A Thing

Peoples
Places
Things

ABSTRACT

In recent years, Information-centric Networking (ICN) has received much attention from both academic and industry participants. ICN offers a data-centric means of inter-networking that is radically different from today's host-based IP networks. Security and privacy issues in ICN have become increasingly important as ICN technology gradually matures and nears real-world deployment. As is well known, in today's Internet, security and privacy features were originally not present and had to be incrementally and individually retrofitted (with varying success) over the last 35 years. In contrast, since ICN-based architectures (e.g., NDN, CCNx, etc.) are still evolving, it is both timely and important to explore ICN security and privacy issues as well as devise and assess possible mitigation techniques.

This report documents the program and outcomes of the Dagstuhl Seminar 16251 "Information-centric Networking and Security." The goal was to bring together researchers to discuss and address security and privacy issues particular to ICN-based architectures. Attendees represented diverse areas of expertise, including: networking, security, privacy, software engineering, and formal methods. Through presentations and focused working groups, attendees identified and discussed issues relevant to security and privacy, and charted paths for their mitigation.

1. INTRODUCTION

Dagstuhl seminar 16251 "Information-centric Networking and Security" was a short workshop held June 19-21, 2016. The goal was to bring together researchers with different areas of expertise relevant to ICN to discuss security and privacy issues particular to ICN-based architectures. These problems have become increasingly important as ICN technology gradually matures and nears real-world deployment.

Threat models are distinct from IP. Differentiating factors between the two include new application design patterns, trust models and management, as well as a strong emphasis on object-based, instead of channel-based, security. Therefore, it is both timely and important to explore ICN security and privacy issues as well as devise and assess possible mitigation techniques. This was the general purpose of the Dagstuhl seminar. To that end, the attendees focused on the following issues:

- What are the relevant threat models with which ICN must be concerned? How are they different from those in IP-based networks?
- To what extent is trust management a solved problem in ICN? Have we adequately identified the core elements of a trust model, e.g., with NDN trust schemas?
- How practical and realistic is object-based security when framed in the context of accepted privacy measures used in IP-based networks?
- Are there new types of cryptographic schemes or primitives ICN architectures should be using or following that will enable (a) more efficient or secure packet processing or (b) an improved security architecture?

The seminar answered (entirely or partially) some of these questions and fueled discussions for others. To begin, all participants briefly introduced themselves. This was followed by several talks on various topics, ranging from trust management and identity to privacy and anonymity. Subsequently, the attendees split into working groups to focus more intensely on specific topics. Working group topics included routing on encrypted names, ICN and IoT, non-privacy-centric aspects of ICN security, as well as trust and identity in ICN. Once the working group sessions were over, a representative from each presented outcomes to all attendees. (These are documented in the remainder of this report.) The major takeaways from the seminar were as follows.

First, the ICN community still does not have a clear answer for how to handle namespace and identity management. While trust management in ICN can be distributed and function without a global PKI, it seems difficult to break away from this model for namespace management and arbitration. This has strong implications on how names are propagated in the routing fabric. Can any producer application advertise any name, anywhere in the network? If not, how can name prefix advertisements be constrained or limited?

Second, given that ICN focuses on object security, the need for and use of transport protocols that provide forward secrecy should be deferred to higher layers. Attendees found

that while most ICN-based architectures do not preclude forward secrecy, it should not be a requirement at the network layer.

Third, there is still deep uncertainty about whether ICN should embrace a content locator and identifier split. Names in architectures such as NDN and CCN serve as both a locator and identifier of data, though there are extensions that permit explicit locators (e.g., through the use of NDN LINK objects). This distinction is necessary under the common understanding that routing should concern itself with topological names. Finding data through non-topological names should not be in the data plane as part of the global routing space. However, if we revert to a distinction between topological locators and identifiers, then features unique to ICN become much more limited. One facet that is certainly unique to ICN is how software is written. Specifically, we have the opportunity to move beyond the mental model of a fixed address space and re-design existing network stacks and APIs.

Fourth, privacy seems difficult to achieve without major architectural changes to ICN-based systems. In particular, since data names reveal a great deal of information to the passive eavesdropper, privacy demands that names and payloads have no correlation. However, achieving this seems infeasible without the presence of an upper-layer service akin to one that would resolve non-topological identifiers to topological names.

Lastly, there are no compelling reasons to apply esoteric (and often untested) cryptographic techniques in ICN, at least at the network layer. Computationally bounded and "boring" cryptographic primitives, such as digital signatures, hash functions, etc., should be the extent of per-packet cryptographic processing done by routers. Anything more would become fodder for Denial-of-Service attacks that could render the entire infrastructure ineffective. However, architecture designs should not restrict themselves to specific algorithms. In other words, there must be flexibility in accommodating multiple (and evolving) cryptographic primitives. This could be useful if, for example, post-quantum digital signature schemes become necessary for the longevity of content authenticators.

We thank Schloss Dagstuhl for providing a stimulating setting for this seminar. Much progress was made over the course of the seminar and since its completion. This is mainly because of the ease of face-to-face collaboration and interaction at Dagstuhl.

2. NAMESPACE AND IDENTITY MANAGEMENT

XXX

3. OBJECT SECURITY BUT NO FORWARD SECRECY

XXX

4. LOCATORS AND IDENTIFIERS

XXX

5. THE FUTILITY OF PRIVACY

XXX

6. BORING CRYPTO

XXX

7. CONCLUSION AND FUTURE WORK

XXX