


Development Proposal: Security Variant of TruCol protocol

Towards a 2022 Blackhat (USA) presentation

Chihab Amghane ✉ 

Radboud University

Victoria Bosch ✉ 

Radboud University

Rashim Charles ✉ 

Radboud University

Marc Droogh ✉ 

Delft University of Technology

Clara Main ✉ 

Radboud University

Chinari Subhechha Subudhi ✉ 

Delft University of Technology

Akke Toeter ✉ 

Delft University of Technology, Radboud University

Eric van der Toorn ✉ 

Delft University of Technology

1 Introduction

This document presents a planning proposal for the development of a Trustless Security protocol with the short-term purpose of presenting the protocol during the 2022 Blackhat (USA) conference. The aim of the proposed security proposal is to help ethical hackers retrieve their bounties without ambiguity, whilst simultaneously enabling companies to show their customers how much money is staked on their open source software stacks being secure.

To explain how the protocol may help both of these stakeholders (ethical hackers and companies using open source software), we will first describe, what we think is, the status quo. Then we will explain how the protocol changes, what we think is, the status quo. This will be done in Section 2. Next, Section 3 describes strategies to specify how the protocol may be implemented. The limitations and weaknesses of our strategy and protocol are detailed in Section 4. Since we are relatively new to the field of cyber security, we would like to ask feedback on:

- The validity of our assumptions.
- The added value of this protocol in real life applications.
- Any perspectives we might have overlooked.

These questions are specified in Section 5. The information used to generate a planning towards the Blackhat presentation is included in Section 6. A brief conclusion to this proposal is presented in Section 7.

2 Protocol

To provide some context for the environment in which the proposed protocol interacts, we give some assumptions describing the status quo.



© ;
licensed under Creative Commons License CC-BY 4.0

42nd Conference on Very Important Topics (CVIT 2016).

Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:5

Leibniz International Proceedings in Informatics



LIPIC Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2.1 Assumptions

2.1.1 Ethical Hacker - perspective

1. We assume it is not always as easy and/or attractive for whitehat hackers/ethical hackers to publish an exploit and retrieve an accompanying financial reward for the publication. This assumption is based on popular media such as darknet diaries, posts on news.ycombinator.com, hackernoon and possibly other sources. This assumption is based on (a combination of) the following sub-assumptions:
 - a. Vulnerabilities may be discovered at small/non-profit software development companies that have not allocated a large budget fraction to security.
 - b. Ambiguity in the specification of the bug bounty/reward program may be interpreted in the advantage of the company during triage.
 - c. The triage process may take a relatively long time, requiring the ethical hacker to have sufficient funds to sustain living costs coverage until the pay-out.
 - d. A conservative/carefulness in the ethical hacker towards approaching the company with respect to the legality of discovering the vulnerability may hinder/slow down the vulnerability disclosure process.
 - e. The effort required to contact the company and convince them of the seriousness of the bug may consume unnecessary resources.

2.1.2 Company - perspective

1. We assume cyber security vulnerabilities become increasingly more relevant in our increasingly more digitized world. This assumption may be seen as being substantiated by for example the *Cyber Security Assessment Netherlands 2021 (CSAN 2021)* as presented by the Dutch National Coordinator Counterterrorism and Safety of the Ministry of Justice and Security. Currently there is only the Dutch version available at: <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021>. We assume that this trend can be extrapolated from a Dutch perspective to a more global perspective, given the international media coverage of for example many ransomware attacks.
2. We assume that companies are interested, or will become more interested, in showing their customers and/or stakeholders (a quantified perspective on) *how* secure their technology is. We assume it can be quite challenging to convey this perspective clearly due to the following factors:
 - a. Vulnerabilities can be found in various sections of the company, ranging from social engineering, misconfiguration to zero-day exploits. It is difficult to give customers a comprehensive yet concise/simple insight in how "secure" all these attack surfaces are.
 - b. The impact of a vulnerability may be ambiguous or not easily quantifiable. For example, for some companies, vulnerabilities may allow malicious actors to take over critical infrastructure, whilst other vulnerabilities may lead to dataleaks or other undesired side-effects.
 - c. It may be difficult to accurately assess the capabilities of malicious adversaries.
3. We assume some companies might be unfamiliar with vulnerability disclosure and accompanying triage processes, these delicate processes may seem intimidating for new companies that want to start paying attention to their cybersecurity, and this may lead to a lower allocation of cyber security budget. *Note, this assumption is based entirely on imagination, no real world evidence has been found that this is indeed the case.*

2.2 Solution

For a specific type of vulnerability, some, to all of these concerns can be alleviated. The scope/applicability of the protocol is visualised in Figure 1.

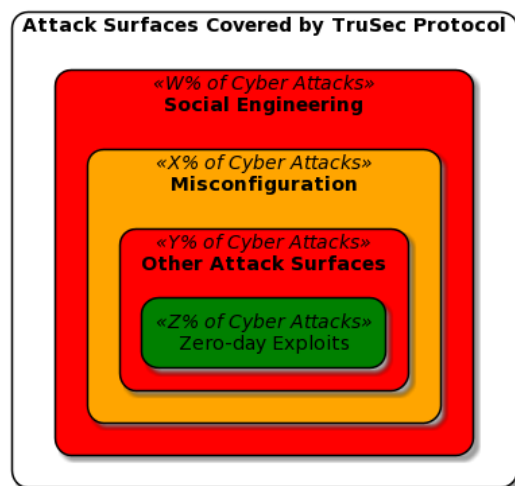


Figure 1 The proposed TruSec protocol is not suited to deal with social engineering attacks, nor is it ideal for misconfiguration exploits. Instead, it is designed to increase the rate of discovery of zero day exploits.

With this scope defined, one can look at how companies and ethical hackers interact with it. This is visualised in Figure 2.

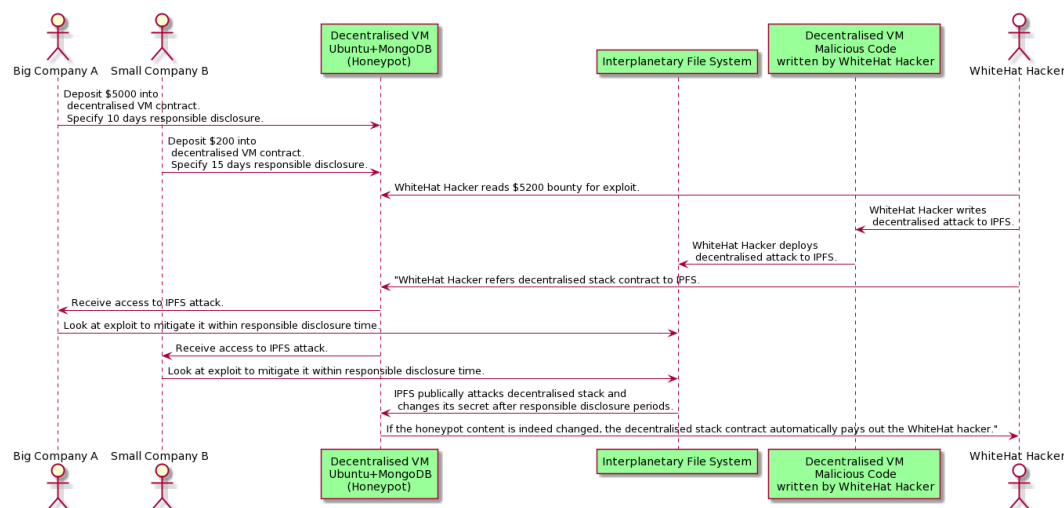


Figure 2 Rough sketch describing the interaction of the TruSec protocol. This is an ever-lasting cycle, where at the end of the process, companies can re-deploy the patched decentralised stack, and allocate new funds. Whitehat hackers can scan for new attacks.

2.3 Development Strategy

Based on our work on the TruCol protocol, we estimate that the development of a rough code POC would cost our student team between 3-10K euro. To have a somewhat acceptable

code quality POC generated by actual employees, our first cost estimates would be in the order a few hundred thousand euros. We imagine a fully functional and secure, audited implementation of the TruSec protocol may involve somewhere up to a million euros.

Since we currently do not possess the means to allocate such funds into the development of the POC, we propose the following. Our team is highly motivated to develop a detailed and thorough specification of the protocol, such that it may be presented at Blackhat 2022 (USA). At the end of such a presentation, if accepted, we can reach out to industry to see if there is interest in developing the protocol in collaboration with some leading cyber security companies. This prevents allocating funds to a project for which no vast industry-wide interest has been generated, whilst still enabling people from all across the world to leverage the protocol if they see fit.

3 Implementation

4 Discussion

4.1 Related Work

5 Questions

6 Planning

This section summarises the information required to generate a planning towards a Call for Papers submission for the Blackhat 2022 USA submission.

6.1 Schedule

The 2022 Blackhat (USA) edition takes place on 2022-08-06 to 2022-08-11. Even though the call for papers is not yet open, one can develop a planning analog to the call for papers for the 2021 Blackhat USA edition. For that conference, the dates were specified as:

Source: <https://www.blackhat.com/us-21/call-for-papers.html>

- Call for Papers Opened: February 2, 2021
- Call for Papers Closed: April 10, 2021
- Notification to Submitters: end of May, 2021
- Event Dates: July 31 - August 5, 2021

Hence, shifting the planning with one week, since the 2022 edition will occur one week later:

- Call for Papers Opened: February 9, 2021
- Call for Papers Closed: April 17, 2021
- Notification to Submitters: end of May, 2021
- Event Dates: August 06 - August 11, 2022

6.2 Deliverables

To create a successful submission to the Blackhat 2022 (USA) edition, the following deliverables are required:

1. A track specification.
 - Source: <https://www.blackhat.com/html/tracks.html>
2. *Assumed:* Abstract specification
 - Source: <https://i.blackhat.com/docs/cfp-sample-submissions.pdf>
3. *Assumed:* Presentation Outline

- 135 ■ Source: <https://i.blackhat.com/docs/cfp-sample-submissions.pdf>
- 136 4. *Assumed:* Attendee Takeaways
- 137 ■ Source: <https://i.blackhat.com/docs/cfp-sample-submissions.pdf>
- 138 5. *Assumed:* Why Black Hat motivation.
- 139 ■ Source: <https://i.blackhat.com/docs/cfp-sample-submissions.pdf>
- 140 6. *Assumed:* Presentation slides.
- 141 ■ Source: Imagination.

142 6.2.1 Submission Requirements (ASIA)

143 The following Blackhat submission requirements are specified for the ASIA event:

144 Source: <https://www.blackhat.com/call-for-papers.html>

- 145 1. Submissions may only be entered by researchers/speakers (no submissions from PR
- 146 firms/marketing representatives).
- 147 2. Black Hat does not accept product or vendor-related pitches. Black Hat will disqualify
- 148 any product or vendor pitch.
- 149 3. Submissions must clearly detail the concepts, ideas, findings, and solutions a researcher
- 150 or speaking team plans to present.
- 151 4. Submissions that highlight new research, tools, vulnerabilities, etc. will be given priority.
- 152 5. Submissions that include White Papers are highly encouraged and will also be given
- 153 priority.
- 154 6. Black Hat will disqualify incomplete submissions; complete your submission in its entirety.
- 155 7. Individuals may submit more than one proposal, but each proposal must be submitted
- 156 via a separate submission form.
- 157 8. Each submission must include detailed biographies of the proposed speaking team.
- 158 9. Submitters will be contacted directly if Review Board members have any questions about
- 159 a submission.

160 6.2.2 Tailoring Submission

161 Suggested resources to tailor the submission to maximise acceptance probability:

162 Source: the recommendation section of: <https://asia-briefings-cfp.blackhat.com/>.

- 163 ■ Example submissions: <https://i.blackhat.com/docs/cfp-sample-submissions.pdf>
- 164 ■ Tips: <https://insinuator.net/2017/04/some-quick-tips-for-submitting-a-talk-to-black-hat-or-tr>
- 165 ■ Acceptance: <https://www.helpnetsecurity.com/2016/03/30/how-to-get-your-talk-accepted-at-black-l>
- 166 ■ Tips: [https://hexsec.blogspot.com/2012/12/create-good-security-cfp-responses.](https://hexsec.blogspot.com/2012/12/create-good-security-cfp-responses.html)
- 167 html
- 168 ■ Pitfall avoidance: <https://research.kudelskisecurity.com/2020/04/02/5-common-cfp-submission-mistake>

169 7 Conclusion and Recommendations

170 — References —