Institution: Royal Holloway, University of London

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: Cryptographic Analysis and Improvement of Transport Layer Security (TLS)

1. Summary of the impact (indicative maximum 100 words)

By default, Internet traffic is vulnerable to eavesdropping and modification. TLS is a protocol that has become the *de facto* method for securing application-layer messages. TLS is implemented in all major web browsers and servers and is used daily by hundreds of millions of people for applications such as e-commerce, social networking and Internet banking. Royal Holloway researchers identified flaws in the way in which TLS encrypts data, resulting in practical attacks that compromised the security goals of TLS. The researchers also helped major vendors, such as Google, Microsoft and Oracle, to assess and develop countermeasures to the attacks.

2. Underpinning research (indicative maximum 500 words)

Since 2005, Prof. Paterson of the Information Security Group at Royal Holloway has studied the extent to which protocols designed to secure Internet traffic succeed in achieving their respective objectives. Many network applications (including, but by no means limited to, e-banking, e-commerce, social networking, and communications and system control) depend on the security guarantees provided by protocols such as IPsec, SSL/TLS and SSH. Thus the exploitation of any vulnerability in these protocols could have significant adverse consequences. Furthermore, these protocols and their many configuration options have not been scrutinized with the same level of rigour and detailed analysis as would be expected in leading edge academic research on cryptography.

Paterson and his PhD students began a systematic analysis of IPsec and SSH, publishing a number of influential papers in the period 2006 to 2010 identifying exploitable flaws in these protocols. TLS then became a natural target for Paterson's attention. To date, he has co-authored a series of three papers on TLS [1,2,3], all in high-quality conference venues, with [2] winning a Distinguished Paper Award at NDSS 2012.

In the first paper in the series [1], Paterson, working with US cryptographers Ristenpart and Shrimpton, showed that, provided TLS is implemented carefully so as to remove timing attacks (a special class of attack exploiting information leaked through the running time of cryptographic algorithms), the encryption scheme used by TLS to provide confidentiality is in fact sound. This is despite TLS using a rather non-standard construction for its encryption.

The second paper [2], written with Paterson's PhD student AlFardan, provided a security analysis of DTLS, a close relative of the TLS protocol. It showed that the leading OpenSSL implementation of DTLS had not been properly protected against known timing attacks. This result was surprising, given the prominence of the implementation and the expectation that, since the known attacks were well publicised, all implementations should by now be immune to them.

The final paper [3] demonstrated that even when all the standardised countermeasures against known attacks were deployed, TLS was still vulnerable to attacks breaking the confidentiality of its encryption scheme. The attacks, called "Lucky 13", arise from the fact that TLS uses a MAC-then-pad-then-encrypt construction, so that the exact processing time for packet decryption depends on how much of it is message and how much of it is padding. This is used in the attack to force the implementation to leak information about the plaintext via the running time of the decryption process; in turn this information leaks via the time at which TLS error messages appear on the network. The Lucky 13 attacks led directly to the impacts described below.

The research has had an immediate impact on improving the security of the TLS. It has also helped to promote a new approach to the design and analysis of secure protocols. In particular, Paterson co-organised two research workshops in 2012 and 2013 (at Cambridge and Stanford) designed to bring together researchers who work in theoretical aspects of cryptography with people working on standardization and in industrial deployment of cryptography. The first had an

attendance of more than 100, the second over 300. In both cases, roughly half the audience was from industry.

3. References to the research (indicative maximum of six references)

Key research outputs:

1. K.G. Paterson, T.E. Shrimpton and T. Ristenpart, Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol. In *D.H. Lee and X. Wang (eds.), ASIACRYPT 2011*, Lecture Notes in Computer Science Vol. 7073, pp. 372-389, Springer, 2011.
2. N.J. AlFardan and K.G. Paterson, Plaintext-Recovery Attacks Against Datagram TLS. In *Network and Distributed System Security Symposium (NDSS 2012)*. (Winner of Google Distinguished Paper Award.)
3. N.J. AlFardan and K.G. Paterson, Lucky 13: Breaking the TLS And DTLS Record Protocols. *IEEE Symposium on Security and Privacy 2013*, pp. 525-540, IEEE Computer Society, 2013. Available from www.isg.rhul.ac.uk/tls

Research grant:

- Kenneth G. Paterson (PI), "Cryptography: Bridging Theory and Practice", Leadership Fellowship award from EPSRC, 2010-2015, value £1,239,094.

Evidence of quality:

- The above-referenced papers appear in competitive conferences in the information security/cryptography area. Acceptance rates: Asiacrypt 2011: 15%; IEEE Security and Privacy 2013: 12%; NDSS 2012: 18% (http://icsd.i2r.a-star.edu.sg/staff/jianying/conference-ranking.html).
- Paper [2] was one of two awarded a Google Distinguished Paper Award at NDSS 2012. It was also awarded a "best elevator pitch" prize at the 2012 GCHQ Academic Centres of Excellence in Cybersecurity Conference.
- The EPSRC Leadership Fellowship scheme is a highly competitive national scheme. In the year of the award to Paterson, there were over 600 applicants to this scheme and its sister scheme (Career Acceleration Awards) and 41 awards were made.

4. Details of the impact (indicative maximum 750 words)

Who benefits? Just about everything that we do on the Internet, including e-commerce, website logins and e-mail relies for its security on TLS, so a vulnerability in TLS has a blanket impact, affecting users, 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 2.4 billion (2012) Internet users, which includes the 2.2 billion email users and the 600 million+ website owners, as well as the companies that provide service hosting solutions and the service providers that run them. The global scale of TLS deployment is confirmed in paragraph 2 of the letter of support from the Director, Security and Cryptography at Microsoft Research. He states "As TLS is used so widely, research results concerning the security of the TLS protocol (both positive and negative) are particularly valuable to the security community."

How do they benefit? The global annual value of e-commerce alone has been estimated at several trillions of USD. 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. As noted further in the supporting letter from Microsoft Research, "Given the significance of the Lucky 13 vulnerability, responsible disclosure of the vulnerability to the major implementations of TLS was critical to keeping users worldwide safe from exploits of the vulnerability." The longer-term beneficiary is the emerging electronic society at large, which will benefit from having more secure, and therefore more

confidence-inspiring, systems.

What is the link between the research and the benefit? The research itself identifies vulnerabilities in TLS, which if exploited would seriously undermine the security of Internet services, leading to fraud and data theft. In a letter of support from the Security Area Director of the Internet Engineering Task Force (IETF), writes that the research "not only extended the state of the art in cryptographic research, but also represented a real threat to the security of TLS." This direct link is confirmed in the letter from Microsoft Research where it is stated that the work "demonstrated a real, credible and actionable timing channel attack on TLS".

The research team developed practical exploits, so that the problems could be better communicated to influential parties in industry and government. The research also identified mitigation strategies to limit the exploitability of the vulnerabilities. Paterson and his collaborator worked directly with large companies and organisations that maintain open-source implementations of TLS to help them develop and test patches ahead of the public announcement of the research. The IETF Security Area Director writes "Professor Paterson's approach to informing the IETF about his work and helping to repair the protocol was commendable. It set a new benchmark for how academics can work with the IETF to responsibly disclose vulnerabilities". As a result of this approach, the majority of affected vendors were able to issue patches on the same day as, or within a few days of, the research being made public on February 4th 2013. The breadth of the impact is confirmed in the letter from Microsoft Research: "updates to OpenSSL, GnuTLS, and other major TLS implementations were required, and these patches triggered a wave of patches to software and operating systems from Apple, Debian, HP, Redhat, SUSE, Oracle, IBM, and others".

As specific examples, the following organisations deployed patches:

- OpenSSL (as used in Apache, the world's leading web server by use: over 50 million websites use Apache as of March 1st 2013, including youtube, Wikipedia and linkedin),
- Mozilla NSS (as used in Google's Chrome and Mozilla's Firefox web browsers, between them, accounted for 79% of all web browsing in January 2013).
- Oracle, who issued a special critical patch to their Java software to address the attacks.
- Google: their Senior Staff Software Engineer and a prominent TLS expert who maintains Google's TLS implementation writes in his letter of support "By minimising the window of exploitation, the benefits of the research to users of TLS were maximised" and "Their approach to working with Google to resolve the security issue in SSL/TLS was exemplary".

In short, the research has led to security improvements in protocols and systems used by the majority of the world's Internet users. The research will have impact in the longer-term – as noted by the co-chair of the TLS Working Group at the IETF, in his letter of support: "Dr. Paterson's research has lead directly to a re-evaluation of the algorithms in use by TLS implementations and is likely to lead to specification changes to further harden TLS".

5. Sources to corroborate the impact (indicative maximum of 10 references)

Between them, these letters corroborate the novelty and real-world impact of the research, and confirm the direct link between the research and its impact:

- Letter of support from the IETF Security Area Director.
- Letter of support from the Director, Security and Cryptography, Microsoft Research.
- Letter of support from the Senior Staff Software Engineer, Google Inc.
- Letter of support from the co-chair TLS working group at IETF.

To corroborate the widespread and immediate actions taken by the industry as a direct result of Prof Paterson's research being made public:

- OpenSSL security advisory: http://www.openssl.org/news/secadv_20130205.txt

- Mozilla NSS security advisory:
  https://developer.mozilla.org/en-US/docs/NSS/NSS_3.14.3_release_notes
- Oracle security advisory:
  http://www.oracle.com/technetwork/topics/security/javacpufeb2013update-1905892.html
- Common Vulnerabilities and Exposures database entry for Lucky 13 attack, listing affected products and vendors:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169