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.

42nd Conference on Very Important Topics (CVIT 2016).
Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:3
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2 Protocol

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 succesfull 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
   - Source: `https://i.blackhat.com/docs/cfp-sample-submissions.pdf`
4. *Assumed:* Attendee Takeaways
   - Source: `https://i.blackhat.com/docs/cfp-sample-submissions.pdf`
5. *Assumed:* Why Black Hat motivation.
   - Source: `https://i.blackhat.com/docs/cfp-sample-submissions.pdf`
6. *Assumed:* Presentation slides.
   - Source: Imagination.

6.2.1 Submission Requirements (ASIA)

The following Blackhat submission requirements are specified for the ASIA event:
Source: `https://www.blackhat.com/call-for-papers.html`

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

6.2.2 Tailoring Submission

Suggested resources to tailor the submission to maximise acceptance probability:
Source: the recommendation section of: `https://asia-briefings-cfp.blackhat.com/`.

- Example submissions: `https://i.blackhat.com/docs/cfp-sample-submissions.pdf`
- Tips: `https://insinuator.net/2017/04/some-quick-tips-for-submitting-a-talk-to-black-hat-or-trc`
- Acceptance: `https://www.helpnetsecurity.com/2016/03/30/how-to-get-your-talk-accepted-at-black-h`
- Tips: `https://hexsec.blogspot.com/2012/12/create-good-security-cfp-responses.html`
- Pitfall avoidance: `https://research.kudelskisecurity.com/2020/04/02/5-common-cfp-submission-mistak`

7 Conclusion and Recommendations

References