NETWORK FORENSIC INVESTIGATIONS OF TUNNELED TRAFFIC: A CASE STUDY

JAN PLUSKAL1, MICHAL KOUTENSKÝ1, MARTIN VONDRÁČEK1, ONDŘEJ RYŠAVÝ1

**Keywords: Network traffic forensics, Generic Stream Encapsulation, Network forensic and analysis tool**

**The increasing importance of network forensics in the investigations conducted by Law Enforcement Agencies (LEA) is indisputable. Today's internet does not carry ordinary TCP/IP traffic but utilizes many other encapsulations and tunneling protocols. In this paper, we overview the most used tunneling protocols and their features concerning digital forensic analysis. A case study of Generic Stream Encapsulation describes how the investigator can obtain encapsulated application data from within.**

**The LEA uses lawful interception [16] as a tool to obtain indisputable evidence supporting cyber criminality investigations. We intend to provide an overview of common encapsulation protocols that are commonly used on today’s internet. This may be beneficent for network forensic practitioners that are responsible for the investigation, and executives that oversee selecting appropriate network forensic tools. As we have shown [17], network forensic analysis tools tend to lack complexity and support only a limited range of tunneling protocols. We show in this paper that some tunneling protocols [7, 8, 11, 12] that are not encrypted can be easily processed and contained information that may provide great value for investigators. Also, extracting meta information from encrypted tunneling protocols** **[9, 10, 14, 15] may yield at least metainformation that can be correlated to other activities. Therefore, omitting encapsulation and tunneling protocols may lead to false evidence.**

**We provide a case study focused on the Generic Stream Encapsulation (GSE) [1, 2, 3, 4, 5, 6] protocol. The GSE may be used to carry IP network traffic [13] in satellite communication. We show that without support for GSE in network forensic analysis tools used by investigators, evidence might not be obtained.**

**References**

1. ETSI. 2011. ETSI TS 102 771 V1.2.1 - *Digital Video Broadcasting (DVB); Generic Stream Encapsulation (GSE) implementation guidelines.* European Telecommunications Standards Institute.

2. ETSI. 2014. ETSI EN 302 307-1 V1.4.1 - *Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications.* Part 1: DVB-S2. European Telecommunications Standards Institute.

3. ETSI. 2014. ETSI TS 102 606-1 V1.2.1 - *Digital Video Broadcasting (DVB); Generic Stream Encapsulation (GSE); Part 1: Protocol.* European Telecommunications Standards Institute.

4. ETSI. 2014. ETSI TS 102 606-2 V1.1.1 - *Digital Video Broadcasting (DVB); Generic Stream Encapsulation (GSE); Part 2: Logical Link Control (LLC).* European Telecommunications Standards Institute.

5. ETSI. 2014. ETSI TS 102 606-3 V1.1.1 - *Digital Video Broadcasting (DVB); Generic Stream Encapsulation (GSE); Part 3: Robust Header Compression (ROHC) for IP.* European Telecommunications Standards Institute.

6. ETSI. 2015. ETSI TR 102 376-1 V1.2.1 - *Digital Video Broadcasting (DVB); Implementation guidelines for the second generation system for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2; Part 1: DVB-S2.* European Telecommunications Standards Institute.

7. Dino Farinacci, Stanley P. Hanks, Tony Li, and Paul S. Traina. 1994. *Generic Routing Encapsulation (GRE).* RFC 1701.

8. Robert E. Gilligan and Erik Nordmark. 2005. *Basic Transition Mechanisms for IPv6 Hosts and Routers.* RFC 4213.

9. Stephen Kent. 2005. *IP Authentication Header.* RFC 4302.

10. Stephen Kent. 2005. *IP Encapsulating Security Payload (ESP).* RFC 4303.

11. Jeroen Massar. 2004. *AYIYA: Anything In Anything. Internet-Draft draft-massar-v6ops-ayiya-02.* Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-massar-v6ops-ayiya-02 Work in Progress.

12. Charles E. Perkins. 1996. *IP Encapsulation within IP.* RFC 2003.

13. Karen Seo and Stephen Kent. 2005. *Security Architecture for the Internet Protocol.* RFC 4301.

14. Andrew J. Valencia, Glen Zorn, William Palter, Gurdeep-Singh Pall, Mark Townsley, and Allan Rubens. 1999. *Layer Two Tunneling Protocol "L2TP".* RFC 2661.

15. Glen Zorn, Gurdeep-Singh Pall, and Kory Hamzeh. 1999. *Point-toPoint Tunneling Protocol (PPTP).* RFC 2637.

16. Matthew Ponsford. 2017. *The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information.* Canadian Journal of Law & Technology 15(2017), 1.

17. Jan Pluskal, Martin Vondráček, and Ondřej Ryšavy. 2019. *Network ` Forensics in GSE Overlay Networks.* In Proceedings of the 6th Conference on the Engineering of Computer Based Systems. ACM, 12.

**Number of pages: 6**

**Number of cited literature: 43**

**Number of figures: 3**

**Number of tables: 1**

Article presentation

Each article will be accompanied by a presentation on 1 page with the following content: article title, list of authors with affiliation, electronic correspondence address of the first author, extended abstract containing the article purpose, originality elements, minimal litterature cited.

They would given also the following data: number of pages, number of litterature cited, number of figures and number of tables.