

Contribution Title^{*}

First Author¹[0000–1111–2222–3333], Second Author^{2,3}[1111–2222–3333–4444], and
Third Author³[2222–3333–4444–5555]

¹ Princeton University, Princeton NJ 08544, USA

² Springer Heidelberg, Tiergartenstr. 17, 69121 Heidelberg, Germany
`lncs@springer.com`

<http://www.springer.com/gp/computer-science/lncs>

³ ABC Institute, Rupert-Karls-University Heidelberg, Heidelberg, Germany
`{abc,lncs}@uni-heidelberg.de`

Abstract. Virtual Private Network (VPN) protocols are widely used to create a secure mode of communication between several parties over an insecure channel. A common use-case for VPNs is to secure access to company networks. Therefore errors in VPN software are often severe. IPsec is a VPN protocol that uses the Internet Key Exchange protocol (IKE). IKE has two versions, IKEv1 and the newer IKEv2. While several papers have investigated IPsec-IKEv2 in the context of Automata learning, no such work has been performed for IPsec-IKEv1. In this short paper we describe the IPsec-IKEv1 protocol and show the steps taken to learn the state-machine of an IPsec server. Finally we present our learned model and discuss its potential applications.

Keywords: IPsec · Automata Learning · AALpy.

1 Introduction

VPNs are used to allow secure communication over an insecure channel. The importance of VPN software has increased dramatically since the beginning of the COVID-19 pandemic due to the influx of people working from home [1]. This makes finding vulnerabilities in VPN software more critical than ever. IPsec is a VPN protocol and most commonly uses the IKE protocol to share authenticated keying material between involved parties. Therefore, IKE and IPsec are sometimes used interchangeably. We will stick to the official nomenclature of using IPsec for the full protocol and IKE for the key exchange only. IKE has two versions, IKEv1 IKEv2, with IKEv2 being the newer and recommended version [2]. However, despite IKEv2 supposedly replacing its predecessor, IKEv1 is still in widespread use today. This is reflected by the company AVM to this day only offering IKEv1 support for their popular Fritzbox routers [3].

State models of protocol implementations are useful tools in testing. They can for example be used to compare versions and to generate test cases automatically TODO: REFERENCES!. One method of generating these models is

^{*} Supported by organization x.

to use Automata Learning. TODO: MORE ON AUTOMATA LEARNING 1-2 SENTENCES! Several papers have investigated IPsec-IKEv2 using Automata Learning, however so far none have looked at IKEv1.

We show the process of learning a state model from an example IPsec-IKEv1 server. We use the Active Automata Learning framework AALpy for model learning with a custom python interface between AALpy and the IPsec server.

In this short paper we first go over preliminary information on VPNs and Automata Learning. Then we present the used Active Automata Learning framework TODO: MAYBE ADD THIS TO PRELIMINARIES AS WELL! and discuss related works. In chapter 4 we present our custom interface between AALpy and the IPsec server and discuss design choices as well as implementation difficulties. Finally we present the learned model and discuss its potential applications and further work.

2 Preliminaries

3 Related Work

4 IPsec Interface

5 Evaluation

6 Conclusion

6.1 A Subsection Sample

Please note that the first paragraph of a section or subsection is not indented. The first paragraph that follows a table, figure, equation etc. does not need an indent, either.

Subsequent paragraphs, however, are indented.

Sample Heading (Third Level) Only two levels of headings should be numbered. Lower level headings remain unnumbered; they are formatted as run-in headings.

Sample Heading (Fourth Level) The contribution should contain no more than four levels of headings. Table 1 gives a summary of all heading levels. Displayed equations are centered and set on a separate line.

$$x + y = z \tag{1}$$

Please try to avoid rasterized images for line-art diagrams and schemas. Whenever possible, use vector graphics instead (see Fig. ??).

Table 1. Table captions should be placed above the tables.

Heading level	Example	Font size and style
Title (centered)	Lecture Notes	14 point, bold
1st-level heading	1 Introduction	12 point, bold
2nd-level heading	2.1 Printing Area	10 point, bold
3rd-level heading	Run-in Heading in Bold. Text follows	10 point, bold
4th-level heading	<i>Lowest Level Heading.</i> Text follows	10 point, italic

Theorem 1. *This is a sample theorem. The run-in heading is set in bold, while the following text appears in italics. Definitions, lemmas, propositions, and corollaries are styled the same way.*

Proof. Proofs, examples, and remarks have the initial word in italics, while the following text appears in normal font.

For citations of references, we prefer the use of square brackets and consecutive numbers. Citations using labels or the author/year convention are also acceptable. The following bibliography provides a sample reference list with entries for journal articles [?], an LNCS chapter [1], a book [?], proceedings without editors [?], and a homepage [?]. Multiple citations are grouped [?,?,?], [?,?,?,?].

Acknowledgements Please place your acknowledgments at the end of the paper, preceded by an unnumbered run-in heading (i.e. 3rd-level heading).

References

1. Abhijith, M., Senthilvadivu, K.: Impact of vpn technology on it industry during covid-19 pandemic. In: IJEAST (2020)
2. Barker, E., Dang, Q., Frankel, S., Scarfone, K., Wouters, P.: Guide to ipsec vpns (2020-06-30 00:06:00 2020). <https://doi.org/https://doi.org/10.6028/NIST.SP.800-77r1>
3. GmbH, A.C.V.: Connecting the fritz!box with a company's vpn. <https://en.avm.de/service/vpn/tips-tricks/connecting-the-fritzbox-with-a-companys-vpn/>, accessed: 2022-09-09