Institution: Royal Holloway, University of London		
Unit of Assessment: 11 Computer Science and Informatics		
Title of case study: Cryptographic Analysis of RC4 and Improvement of Transport Layer Security: Enhancing the Security of the Global Digital Infrastructure		
Period when the underpinning research was undertaken: 2013-2015		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): Proessor Kenneth Paterson	**Role(s) (e.g. job title):** Professor of Information Security and EPSRC Leadership Fellow	**Period(s) employed by submitting HEI:** 2001-2019
Period when the claimed impact occurred: 2013-2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

The Transport Layer Security (TLS) protocol is used by billions of people on a daily basis for secure web browsing, and many other activities such as e-commerce, social networking and Internet banking. In 2013, Paterson led a team that found significant cryptographic weaknesses in the RC4 encryption algorithm when used in the TLS protocol. At that time, RC4 was used in approximately 50% of all TLS-secured web browsing sessions. As a direct consequence of the research, major vendors including Apple, Google, Microsoft and Mozilla removed RC4 as an encryption option in their browsers, and the RC4 usage figure is now well below 1%. By identifying and fixing a problem in a protocol that is core to Internet security, the research has benefitted the world's digital infrastructure and its billions of daily users.

2. Underpinning research

By default, Internet traffic is vulnerable to eavesdropping and modification. Transport Layer Security (TLS) is a protocol that has become the *de facto* method for securing application-layer messages sent on the Internet. TLS is implemented in all major web browsers and servers and is used daily by billions of people for applications such as e-commerce, social networking and Internet banking.

In a sequence of papers published in top conference venues beginning in 2013 [R1 to R5], a team led by Prof. Paterson identified flaws in the way TLS encrypts data when it uses a particular encryption algorithm, RC4. This resulted in cryptographic attacks that compromised the confidentiality goal of TLS. The flaws result from the RC4 algorithm having many tiny biases in its outputs. These biases make it possible to infer plaintext data that should be protected by TLS in certain situations, such as when TLS is used to protect browser-to-website communications. The team systematically explored RC4 biases, found ways to exploit them in attacks in the TLS context, did simulation work to estimate attack complexities, and then implemented the attacks to validate the findings [R1]. As part of the follow-up work, the team analysed the attack scenarios more carefully and uncovered even more powerful attacks [R4]. This work established that RC4 in TLS had no long-term future. In turn this forced the industry to act in changing how browsers use TLS.

At the time the 2013 analysis [R1] was announced, roughly 50% of all TLS traffic was using RC4. This figure had become inflated because of prior work attacking the other widely deployed encryption mode in TLS, the subject of a REF 2014 case study from RHUL. Paterson's team, and other researchers (notably Vanhoef and Piessens at USENIX 2015), then built on the 2013 paper to drive the attacks towards practicality. The end result was that the continued used of

RC4 in TLS became indefensible. By the middle of 2018, less than 1% of all TLS traffic was using RC4 [R5].

In addition, Paterson's 2014 papers at FSE [R2] and ASIACRYPT [R3] showed that similar attacks could be applied to an important wireless encryption protocol, WPA/TKIP. In their follow-up work in 2015, Vanhoef and Piessens showed that the 2014 WPA/TKIP attack could be made fully practical, meaning that this protocol is no longer safe to use.

The initial team consisted of AlFardan (PhD student, now Principal Security Architect at Cisco), Bernstein (Research Professor at University of Illinois, Chicago), Paterson (EPSRC Leadership Fellow, now Professor of Computer Science at ETH Zurich), Poettering (PDRA, now at IBM Research, Switzerland) and Schuldt (PDRA, now permanent staff member at AIST Japan). One of the follow-up works involved van der Merwe (EPSRC CDT PhD student, now Head of Cryptographic Engineering with Mozilla) and Garman (visiting scientist from Johns Hopkins University, USA, now Assistant Professor at Purdue University). One of the papers was an invited paper at ASIACRYPT 2014 [R3], corresponding to Paterson's prestigious invited talk at the same conference. Another of the papers [R5] won a Distinguished Paper Award at ACM Internet Measurement Conference in 2018.

3. References to the research

[R1] N.J. AlFardan, D.J. Bernstein, K.G. Paterson, B. Poettering and J.C.N. Schuldt. On the Security of RC4 in TLS. In *USENIX Security Symposium 2013*. Online at: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/alFardan.
Top security conference (acceptance rate in 2013: 15.9%)

[R2] K.G. Paterson, B. Poettering and J.C.N. Schuldt. Plaintext recovery attacks against WPA/TKIP. In *C. Cid and C. Rechberger (eds.), Fast Software Encryption 2014*, Lecture Notes in Computer Science, Vol. 8540, pp. 325-349, Springer 2014.
Online at: https://link.springer.com/chapter/10.1007/978-3-662-46706-0_17
Full version online at: http://eprint.iacr.org/2013/748
Top venue for research in symmetric cryptography (acceptance rate in 2014: 31.3%).

[R3] K.G. Paterson, B. Poettering and J.C.N. Schuldt. Big Bias Hunting in Amazonia: Large-scale Computation and Exploitation of RC4 Biases (Invited Paper) In *T. Iwata and P. Sarkar (eds.), ASIACRYPT 2014*, Lecture Notes in Computer Science Vol. 8873, pp. 398-419, Springer, 2014. Online at: https://doi.org/10.1007/978-3-662-45611-8_21
Invited paper and talk at one of the top three annual cryptography conferences (acceptance rate in 2014: 21.6%).

[R4] C. Garman, K.G. Paterson and T.J. van der Merwe. Attacks only get better: Password recovery attacks against RC4 in TLS. In *USENIX Security Symposium 2015.* Online at: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/garman
Top security conference (acceptance rate in 2015: 15.7%).

[R5] P. Kotzias, A. Razaghpanah, J. Amann, K.G. Paterson, N. Vallina-Rodriguez and J. Caballero. Coming of Age: A Longitudinal Study of TLS Deployment. Proceedings of the Internet Measurement Conference 2018, IMC 2018, Boston, MA, USA, October 31 - November 02, 2018. ACM 2018, pp 415-428. Online at: https://conferences.sigcomm.org/imc/2018/papers/imc18-final193.pdf
Winner of one of three distinguished paper awards at the leading venue for research on large-scale measurement of the Internet (acceptance rate in 2018: 24.7%).

Funding:

- Paterson (PI), EPSRC Leadership Fellowship (EP/H005455/1) "Bridging Theory and Practice in Cryptography", 2010-2015, GBP1,239,094 (funded research of Paterson, Poettering, Schuldt).

- Paterson (co-I), CDT in Cyber Security (EP/K035584/1), 2013-2019, GBP3,807,975 (funded research of van der Merwe).
- Paterson (joint PI), GBP52,000 and INR1,500,000 (both approximate figures) from EPSRC and DST, India for twinned workshops at ISI Kolkata and ICMS Edinburgh on "Security of Symmetric Ciphers in Network Protocols", under the EPSRC-DST Indo-UK Initiative in Applied Mathematics, 2014-2015.

4. Details of the impact

Accelerating the deprecation of RC4 and improvement of Transport Layer Security

In February 2015, the IETF, the organization that maintains the TLS standard, published a document entitled "Prohibiting RC4 Cipher Suites" formally deprecating the use of RC4 in TLS, see [E8]. This document cites Paterson's 2013 research paper, stating "*Recent cryptanalysis results […] exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts. These recent results are on the verge of becoming practically exploitable […] As a result, RC4 can no longer be seen as providing a sufficient level of security for TLS sessions.*"

Major vendors, including **Apple, Google, Microsoft and Mozilla changed the way their desktop and mobile browsers perform encryption** in TLS as a direct consequence of the research. This is clearly evidenced in the accompanying letters of support from Apple [E1], Google [E2] and Mozilla [E3], and from the formal Microsoft announcement in September 2015 that RC4 would no longer be supported in its browsers [E6]; similar public announcements were made by Google [E5] and Mozilla [E7], also in September 2015. These four vendors account for the vast majority of the web-browsing market. Google, Microsoft and Mozilla performed a coordinated switch off of RC4 in their browsers in early 2016, while Apple disabled RC4 in version 10 of Safari desktop (and in iOS 10 in mobile clients) in September 2016.

The world's leading content distribution networks and website hosting services also changed their default configurations to stop using RC4. A good example is provided by Cloudflare, whose letter of support [E4] states that Paterson's research "*represented a real threat to the security of TLS*" and also states that *"[a]s a result of the work, Cloudflare changed the TLS configuration for millions of web domains*".

The amount of TLS traffic encrypted using RC4 has dropped sharply – from approximately 50% of all traffic in 2013 to reach less than 1% by the middle of 2018. This drop is documented in Paterson's award-winning paper published at ACM IMC 2018, and there is a clear correlation between a drop in the amount of RC4 traffic with the switching off of support for RC4 in major browsers (see figure below, taken directly from the ACM IMC paper) (R5).

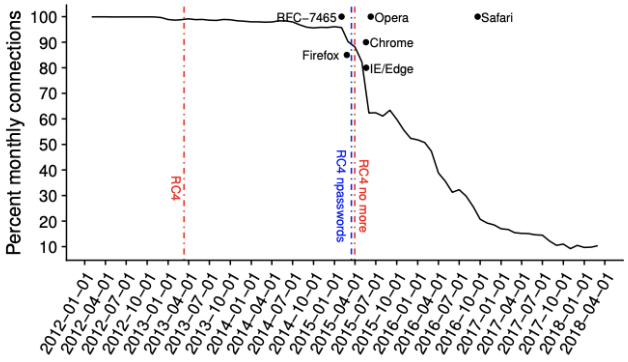

Figure 6: Percentage of connections where the client advertises RC4 cipher suites. Lines represent the dates of high profile attacks; black dots the dates that browsers dropped RC4 support.

As well as leading to the abandonment of RC4 in TLS in web browsers, Paterson's RC4 research promoted the widespread adoption of TLS 1.2 in web browsers and web servers. TLS 1.2 was standardized in 2008 but, in early 2013, before Paterson's RC4 research was announced, none of the four main web browsers supported this later version of TLS offering stronger encryption options. By mid-2018, all four browsers did, and the amount of traffic using stronger encryption algorithms (namely AES-GCM) is now approximately 90% (the majority of the remainder still uses CBC mode, and, as noted above, almost none uses RC4). To quote from Mozilla's letter of support [E3], "*As a direct result of this work, the TLS community rapidly moved to deprecate RC4, resulting in RFC 7465, which banned them entirely*" and "*Dr. Paterson's work was also a major impetus behind the move to AES-GCM.*" This impact is also evidenced by Apple's letter of support [E1]: "*TLS 1.2 adoption rates went from a negligible percentage in 2013 to around 90% by 2016*".

In April 2014, the IETF TLS Working Group began to work on a new version of TLS, and this work was completed in late 2018 with the issuance of TLS 1.3 as RFC 8446 (https://tools.ietf.org/html/rfc8446). This new version does not allow RC4 at all; the TLS Working Group's charter (https://datatracker.ietf.org/wg/tls/charter) explicitly says that one of the priorities for TLS 1.3 was to "*Update record payload protection cryptographic mechanisms and algorithms to address known weaknesses in the CBC block cipher modes and to replace RC4*." Thus, Paterson's research is having a long-lasting impact on the development of the TLS protocol as a whole. To quote from Mozilla's letter [E3], "*It is very rare to see this direct and immediate an impact by research on a standard as widely deployed as TLS*".

Beyond the impact of the research on the web, it has impacted other sectors including improving the security of card payment data protection. The initial RHUL attack on RC4 in 2013 was assigned a Common Vulnerabilities and Exposures record (CVE-2013-2566). In 2014 the CVE score eventually became high enough that the US Department of Commerce National Institute of Standards and Technology (NIST) published "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" [E9] in which the use of RC4 was not approved. Following the NIST guidelines in February 2015 the Payment Card Industry Security Standards Council banned the use of RC4 when assessing compliance with the PCI-DSS standard for payment data protection [E10].

Global benefits of improved security

Since just about everything that we do on the Internet, including e-commerce, website logins and e-mail relies for its security on TLS, a vulnerability in TLS has a blanket impact, affecting individuals, service providers, merchants, governments, utilities and the military. More succinctly, identifying and fixing a security problem in a protocol that is core to Internet security benefits the approximately 4,800,000,000 Internet users (http://www.internetlivestats.com/internet-users/), which includes the 2,200,000,000 email users and the approximately 600,000,000 website owners, as well as the companies that provide service hosting solutions and the service providers that run them. The global annual value of e-commerce alone has been estimated at several trillions of US dollars. To suggest a percentage of this that could be affected by the research would be speculation, and of course by detecting and preventing a problem we lose the chance to measure its effects. However, it is clear that the total value of e-commerce makes it an enormous target that justifies attacker efforts to implement very sophisticated attack strategies, and so the research to identify and fix serious vulnerabilities in TLS, the main protocol used to secure e-commerce, and thereby to contain losses, is absolutely vital. The longer-term beneficiary is the emerging electronic society at large, which will benefit from having more secure, and therefore more confidence-inspiring systems. We conclude by quoting from Cloudflare's letter of support [E4]: "*This research was highly significant: TLS is one of the world's most important secure protocols, and the foundation for most secure communications on the Internet, so understanding and improving its security is of critical importance to Cloudflare's mission and the Internet at large*."

5. Sources to corroborate the impact

[E1] Letter of support from Christopher A. Wood, IETF TLS Working Group co-chair and, formerly, engineer at Apple.

[E2] Letter of support from Adam Langley, Principal Software Engineer, Google.

[E3] Letter of support from Eric Rescorla, editor of TLS 1.3 specification and Chief Technology Officer for Firefox, Mozilla.

[E4] Letter of support from Nick Sullivan, Head of Research at Cloudflare.

[E5] Google announcement concerning intent to deprecate RC4, 01/09/2015: https://groups.google.com/a/chromium.org/forum/#!msg/security-dev/kVfCywocUO8/vgi_rQuhKgAJ

[E6] Microsoft announcement concerning end of support for RC4, 01/09/2015: https://blogs.windows.com/msedgedev/2015/09/01/ending-support-for-the-rc4-cipher-in-microsoft-edge-and-internet-explorer-11/

[E7] Mozilla announcement of plan to end support for RC4, 01/09/2015: https://groups.google.com/forum/#!topic/mozilla.dev.platform/JIEFcrGhqSM/discussion

[E8] A. Popov, “Prohibiting RC4 cipher suites”, RFC 7465 (February 2015): https://tools.ietf.org/html/rfc7465

[E9] NIST Special Publication 800-52 Revision 1, ‘Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations’ (April 2014) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

[E10] PCI SSC Bulletin on impending revisions to PCI DSS, PA-DSS (13/02/2015): https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revisions_SSL_update.pdf).