Institution: Royal Holloway, University of London

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: Analysis of IT Security Techniques for International Standardisation

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

The development of any substantial security system is informed by international standards. In particular, system designers refer to these standards when deciding which cryptographic primitives and what key sizes to use. Thus it is essential that the guidelines and best practice published in standards are accurate and robust. Of the official standards bodies concerned with security, the most influential is ISO. Prof. Chris Mitchell has been a UK representative expert to ISO since 1992. His research has led to a number of important amendments to ISO standards and he has played a major role in drafting (and maintaining) those standards.

2. Underpinning research (indicative maximum 500 words)

Prof. Chris Mitchell has worked in the Information Security Group at Royal Holloway since 1990. His work with standardisation bodies dates back to 1988 when he worked at HP Laboratories. In 1992 he was selected as a UK expert representative to the international ISO body. Mitchell's work on standardisation committees motivated academic research assessing the quality of existing standards and "standards-track" proposals. ISO now refers to the resulting security standards research thread as *The Analysis of IT Security Techniques for International Standardisation*.

Message authentication codes (MACs) are a form of "cryptographic fingerprint", computed by the sender of a message and used by the recipient to verify that the message has not been modified in transit. As such, MACs play an extremely important role in security protocols. The security of a MAC rests solely on the assumption that only the sender and the receiver know the cryptographic key used to generate it. An attacker can always try to recover a cryptographic key by brute force, but such attacks can be rendered infeasible if a suitable key size is chosen.

Thus, it is important that an attacker has no strategy for recovering a key that is significantly faster than brute force. Mitchell and his co-authors demonstrated a number of flaws in the RMAC [4] and MacDES [2,3] algorithms, both of which were considered for inclusion in international standards. These flaws lead to a key recovery attack that is significantly quicker than brute force. It is also possible that an attacker may gain an advantage if he is able to *forge* a MAC: that is, to compute (without knowledge of the key) a MAC that will be accepted by the verifier. Mitchell and co-authors demonstrated forgery attacks against MacDES [2,3].

It is very common for two parties, who have had no prior communication, to wish to communicate securely over the Internet. Thus, *key agreement protocols* are a vital part of internetwork communication and are a core component of all security standards. Mitchell et al. demonstrated that many key agreement protocols are inherently unfair, in the sense that one of the protocol participants has an undue influence on the key that is generated by the protocol [5]. This may be important if one of the protocol participants has malicious objectives. The authors also suggested a simple modification to the affected protocols that would eliminate the problem.

The final piece of research showed that many protocols in international standards are vulnerable to *parsing ambiguity attacks* [1]. Informally, these attacks arise because protocol specifications are not sufficiently specific about the format of messages, enabling an attacker to manipulate the contents of messages from previous protocol runs and inject the resulting messages into new protocol runs, thereby compromising the goals of the protocol. The research highlights the need for precision in the definition of protocol specifications, so that developers are able to develop robust implementations of the protocols.

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

References [2], [4] and [5] in particular, indicate the quality of the under-pinning research.

[1] L. Chen and C. J. Mitchell, 'Parsing ambiguities in authentication and key establishment protocols', *Journal of Electronic Security and Digital Forensics*, **3 no. 1** (2010) 82-94.

[2] D. Coppersmith, L. R. Knudsen and C. J. Mitchell, 'Key recovery and forgery attacks on the MacDES MAC algorithm', in: M. Bellare (ed.), *Advances in Cryptology - Proceedings of Crypto 2000*, August 2000, Springer-Verlag (**LNCS 1880**), Berlin (2000), pp.184-196.

[3] D. Coppersmith and C. J. Mitchell, 'Attacks on MacDES MAC Algorithm', *Electronics Letters*, **35** (1999) 1626-1627.

[4] L. R. Knudsen and C. J. Mitchell, 'Partial key recovery attack against RMAC', *Journal of Cryptology*, **18** (2005) 375-389.

[5] C. J. Mitchell, M. Ward and P. Wilson, 'Key control in key agreement protocols', *Electronics Letters*, **34** (1998) 980-981.

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

Many systems that require communication over an internetwork and the Internet, in particular, require robust cryptographic mechanisms. Typically, a large-scale system or application may be designed to last for 20-30 years, and cryptographic mechanisms are expected to be resilient to changes in the capabilities of attackers and hardware. Good practice demands that systems developers refer to international standards, particularly where issues of interoperability and security are concerned. In short, the impact of a change to a standard is, therefore, far-reaching and long-lasting. We now discuss the impact of Mitchell's research on international standards. In brief:

- the analysis of RMAC [4] and of MacDES [2,3], which disproved the originally anticipated security benefits, led to a revision of ISO/IEC 9797-1 [6].
- the analysis of a Diffie-Hellman key agreement mechanism [5] necessitated changes to the ISO/IEC 11770-3 standard [10-12] (which now references Mitchell's work – reference 19 in the bibliography of ISO/IEC 11770-3:2008 [11] is the same as [5] above, and is cited on page 10);
- the analysis of entity authentication protocols [1], first published as a preprint in 2008 (http://eprint.iacr.org/2008/419), resulted in ISO asking Mitchell to correct six standards documents [7-12].

Evidence of the relevance of Mitchell's research to, and its impact on, security standards includes the fact that Mitchell was the winner of the prestigious IEC (International Electrotechnical Commission) 1906 award for outstanding contribution to standardisation (in 2010). The impact of this case-study research is now further discussed under two categories; MACs and Entity Authentication/Key sharing.

A MAC is a fundamental cryptographic mechanism used in almost all security systems and protocols to ensure the integrity of the received data and to authenticate (confirm the identity of) its source. If a standardised MAC is ineffective then messages (that are assumed to be invulnerable to tampering) may be maliciously modified and accepted as genuine. Without a reliable MAC, a party can neither rely on the data it receives nor the identity of the entity that (claimed to have) sent it. Given that MACs are an integral part of security protocols such as SSL and every system that employs symmetric cryptography, the existence of a flaw in a MAC algorithm could have very serious consequences. In the global financial world alone such a flaw could jeopardise the trillions of dollars of e-commerce transactions. If we consider the UK, there were 164 million payment

cards in 2012 accounting for transactions totalling £474 billion (UK Cards Association). In the UK banking industry there were 7 billion inter-bank transfers, of which 6.3 billion were electronic and reliant on cryptographic protocols.

Mitchell's research discovered a flaw in the RMAC mechanism that was being standardised by the National Institute of Standards and Technology (NIST). As a direct result, NIST removed RMAC from the standard in 2005. MacDES had been proposed as an improvement to existing MAC mechanisms with the expectation that companies/governments would eventually migrate to the 'improved' solution. Mitchell showed that the security properties of MacDES were no better than earlier mechanisms, thereby saving organisations from performing extremely costly and unjustified system upgrades, and avoiding damage to ISO's credibility. The current version of ISO/IEC 9797-1 [6], published in 2011, continues to include references to Mitchell's research on attacks against MACs: references [17] and [18] in the bibliography of ISO/IEC 9797-1:2001 correspond to [2] and [3] above, and are cited on page 33 of ISO/IEC 9797-1:2011; other influential work by Mitchell is listed in the 9797-1 biography as [22] and [23], which are cited on page 32. In summary. Mitchell's contribution to our understanding of MAC algorithms and their vulnerabilities over the last 15 years has led to substantial improvements to international standards, thereby having a wide and lasting impact on the development of secure ICT systems.

Entity authentication and key agreement mechanisms are fundamental aspects of secure communication, both being a prerequisite to the establishment of a secure cryptographic channel. These mechanisms are particularly important for communication over an internetwork, when the communicating parties may not share a cryptographic key in advance. Thus, the correctness of entity authentication and key agreement protocols benefits all users of the Internet and is vital in the growing machine-to-machine communications market. If entity authentication fails then a protocol participant cannot verify the identity of the party with which it is communicating. Flaws in authentication allow for impersonation attacks, such as fake e-commerce web sites, phishing, and identity and data theft. Moreover, if the key agreement mechanism is flawed, then transmitted data (which could include PINs, passwords, personal and financial details) may be accessible to attackers.

The ISO/IEC 9798 standard is the most influential standard for authentication protocols. Mitchell's research determined that there were significant vulnerabilities in these protocols (a fact missed by many other experts) and, as a result, was asked to make changes to parts 2, 3 and 4 of this standard and also to parts 2, 3 and 4 of ISO/IEC 11770 to remove the vulnerabilities. In separate work, Mitchell also discovered that part 3 of ISO/IEC 11770 did not describe a valid/precise use of the Diffie-Hellman key exchange protocol. Mitchell was asked to provide correct guidance for the use of the key exchange protocol and his research is referenced within the current standard. This has resulted in the publication, in 2009 and 2010, of technical corrigenda to parts 2—4 of both ISO/IEC 9798 [7-9] and 11770 [10-12].

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

Source [6] corroborates the impact of Mitchell's research on MAC algorithms [2-4]; sources [7-12] corroborate the impact of Mitchell's research on authentication protocols [1,5].

[6] ISO/IEC 9797-1:2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block (revision of ISO/IEC 9797-1:1999) cipher.

[7] ISO/IEC 9798-2:2008/Cor1:2010. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.

[8] ISO/IEC 9798-3:1998/Cor1:2009. Information technology – Security techniques – Entity

authentication – Part 3: Mechanisms using digital signature techniques.

[9] ISO/IEC 9798-4:1999/Cor1:2009. Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.

[10] ISO/IEC 11770-2:2008/Cor1:2009. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric techniques.

[11] ISO/IEC 11770-3:2008/Cor1:2009. Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.

[12] ISO/IEC 11770-4:2006/Cor1:2009. Information technology – Security techniques – Entity authentication – Part 4: Mechanisms based on weak secrets.