# Tutorial: Security and Synchronization in Named Data Networking (NDN)

Hila Ben Abraham
Washington University in St. Louis
hila@wustl.edu

Alex Afanasyev, Yingdi Yu, Lixia Zhang
UCLA IRL
{afanasyev, yingdi, lixia}@cs.ucla.edu

Steve DiBenedetto
Colorado State University
dibenede@cs.colostate.edu

Jeff Thompson, Jeff Burke
UCLA REMAP
{jefft0, jburke}@remap.ucla.edu

## ABSTRACT

This full day tutorial on synchronization and security in Named Data Networking (NDN) will share important architectural concepts we are exploring in these areas, the software we have built to perform these tasks, and remaining open issues. In particular, it will emphasize how the existing open source toolset provides a platform for exploring the open research questions.

## 1. INTRODUCTION

Named Data Networking (NDN) is one of the most prominent ICN architectures and software platforms available to the research community. The NDN codebase is published under an open source license and widely used in experimentation; a 26 node international testbed is available for research use. In previous years, the NDN project team has presented tutorials to introduce the basics of the architecture and its software platform, both to promote related research and to encourage community contribution to the open source software platform. These earlier tutorials focused primarily on introductory material—in particular, Interest/Data exchange mechanisms and basic content verification. However, many of the field's most interesting research challenges lie in areas that build on these basics. In particular, **mechanisms for access control and trust verification, along with new transport protocols building on Interest/Data exchange**, are important areas of work for the NDN project team.

This tutorial will share important architectural concepts we are exploring in these areas, the software we have built to perform these tasks, and remaining open issues. In particular, it will emphasize how the existing open source toolset provides a platform for exploring the open research questions.

We hope to engage participants both in using deeper and emerging features of the available toolset, and in tackling these critical problem spaces with us. In addition to referencing a variety of existing examples, the tutorial will use the creation of a modern browser-based application to illustrate three such topics where the ideas have progressed such that we can build experimental libraries to work with them: **1) multi-party synchronization, 2) schematized trust, 3) encryption-based access control.**

## 2. TYPE OF TUTORIAL

Combination of introductory material about the architectural concepts, solution space, and available open source prototype implementations, with motivation/demonstration examples that can be followed in real-time by the tutorial participants. We expect the duration of the tutorial to be a full day, approximately 7.5 hours including a 1-hour working lunch break.

## 3. CONTENT OUTLINE

### 3.1 Welcome and introduction, recap of NDN software platform and testbed

(45 minutes)

Objective: Review architecture, platforms and key challenges, motivation of tutorial topics.

a. Recap of NDN libraries, NFD forwarder, and repository implementations, focused on typical configuration concerns and the emphasis of the tutorial.
b. Review of storage options—forwarder content store, repository, application in-memory storage. Discuss the data custodian design pattern used in the rest of the tutorial.
c. Introduction of basic NDN data-centric security and the minimum requirements and recommendations for NDN applications.

### 3.2 Running application example

(15 minutes)

Objective: Present the running example of the tutorial: *Build a secure, peer-to-peer browser-based messaging system (vis-à-vis Slack[1]), using NDN to provide Firebase[2]-like features with local data custodians instead of cloud infrastructure.*

### 3.3 Multi-party Synchronization (Part 1)

(45 minutes)

Objective: Introduce the practical role of sync as a communication protocol, and available tools.

a. **Motivation & concept**: Synchronization as a new transport approach, open questions, and envisioned use cases. How we are moving from general sync concept to specific sync designs, role that sync plays in the sample application.
b. **Design patterns:** Introduction and comparison of application design patterns based on current applications, including ChronoShare, NLSR, NDNFit. Achieving related patterns in higher layers of the TCP/IP world (e.g., Firebase).
c. **Solution space**: Discuss challenges and options in creating sync-based protocols, including ChronoSync, CCNx Sync, ISync, and others. Provide overview of libraries and code available for exploration by others.

### 3.4 Multi-party Synchronization (Part 2)

(45 minutes)

a. **Application example:** Illustrate sync in action by starting to build our running example - a simple browser-based, peer-to-

[1] http://slack.com/

[2] http://firebase.com/

peer messaging application using sync. Begin by creating a simple library with features similar to *Firebase*. Participants can optionally follow along using NDN-JS in their browser.

b. **Future work**: Brief introduction to research challenges and moving forward with sync-based designs.

## 3.5 Beyond Static Content Distribution

(60 minutes, during lunch)

a. **Presentation**: *Why caching is not the most exciting part of NDN*. Opportunities to use the open source platform to explore NDN advantages related to the tutorial topics for important applications beyond static content distribution. Topics including: Support for ad hoc connectivity; potential solutions to design and security challenges for IoT and M2M; supporting content distribution on the web.

b. **Discussion**: Review and discuss available, upcoming, and desired open source software tools for NDN research beyond content distribution. Opportunities to become involved in the open source development of NDN.

## *3.6* Schematized Trust (Part 1)

(45 minutes)

Objective: Introduce schematized trust verification for Data using the current NDN security library, and discuss related developments such as certificate formats and library support.

a. **Motivation & concept**: Introduction to trust schema: Creating powerful, named-based schemes for verification of data authenticity and supporting automated generation of keys. Role that schematized trust plays in the sample application.

b. **Design patterns**: Examples of hierarchical trust schema that the NDN team is exploring in different applications, such as routing security, building automation, and mobile health.

c. **Solution space**: Current and planned NDN Certificate format; library support for trust schema; tools available to create key hierarchies; and a brief introduction on example ways keys can get certified by local trust anchors (e.g., NDN testbed root or other). Pointers to how other types of verification (e.g., "web of trust") can be implemented using the available libraries.

## *3.7* Schematized Trust (Part 2)

(60 minutes)

Objective: Introduce schematized trust verification for Data using the current NDN security library.

a. **Application example**: Updating the example application to provide hierarchical verification that messages are from the authorized members of the tutorial group.

b. **Future work**: Discussion of how open research questions can be explored by building on the available platforms.

## 3.8 Encryption-based Access Control, Briefly

(90 minutes)

Objective: Introduce encryption-based access control using NDN and extend the sample application via experimental NDN libraries for group encryption.

a. **Motivation & concept**: Briefly introduce the notion of data-centric security and compare to channel-based security. Concept for access control in the sample application.

b. **Design patterns**: Access control patterns emerging in current applications explored by the NDN team, as well as other related previous work in other fields.

c. **Solution space**: Available open source tools and libraries and upcoming plans for development.

d. **Application example**: Using the NDNFit application as an example, illustrate basic encryption-based access control.

## 3.9 Conclusion and wrap-up discussion

(30 minutes)

# 4. Previous Tutorials

The NDN team has provided tutorials, including hands-on workshops, at venues including: GENI Engineering Conference 21, October 20-23, 2014, Indiana University; ACM 1st Information-Centric Networking (ICN) Conference, September 24, 2014, Paris, France; NDN Community Meeting 2014, September 3, UCLA; AsiaFI NDN Hands-on Workshop, March 19-21, 2012, Seoul National University, Korea. These previous tutorials have focused on how to get started using the NDN codebase to build applications using basic Interest/Data exchange. Given that many in the ICN community are now familiar with this topic, we propose in this tutorial to cover the two "intermediate" topics of multi-party synchronization and security (specifically, hierarchical trust verification and encryption-based access control) that we expect will be beneficial to researchers in the community and also bring additional feedback to the NDN team as we develop tools in these important areas.

# 5. Requirements for the Tutorial Room

The tutorial room must provide: 1) At least one data projector, XGA resolution or better, on which code examples can be clearly viewed by all participants. Preferred are two independently fed data projectors – one for a running code example and one for slides / reference material. 2) Sound reinforcement (microphone) for presenters, at a minimum. 3) Wired internet access, preferably unfiltered with a static IP. Either the conference organizers (preferred) or the NDN project team (if necessary) will provide: 1) A NAT-capable router with a local LAN segment dedicated to the tutorial, connected to the above wired internet service. There should be no restrictions on local traffic. 2) Wireless access points connected to the LAN side of the router sufficient to provide access for all tutorial participants. Finally, the NDN team will include a few tutorial helpers that will walk around to provide hands-on assistance where necessary. The room layout should support this, if possible (i.e., relatively wide aisles between seating rows, etc.).

# 6. Requirements for the Attendees

Attendees must bring a laptop capable of running the most recent version of Chrome and/or Firefox. All required examples will be in Javascript. Ideally, laptops should also have pre-installed and tested the full Named Data Networking platform, which has been tested most extensively on modern versions of Ubuntu Linux and Mac OS X. Time will not be allocated in the tutorial for troubleshooting participants' installations. *For those who wish to work with it, the NDN Platform must be installed and tested prior to the tutorial; we will provide limited email support to participants who encounter any trouble in the weeks leading up to the tutorial.*

Attendees should have some reasonable conceptual and practical familiarity with the NDN architecture and the fundamentals of Interest/Data exchange. Ideally, they should be comfortable with Javascript, including the basic debugging tools available in the browser, as well as getting around in the Unix shell.

Prior to the tutorial, we will distribute key references on the architecture to the participants, as well as recommendations for hands-on examples that will build familiarity with basic functions in the NDN Javascript library and serve as a recap of the needed

understanding of the language itself. Unlike previous years, this is not a basic introduction to NDN applications. It is an intermediate level tutorial that requires either some basic experience with NDN or similar ICN architectures, *or* a willingness to follow along with topics that build on basics that will only be covered briefly.

## 7. LIMITATIONS ON PARTICIPATION

As long as all participants can work comfortably on their own laptop, with power and network access, as well as access to local resources on a network that we provide, we do not see that any limitations will be needed.

## 8. REPRESENTATIVE REFERENCES


[1] claffy, kc, J. Polterock, A. Afanasyev, J. Burke, L. Zhang. "The First Named Data Networking Community Meeting (NDNcomm)", In submission to *ACM SIGCOMM Computer Communication Review (CCR)*, 2015.

[2] Jacobson, Van, et al. "Networking named content." *Proceedings of the 5th international conference on Emerging networking experiments and technologies.* ACM CoNEXT, 2009.

[3] Shang, W., J. Thompson, M. Cherkaoui, J. Burke, L. Zhang. "NDN.JS: A JavaScript Client Library for Named Data Networking." *Proceedings of IEEE INFOCOMM 2013 NOMEN Workshop*, April 2013.

[4] Yu, Y., A. Afanasyev, D. Clark, k. claffy, V. Jacobson, L. Zhang. "Schematizing and Automating Trust in Named Data Networking." *NDN Technical Report NDN-0030*, Revision 2, June 2, 2015.

[5] Zhu, Z., A. Afanasyev. "Let's ChronoSync: Decentralized Dataset State Synchronization in Named Data Networking," *Proceedings of the 21st IEEE Intl. Conf. on Network Protocols (ICNP 2013)*, Goettingen, Germany, October 2013.