

Formal Methods and CyberSecurity

J.H. Davenport

Department of Computer Science
University of Bath, Bath BA2 7AY, U.K.
masjhd@bath.ac.uk

Formal methods have been largely thought of in the context of safety-critical systems, where they have achieved major acceptance. Tens of millions of people trust their lives every day to such systems, based on formal proofs rather than “we haven’t found a bug” (yet!). Why is “we haven’t found a bug” an acceptable basis for systems trusted with hundreds of millions of people’s personal data?

This paper looks at some of the issues in CyberSecurity, and the extent to which formal methods, ranging from “fully verified” to better tool support, could help. Alas [58] only recommended formal methods in the limited context of “safety critical applications”: we suggest this is too limited.

1 Introduction

CyberSecurity¹ failures abound, and the number of people that can be affected by even a single failure is amazing — 148 million for Equifax [10] and probably more for the Starwood² breach: [5] states 500 million, but [33] “downgrades” this to 383 million. The financial costs can be substantial: bankruptcy in the case of American Medical Collection Agency [24] and a provisional £183M fine for British Airways [67]. These problems have attracted attention at the highest scientific levels [58].

There are many reasons for CyberSecurity failures, and even a given failure may have multiple causes. For example, the U.S. Government investigation [69] into Equifax states “Equifax’s investigation of the breach identified four major factors including identification, detection, segmenting of access to databases, and data governance that allowed the attacker …”. However, none of these would have been triggered had it not been for the original bug in the Apache code [39], which was of the well-known (Number 1 Application Security Risk in [54]) family of “Injection” (or “Remote Code Execution”) attacks, and which would probably have been detected by an automatic taint analysis tool such as [40].

Though attributing causes at scale is difficult, a well-known textbook [43] claims that about 50% of security breaches are caused by coding errors. Hence it behoves security practitioners to look seriously at coding errors, while recognising that this is only one facet of the problem. This is taken up by the Payments Card Industry in [57], essentially the only world-wide mandatory security standard, in two requirements.

6.5 Address common coding vulnerabilities in software-development processes as follows:

- Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities;
- Develop applications based on secure coding guidelines.

¹The precise definition of CyberSecurity is debatable: we can take it as failures of security, generally defined as “preserving the CIA — Confidentiality, Integrity and Availability” of digital information, where computer system played a critical part in the failure.

²Generally called “Marriott”, but in fact due to the Starwood chain before Marriott took it over.

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes;
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

It is noteworthy that, despite apparently insisting on secure coding in 6.5, they require the additional defences in 6.6, realising that *errare humanum est*, and the 6.5-developed code may not actually be secure. Is it possible (the author thinks so, but the experiment has yet to be performed) that adding formal methods to 6.5 would render 6.6 redundant? Full formal verification of a complete system should certainly suffice.

Complete formal verification is the only known way to guarantee that a system is free of programming errors. [35, describing seL4: a verified operating system]

Such a verified operating system has been used in medical devices, but probably not sufficiently widely, as 500,000 already-fitted pacemakers have had to be upgraded through security weaknesses [66], and insulin pumps are also vulnerable [51]. See [30] for a recent update on seL4. However, most of us do not have the opportunity to start from scratch, and have to live on top of imperfect, unverified systems, interoperating with other systems via large, generally unverified, protocols, such as TLS.

2 TLS and its issues

The TLS protocol (and its predecessor SSL) are the basis of most Internet security, underpinning, for example, [https](https://www). They also have displayed some of the most prominent problems.

Correctness Paulson [56] “Proved TLS Secure”, according to folklore. More precisely, the abstract states “All the obvious security goals can be proved”, but the paper itself is more nuanced.

Is TLS really secure? My proofs suggest that it is, but one should draw no conclusions without reading the rest of this paper, which describes how the protocol was modelled and what properties were proved. I have analyzed a much simplified form of TLS; I assume hashing and encryption to be secure.

There has been much work on TLS security since, e.g. [28, 37]. In particular, the latter used ‘real’ encryption, the RSA PKCS #1 v1.5, recommended, rather than ‘ideal’ encryption. Again, these all focus on the idealised protocol, rather than implementations.

Heartbleed [49] This, arguably the most serious security issue of 2014, at least as perceived by the media (for example [4]) and the public (for example [63]), was a bug in a particular, but very widely used, implementation (OpenSSL) of TLS, and hence instantly falls outside the scope of [56]. Furthermore, it was a bug in an extension [61] which postdates [56]. [61] states “This document does not introduce any new security considerations”, which is also true.

The bug itself was a bounds checking bug, and thus could have been flagged by even relatively weak static analysis tools. Looking a bit deeper, it was caused by assuming that the other end was behaving correctly. This seems to be a general class of errors, oddly missing from [1].

Poodle [46, 50] This also appeared in 2014. It requires two “features” to operate.

1. Many TLS implementations contain ways to downgrade to SSL 3.0 if the other end doesn't support TLS itself. However this downgrade (again, a feature of implementations, so outside the scope of [56]) is typically not a proper protocol negotiation, and can be subverted by an active attacker. As [1] state "where the identity of a principal is essential to the meaning of a message, it should be mentioned explicitly in the message", and indeed should be authenticated.

2. Once downgraded to SSL 3.0, the attacker can exploit this.

The most severe problem of CBC encryption in SSL 3.0 is that its block cipher padding is not deterministic, and not covered by the MAC (Message Authentication Code): thus, the integrity of padding cannot be fully verified when decrypting. [46]

Paulson [56] states, not unreasonably, "I assume hashing and encryption to be secure", as this is a separate set of proof technologies, and generally only produces relative security proofs.

Hence we have a proof of correctness of a (simplified, but in fact the simplification is irrelevant here) version of an abstract protocol, and major bugs in implementations. One is a "coding" bug, while the other is a combination of a protocol bug and a cryptography bug. Though not directly relevant to this paper, [60] demonstrates that Heartbleed (and Poodle) had a major positive effect on the OpenSSL project.

3 Agile versus Secure

"Agile Development" [6] is a major theme in software development. Mark Zuckerberg can be said to have taken this theme to the extreme in 2009.

"Move fast and break things" is Mark's prime directive to his developers and team. "Unless you are breaking stuff," he says, "you are not moving fast enough." [9]

In both safety-critical and security-conscious programming, "breaking things" comes with a very high price. Aeroplanes can't be uncrashed, and data can't be unleaked.

The problems with using "Agile" methods in security are well-documented, at practitioner level, e.g. a recent "Security + Agile = FAIL" presentation [38], in many theoretical analyses as well as the interview-based research in [3] for small teams and [29] for large multi-team projects. Both mention team expertise in security as a significant problem.

[3] The overall security in a project depends on the security expertise of the individuals, either on the customer or developer side. This corresponds to the agile value of "individuals and interaction over processes and tools" [6, Value 1].

[29] The interviewees generally agree that more could be done to provide security education and training to employees. Without prompting, several interviewees mentioned training as an important factor for increasing security awareness and expertise.

It is very hard to take security seriously in this setting.

[3] security "is only of interest [to the customer] when money-aspects are concerned".

[29] One Test Manager articulated his team view that "security is not currently seen as part of working software, it only costs extra time and it doesn't provide functionality". With less focus on providing extensive (security) documentation typical for agile, ineffective knowledge sharing between security officers and agile team members is especially problematic.

[64]³ “Security is often referred to as a NFR [non-functional requirement] in that it is expected to be included as part of high quality code development, but is rarely listed as an explicit requirement. As a result, developers prioritise security below more-visible functional requirements or even easy-to-measure activities such as closing bug tracking tickets.”

It would be tempting to conclude that “Agile” and “Secure” are, or at least are close to being, mutually contradictory. But there has been some analysis of the same apparent contradiction in the safety-critical industry [15]. Other than “Embedded Systems”⁴ [15, §3.6], this analysis of the problems is fairly close to the practitioner view in [38], and we could reasonably ask what lessons could be carried across.

4 The Need for Tools

There are two key points.

[15, §4.1] Strong static verification tools tend to complement (not replace) human-driven review⁵. The tools are very good at some problems (e.g. global data flow analysis, theorem proving) where humans are hopeless, and vice versa. If we do the static verification first, then we can adjust manual review processes and check-lists to take advantage of this.

[15, §6] The sixty-four-million-dollar-question, it seems, is how much “up-front” work is “just right” for a particular project. We doubt theres a one-size-fits-all approach, but surely the answer should be informed by disciplined requirements engineering of non-functional properties (e.g. safety, security and others) that can inform the design of a suitable architecture and its accompanying satisfaction argument.

Facebook grew, security (and “product quality” in general: it is not clear whether security was the main driver here) became more important, and by 2014 Zuckerberg had changed his views.

“Move fast with stable infrastructure.” It “may not be quite as catchy as ‘move fast and break things,’” Zuckerberg said with a smirk. “But it’s how we operate now.” [62]

One might think his views were converging with the views of [15]. However, the Heartbleed story should remind us that the fact that a modification “has no new security considerations” *as designed* [61] doesn’t mean that an implementation of that idea has no new security considerations. Hence the call in [15, §4.1] for strong static verification tools. Such tools are generally seen as expensive and slowing down the development process, but [11] shows that they need not be. In particular, they show that, for a real application (890,000 physical lines of Ada code), the cost of incremental verification can be reduced from “nightly” to “coffee”, and hence can reasonably form part of a continuous integration toolchain, as is done at the company studied in [11]. Readers might comment that their own applications are not in Ada, but [17, §5.6] discusses mixed-language programming, especially with C. A similar point is made in [21], describing the Infer tool running on Java/Objective C/C++, where moving from overnight reporting to near real-time reporting moved the fix rate from 0% to 70%.

That these techniques are reaching the mainstream of CyberSecurity can be seen from Amazon Web Services adoption of them [70], Google [59], Facebook [21], and the recent DefectDojo release by OWASP [55].

⁴Actually, Embedded Systems are a comparatively neglected, but important, CyberSecurity area. See, for example, [52] for a description of a pervasive design fault in the “home security” market.

⁵A point made in the context of XP and Agile in 2004 [71].

5 The Scope of Tools and Formal Methods

There is a substantial range of tools, and degrees of formality, and [15, §6] is probably correct in saying “We doubt there’s a one-size-fits-all approach”. At one extreme, there are the humble, but still surprisingly effective, `lint` and its equivalents, looking, essentially, for dangerous or dubious, though legal, syntax.

5.1 Ada and SPARK

At the other extreme, there are languages, such as the SPARK Ada subset [17] designed with verification in mind and heavily employed in the safety-critical sector such as railways and air traffic control, which can also be deployed for demanding secure applications, such as an RFC4108-compliant [31] secure download system for embedded systems [16].

5.2 C/C++

There is, however, a large middle ground between these two extremes. Even if the application is required to be in C or C++, there is a lot to be said for sticking to a safer (even if not provably safe) subset of the language *and associated libraries*, such as eschewing `strcpy` in favour of `strncpy`. This can often be enforced by static verification tools. We note that Google’s “Zero Day” project reports [26] that 68% of all such zero-day exploits (i.e. exploits discovered in the wild first) were caused by memory corruption errors, and Microsoft report a very similar story [68].

There is a good survey of such subsets and standards in [14, Appendix F]. As that notes, the ISO standard for secure C coding [34] has the unusual (for this middle ground) but important concept of “taint analysis” (as in [40]): input data should be considered “tainted” until it has been sanitised. This is particularly important for network-oriented applications, where it is natural for the programmer to believe that the other party is behaving correctly (see **Heartbleed** above).

5.3 Java

Closer to the SPARK Ada end of the spectrum we find Safety-Critical Java [13]. The author does not have enough experience with this to comment directly. However, the Java ecosystem (Stack Overflow etc.) is far from security-aware [44]. The fact that an application is in Java doesn’t mean it’s free from security coding errors: see [25] for a recent example.

There is a static analysis security tool for Java described in [40]. As with [34], this has “taint analysis” as its major feature, and at the time it spotted some significant-seeming problems.

5.4 JavaScript

JavaScript is a particular problem for Security. There are some verification tools, e.g. GATEKEEPER as described in [27]. However, even if it were possible to guarantee a particular piece of stand-alone JavaScript, that is not how the current paradigm operates. As [45] writes:

Much of the power of modern Web comes from the ability of a Web page to combine content and JavaScript code from disparate servers on the same page. While the ability to create such mash-ups is attractive for both the user and the developer because of extra functionality, code inclusion effectively opens the hosting site up for attacks and poor programming practices within every JavaScript library or API it chooses to use.

Though not explicit in this statement, an additional weakness is that this combination is *dynamic*. The obvious solution would be some kind of sandboxing of the external resources relied upon, but the nature of JavaScript makes this difficult. [41] describe one such sandboxing, but it only works for a subset of JavaScript and relies on a combination of filtering, rewriting and wrapping to guarantee security. That it can do so at all is a remarkable feat of formal methods, given that previous attempts such as Facebook’s FBJS have subtle flaws [42], and that the formal semantics of JavaScript being relied upon are very much a piece of reverse engineering.

In fact the dynamic loading from multiple sites is often not good for performance, and web performance engineers recommend tools to bundle the pages: this could usefully be combined with the sort of protection described by [41].

An alternative solution is used by Google, who are introducing a form of taint analysis into Chrome [36] through run-time typing. When enabled, this means that the 60+ dangerous DOM API functions can only be called with arguments whose type is that emitted by TrustedTypes functions. Google expects that these functions would be manually verified, but this does open the door to formal verification of *certain* security policies in what is currently a very challenging environment for formal methods. We note the complex interaction between

- the server

6 Education

[57, Requirement 6.5] called for education of developers. Education of mainstream programmers, as opposed to CyberSecurity specialists, in CyberSecurity has been neglected until recently, and this neglect has been lamented as far as the Harvard Business Review [12]. Developments in professional accreditation are changing this [20]. However, there are limitations, even beyond *errare humanum est*, in relying on education.

1. There is experimental evidence that both trained students [48] and professional developers [47] will ignore security considerations unless *explicitly* instructed to take them into account. Lest this be thought to be a purely academic exercise with little relevance to the real world, consider the recent ~~¥~~55M password problem described in [19].
2. There is field evidence that explicit requirements such as [57] are ignored in practice, e.g. the Forever 21 breach [7], or Macy’s [8]. They may also not be communicated down the software supply chain, as in the Ticketmaster case [32].
3. Many educational resources, both formal textbooks [65] and informal resources such as Stack Overflow [22], pay very little attention to security, and indeed can be positively harmful. The discussion in Stack Overflow (analysed in [44, §4.3.1]) of cross-site request forgery (CSRF — this was in the OWASP top 10 in 2013 [53], but dropped from [54] “as many frameworks include CSRF defenses”) is especially worrying. By default, Spring implicitly enables protection against this. But all the accepted answers to CSRF-related failures simply suggested disabling the check. There were no negative comments about this, and indeed a typical response is “Adding `csrf().disable()` solved the issue!!! I have no idea why it was enabled by default”.

As we have noted, [57] both mandates education and does not rely solely on it.

However, as the safety-critical community laments (at least in the U.K. and U.S.A.: cultures do differ here), there is very little training in formal methods for most undergraduates.

7 Conclusions

As the media never tire of saying, there are far too many security breaches, and, though they have multiple causes, [43] claims that about 50% of security breaches are caused by coding errors. There appears to be a culture of accepting these, with the U.S. Government investigation [69] into Equifax blaming many factors but not the actual bug, and [57] taking a “necessary but not sufficient” approach to education in secure coding.

Education Could certainly do better [12], though there are encouraging signs [20] and useful ideas when it comes to improving informal resources [23]. However, informal resources can be dangerous when it comes to security, and [20] recommends giving *all* students the advice in [18]: “If you pick up a SSL/TLS answer from Stack Overflow, there’s a 70% chance it’s insecure”.

More training in formal methods would be welcomed, at least in those cultures where it is lacking.

Customers/Managers need to be much more upfront about security requirements [48, 47], and enforce (e.g. by requiring tool support during any CI/CD process, such as [11] describe) at least “middle ground” requirements. In the case of outsourced development, explicit penalty clauses for failing penetration tests should concentrate the developers’ minds.

C/C++ people These programmers should be much more aware of techniques for secure coding, such as those described in [14, Appendix F], and the various tools for static analysis.

Java people In view of the significance of injection attacks (Number 1 in [54]), programmers should be aware of taint analysis, as in [40].

JavaScript people There are some techniques, such as [41], for protecting JavaScript applications, but they are not deployable in the the typical JavaScript “dynamic loading web page” environment. Furthermore this environment is basically antithetical to security, as British Airways is learning to the cost of £183M [67].

- 1) Hence the first real challenge of JavaScript lies with the tool makers: there are, as far as the author knows, no JavaScript verifiers in existence, and no page-bundler that checks for version drift, or does incremental verification (which might be comparatively cheap, as in [11]).
- 2) An alternative approach might be to change the JavaScript model. This is advocated in [72], based on their analysis of what third-party scripts do in the wild. This is not a completely radical idea: Google is testing its TrustedTypes feature [36], with the motivation “The DOM API is insecure by default and requires special treatment to prevent XSS”.

Empirical Research There is not much analysis of the efficacy of various techniques in security programming. [2] compares various techniques, and states the following.

Based on our case study [of two large programs], the most efficient vulnerability discovery technique is automated penetration testing. Static analysis finds more vulnerabilities but the time it takes to classify false positives makes it less efficient than automated testing.

This assumes that “false positives” are acceptable, a debatable point of view. It would be good to have more such research.

Tool developers There is a lack of tools (or at least a lack of awareness of tools) that can be neatly integrated into a security programming toolchain the way such tools are integrated in safety-critical toolchains [11].

Acknowledgements: The author is grateful to the Fulbright Programme for a CyberSecurity Scholarship, and to many correspondents and discussions, notably with Tom Crick, Alastair Irons and Tom Prickett; also Tim French. The FROM2019 referees made useful comments.

References

- [1] R.J. Anderson & R.M. Needham (1995): *Programming Satan's Computer*. In: *Computer Science Today, Springer Lecture Notes in Computer Science* 1000, pp. 426–440.
- [2] A. Austin & L. Williams (2011): *One technique is not enough: A comparison of vulnerability discovery techniques*. In: *Proceedings 2011 International Symposium on Empirical Software Engineering and Measurement*, pp. 97–106.
- [3] S. Bartsch (2011): *Practitioners' Perspectives on Security in Agile Development*. In *International Conference on Availability Reliability and Security*, pp. 479–484.
- [4] BBC (2014): US government warns of Heartbleed bug danger. <https://www.bbc.co.uk/news/technology-26985818>.
- [5] BBC (2018): Marriott hack hits 500 million Starwood guests. <https://www.bbc.co.uk/news/technology-46401890>.
- [6] Beck, K. et al. (2001): *The Agile Manifesto*. <http://agilemanifesto.org/>.
- [7] C. Biscoe (2018): MyFitnessPal data breach: 150 million app users affected. <https://www.itgovernance.co.uk/blog/myfitnesspal-data-breach-150-million-app-users-affected/>.
- [8] A. Blackmon (2018): Macy's hit by data breach. <https://eu.freep.com/story/money/business/2018/07/06/macys-data-breach/214000002/>.
- [9] H. Blodget (2009): Mark Zuckerberg On Innovation. <https://www.businessinsider.com/mark-zuckerberg-innovation-2009-12>.
- [10] Bloomberg (2018): *Equifax Hack Lasted for 76 Days, Compromised 148 Million People, Government Report Says*. <http://fortune.com/2018/12/10/equifax-hack lasted-for-76-days-compromised-148-million-people-gov-report-says/>.
- [11] M. Brain & F. Schanda (2012): *A Lightweight Technique for Distributed and Incremental Verification*. In Rajeev Joshi, Peter Müller & Andreas Podelski, editors: *Verified Software: Theories, Tools, Experiments, LNCS 7152*, Springer, Berlin–Heidelberg–New York, pp. 114–129, doi:10.1007/978-3-642-27705-4_10.
- [12] J. Cable (2019): *Every Computer Science Degree Should Require a Course in Cybersecurity*. <https://hbr.org/2019/08/every-computer-science-degree-should-require-a-course-in-cybersecurity>.
- [13] A. Cavalcanti, A. Miyazawa, A. Wellings, J. Woodcock & S. Zhao (2017): *Java in the Safety-Critical Domain*. *SETSS 2016: Engineering Trustworthy Software Systems*, pp. 110–150.
- [14] Centre for the Protection of National Infrastructure (2019): *Rail Code of Practice for Security-Informed Safety*. CPNI.
- [15] R. Chapman (2016): *Industrial experience with Agile in high-integrity software development*. In M. Parsons & T. Anderson, editors: *Developing Safe Systems: Proceedings of the Twenty-fourth Safety-critical Systems Symposium*, Safety-Critical Systems Club, pp. 143–154.
- [16] R. Chapman (2018): *Development and Formal Verification of Secure Updates for Embedded Systems* (slides from Verification 2018). <http://www.testandverification.com/conferences/verification-futures/vf2018/>.
- [17] R. Chapman & Y. Moy (2018): *AdaCore Technologies for Cyber Security*. <https://www.adacore.com/books/adacore-tech-for-cyber-security>.
- [18] M. Chen, F. Fischer, N. Meng, X. Wang & J. Grossklags (2019): *How Reliable is the Crowdsourced Knowledge of Security Implementation?* <https://arxiv.org/abs/1901.01327>.
- [19] C. Cimpanu (2019): *7-Eleven Japanese customers lose \$500,000 due to mobile app flaw*. <https://www.zdnet.com/article/7-eleven-japanese-customers-lose-500000-due-to-mobile-app-flaw/>.

- [20] T. Crick, J.H. Davenport, A. Irons & T. Prickett (2019): *A UK Case Study on Cybersecurity Education and Accreditation*. <https://arxiv.org/abs/1906.09584>.
- [21] D. Distefano, M. Fähndrich, F. Logozzo & P.W. O’Hearn (2019): *Scaling static analyses at Facebook*. *Communications of the ACM* 62, pp. 62–70.
- [22] F. Fischer, K. Böttlinger, H. Xiao, C. Stransky, Y. Acar, M. Backes & S. Fahl (2017): *Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security*. *38th IEEE Symposium on Security and Privacy (SP)*, pp. 121–136.
- [23] F. Fischer, H. Xiao, C.-Y. Kao, Y. Stachelscheid, B. Johnson, D. Razan, P. Fawkesley, N. Buckley, K. Böttlinger, P. Muntean & J. Grossklags (2019): *Stack Overflow Considered Helpful! Deep Learning Security Nudges Towards Stronger Cryptography*. *28th USENIX Security Symposium (USENIX Security 19)*.
- [24] N. Ford (2019): *Medical debt collection agency files for bankruptcy protection after data breach*. <https://www.itgovernance.co.uk/blog/medical-debt-collection-agency-files-for-bankruptcy-protection>
- [25] Google (Chris Povirk) (2018): *Denial of Service vulnerability for servers that use Guava and deserialize attacker data*. <https://groups.google.com/forum/#!topic/guava-announce/xqWALw4W1vs/discussion>.
- [26] Google (Project Zero) (2019): *0day “In the Wild”*. <https://googleprojectzero.blogspot.com/p/0day.html>.
- [27] S. Guarnieri & B. Livshits (2009): *GATEKEEPER: Mostly Static Enforcement of Security and Reliability Policies for JavaScript Code*. In: *USENIX Security Symposium*, 10, pp. 76–85. Available at http://static.usenix.org/events/sec09/tech/full_papers/sec09_javascript.pdf.
- [28] C. He, M. Sundararajan, A. Datta, A. Derek & J.C. Mitchell (2005): *A Modular Correctness Proof of IEEE 802.11i and TLS*. In: *Proceedings 12th ACM conference on Computer and communications security*, pp. 2–15.
- [29] A. van der Heijden, C. Broasca & A. Serebrenik (2018): *An Empirical Perspective on Security Challenges in Large-scale Agile Software Development*. In: *Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, ESEM ’18, ACM, New York, NY, USA, pp. 45:1–45:4, doi:10.1145/3239235.3267426. Available at <http://doi.acm.org/10.1145/3239235.3267426>.
- [30] G. Heiser (2019): *What’s new in the world of seL4*. https://archive.fosdem.org/2019/schedule/event/world_of_sel4/
- [31] R. Housley (2005): *Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages*. RFC-4108.
- [32] Inbenta (CEO) (2018): *Inbenta and the Ticketmaster Data Breach*. <http://web.archive.org/web/20181121184620/>.
- [33] L. Irwin (2019): *Marriott downgrades severity of 2018 data breach: 383 million customers affected*. <https://www.itgovernance.co.uk/blog/marriott-downgrades-severity-of-2018-data-breach-383-million-customers-affected>
- [34] ISO/IEC (2013): *TS 17961:2013, Information technology — Programming languages, their environments & system software interfaces — C Secure Coding Rules*. <https://www.iso.org/standard/61134.html>.
- [35] G. Klein, K. Elphinstone, G. Heiser, J. Andronick, D. Cock, P. Derrin, D. Elkaduwe, K. Engelhardt, R. Kolanski, M. Norrish & T. Sewell (2009): *seL4: Formal verification of an OS kernel*. In *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*, pp. 207–220.
- [36] K. Kotowicz (2019): *Trusted Types help prevent Cross-Site Scripting*. <https://developers.google.com/web/updates/2019/02/trusted-types>.
- [37] Hugo Krawczyk, Kenneth G. Paterson & Hoeteck Wee (2013): *On the Security of the TLS Protocol: A Systematic Analysis*. In Ran Canetti & Juan A. Garay, editors: *Advances in Cryptology – CRYPTO 2013*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 429–448.
- [38] A. Lane (2018): *Security + Agile = FAIL*. <https://securosis.com/assets/library/presentations/Security/AgileFAIL.pdf>
- [39] L. Lenart (2017): *Security Bulletin S2-045*. <https://cwiki.apache.org/confluence/display/WW/S2-045>.
- [40] V.B. Livshits & M.S. Lam (2005): *Finding Security Vulnerabilities in Java Applications with Static Analysis*. In: *Proceedings USENIX Security Symposium*, pp. 271–286.

- [41] S. Maffeis, J.C. Mitchell & A. Taly (2009): *Isolating JavaScript with Filters, Rewriting, and Wrappers*. In: *Proceedings ESORICS 2009*, pp. 505–522.
- [42] S. Maffeis & A. Taly (2009): *Language-based isolation of untrusted Javascript*. In: *Proceedings 22nd IEEE Computer Security Foundations Symposium*, pp. 77–91.
- [43] G. McGraw (2006): *Software Security — Building Security In*. Addison-Wesley.
- [44] N. Meng, S. Nagy, D. Yao, W. Zhuang & G. Arango Argoty (2018): *Secure coding practices in Java: Challenges and vulnerabilities*. In *2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*, pp. 372–383.
- [45] L.A. Meyerovich & B. Livshits (2010): *ConScript: Specifying and enforcing fine-grained security policies for Javascript in the browser*. In: *2010 IEEE Symposium on Security and Privacy*, IEEE, pp. 481–496.
- [46] B. Möller, T. Duong & K. Kotowicz (2014): *This POODLE Bites: Exploiting The SSL 3.0 Fallback (Security Advisory)*. <https://www.openssl.org/~bodo/ssl-poodle.pdf>.
- [47] A. Naikashina, A. Danilova, E. Gerlitz, E. von Zezschwitz & M. Smith (2019): ”If you want, I can store the encrypted password”: A Password-Storage Field Study with Freelance Developers. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, pp. 140:1–140:12, doi:<https://doi.org/10.1145/3290605.3300370>.
- [48] A. Naikashina, A. Danilova, C. Tiefenau & M. Smith (2018): *Deception Task Design in Developer Password Studies: Exploring a Student Sample*. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, pp. 297–313.
- [49] National Institute for Standards and Technology (2014): CVE-2014-0160 Detail. <https://nvd.nist.gov/vuln/detail/CVE-2014-0160>.
- [50] National Institute for Standards and Technology (2014): CVE-2014-3566 Detail. <https://nvd.nist.gov/vuln/detail/CVE-2014-3566>.
- [51] L.H. Newman (2019): *Hackers Made an App That Kills to Prove a Point*. <https://www.wired.com/story/medtronic-insulin-pump-hack-app>.
- [52] T.J. O'Connor, W. Enck & B. Reaves (2019): *Blinded and Confused: Uncovering Systemic Flaws in Device Telemetry for Smart-Home Internet of Things*. In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 140–150.
- [53] Open Web Application Security Project (OWASP) (2013): *The Ten Most Critical Web Application Security Risks*. https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf.
- [54] Open Web Application Security Project (OWASP) (2017): *The Ten Most Critical Web Application Security Risks*. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main.
- [55] Open Web Application Security Project (OWASP) (2019): *DefectDojo: OpenSource Application Security Management*. <https://www.defectdojo.org>.
- [56] L.C. Paulson (1999): *Inductive Analysis of the Internet Protocol TLS*. *ACM Trans. Information and System Security* 2, pp. 332–351.
- [57] Payment Card Industry Security Standards Council (PCI SSC) (2018): *Requirements and Security Assessment Procedures Version 3.2.1*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.
- [58] Royal Society (2016): *Progress and research in cybersecurity: Supporting a resilient and trustworthy system for the UK*. <http://royalsociety.org/cybersecurity>.
- [59] C. Sadowski, E. Aftandilian, A. Eagle, L. Miller-Cushion & C. Jaspan (2018): *Lessons from building static analysis tools at Google*. *Commun. ACM* 61(4), pp. 58–66.
- [60] R. Salz (2017): *Software engineering and OpenSSL is not an oxymoron (presentation at Real World Cryptography 2017)*. <https://rwc.iacr.org/2017/Slides/rich.saltz.pdf>.
- [61] R. Seggelmann, M. Tuexen & M. Williams (2012): *Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension*. <https://tools.ietf.org/html/rfc6520>.

- [62] N. Statt (2014): *Zuckerberg: 'Move fast and break things' isn't how Facebook operates anymore.* <https://www.cnet.com/news/zuckerberg-move-fast-and-break-things-isnt-how-we-operate-anymore/>.
- [63] J. Steinberg (2014): *Massive Internet Security Vulnerability – Here's What You Need To Do.* <https://www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-y>
- [64] M. Tahaei & K. Vaniea (2019): *A Survey on Developer-Centred Security.* https://groups.inf.ed.ac.uk/tulips/papers/A_Survey_on_Developer_Centred_Security.pdf.
- [65] C. Taylor & S. Sakharkar (2019): *');DROP TABLE textbooks;–: An Argument for SQL Injection Coverage in Database Textbooks.* In Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19). ACM, pp. 191–197.
- [66] The Guardian (2017): *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears.* <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-f>
- [67] The Guardian (2019): *BA faces £183m fine over passenger data breach.* <https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways>.
- [68] G. Thomas (2019): *A proactive approach to more secure code.* <https://msrc-blog.microsoft.com/2019/07/16/a-proactive-approach-to-more-secure-code/>.
- [69] United States Government Accountability Office (2018): *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* <https://www.gao.gov/assets/700/694158.pdf>.
- [70] W. Vogels (2019): *Proving security at scale with automated reasoning.* <https://www.allthingsdistributed.com/2019/05/proving-security-at-scale-with-automated-reasoning.h>
- [71] J. Wäyrynen, M. Bodén & G. Boström (2004): *Security Engineering and eXtreme Programming: an Impossible Marriage? Extreme programming and agile methods-XP/Agile Universe*, pp. 117–128.
- [72] M. Zhang, W. Meng, S. Lee, B. Lee & X. Xing (2019): *All Your Clicks Belong to Me: Investigating Click Interception on the Web.* <https://www.microsoft.com/en-us/research/uploads/prod/2019/03/zhang-observer.pdf>.