation, “Internet Security threat Report,” April 2015. [Online]. Available: http://www.symantec.com/security_response/publications/threatreport.jsp.

[2] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

[3] J. Sigholm and M. Bang, “Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats,” in *Proceedings of the IEEE European Conference in Intelligence Security Informatics*, Uppsala, Sweden, 2013.

[4] J. Sigholm, “Non-State Actors in Cyberspace Operations,” *Journal of Military Studies*, vol. 4, no. 1, 2013.

[5] Center for Strategic and International Studies, “Net Losses: Estimating the Global Cost of Cybercrime,” June 2014. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[6] D. Wagner and B. Schneier, “Analysis of the SSL 3.0 Protocol,” in *Proceedings of the Second USENIX Workshop on Electronic Commerce*, Oakland, USA, 1996.

[7] S. Turner and T. Polk, “Prohibiting Secure Sockets Layer (SSL) Version 2.0,” Internet Engineering Task Force (IETF) Request for Comments: 6176, 2011.

[8] B. Amann, R. Sommar, M. Vallentin and S. Hall, “No Attack Necessary: The Surprising Dynamics of SSL Trust Relationships,” in *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC)*, New Orleans, USA, 2013.

[9] M. Bland, “Finding More Than One Worm in the Apple,” *ACM Queue*, vol. 12, no. 5, 2014.

[10] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey and J. A. Halderman, “The Matter of Heartbleed,” in *Proceedings of the Internet Measurement Conference (IMC)*, Vancouver, Canada, 2014.

[11] B. Möller, T. Duong and K. Kotowicz, “This POODLE Bites: Exploiting the SSL 3.0 Fallback,” Google security advisory, September 2014. [Online]. Available: https://www.openssl.org/~bodo/ssl-poodle.pdf.

[12] G. Greenwald, No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State, Metropolitan Books, 2014.

[13] M. Dunn Cavelty, “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities,” *Journal of Science and Engineering Ethics*, no. April, 2014.

[14] J. Buchanan and W. C. Stubblebine, “Externality,” *Economica*, vol. 29, no. 116, pp. 371-384, 1962.

[15] A. Freier, P. Karlton and P. Kocher, “The Secure Sockets Layer (SSL) Protocol Version 3.0,” Internet Engineering Task Force (IETF) Request for Comments: 6101, 2011.

[16] A. Guarino, “The State vs the People,” *IEEE Engineering & Technology*, vol. 8, no. 10, pp. 43-45, 2013.

[17] A. Arnbak, H. Asghari, M. van Eeten and N. van Eijk, “Security Collapse in the HTTPS Market - Assessing legal and technical solutions to secure HTTPS,” *ACM Queue*, vol. 12, no. 8, 2014.

[18] K. Zetter, “Google Hack Attack Was Ultra Sophisticated, New Details Show,” Wired, 14 January 2010. [Online]. Available: http://www.wired.com/2010/01/operation-aurora/.

[19] C. Herley, “So long, and no thanks for the externalities: the rational rejection of security advice by users,” *Proceedings of the workshop on New Security Paradigms (NSPW)*, 2009.

[20] S. Bradner, “IETF Structure and Internet Standards Process,” *Presentation at the 78th IETF*, Maastricht, the Netherlands, 2010.

[21] B. Schneier, “Information Security and Externalities,” European Network and Information Security Agency (ENISA) quarterly newsletter, 2007.

[22] High Representative of the European Union for Foreign Policy, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” 2013.

[23] Qualys, Inc, “SSL Pulse, a non-commercial research effort,” [Online]. Available: https://www.trustworthyinternet.org/ssl-pulse/.

[24] P. A. Gerosky, “Models of technology diffusion,” *Research Policy*, vol. 29, no. 4-5, pp. 603-625, 2000.

[25] J. Sigholm and E. Larsson, “Determining the Utility of Cyber Vulnerability Implantation: The Heartbleed Bug as a Cyber Operation,” *Proceedings of the IEEE Military Communications Conference (MILCOM)*, pp. 110 - 116, 2014.

[26] G. Akerloff, “The Market for ‘Lemons’: Quality Uncertainty and the Market Mechanism,” *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488-500, 1970.

[27] R. Nader, Unsafe at Any Speed: The Designed-in Dangers of the American Automobile, USA: Grossman Publishers, 1965.

[28] M. S. Tobias Lauinger, K. Onarlioglu, G. Wondracek, E. Kirda and C. Kruegel, “Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting,” in *20th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, USA, 2013.