CCR Example File

A
TU Darmstadt, Germany
a@tu-darmstadt.de

B
Northeastern University, USA
b@neu.edu

C
KTH, Sweden
c@kth.se

D
ETH, Switzerland
d@inf.ethz.ch

E
Aalborg University, Denmark
e@cs.aau.dk

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

Based on the Dagstuhl Seminar 15102, this paper initiates the study of more structured approaches to describe secure routing protocols and the corresponding attacker models, in an effort to better understand existing secure routing protocols, and to provide a framework for designing new protocols.

CCS CONCEPTS

• **Networks** → **Routing protocols**; • **Security and privacy** → **Security protocols**;

KEYWORDS

Taxonomy, Adversarial Models

1 INTRODUCTION

Communication networks have become a critical infrastructure, as other critical infrastructures increasingly rely on them. As routing lies at the heart of any communication network, the security of the underlying routing protocol is crucial to prevent attacks and ensure availability. However, the routing system is not only one of the most complex and fragile components in the global information infrastructure, but also one of the least protected ones [1].

ACKNOWLEDGMENTS

The discussions leading to this editorial were initiated during Dagstuhl Seminar 15102 on *Secure Routing for Future Communication Networks*, and we thank all participants for their contributions.

REFERENCES

[1] D. Montgomery and S. Murphy. Toward secure routing infrastructures. *Security Privacy, IEEE*, 4(5):84–87, 2006.