Brno University of Technology
Faculty of Information Technology
Department of Information Systems

Opinion on "Lawful Interception: Identify Detection"

Author: Ing. Libor Polčák
Supervisor: Prof. Ing. Miroslav Švéda, CSc.

Work Extent: 161 pages of text in the dissertation and an additional 21 pages of appendices.

1. Introduction

This work focuses on identity detection using IPv6 features. Three technical methods for identity detection are proposed along with formalizations. Specifically, IPv6 assignment tracking (Ch. 6), clock-skew based remote identification (Ch. 7), and the application of identity graphs to model identification features (Ch. 8). Overall, these approaches allow for the identification of one or more identities of a system based on network traffic.

The author identifies how identities can be created from IPv6 traffic. He models IPv6 with a timed transducer. Especially interesting are the states of the timed transducer (p.66). After formal modeling of state and transitions, a monitor can use this information to associate identities. IPv6 implementations were discussed and experimentation on a real network was conducted.

Next the author attempted the clock-skew based approach for remote identification. The author admits that this approach is not reliable for short-term identity detection. However, instead of being simply a negative result, this method does appear to be effective with long-term monitoring on some systems.

Finally, arguably the main chapter of this thesis is chapter 8, which focuses on building extended identity graphs from system or application features. These features are categorized, and restrictions are placed on graph edge or node creation depending on the language of the warrant.

2. General Results

Identification for lawful interception, especially in the context of IPv6, is a relevant topic that is worth exploring. Further, the candidate shows a clear ability to conduct scholarly research, and – according to the text – supervise students in their research. From the bibliography, it appears that the core of this dissertation has been published.

Each chapter is a stand-alone 'complete study' with a common theme of identity detection. It would have been interesting to see timed transducers and related features from chapter 6 somehow relate to the identity graph generation in chapter 8. It may have made more sense to propose identity graphs, and then analyze IPv6, clock-skew and other identifying features in terms of this theory.

This thesis includes several novel studies, however, one of the greatest contributions to knowledge is the representation of an LI warrant *language* as a constraint on the state of the identity graph. The author created such constraints for practical purposes, but the concept is important to all digital investigations, not just legal interception. Especially interesting would be the automated mapping of warrant language to state restrictions.

3. Selected Remarks and Inquiries

- Several tables have undefined terms. The most important is probably Table 8.1 “Durability” data. What do these durability lengths of time mean?
- Several locations the author makes statements that are empirically tested, however, the corresponding data that the author uses is not provided or referenced. Please provide data when making a claim.
- As stated before, each chapter feels like its own independent work. More of an effort should be made to combine the concepts.
- Section III “Evaluation” contains no evaluation. Only a discussion about the practical applications of the concepts. The reason for this is likely because each proposal already contains an evaluation. I would like to see more testing of the proposed methods compared to other techniques. As far as I can tell, chapter 9 is essentially ‘future works’. Some interesting topics are discussed, but not in-depth enough to warrant their own section / chapter.

4. Conclusion

This was an interesting and useful piece of work. The approach, methods and formalizations in this thesis are appropriate and systematic. The author’s research results demonstrate his ability to contribute to the field.

With respect to the comments above, **this thesis meets the requirements of the proceedings**. I recommend Mr. Libor Polčák to be awarded the degree of Doctor of Philosophy.

Prof. Joshua I. James
joshua.i.james@hallym.ac.kr
Legal Informatics and Forensic Science Institute
Hallym University
Chuncheon, South Korea