Taxonomy of Man-in-the-Middle Attacks on HTTPS

Shaun Stricot-Tarboton
Cyber Security lab,
University of Waikato
Hamilton, New Zealand

Sivadon Chaisiri
Cyber Security lab,
University of Waikato
Hamilton, New Zealand

Ryan K L Ko
Cyber Security lab,
University of Waikato
Hamilton, New Zealand

***Abstract*—With the increase in Man-in-the-Middle (MITM) attacks capable of breaking Hypertext Transfer Protocol Secure (HTTPS) over the past five years, researchers tasked with the improvement of HTTPS must understand each attacks characteristics. However with the large amount of attacks it is difficult to discern attack differences, with out any existing classification system capable of classifying these attacks. In this paper we provide a framework for classifying and mitigating MITM attacks on HTTPS communications. The identification and classification of these attacks can be used to provide useful insight into what can be done to improve the security of HTTPS communications. The classification framework was used to create a taxonomy of MITM attacks providing a visual representation of attack relationships, and was designed to flexibly allow other areas of attack analysis to be added. The classification framework was tested against a testbed of MITM attacks, then further validated and evaluated at the INTERPOL Global Complex for Innovation (IGCI) with a forensic taxonomy extension, and forensic analysis tool.**

Keywords*—*HTTPS, TLS, SSL, Man-in-the-Middle, taxonomy, communications security, classification framework, cyber security.

I. Introduction

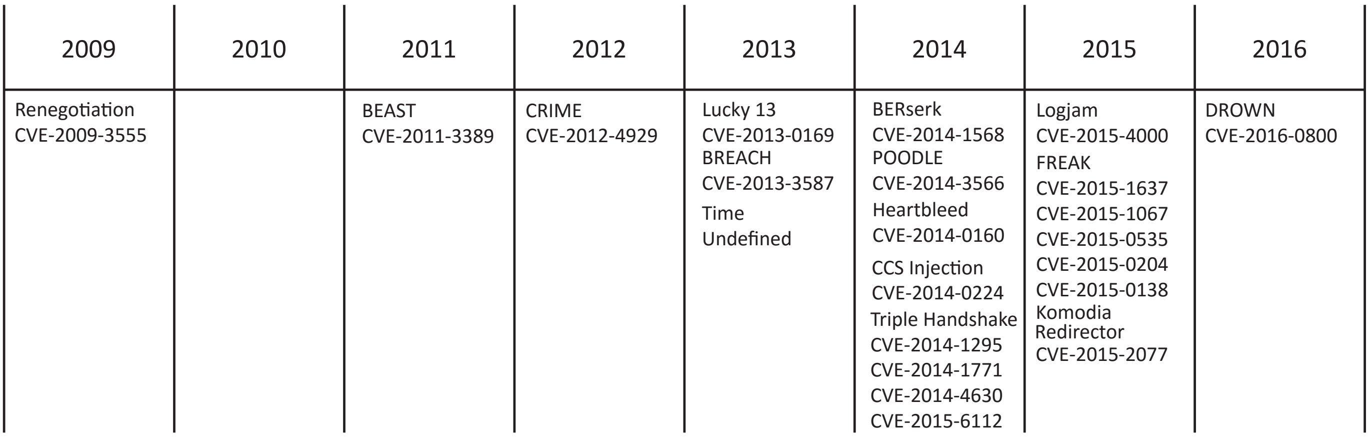
Online transactions and communications are reliant on the connection between client and server being secure. This has led to HTTPS becoming synonymous with online security, due to its simple layering of HTTP on top the older SSL or the more recent TLS protocols. The HTTPS protocol is stated to provide cryptographic strength to web servers and corresponding web sites [1], with the latest version of TLS standards also stating that it is designed to prevent eavesdropping, tampering, and message forgery [2]. However, the HTTPS protocol, and consequently the SSL/TLS protocols, have historically been compromised by many different types of MITM attacks and have been subject to more recent attacks as well. A survey of the most popular websites by the cloud security and compliance company *Qualys* (April 2016) found that 58.3% of websites have inadequate security and support insecure versions of SSL/TLS [3]. Attackers can use a MITM attack to decrypt secure communications leading to the compromise of user credentials, private keys, and any other encrypted data sent over the network. This is very concerning as the widespread adoption of HTTPS as best practice for securing websites, and having users becoming accustomed to the use of HTTPS, may lead to a false sense of security. In most cases, the client and server may never be aware that their security has been compromised, and that an attacker has complete control over the information crossing the network. Therefore, it is important to understand the manner in which these attacks are implemented and what can be done to mitigate them.

The objective of this research project is to help improve HTTPS and SSL/TLS protocols by providing an understanding of MITM attacks against HTTPS. Providing an understanding of MITM attacks can be accomplished by developing a classification framework that can be used to identify, analyse, and classify MITM attacks into a taxonomy. Using this MITM attack taxonomy, users will be able to quickly understand how attacks are implemented and allow for faster mitigation of new or existing MITM attacks. This will allow future implementations of HTTPS and SSL/TLS protocols to become more resilient to MITM attacks, by mitigating the identified vulnerabilities associated with the attack implementations.

II. Related Works

The primary focus of this research project is MITM attacks against the HTTPS protocol. The use of SSL/TLS within HTTPS is designed to prevent eavesdropping, tampering, or message forgery [4], [5], [6], [2]. However, historically there have been several security issues with the layering of the SSL/TLS protocols on top of HTTP to create HTTPS. In 1999, the authentication for HTTP was stated to be vulnerable to MITM attacks where the attacker could eavesdrop on communications between clients and servers [7]. This vulnerability was then carried over to HTTPS, which was rendered insecure due to underlying HTTP authentication [8]. In both of these scenarios, the attacker would be able to modify the communications to support weak authentication, or remove authentication entirely. A study conducted in 2005 suggested that HTTPS provided little real protection against MITM attacks, and that the actual insecurity of existing browsers was largely due to the user's interaction [9]. Since the introduction of HTTPS, communications have become more secure with each new version of SSL/TLS. This is largely due to the use of more advanced encryption methods as best practice for websites using HTTPS. A study of advanced encryption methods used in web servers between February 2005 to November 2006 showed a general positive trend in the adoption of strong key sizes. It also showed that 85% of surveyed web servers supported the insecure SSL 2.0 protocol [10]. In both of these studies, the researchers identified that insecure protocols could allow attackers to bypass advanced encryption methods using MITM attacks. Although these studies are ten years old, flaws still exist in current versions of the SSL/TLS protocols [11], [12], used to implement a variety of MITM attacks [13], [14].

As can be seen in the Fig. 1, MITM attacks have progressively become more numerous over the past five years with the majority of known MITM attacks occuring in 2014 and 2015. With such a large number of attacks occurring identifying characteristic differences in MITM attacks and their



2009	2010	2011	2012	2013	2014	2015	2016
Renegotiation CVE-2009-3555		BEAST CVE-2011-3389	CRIME CVE-2012-4929	Lucky 13 CVE-2013-0169 BREACH CVE-2013-3587 Time Undefined	BERserk CVE-2014-1568 POODLE CVE-2014-3566 Heartbleed CVE-2014-0160 CCS Injection CVE-2014-0224 Triple Handshake CVE-2014-1295 CVE-2014-1771 CVE-2014-4630 CVE-2015-6112	Logjam CVE-2015-4000 FREAK CVE-2015-1637 CVE-2015-1067 CVE-2015-0535 CVE-2015-0204 CVE-2015-0138 Komodia Redirector CVE-2015-2077	DROWN CVE-2016-0800

Fig. 1. Timeline of MITM attacks with Common Vulnerabilities and Exposures identifiers

relation to other MITM attacks is difficult without the use of a classification system. There are several existing examples when considering the classification or categorisation of cyber attacks. However, the majority of related works tend to either develop a classification system too broad to be useful in the understanding of MITM attacks characteristics, or with a overly specific focus on a particular system or cyber attack.

An example of an existing classification systems is the computer and networks incidents taxonomy [15] which is based of a taxonomy of computer and network attacks developed by the same researcher [16]. The incidents taxonomy identifies attackers, tool, vulnerability, action, target, unauthorised result, and objectives as the main classification categories. These taxonomies provides a good framework for incident or attack classification, however they lack the depth needed to understand the attacks. As an example of this is the vulnerability category, which identifies design, implementation, and configuration as possible attack classifications. These three classifications are applicable to a majority of attacks however, when classifying MITM attacks on HTTPS these vulnerabilities are not helpful in identifying the actual vulnerable areas. These taxonomies were later revised to update the classifications within the categories, including vulnerability [17], [18]. However these revisions were not significant enough to provide a deep understanding of MITM attack characteristics. Other generic taxonomies include a taxonomy of operational risk [19], a taxonomy of network and computer attacks [20], and a taxonomy of computer attacks with applications to wireless networks [21]. Although these taxonomies provide a good framework for classifying a variety of attacks they are limited by their capability to identify specific attack characteristics. Existing taxonomies that are capable of identifying specific characteristics, include a taxonomy of computer worms [22], Distributed Denial-of-Service attacks [23] and a taxonomy of cyber attacks on Supervisory Control and Data Acquisition Systems [24]. However, these taxonomies are too narrow to be used to classify MITM attacks unlike the generic taxonomies. These related works, provide a basis upon which a classification system can be developed to provide the necessary depth needed to understand and adequately identify characteristic differences in MITM attacks with relation to other MITM attacks.

III. Taxonomy of Man-in-the-middle Attacks

A. Methodology

From the related works, it is apparent that current area of cyber security research lacks a suitable MITM classification system that can identify and classify MITM implementation characteristics. The development of a classification system specifically for MITM attacks would be sufficient, however it would inherently suffer the same limitations as existing classification systems. The issue with the majority of existing classifications systems is that they either distinctly lack the flexibility needed to classify a range of attacks, or lack the depth needed to provide an understanding of MITM attack. In order to address these issues the proposed classification framework incorporates both broad and specific categories of classification which are capable of being applied to a range of attacks, including MITM attacks. This classification system will provide the necessary depth and understanding of MITM attack implementations against HTTPS, while allowing categories to remain relatively flexible to accommodate other attack types. The approach for developing a flexible classification framework that can be applied to a range of cyber attacks, including MITM attacks, requires that the classification system be based upon common attack characteristics. The stages required to develop this classification framework are outlined as follows:

1) Research
    - Identify historical issues with HTTPS
    - Define MITM attacks
    - Analysis of related works and existing taxonomies
2) Planning
    - Define classification framework
    - Gather list of MITM attack on HTTPS
3) Development
    - Identify broad attack characteristics
    - Identify specific MITM attack characteristics
    - Define broad classifications
    - Define specific classification
    - Place categories in hierarchical order based on implementation necessity

4) Testing
   - Test classification framework with identified MITM attacks
5) Validation and evaluation
   - Classification framework extension
   - Classification framework technical application

In the initial research stage, it is necessary to understand the historical issues with HTTPS, before defining MITM attacks and researching related works. Within this stage, the idea for developing a classification framework was established after the discovery that no existing classification system could effectively classify MITM attacks. A planning stage is needed to define the classification categories that will be developed in the next stages. For this research project it was decided that the developed classification framework would provide three generic categories that can be used to classify any attack type, while providing a single category that has MITM specific classifications. In this case the specific category identifies the vulnerability used to implement the MITM attack. Although this single category will be developed specifically for MITM attacks, it can easily incorporate identified vulnerabilities of other attacks. As with the specific category, the three generic categories can also be modified to incorporate future additions, should new attacks require their expansion. Also in the planning stage, a list of current and historical MITM attacks should be gathered and compiled from the related works, in order to be used as test cases for the classification development and refinement. In this research project the list of MITM attacks presented in this classification framework and taxonomy were assembled from a variety of sources, with the list being initially gathered from a summary of known attacks on SSL/TLS [11], [13]. These were then cross-referenced with lists found on the Trustworthy Internet Movement website [3], and Common Vulnerabilities and Exposures website [25]. Additional attacks were added through the process of extended research into vulnerabilities that allow attackers to establish MITM attacks. The development stage identifies attack characteristics that define the broad and specific classifications that will be used in the framework. These are then ranked in order of attack implementation. After development, the classification system can be tested with the identified MITM attacks, and then validated and evaluated with an extension or technical application.

B. Man-in-the-Middle Classification

In both historical and current MITM attacks, there are several characteristics that can be identified. By identifying these unique characteristics and analysing similarities between a range of MITM attacks, a new four tiered classification framework has been developed. These four tiers, namely; *State*, *Target*, *Behaviour*, and *Vulnerability*, appear in the taxonomy in hierarchical order of precedence. The order of precedence was determined by prioritising the three broad tiers (*State*, *Target* & *Behaviour*) that are applicable to a range of cyber-attacks over the MITM specific tier (*Vulnerability*). This was to ensure that broader characteristics would appear first in the taxonomy with each tier becoming progressively more specific to an attack. As there is only one MITM specific tier, *Vulnerability*, this is given the lowest priority. The remaining broad tiers are prioritised based on key characteristics of MITM attack implementations, resulting in the *State* tier having the highest priority followed by, *Target*, and *Behaviour*. The summary of the four tiered MITM classification framework is shown in Fig. 2. The main benefit of this classification framework is its flexibility, allowing each tier to be expanded or additional tiers to be added when needed. It is important to note that each tier of classification is designed so that the classifications within the tiers are mutually exclusive. All currently identified MITM attacks possess two common characteristics, *Conditional* and *Active*. This has resulted in the MITM taxonomy seen in Fig. 3 not having the *Unconditional*, *Server*, and *Passive* classifications. These classifications are part of broad tiers of classification which are applicable to a wide range of attacks, and have been included for completion of the tiers and to avoid future confusion.

C. Tier 1 State

The first tier of the classification framework is *State*, which identifies if attacks have any conditions or prerequisites that need to be met prior to the attack implementation. This tier of classification specifically applies to the methods that an attacker uses to launch an attack. There are two classifications for this tier, *Conditional* and *Unconditional*.

1) Conditional: The *Conditional* classification is given to attacks that require certain prerequisites or conditions to be met prior to attack implementation. This classification specifically applies to the requirements that an attacker cannot change during an attack, and therefore must rely on these requirements being met prior to the attack implementation. In most scenarios, this is due to an attacker not directly having the ability to configure certain attack requirements.

2) Unconditional: The *Unconditional* classification is given to attacks that do not possess any prerequisites or conditions for attack implementation. These attacks are often self-contained and can be implemented in most scenarios. In cases where the attacker can resolve any attack requirements and successfully implement the attack, the *Unconditional* classification can be used.

D. Tier 2 Target

The second tier in the classification framework, *Target*, identifies the target of a particular attack. In most cases, the attacker will have a direct impact on the client or server, which directly indicates the MITM attack target. However, in scenarios where the attacker focuses on the sensitive information contained within an HTTPS connection, the target of the attack is not directly indicated. In these situations, the target is implied by identifying the source of the network traffic containing the sensitive information that the attacker is focused on obtaining. There are three different classifications for this tier, *Client*, *Server*, or both *Client & Server*.

1) Client: The *Client* classification is given to attacks that directly affect the client or any client side network traffic. In scenarios where the attack implementation directly affects the client or client side network traffic, and secondarily the server or server side network traffic, the classification can be used to reflect a bias towards the client. However, in most cases, it should be classified as *Client & Server*.

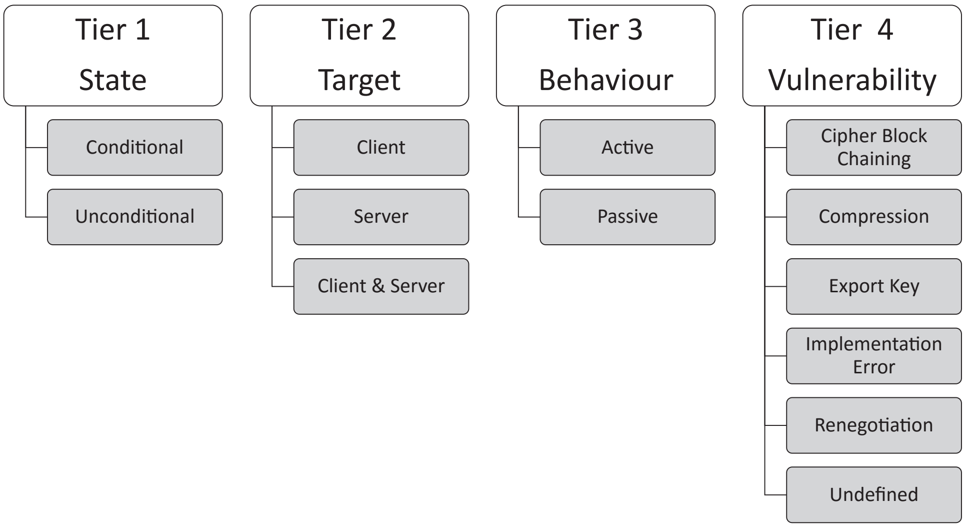


Fig. 2. Taxonomy classification summary

2) Server: The *Server* classification is given to attacks that directly affect the server or any server side network traffic. In scenarios where the attack implementation directly affects the server or server side network traffic, and secondarily the client or client side network traffic, the classification can be used to reflect a bias towards the server. However, in most cases, it should be classified as *Client & Server*.

3) Client & Server: The *Client & Server* classification is given to attacks that directly affect both the client and server side operations. This classification is also applicable to attacks that have *State* requirements in both client and server, however this is subject to how the attacks affect the client or server. In cases where the attack implementation has a clear bias towards a client or server, the attack can be given the classification based on its bias, however in most cases it is best to use the *Client & Server* classification to reflect that both sides are affected.

E. Tier 3 Behaviour

The third tier of the classification framework is *Behaviour*, which identifies the behavioural characteristics of MITM attacks. This tier of classification specifically applies to the methods used to launch an attack and the aggressiveness of these methods during the attack. There are two classifications for this tier, *Active* or *Passive*.

1) Active: The *Active* classification is given to attacks that use aggressive methods for attack implementation and execution. These attacks often require input from the attacker to carryout the attack. Characteristics of an *Active* attack include executing malicious code, altering connection settings, or exploiting a vulnerability.

2) Passive: The *Passive* classification is given to attacks that do not use aggressive methods for attack implementation and execution. These attacks are often furtive and do not require the attacker's input to carry out the attack once implemented. Characteristics of a *Passive* attack include the collection or observation of network traffic, and the analysis of data patterns.

F. Tier 4 Vulnerability

The fourth tier of the classification framework is *Vulnerability*, which identifies the vulnerabilities that attackers leverage to implement MITM attacks. This tier of classification, unlike the previous tiers, contains the *Undefined* classification which serves two purposes. The first purpose is to signify an unidentified vulnerability and the second is to allow future expansion. There are currently six classifications for this tier, *Cipher Block Chaining*, *Compression*, *Export Key*, *Implementation Error*, *Renegotiation* and *Undefined*.

1) Cipher Block Chaining: This classification applies to attacks that exploit block cipher encryption methods which have Cipher Block Chaining (CBC) as a mode of operation. Attackers can exploit inherent vulnerabilities in the CBC mode of operation to decrypt the contents of an HTTPS message.

2) Compression: This classification applies to attacks that exploit message compression. A key part of HTTPS communications is the compression of message contents to reduce resource usage. Attackers can exploit message compression by comparing size differences, allowing the inference of message contents.

3) Export Key: This classification applies to attacks that exploit export grade security keys. These keys were originally introduced to comply with United States cryptography export regulations [26], [27]. The regulations limited the strength of cryptography software with the intention that the weaker export keys could be broken by United States government agencies. However, attackers are also able to exploit these export grade security keys in order to attack the HTTPS communications and decrypt the contents of the communications.

4) Implementation Error: This classification applies to attacks that exploit an implementation error. These errors are typically the result of a poorly applied security feature or a bug in the system. Attackers can exploit these implementation errors to launch attacks.

5) Renegotiation: This classification applies to attacks that exploit the Renegotiation feature in HTTPS. Renegotiation

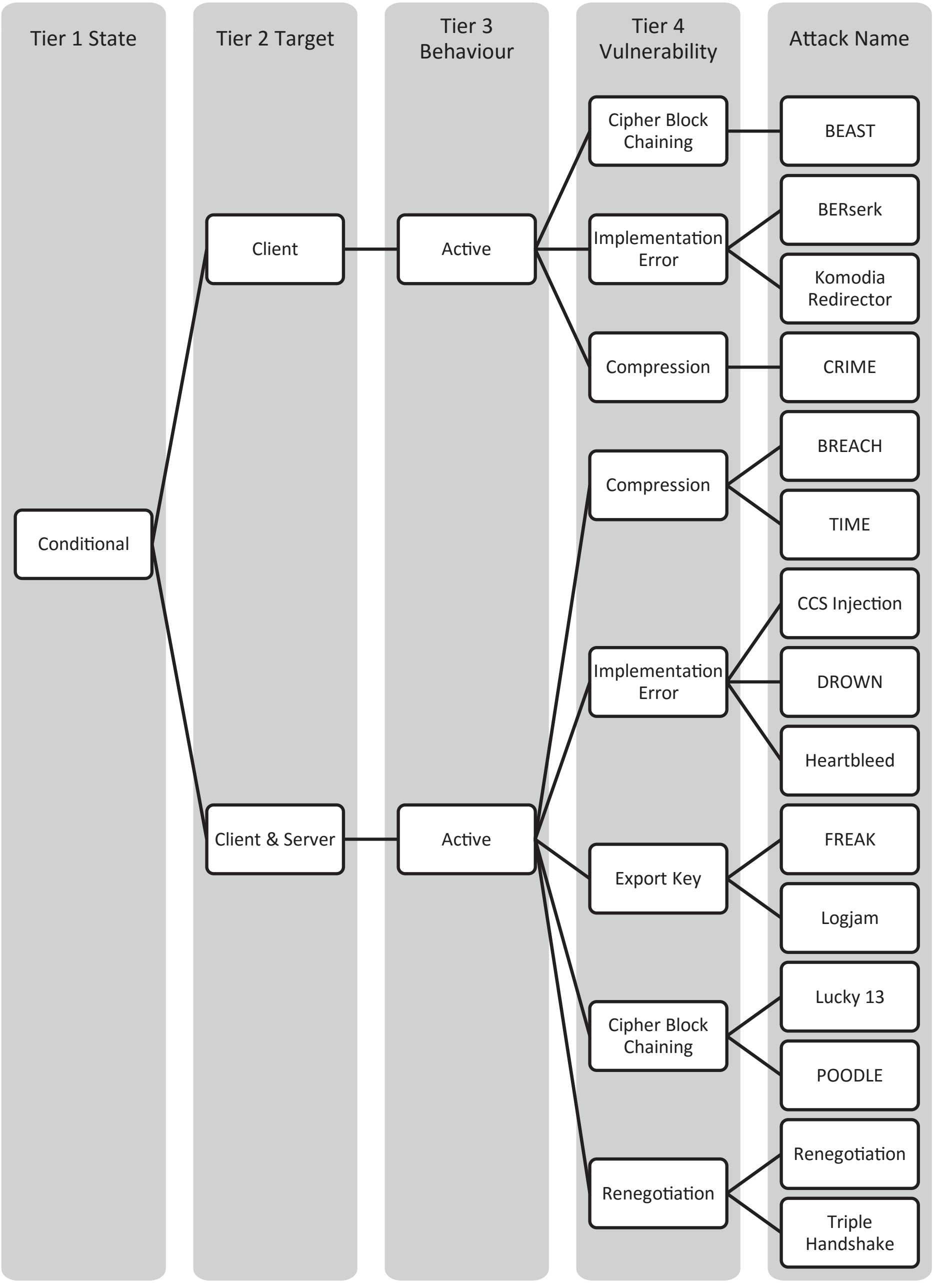


Fig. 3. Man-in-the-Middle Taxonomy of attacks

allows HTTPS connection parameters and keys to be changed in existing connections upon request. Attackers can exploit the Renegotiation feature to make their own connection and then splice another connection to use the attackers' connection settings.

6) Undefined: This classification is used to signify a vulnerability that is not included in this classification, or has not yet been identified. This classification is also a place holder for future vulnerabilities that are discovered, and allows for future expansion of the tier.

IV. Validation and Open Issues

A. Verification and Validation

The new MITM classification framework is verified and validated with the development of the Forensic Taxonomy Extension (FTE) and analysis tool ForensicTMO. The extension and tool are based on forensic requirements set out by law enforcement at the INTERPOL Global Complex for Innovation (IGCI), who provided essential input and feedback during the development process. Through the processes of developing the FTE, the flexibility of MITM classification framework has been verified and validated. In addition, the forensic analysis tool (ForensicTMO) is a tangible outcome, that provides a proof of concept for the technical application of the classification framework. The research and development of the FTE and ForensicTMO were used to help address the forensic and attribution themes, however the same process of research and development could be applied to any number of additional areas of interest. In this case, this benefits law enforcement by providing a quick preliminary analysis of cybercrime investigations. The combination of the FTE and MITM classification framework during the development process led to the creation of a high level cybercrime taxonomy, which also verifies and validates the new MITM classification framework. This high level cybercrime taxonomy shown in Fig. 4, integrates the MITM classification framework into the *Type* category of the FTE.

The cybercrime taxonomy is designed to provide the detailed attack classification offered by the MITM framework to all of the classifications that fall under the *Type* category. Each colour in Fig. 4 is of significance. Orange is used to identify the *Man-in-the-Middle* classification in the *Type* category, and the fourth tier *Vulnerability* classifications: *Cipher Block Chaining*, *Compression*, *Export Key*, *Implementation Error*, and *Renegotiation*. This is to indicate that the fourth tier classifications are specifically applicable to the *Man-in-the-Middle* classification found in the *Type* category. Further research is needed to determine if any of the currently identified fourth tier *Vulnerabilty* classifications are applicable to other attack types. Grey classifications within the first, second and third tiers of the MITM framework are designed to be applicable to other attacks types within the *Type* category. As these tiers are flexible, they allow for additions to be made when necessary. These four tiers of classification are designed to be mutually exclusive. The *Undefined* classification in the *Type*, *Vulnerability*, *Motive*, and *Offender* categories are also grey to depict they are not directly associated with a particular attack type. This classification is used to signify a classification which has not been included or identified in this category and provides each category with the flexibility to allow future classifications. The use of advanced blended and multilayer attacks was not considered until the development of the FTE. Although, it is uncommon for these advanced attacks to make use of a MITM attack, it is not impossible. Conversely, the *Trojan*, *Worm*, *Virus*, *Adware*, *Ransomware*, and *Spyware* attack types will often be blended or layered. This can be largely attributed to these attacks being representations of *Malware* or malicious software, and are coloured green in Fig. 4. Similarly to the green *Malware* attack types, the blue *Phishing* and *Spear Phishing* attack types have been grouped together as representations of *Social Engineering*. Yellow represents the *Denial-of-Service* attack type.

B. Limitations and Open Issues

There are a few limitations and remaining open issues with the MITM classification framework, FTE, and ForensicTMO, as well as with the security of HTTPS and the current versions of TLS. The open issues in relation to the security of HTTPS and the current versions of the TLS protocol, include:

- Improper use of padding in the Cipher Block Chaining mode of encryption,
- Reflected HTTPS requests inadvertently revealing message contents,
- HTTP compression of messages inadvertently revealing message contents,
- Export keys and cross-protocol support in client and server infrastructure,
- Insecure default security settings for server infrastructure, and
- Improper use of HTTPS renegotiation.

In addition, there are MITM attacks which are still currently viable on a small minority of servers due to the lack of compliance with standards of best practice, and on clients that are not using up-to-date software. Some of these MITM attacks include the BEAST, CRIME, CCS Injection, and POODLE attacks [3]. Taking all of this into consideration, the inherent issues with the current ageing HTTPS protocol has become more apparent with each new attack implementation. The release of TLS 1.3, still in development, will hopefully rectify or address some of these open issues [28].

There are also limitations with the MITM classification framework, FTE and ForensicTMO. In order to use the current MITM classification framework with advanced blended and multilayer attacks, each attack needs to be individually classified. The FTE and ForensicTMO are limited in their analysis of cybercrimes to the *Type*, *Motive*, and *Offender* categories. This means that there are scenarios where the preliminary analysis of a cybercrime returns all possible results. This is an undesirable side-effect of providing an analysis based on several historical cybercrimes, as these may have been carried out using any combination of possible types, motives or offenders. In order to reduce the selection, additional knowledge of the cybercrime is required. This falls outside the current capabilities of the FTE and ForensicTMO, and requires further research and development.

V. Conclusion and Future work

This paper has identified the increasing trend of MITM attacks against HTTPS, and the lack of existing classification systems. The development of a MITM classification framework which provides the depth of knowledge needed to effectively understand MITM attacks and the mitigation solutions for these attacks, is the main contribution of this research. The classification framework was validated and verified at the IGCI. Direct interaction with law enforcement and understanding the challenges faced during cybercrime investigations, provided the necessary motivation to extend the MITM classification framework to include areas of forensics and attribution. As a result, the FTE was then further developed into a forensic analysis tool called ForensicTMO, which provides a preliminary analysis of cybercrimes, giving an initial direction to a cybercrime investigation. The evaluation of the MITM classification framework and the FTE, when integrated together, allowed a high level cybercrime taxonomy to be developed. This cybercrime taxonomy allows the user to understand attack implementation details, while also providing broader forensic aspects that could apply to these classified attacks. This proved that the developed classification framework is flexible enough to incorporate additions needed to provide an understanding of an attack type and can be modified to meet the users' needs. The flexibility of the framework allowed it to be used

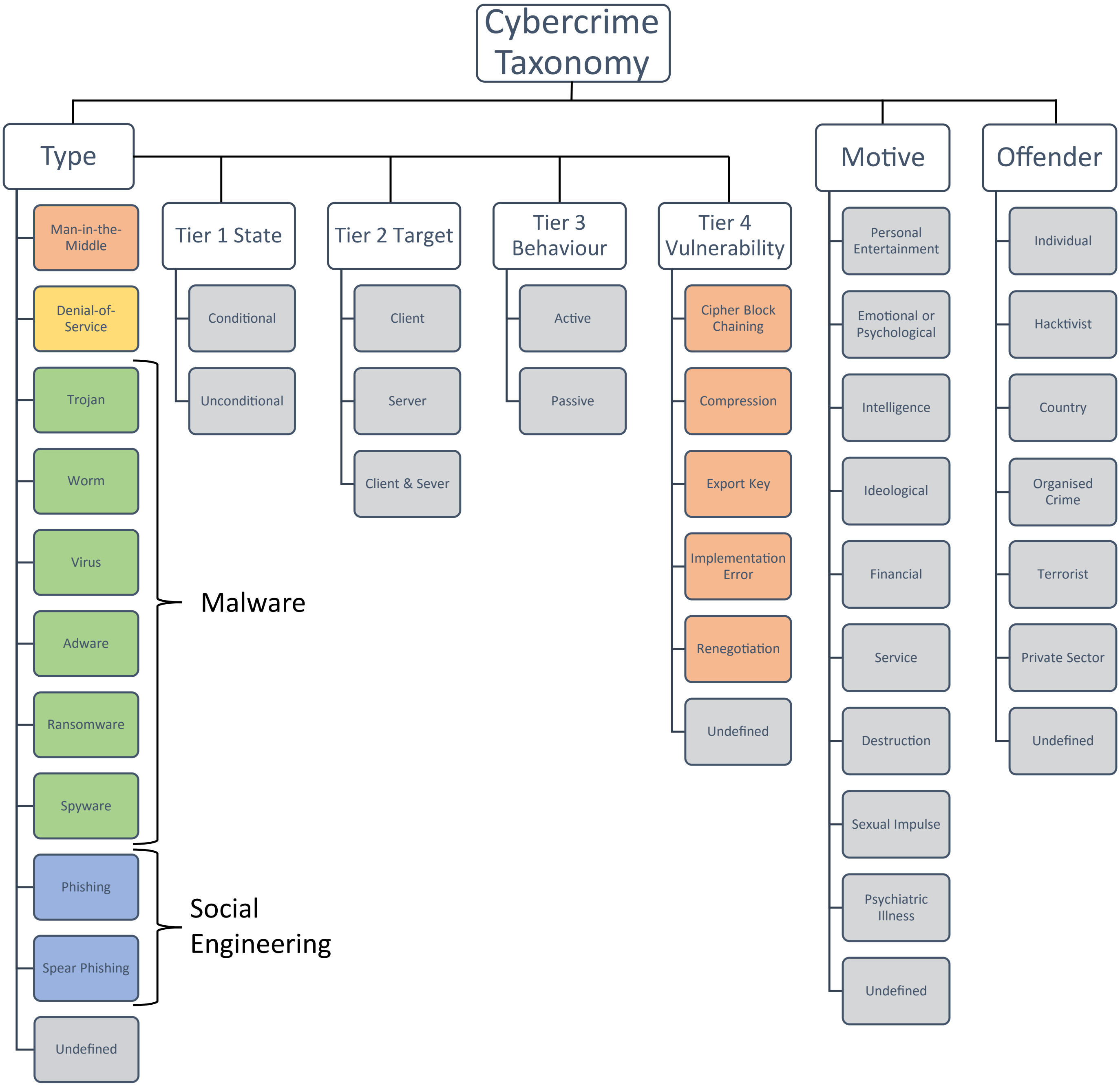


Fig. 4. High level cybercrime taxonomy showing the integration of the MITM classification framework into the FTE

as a technical solution for law enforcement. This highlights the value that this work adds to cybercrime investigations. The limitations and remaining open issues, discussed above, provide the basis for potential future areas of research and development. A future enhancement of the MITM classification framework would be to develop it into a tool that can provide a visual taxonomy of the classified attacks. The classification framework could be further developed to classify the other attack types found in the FTE. These could then be used to create a taxonomy for each attack type, when further developing the high level cybercrime taxonomy. The classification framework could be tested with the remaining attack types in the *Type* category. Finally, the FTE and ForensicTMO could be improved by identifying certain patterns in the *Type*, *Motive*, and *Offender* categories in relation to historical attacks. This would allow law enforcement to identify similar patterns in new attacks and potentially improve aspects of offender attribution.

Acknowledgements

This research is supported by STRATUS (Security Technologies Returning Accountability, Trust and User-Centric Services in the Cloud) (https://stratus.org.nz), a science investment project funded by the New Zealand Ministry of Business, Innovation and Employment (MBIE). The authors would like to thank the INTERPOL Global Complex for Innovation for feedback relating to the validation and evaluation of this taxonomy. Additionally we would like to thank the members of the Cyber Security Lab, Jeff Garae and Dr. Harris Lin, for their feedback regarding the classification framework and taxonomy of MITM attacks.

REFERENCES

[1] R. Oppliger, *SSL and TLS*. Artech House, 2009.

[2] T. Dierks and E. Rescoria, "Rfc 5246 - the transport layer security (tls) protocol version 1.2," 2008. [Online]. Available: http://tools.ietf.org/html/rfc5246

[3] Trustworthyinternet.org, "Trustworthy internet movement - ssl pulse," 2012. [Online]. Available: https://www.trustworthyinternet.org/ssl-pulse/

[4] A. Freier, P. Karlton, and P. Kocher, "Rfc 6101 - the secure sockets layer (ssl) protocol version 3.0," 2011. [Online]. Available: http://tools.ietf.org/html/rfc6101

[5] T. Dierks and C. Allen, "Rfc 2246 - the tls protocol version 1.0," 1999. [Online]. Available: http://tools.ietf.org/html/rfc2246

[6] T. Dierks and E. Rescoria, "Rfc 4346 - the transport layer security (tls) protocol version 1.1," 2006. [Online]. Available: http://tools.ietf.org/html/rfc4346

[7] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "Http authentication: Basic and digest access authentication," 1999. [Online]. Available: https://www.ietf.org/rfc/rfc2617.txt

[8] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-middle in tunnelled authentication protocols," in *Security Protocols*. Springer, 2003, pp. 28–41.

[9] H. Xia and J. C. Brustoloni, "Hardening web browsers against man-in-the-middle and eavesdropping attacks," in *Proceedings of the 14th international conference on World Wide Web*. ACM, 2005, pp. 489–498.

[10] H. Lee, T. Malkin, and E. Nahum, *'Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices*, 2007.

[11] R. Holz, Y. Sheffer, and P. Saint-Andre, "Rfc 7457 - summarizing known attacks on transport layer security (tls) and datagram tls (dtls)," 2015. [Online]. Available: http://tools.ietf.org/html/rfc7457

[12] ——, "Rfc 7525 - recommendations for secure use of transport layer security (tls) and datagram transport layer security (dtls)," 2015. [Online]. Available: https://tools.ietf.org/html/rfc7525

[13] P. G. Sarkar and S. Fitzgerald, "Attacks on ssl a comprehensive study of beast, crime, time, breach, lucky 13 & rc4 biases," *Internet: https://www.isecpartners. com/media/106031/ssl_attacks_survey. pdf [June, 2014]*, 2013.

[14] C. Meyer and J. Schwenk, "Sok: Lessons learned from ssl/tls attacks," in *Information Security Applications*. Springer, 2013, pp. 189–209.

[15] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," *Sandia National Laboratories*, 1998.

[16] J. D. Howard, "An analysis of security incidents on the internet 1989-1995," DTIC Document, Tech. Rep., 1997.

[17] S. Kiltz, A. Lang, and J. Dittmann, "Taxonomy for computer security incidents," *Cyber Warfare and Cyber Terrorism*, pp. 412–417, 2007.

[18] L. Janczewski and A. Colarik, *Cyber warfare and cyber terrorism*. IGI Global, 2007.

[19] J. J. Cebula, M. Popeck, and L. Young, "A taxonomy of operational cyber security risks version 2," 2014.

[20] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, no. 1, pp. 31–43, 2005.

[21] D. L. Lough, "A taxonomy of computer attacks with applications to wireless networks," 2001.

[22] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A taxonomy of computer worms," in *Proceedings of the 2003 ACM workshop on Rapid malcode*. ACM, 2003, pp. 11–18.

[23] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[24] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*. IEEE, 2011, pp. 380–388.

[25] Cve.mitre.org, "Cve -common vulnerabilities and exposures (cve)," 2016. [Online]. Available: https://cve.mitre.org/

[26] "Code of federal regulations, title 22: Foreign relations, chapter i: Department of state, sub-chapter m: International traffic in arms regulations, part 121: The united states munitions list, sectionsection 121.1," 1992. [Online]. Available: https://epic.org/crypto/export_controls/itar.html

[27] "Code of federal regulations, title 22: Foreign relations, chapter i: Department of state, sub-chapter m: International traffic in arms regulations, part 121: The united states munitions list, section 121.1," 2016. [Online]. Available: http://www.ecfr.gov/cgi-bin/text-idx?node=se22.1.121_11

[28] E. Rescorla, "draft-ietf-tls-tls13-12 - the transport layer security (tls) protocol version 1.3," 2016. [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-tls13-12