Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication

PROJECT SUMMARY

Internet-of-Things (IoT) applications face severe security challenges related to the reliable and secure data exchanges, especially in constrained network environments. The proposed project aims to address these challenges at the architectural level by substituting IoT trustful authentication with less trust, even trustless, consensus, which has been successfully tested, implemented, and applied in many application domains. The proposed work in the FC^2 focus area *Cyber-Physical Systems Security and the Internet of Things* aims to address these challenges at the architectural level by supplementing the existing RESTful application semantics with a notion of data-centric security, one of the core principles behind the proposed Named Data Networking architecture [22].

Most of the emerging IoT applications, including smart home, smart farming, and many others, are content-oriented in nature, relying on HTTP or CoAP protocols to deliver requests and retrieve the requested data. However, these Web-like protocols have inherent connection/node-oriented underlying communication and security semantics, establishing the point-to-point trust or shared group trust using logically centralized TLS and DTLS mechanisms, with limited assurance of authenticity and integrity of the exchanged content.

Intellectual Merit: Inspired by the research results from the Named Data Networking (NDN) project [22], the proposed work will address critical IoT security problems by developing a backward-compatible extension to HTTP/CoAP protocols that directly associate authenticity information with REST objects. By applying principles of NDN, clients will send uniquely named cryptographically signed requests and receive signed responses, without dependency on the underlying connection, group channel, or data storage authenticity.

In addition, the emergence of blockchain technology radically changed the landscape of IoT object authentication. We will apply principles of blockchain to define trustworthiness of data in terms of trustless consensus, which perfectly fits the situation of IoT, where many heterogeneous nodes with little hardware/software resource collaborate to provide huge amount of dubious data. In this proposal, we plan to replace the proof-of-work (PoW) based mining functionality with NDN based proofing, for example, with proof-of-content, using verification of content with hashing, matching content with name, proof-of-content with interest path, or proof-of-content with request history, etc. All these approaches should still be NP-complete operation in NDN framework, but can be computed/derived/proved in a distributed, collaboration-based, peer-to-peer manner.

Broader impact: By developing a content-based, blockchain style, security architecture for the IoT, this project will explore new directions to address security challenges and contribute patents and open source software for augmenting IoT security. By exploring the integration and intersection among IoT, blockchain, and NDN, the conceptual impact of this project may well exceed our original expectation. This innovative approach will inspire others to further examine great potential challenges and opportunities in similar directions or manners. The PI will help students learn to think architecturally in examining solutions.

Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication

TABLE OF CONTENTS

PROJECT NARRATIVE

1 Introduction

The Internet-of-Things (IoT) is a set of emerging technologies that cover a broad range of application scenarios, ranging from sensing and automation in smart homes, smart health, smart enterprises, smart cars, smart cities, etc. Although many of such IoT applications are substantially different from traditional applications and operate in much challenging network conditions (sometimes with limited or only ad hoc connectivity), such applications are usually built using RESTful interfaces on top of Web-like (HTTP and CoAP [20]) protocols. The semantics of IoT applications (e.g., retrieving temperature reading at a specific location, obtaining current reading of the blood pressure) usually does not match to the connection/node-oriented nature of these Web-like protocols nor the traditional approaches to secure communication. In other words, HTTP/CoAP secures communication by establishing the point-to-point trust or shared group trust using TLS [7] and DTLS [19] mechanisms, which provides limited assurance of authenticity and integrity of the exchanged content and inherits well-known security issues and challenges. Vulnerabilities in TLS/DTLS and its implementations have regularly and infamously undermined the security of millions of Web-based applications [5, 8, 9, 12]. Specifically to IoT, power constraints and general scalability concerns drive adoption of proxy and middlebox based mechanisms [6] (e.g., requests are queued at the dedicated proxy while waiting for a IoT device's power-on cycle), which further breaks the ability of HTTP/TLS and CoAP/DTLS to ensure end-to-end protection and exposing content to additional points of attack. Under the secure channel model, these middleboxes are able to see and modify the data passing through them, so they too can be attacked to compromise services. Besides content, HTTPS servers and middleboxes have to safeguard their private keys, yet these keys need to be kept accessible to the servers all the time in order to satisfy requests.

Many of the security problems affecting the IoT domain are due to a fundamental incongruity between RESTful application semantics and its underlying TLS and DLTS security mechanisms and defenses. The REST-based applications are *content-oriented* by nature: requests for content (command) at a particular URL and responses containing the requested data (results of the command). In contrast, the most important Web security mechanisms apply a *server-oriented* architecture that focuses on protecting connections to particular servers. For example, TLS and DTLS attempt to provide a confidential and authenticated channel between clients and servers. This approach was not the result of research but historical convenience, since the RESTful applications were constructed on top of the TCP/IP and UDP/IP protocol stacks, which can only provide point-to-point connections between clients and servers, thus security protection was patched onto these connections.

We propose to address the security challenges of the emerging IoT applications using a fundamentally different approach: embedding authentication of RESTful objects in the RESTful protocol itself [1]. Under this security model, each REST command and response is signed using a public key, ensuring reliable authenticity of the object regardless how it is delivered to/from IoT device. Policies about *who* can create or access response, and about *what* executable content is allowed to do in the context of an application, can be tightly bound to the REST object itself, rather than merely to the service or service domain at which it is hosted. Our work will address

the architectural design of the REST Object Authentication in IoT applications, enabling simple yet powerful mechanism to augment existing IoT applications with additional level of authenticity assurances.

This approach is inspired by the experience of designing a content-based network architecture for the Named Data Networking (NDN) project [18, 22] as part of the NSF Future Internet Architecture program. NDN shares several basic properties with the RESTful IoT applications, as we elaborate in Section 2. Both deliver data using a named request/response model, and content can be cached anywhere. Because NDN decouples content delivery from content security, it enables consumers to retrieve content from any location and through any channel. By developing ways to apply similar security mechanisms to today's HTTP and CoAP-based applications, we can meet the pressing need to provide secure communication over a network that is increasingly hostile [3].

In order to realize REST Object Authentication in IoT, we propose to tacke two research questions: enabling authenticity support in HTTP/CoAP and IoT application trust bootstrap (key management).

In the context of *enabling authenticity support in HTTP/CoAP*, we will address the problem of incrementally introducing REST object security semantics, allowing individual objects be signed by the producers, while providing backward compatibility with the existing protocol. We will focus on applying the concept of Trust Schema [21] to design expressive mechanism to specify the authentication model with flexible granularities.

We will study *trust bootstrapping* through trustless consensus, inspired by the blockchain technology. To address inefficiency and requirements for the extreme computational power, we plan to replace the proof-of-work (PoW) based mining functionality with NDN-based proofing. All these approaches should still be NP complete operation in NDN framework, but can be computed/derived/proved in a distributed, collaboration-based, peer-to-peer manners.

An important aspect of our research includes building and deploying a prototype IoT sensory application as part of a simple smart home application. Leveraging collaboration between Florida International University and Florida Polytechnic University, we plan to deploy and run cross-campus performance, security, and red-team evaluations with the prototype application and the developed protocols in general.

2 Data-Centric Security in NDN

The incongruity between data-centric application semantics and channel-based communication model provided by the TCP/IP architecture has been widely recognized by both research and industry communities and is the motivation for development of Named Data Networking (NDN) [11, 18, 22], a concrete design of the Information-Centric Networking (ICN) vision. As we highlight in the rest of this subsection, NDN builds data-centric security directly into the network layer, paving the way for more flexible, secure, and reliable communication.

Our proposed effort will take the lessons learned from NDN and apply NDN principles to build an solution for REST object authenticity. Because both NDN and RESTful protocols are inherently based on named content, there are direct parallels in problem and solution spaces. We also expect to learn new lessons from this proposed research that can be fed back into the NDN research effort to refine the architecture and implementation to meet real applications requirements. Below we

provide a brief overview of NDN and its security model.

2.1 Overview of Named Data Networking (NDN)

Named Data Networking (NDN) changes the Internet's communication model from *delivering packets to an end host* to *retrieving content for a given name*. A host requests content by sending an *interest packet*, which specifies the name of the desired content, and the network responds by sending back a *data packet* containing the requested content. Since the requester only specifies what it wants (i.e., the data name), the network has the freedom to make intelligent decisions on where to forward an interest packet. It could be sent satisfied using an available replica of the data hosted by the original data producer or by a third-party storage provider, or even by an in-router cache containing the requested data. NDN is well aligned with content-oriented semantics of web applications and naturally supports scalable content dissemination.

Figure 1 illustrates the basic operation of an NDN network using the futuristic NDN-based smart home example. NDN names are structured hierarchically and can refer to any piece of content—a chunk of a status response from HVAC system, a temperature sample from a specific location, or an actuation command. For example, data for an HVAC status dataset in an instance of a home automation system may have the name "`/myhome/HVAC/_status/...`", where '/' delineates name components in text representations, similar to URLs. When the status info is ready to be published (e.g., it is published periodically or as a response to the incoming request), an application running inside HVAC creates data packet(s) with the status information, splitting content into multiple segments if necessary. Each piece of NDN data has a unique name and is signed (individually or as a group of data packets) at the time of its production, cryptographically binding the name and the data. Therefore, NDN data packets can be stored and retrieved from anywhere in the network, including opportunistic in-network caches and managed data stores in the cloud. For content that may change dynamically, the name must include additional component to disambiguate different versions. In our example, the HVAC would want to add a versioning component which can either represent the revised content (e.g., a hash of the content), or be a timestamp indicating when the last revision was made, or simply a vision number (e.g., "`/myhome/HVAC/_status/2018-01-11/.../_v=42/_s=1`").

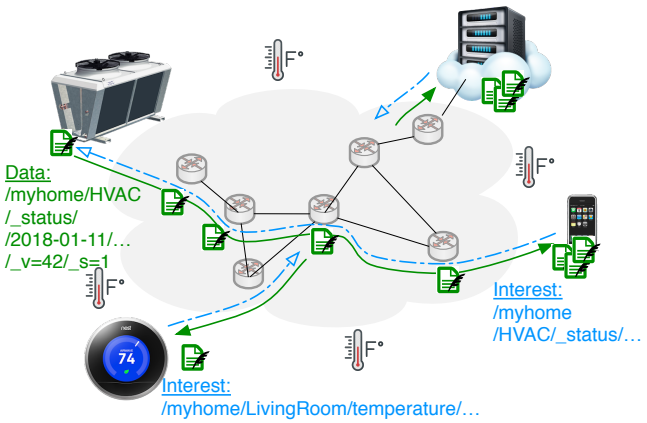


Figure 1: Example of NDN communication

The content is made reachable in the network by announcing its prefix in the routing system. In the example, the router in the smart home would announce "`/myhome`" into the global routing system, while HVAC, Nest thermostat, and temperature sensors would announce specific "`/myhome/HVAC`", "`/myhome/Nest`", "`/myhome/LivingRoom/temperature`" into the local routing system. The cloud storage, when enabled, can also announce "`/myhome`" into the global routing system, en-

abling data backup and communication rendezvous. A consumer (phone app) that wants to obtain HVAC status simply sends an interest packet to the network (e.g., "`/myhome/HVAC/_status`"), with metadata indicating that the latest version is requested. The interest is forwarded through the network to the nearest replica of the data. Once the interest packet meets a data packet with the matching name, the network returns the data packet back to the original requester or requesters along the reverse path of the interest packet. The data packet carrying the status information can be cached by routers along the path, so that when a router receives another interest for the same article, it can immediately satisfy the interest with the cached copy.

We have developed a prototype NDN forwarder [2] and built an NDN testbed [15] that currently spans 39 sites across three continents. We have also developed a set of libraries [13, 14, 23] to support NDN's data-centric networking and security semantics, and used them to demonstrate the power of the architecture by prototyping a wide range of applications, including a name-based link-state routing protocol (NSLR [16]), a managed data storage system (repo-ng [17]), a serverless multi-party chat application (ChronoChat [24]), a video conferencing tool (NdnCon [10]), and a number of others.

2.2 Data-Centric Authenticity

An architectural difference between NDN and the TCP/IP-based Internet is that in NDN every named piece of content (data packet) must be signed. This ensures that the data can be authenticated regardless of how/where it is retrieved. Besides the signature, each data packet also carries additional metadata including the signing key name. To authenticate a data packet, one needs a trust model that defines which keys are authorized to sign which data (trust rules) and one or more trusted keys to bootstrap the trust (trust anchors). Any entity—applications, dedicated network storage elements, and even network routers—that learns the trust model for a given piece of content can verify its authenticity, and may perform necessary actions when the authentication fails (e.g., discard the packet, or try an alternative path to retrieve). Keys in NDN are just another type of data, thus they also have unique names and can be authenticated in the same way as other data packets; data packets carrying public keys are effectively NDN certificates.

One insight we have gained from NDN development is that one can leverage the hierarchically structured names to define general trust model rules as a set of relationships between names of data packets and names of the keys authorized to sign those data packets. Figure 2 illustrates possible key naming hierarchy and data naming hierarchy relation in NDN smart home application.

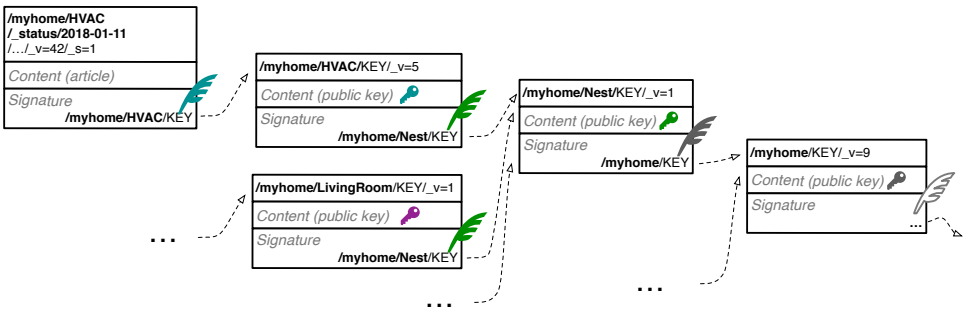


Figure 2: Possible data signing/authentication chains for NDN smart home

This figure also illustrates an application of the principle of least privilege. It is critical to minimize the potential danger for key compromise and to limit the damage once a key is compromised. The principle of least privilege says that a key should be given only the minimal privileges for its assigned tasks. For example, HVAC key can only sign reports from the HVAC system and cannot be used to create living room's temperature reports and vice versa. The naming can be further extended to include time periods, limiting datasets scopes that can be signed buy the key.

2.3 Trust Schema: Establishing Trust Across Namespaces

No single trust model ideally suits all applications and their varied security profiles. Applications may need to express customized trust relationships, as highlighted in the example above. In order to support customizable trust models and yet allow anybody in the network to reliably authenticate every data packet, we have developed *trust schema* mechanisms [21]. A trust schema (or schema in short) formalizes the trust model to a set of generalized relationships between data names and key names, concisely describing the intended authentication paths for data packets, associated trust anchors, and required cryptographic properties for keys and signatures. Note that a schema itself is simply a piece of data that can be put into an NDN data packet, signed based on a higher-level trust model/schema, and made available in the network. Therefore, to authenticate a data packet, it is enough to obtain the corresponding trust schema, perhaps recursively, and properly execute it.

3 Project Objectives

Application of the Named Data Networking principles in realizing REST Object Authentication in IoT requires a system for publishing signed content, including mechanisms to enable content-based authentication and confidentiality semantics in HTTP/CoAP, to define and enforce trust models for IoT applications with various granularity levels, and automate the trust management (certificate management) as much as possible without compromising security.

3.1 Task 1: Enabling Object Authenticity Semantics in HTTP/CoAP

Bringing the advantages of data-centric security requires supporting request and response signatures within existing HTTP/CoAP protocols. The flexibility of HTTP allows us to capitalize on the widespread deployment of the web while maintaining backwards compatibility. This integration of content-based security with HTTP provides a foundation for the rest of our research plan.

Figure 3 illustrates the NDN and HTTP/CoAP packet formats. In comparing the two we see that NDN and HTTP/CoAP contain a name (or URI), metadata, and content. However, the basic HTTP protocol does not define mechanisms to enable content-based authenticity, while the NDN data packet includes an additional signature field, so that consumers can validate content directly.

Although there are several ongoing research efforts to add content-based security semantics into HTTP, the provided solutions are largely piece-meal, e.g., the standardization effort [4] to define data structures and encoding formats for the signed JSON objects. Our plan is to define a systematic architectural solution to add authentication elements into an HTTP/CoAP request/responses. One initial plan is to put these fields into HTTP headers, such as a header that indicates the verification key name, and another header that contains the signature. Encoding these fields

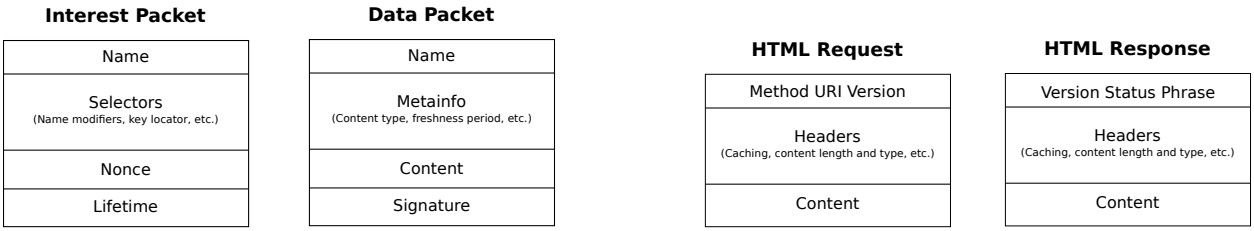


Figure 3: NDN and HTTP/CoAP packet formats

(especially the one for signature) requires careful design and layout, to assure that the signature covers the necessary fields (including content) and that signature can be efficiently created and verified.

3.2 Task 2: Content-Based Authenticity

With the content-based security semantics introduced into HTTP/CoAP, the preliminary content-based authenticity model that we have explored in NDN can be easily integrated with the REST-based IoT applications. In other words, each request/response would carry a digital signature and metadata with the name of the public key that can verify the signature. Public keys would become named content that can be retrieved using the same HTTP/CoAP mechanisms. With this added semantics, it becomes possible to express the trust model of content authentication as the relationship between the URI of the content and the URI of its associated keys, and formalized as a trust schema. The trust schema can be published as a piece of signed JSON object, providing the foundation for constructing flexible yet strict trust models.

As part of this task, we plan to explore the feature of content-based authenticity in enforcing the least-privilege principle in IoT application content production. Because content-based security enables the authenticity for content itself, it highly desirable to limit the scope of keys in order to limit exposure of cryptographic keys and reduce the damage of key compromise. Effectively, this means that producers need to properly and securely manage hierarchy of keys.

3.3 Task 3: Trust Bootstrapping through Trustless Consensus (Blockchain)

IoT authentication, or integrity, was previously most done through trustworthiness building and proving, which usually requires end-to-end verification, or establishing the point-to-point (or end-to-end) trust. The emergence of blockchain technology radically changed the landscape of this domain. The successful applications of blockchain have been proved that the trustworthiness can be substituted with trustless consensus, which perfectly fits the situation of IoT, where many heterogeneous nodes with little hardware/software resource collaborate to provide huge amount of dubious data. However, to effectively adopt the blockchain technology in IoT, like in other application domains, four functionalities, i.e., routing, storage, wallet, and mining, are required. The mining functionality needs tremendous computational power, absolutely not a good fit in the IoT world populated with huge number of low power, low performance, and less expensive IoT devices. In this proposal, we plan to replace the proof-of-work (PoW) based mining functionality with NDN based proofing, for example, with proof-of-content, using verifying content with hashing, matching content with name, proof-of-content with interest path, or proof-of-content with re-

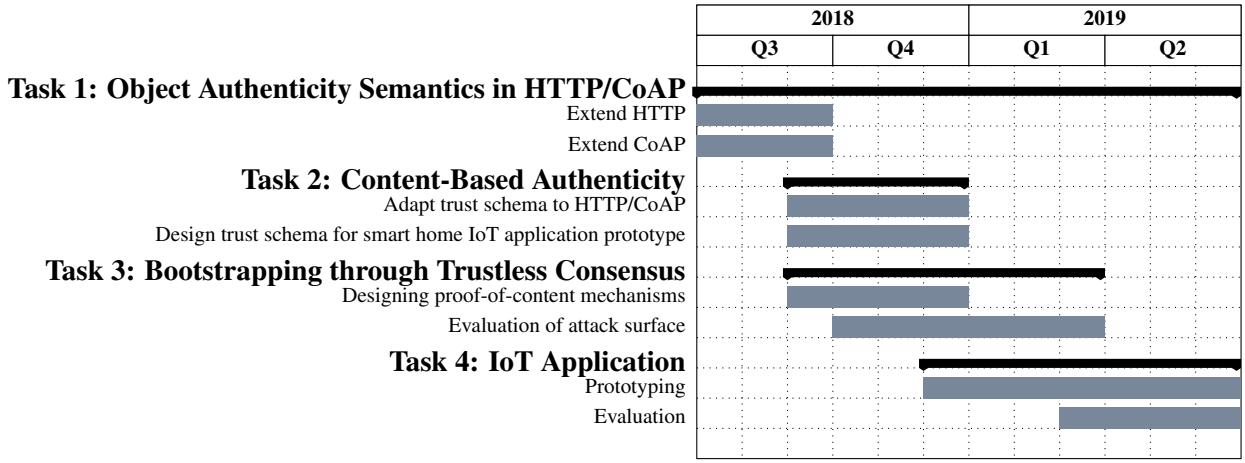
quest history, etc. All these approaches should still be NP complete operation in NDN framework, but can be computed/derived/proved in a distributed, collaboration-based, peer-to-peer manners.

3.4 Task 4: Prototyping and Evaluation

To demonstrate feasibility, qualitative and quantitive advantages of the proposed data-centric authenticity mechanism, the overarching task of this proposal is to build a prototype IoT sensory application as part of a simple smart home application. Using Raspberry PI devices, sensors, and smartphones acting as control and user-facing devices, we plan to develop a set of demos highlighting effectiveness and flexibility of the tight association of the authenticity properties with the communicated data itself. We plan to leverage collaboration between Florida International University and Florida Polytechnic University, we plan to deploy and run cross-campus performance, security, and red-team evaluations with the prototype application and the developed protocols in general.

4 General Work Plan

The following twelve-month research plan has been designed to ensure the on-time and in-budget completion of this project. The plan is largely made of following tasks.



The outcome of the project will be (1) concrete design for secure IoT object authentication; (2) small-scale IoT testbed with prototype of the secure IoT application; and (2) extensive testbed and simulation-based (using ndnSIM framework) evaluation of the proposed design.

5 Broader Impacts

By developing a content-based security architecture for the IoT, this project will explore a new direction to tackle security challenges and contribute open source software for building secure IoT applications. The conceptual impact of the project may well exceed that of specific mechanisms to be developed: this content-based approach will inspire others to further examine its potential power and challenges in its realization. The PI will help students learn to think architecturally in examining solutions.

The proposed research has the potential to fundamentally transform IoT application landscape by providing new foundation for data-centric authentication of the communicated REST objects.

This project will explore a new direction to tackle security challenges and contribute open source software for building secure IoT applications. The conceptual impact of the project may well exceed that of specific mechanisms to be developed: this content-based approach will inspire others to further examine its potential power and challenges in its realization. We also believe that this data-centric security approach is not limited to REST-based IoT applications, but can potentially be applied to all networked applications and data stored in the cloud.

6 Expected Significance

The proposed research initiative will ultimately promote multidisciplinary research in the critical area of Cyber-Physical Systems Security and the Internet of Things, while expanding the role of Florida International University, Florida Polytechnic University, and other SUS institutions in these national high-interest areas.

The research developed under this project will be shared with national and international researchers through publication of conference and journal papers. The protocols developed will be of interest to industrial services providers and standardization bodies, such as IETF and IRTF. The project will aid graduate or undergraduate students in computer science, computer engineering, electrical engineering or related majors at Florida International University (FIU) and Florida Polytechnic University (FPU) in advanced hand-on research in cyber-physical systems, IoT, sensing, intelligent control, and smart technologies. Students with strong ambitions to pursue a career in IT or the life of researchers will recruit with priority. Students will be involved them as co-authors in the research papers. We also plan to incorporate research results of this proposal in ongoing courses and participate at hackathons to engage high school and undergraduate students in computer science research.

References

[1] A. Afanasyev, A. J. Halderman, S. Ruoti, K. Seamons, Y. Yu, D. Zappala, and L. Zhang. Content-based security for the web. In *Proceedings of New Security Paradigms Workshop (NSPW)*, Sept. 2016.

[2] A. Afanasyev, J. Shi, B. Zhang, L. Zhang, et al. NFD developer's guide. Technical Report NDN-0021, Revision 7, NDN Project, October 2016.

[3] J. Angwin, J. Larson, C. Savage, J. Risen, H. Moltke, and L. Poitras. NSA spying relies on AT&T's 'extreme willingness to help'. https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help, 2015. Accessed: September 18, 2015.

[4] R. Barnes. Use cases and requirements for JSON object signing and encryption (JOSE). RFC 7165, 2014.

[5] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and J. K. Zinzindohoue. A messy state of the union: Taming the composite state machines of TLS. In *IEEE Symposium on Security and Privacy (SP)*, pages 535–552, 2015.

[6] B. Carpenter and S. Brim. Middleboxes: Taxonomy and issues. RFC 3234, February 2002.

[7] T. Dierks and E. Rescorla. The transport layer security (TLS) protocol version 1.2. RFC 5246, August 2008.

[8] Z. Durumeric, D. Adrian, M. Bailey, and J. A. Halderman. Heartbleed bug health report. https://zmap.io/heartbleed/. Accessed: September 23, 2015.

[9] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey, and J. A. Halderman. The matter of Heartbleed. In *Proceedings of 14th ACM Internet Measurement Conference (IMC)*, 2015.

[10] P. Gusev. NdnCon (NDN COnfereNcing tool). https://github.com/remap/ndncon. Accessed: September 23, 2015.

[11] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard. Networking named content. In *Proceedings of 5th ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, 2009.

[12] G. Keizer. Apple's OS X 'Rootpipe' patch flops, fails to fix flaw. http://www.computerworld.com/article/2912619/mac-os-x/apples-os-x-rootpipe-patch-flops-fails-to-fix-flaw.html, 2015. Accessed: September 23, 2015.

[13] NDN Project. NDN common client libraries (NDN-CCL). http://named-data.net/codebase/platform/ndn-ccl/. Accessed: September 23, 2015.

[14] NDN Project. ndn-cxx: NDN C++ library with eXperimental eXtensions. http://named-data.net/doc/ndn-cxx/. Accessed: September 23, 2015.

[15] NDN Project. NDN Testbed. http://named-data.net/ndn-testbed/. Accessed: September 23, 2015.

[16] NDN Project. NLSR—Named Data Link State Routing Protocol. http://named-data.net/doc/NLSR/. Accessed: September 23, 2015.

[17] NDN Project. repo-ng: Next generation of NDN repository. https://github.com/named-data/repo-ng. Accessed: September 23, 2015.

[18] NDN Team. Named Data Networking (NDN) Project. Technical Report NDN-0001, Named Data Networking Project, October 2010.

[19] E. Rescorla and N. Modadugu. Datagram transport layer security version 1.2. RFC 6347, 2012.

[20] Z. Shelby, K. Hartke, and C. Bormann. The constrained application protocol (CoAP). RFC 7959, June 2014.

[21] Y. Yu, A. Afanasyev, D. Clark, kc claffy, V. Jacobson, and L. Zhang. Schematizing and automating trust in Named Data Networking. In *2nd ACM Conference on Information-Centric Networking (accepted)*, September 2015.

[22] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang. Named Data Networking. *ACM SIGCOMM Computer Communication Review (CCR)*, 44(3):66–73, Jul 2014.

[23] Z. Zhu and A. Afanasyev. Let's ChronoSync: Decentralized dataset state synchronization in Named Data Networking. In *Proceedings of the 21st IEEE International Conference on Network Protocols (ICNP)*, 2013.

[24] Z. Zhu, C. Bian, A. Afanasyev, V. Jacobson, and L. Zhang. Chronos: Serverless multi-user chat over NDN. Technical Report NDN-0008, NDN Project, October 2012.

Biographical Sketch

ALEXANDER AFANASYEV

School of Computing and Information Sciences
Florida International University
11200 SW 8th St, PG6 140D,
Miami, FL 33199
aa@cs.fiu.edu
+1 (305) 348-4960
https://users.cs.fiu.edu/~afanasyev/

A. Professional Preparation

Bauman Moscow State Technical University, Moscow, Russia, Computer Science, B.S., 2005
Bauman Moscow State Technical University, Moscow, Russia, Computer Science, M.S., 2007
University of California, Los Angeles, Los Angeles, Computer Science, M.S., 2012
University of California, Los Angeles, Los Angeles, Computer Science, Ph.D., 2013

B. Appointments

Assistant Professor, School of Computing and Information Sciences, Florida International University, 2017–present time
Adjunct Assistant Professor, Computer Science Department, UCLA, 2016–present time
Assistant Researcher, Computer Science Department, UCLA, 2015–2016
Postdoctoral Scholar, Computer Science Department, UCLA, 2013–2015
Graduate Student Researcher, Computer Science Department, UCLA, 2008–2013

C. Five Examples of Broader Impact

1. Y. Yu, A. Afanasyev, D. Clark, kc claffy, V. Jacobson, and L. Zhang. Schematizing and automating trust in Named Data Networking. In Proceedings of 2nd ACM Conference on Information-Centric Networking, 2015.
2. "Named Data Networking," L. Zhang, A. Afanasyev, J. Burke, kc claffy, L. Wang, V. Jacobson, P. Crowley, C. Papadopoulos, B. Zhang. ACM SIGCOMM Computer Communication Review, 2014.
3. NFD—Named Data Networking Forwarding Daemon (http://named-data.net/doc/NFD/)
4. W. Shang, Z. Wang, A. Afanasyev, J. Burke, and L. Zhang, "Breaking out of the Cloud: Local Trust Management and Rendezvous in Named Data Networking of Things," in Proceedings of the 2nd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, April 2017.
5. A. Afanasyev, C. Yi, L. Wang, B. Zhang, and L. Zhang. SNAMP: Secure namespace mapping to scale NDN forwarding. In Proceedings of 18th IEEE Global Internet Symposium (GI 2015), 2015.

D. Other Personnel (Collaborators) in Last 5 Years

- Alex J. Halderman (University of Michigan, Ann Arbor);

- Allison Mankin (Salesforce);
- Beichuan Zhang (University of Arizona);
- Bogdan Carbunar (Florida International University);
- Bongjun Ko (IBM T. J. Watson Research Center);
- Cheng Yi (Google);
- Christopher Gibson (IBM, UK);
- Christos Papadopoulos (Colorado State University);
- Chunyi Peng (Ohio State University);
- Daniel Zappala (Brigham Young University);
- David Clark (Massachusetts Institute of Technology);
- Deng Pan (Florida International University);
- Endadul Hoque (Florida International University);
- Eric Osterweil (Verisign);
- Erik Kline (USC Information Sciences Institute);
- Ersin Uzun (PARC);
- GQ Wang (Huawei);
- Giovanni Pau (UPMC-LIP6 / University of California, Los Angeles);
- Jason Cong (University of California, Los Angeles);
- Jeff Burke (University of California, Los Angeles);
- Jiangzhe Wang (AT&T Labs);
- Josh Polterock (University of California, San Diego);
- Jun Bi (Tsingua University);
- Jun Li (Florida International University);
- Kent Seamons (Brigham Young University);
- Kevin Chan (U.S. Army Research Laboratory);
- Kim Claffy (University of California, San Diego);
- Lan Wang (University of Memphis);
- Leonard Kleinrock (University of California, Los Angeles);
- Mario Gerla (University of California, Los Angeles);
- Mark Finlayson (Florida International University);
- Mark Stapp (Cisco);
- Matthias Waehlisch (Freie Universität Berlin);
- Niki Pissinou (Florida International University);
- Pablo Bermell-Garcia (Airbus Group, UK);
- Patrick Crowley (Washington University in St. Louis);
- Peter Reiher (University of California, Los Angeles);
- Priya Mahadevan (Google);
- Ravi Ravindran (Huawei);
- Ryuji Wakikawa (Softbank, Japan);
- Satyajayant Misra (New Mexico State University);
- Scott Ruoti (Brigham Young University);
- Sitharama S. Iyengar (Florida International University);
- Songwu Lu (University of California, Los Angeles);
- Vahab Pournaghshband (California State University, Northridge);
- Van Jacobson (Google);
- Yingdi Yu (Facebook);
- Yu Zhang (Harbin Institute of Technology, China);

- Zhenkai Zhu (LinkedIn)

E. Graduate and Postdoctoral Advisor
- Lixia Zhang, University of California, Los Angeles

F. Graduate Advisees
- Rajender Kumar, Florida International University
- Sanjeev Kaushik Ramani, Florida International University
- Tarannum Islam, Florida International University

F. Undergraduate Advisees
- Alexander Monaco, Florida International University

Biographical Sketch

WEI DING

https://floridapoly.edu/faculty/dr-wei-ding/
wding@floridapoly.edu

A. Education
Northeastern University (China), Computer Science and App, B.S., 1988
University of Science & Tech of China, Computer Science & Tech, M.S., 1996
Louisiana State University, Computer Science, Ph.D., 2006

B. Appointments
Associate Professor, Florida Polytechnic University, College of Innovation and Technology, 2015 - present
Assistant Professor, New York Institute of Technology, Dept. of Computer Science, 2011 - 2014
Assistant Professor, Austin Peay State University, Dept. of Computer Science & Information Technology, 2008 - 2011
Assistant Professor, University of Maine at Fort Kent, Division of Natural and Behavioral Sciences, 2006 - 2008
Senior Programmer, Anhui Electric Power Design Institute, Hefei, China, 1998 - 2001
Project Manager, Anhui Electric Power Design Institute, Hefei, China, 1996 - 1997
Engineer of Automatic Control & Software, Hefei Steel Company, Hefei, China, 1988 - 1993

C. Five Examples of Broad Impact
1. Wei Ding, the representative of Florida Polytechnic University at the Florida Center for Cybersecurity, November 2017 – present.
2. Wei Ding, invited tutorial "Declarative Cyber-Physical Systems and Its Applications," 2017 IEEE International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC2017), Shanghai, China, August 16-18, 2017.
3. Session chair, technical session 6A "Bioinformatics and Bio-Medical Informatics", the 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD 2017), July 29-31 2017, Guilin, China.
4. Wei Ding and José Arriaga, "A Universal Algorithm to Secure Stolen Mobile Devices Using Wi-Fi in Indoors Environments," accepted, 3rd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud'2016), Beijing, China, July 25-27, 2016.
5. Technical Program Committee (TPC) Member, 2015 IEEE International Conference on Communications (ICC'15), Wireless Communications Symposium, London, UK June 8 - 12, 2015.

D. Other Personnels (Collaborators) in Last 5 Years
- Florida Polytechnic University: Sesha Srinivasan, Athanasios Gentimis, Feng-Jen Yang, Jaspreet Dhau, Nicoleta Sorloaica-Hickman, Ryan Integlia, Scott Wallen, Gary R Albarelli, Indira Sukhraj
- Florida International University: S. S. Iyengar, Jerry Miller, Alexander Afanasyev
- Northwestern University: Alan Varteres Sahakian, Giovanni Santostasi, Phyllis Zee
- Columbus State University: Sumanth Yenduri, Lydia Ray
- Georgia Institute of Technology: Michael Cathcart

- New York Institute of Technology: Ricado Cabret, Farshid Delgosha, Ziqian Dong, Paolo Gasti, Ely Rabin, Jason Van Nest, William Werner
- National Cheng Kung University (Taiwan): Hsiao-Hwa Chen
- Austin Peay State University: Yingbing Yu
- University of Southern Mississippi: Louise Perkins, Chabli Boler, John Harris
- Virginia Tech: Bireswar Laha
- Wuhan University (China): Xiaohui Cui

E. Graduate Advisor
S.S. Iyengar, Florida International University

F. Graduate Advisees
- Christopher Didier, Florida Polytechnic University
- José Arriaga, Florida Polytechnic University
- Jiaxin Li, New York Institute of Technology
- Yu Du, New York Institute of Technology
- Kamalpreet Bhangu, New York Institute of Technology
- Weiyu Hsu, New York Institute of Technology

Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication

BUDGET JUSTIFICATION

Florida International University

Investigator: Alex Afanasyev

A. Senior Personnel: $5,000

PI Dr. Alex Afanasyev will lead the research work outlined in this proposal. Dr. Afanasyev will devote 0.45 summer months to the project.

B. Other Personnel: $19,108

Graduate Student support includes support for 1 graduate research assistant in the Fall 2019 and Spring 2020 semesters at the anticipated FIU rate.

C. Fringe Benefits: $3,790

FIU is currently using a fringe benefit rate of 33.76% for Faculty / Administrative; 47.22% for Staff employees; 3.72% for Non Student OPS; 11% for Graduate Student Assistants; .03% for Student OPS employees. This rate is proposed at proposal submission and is an estimate for budgeting purposes only.

D. Travel: $2,421

Domestic Travel is budgeted for the PI and Graduate Student to visit project collaborators, attend relevant Cyber Florida meetings, and to disseminate results at conferences and workshops.

E. Other Direct Costs: $44,681

Other includes tuition for the graduate research assistant at the anticipated FIU in-state rate and 18 credits per year.

Subaward includes $37,500 for Florida Poly's portion of this project, to be led by Dr. Wei Ding.

F. Total Direct Costs: $75,000

G. Indirect Costs: $0

Per the Cyber Florida Collaborative Award Seed Program solicitation, F&A costs are not allowable.

H. Total Direct and Indirect Costs: $75,000

FIU | FLORIDA INTERNATIONAL UNIVERSITY

To Whom it may concern:

The following fringe rates are effective as of March 26, 2018 on all proposals being submitted by Florida International University and will be effective for all awards as of July 1st, 2018:

Employee Group	Pooled Fringe Benefit Rate
College of Medicine (COM) Faculty	23.83%
Admin/Faculty excluding COM Faculty	33.76%
Staff	47.22%
Non Student OPS	3.72%
Graduate Student Assistants	11.00%
Student OPS (excluding Graduate Student Assistants)	0.03%

Below is a detailed breakdown of each of the fringe rates:

	COM Faculty	Admin/ Faculty	Staff	Non Student OPS	Graduate Student Assistants	Student OPS
Social Security	4.16%	5.54%	5.50%	0.00%	0.00%	0.00%
Medicare	1.37%	1.42%	1.27%	1.45%	0.01%	0.03%
Retirement	8.15%	8.55%	8.57%	0.00%	0.00%	0.00%
Health	7.67%	15.18%	29.15%	2.16%	10.99%	0.00%
Life	0.02%	0.05%	0.11%	0.00%	0.00%	0.00%
Disability	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Unemployment Compensation	0.00%	0.02%	0.11%	0.10%	0.00%	0.00%
Tuition Waivers	0.12%	0.59%	1.55%	0.00%	0.00%	0.00%
Parental & Sabbatical Leave	0.23%	1.23%	0.12%	0.00%	0.00%	0.00%
Medical Leave	0.93%	0.21%	0.43%	0.00%	0.00%	0.00%
Sick & Vacation Payouts	1.33%	1.19%	0.75%	0.01%	0.00%	0.00%
Fringe Change	-0.15%	-0.23%	-0.34%	0.00%	0.00%	0.00%
Total	**23.83%**	**33.76%**	**47.22%**	**3.72%**	**11.00%**	**0.03%**

If you have any questions, please do not hesitate to contact me.

Sincerely,

Robert Gutierrez,
Assistant Vice President for Research

OFFICE OF RESEARCH AND ECONOMIC DEVELOPMENT
Modesto Maidique Campus · MARC 430 · Miami, FL 33199 · Tel 305-348-2494 · Fax 305-348-4117 · www.fiu.edu

Florida International University
GRADUATE Tuition and Fees
2018-2019 Academic Year

New Students - Admit Term Fall 2006 or Thereafter

Tuition	Resident	Non-Res	GA/TA Rate (.5 FTE)	RA Rate (Grant pays tuition)
Tuition per credit (matriculation)	$379.95	$900.00	Waived	$379.95
Per Credit Hour Fees	$75.69	$101.69	$75.69	$75.69
Total Tuition and Fees per Credit	$455.64	$1,001.69	$75.69	$455.64
Semester Fees				
Health	$93.69	$93.69	$93.69	$93.69
Athletic	$10.00	$10.00	$10.00	$10.00
Parking Fee (Fall\Spring)	$90.70	$90.70	$90.70	$90.70
Total per Semester Fees (Fall\Spring)	$194.39	$194.39	$194.39	$194.39
Parking Fee (Summer)	$84.58	$84.58	$84.58	$84.58
Total per Semester Fees (Summer)	$188.27	$188.27	$188.27	$188.27

Total Tuition and Fees per semester Not Covered by Assistantship	GA/TA Rate (.5 FTE)	RA Rate (Grant pays tuition)	Full-time Enrollment
Fall 2018 (Includes $10 Photo ID fee)†	$885.60	$4,305.15	**9 credits**
Spring 2019 †*	$875.60	$4,295.15	**9 credits**
Summer 2019 †*	$642.41	$2,922.11	**6 credits**

† add $35 orientation fee if student's first semester.
* add $10 Photo ID fee if student's first semester.

Continuing Students - Admit Term Before Fall 2006

Tuition	Resident	Non-Res	GA/TA Rate (.5 FTE)	RA Rate (Grant pays tuition)
Tuition per credit (matriculation)	$362.71	$882.76	Waived	$362.71
Total Per Credit Hour Fees	$73.97	$99.97	$73.97	$73.97
Total Tuition and Fees per Credit	$436.68	$982.73	$73.97	$436.68
Semester Fees				
Health	$93.69	$93.69	$93.69	$93.69
Athletic	$10.00	$10.00	$10.00	$10.00
Parking Fee (Fall\Spring)	$90.70	$90.70	$90.70	$90.70
Total per Semester Fees (Fall\Spring)	$194.39	$194.39	$194.39	$194.39
Parking Fee (Summer)	$84.58	$84.58	$84.58	$84.58
Total per Semester Fees (Summer)	$188.27	$188.27	$188.27	$188.27

Total Tuition and Fees per semester Not Covered by Assistantship	GA/TA Rate (.5 FTE)	RA Rate (Grant pays tuition)	Full-time Enrollment
Fall 2018 (Includes $10 Photo ID fee)	$870.12	$4,134.51	**9 credits**
Spring 2019	$860.12	$4,124.51	**9 credits**
Summer 2019	$632.09	$2,808.35	**6 credits**

Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication

BUDGET JUSTIFICATION

Florida Polytechnic University

Investigator: Wei Ding

Senior Personnel

On Florida Polytechnic University (FPU) side, Dr. Wei Ding (Co-PI) will monitor collaboration between two institutions, supervise students and other participating parties, and execute the research plan. Dr. Ding (base annual salary of $89,983.92 for academic year, i.e. 9 months): 1.5 credit hour (1/2 month in terms of 9 month academic year). **Total Senior Personnel: $5,000**

Student Salary

Graduate students and undergraduate research assistants will be responsible for project related research activities assigned by the PI and Co-PI. Graduate students will be hired for total 1080 hours. SUS pay rate is $15 per hour for graduate students. Total cost for graduate students is $16,200. FPU will also employ undergraduate research assistants for total 800 hours at the rate of $10 per hour, cost $9,000. **Total for students is $25,200.**

Fringe Benefits

Fringe benefits involves the PI and students. According to the university guidelines, the fringe rate is 27% for Co-PI during regular semesters, with total $1,350. According to the university guidelines, the fringe rate for students is 8%, with total $1296 for graduate students and total $720 for undergraduate students. The total fringe for students is $2,016.
Total Fringe Benefits: $3,366.00.

Travel

The travel costs are based on current low end average round trip airfare on air carriers, the per diem rate for meals and hotel, and other related expenses. Funds are requested to cover the cost of following travel itineraries.

- One time travel to Florida International University (FIU) for collaboration: number of attendees 2, 1 night hotel ($100 per person per night), meals ($50 per person per day), mileage & tolls (500 miles round trip at 44.5cents per mile plus $27.50 in tolls = $250 total, assuming shared personal car). Total: $550
- One time travel to FC2 meeting: number of attendees 2, 2 nights' hotel ($100 per person per night), 2 days' meals ($75 per person per day), mileage and tolls ($250 as above). Total: $950.
- Travel to one TBD Conference: number of attendees 1, round-trip flight ($350), 2 nights hotel ($175 per night, $350 total), 3 days meals ($75 per day), 3 days car rental ($100), conference registration ($400). Total: $1,425.

Total: $2,925 budgeted for the project related travel.

Supplies / Materials

Consumable for office and computer usage **Total: $1,059.00.**

Total Direct Costs

Total direct costs are calculated by adding the values from the sections A through E, which is **$37,500 for one year**.

Associate Professor (Computer Science & Info Technology)
Phone Number +1 (863) 8748524 (Landline)
Email Address wding@floridapoly.edu
Location JD Alexander Florida Polytechnic Main Campus

Terence Parker
Manager

Compensation

Compensation

Totals

Total Salary & Allowances	Total Base Pay	Currency	Frequency
95,464.03	95,464.03	USD	Annual

Compensation

Compensation Package FPU Compensation Package
Grade No Grade - Salary
Total Base Pay Range 0.00 - 0.00 USD Annual
Company Florida Polytechnic University

Plan Assignments

Effective Date	Compensation Plan	Assignment
02/01/2018	Academic Salary Plan	95,464.03 USD Annual

Current and Pending Support

Investigator: Alexander Afanasyev

Support:	Pending
Project/Proposal Title:	Applying Named Data Networking Principles for REST Object Authentication in IoT
Source of Support:	FC2
Total Award Amount:	75,000, 07/01/2018 – 06/30/2019
Person-Months Per Year Committed to the Project:	Summer: 0.45
Brief Overview:	The project proposes to address IoT security problems by developing a content-based security architecture that directly secures RESTful information exchanges end-to-end. By applying principles of Named Data Networking architecture, clients will send secured requests to retrieve uniquely named secured request and receive secured responses, without dependency on the underlying connection, group channel, or data storage security. We will explore both application of the content-based security within the existing IP/HTTP and IP/CoAP infrastructure, as well build a prototype of the native NDN- based IoT framework that provides security directly at the network level. The latter is especially important in constrained environments of many IoT applications, where IP stack cannot function effectively.

Support:	Pending
Project/Proposal Title:	CNS Core: Small: Collaborative: Un-Stealthify: End-to-End Detection of Evasive Middleboxes
Source of Support:	NSF
Total Award Amount:	500,000, 10/01/2019 – 09/30/2022
Person-Months Per Year Committed to the Project:	Summer: 0.5
Brief Overview:	This work proposes development, deployment at different scales, and evaluation of NDNCONF protocol that provides flexible management capabilities for the future Named Data Networking (NDN) networks. The primary goal of the proposed work is to utilize directly all benefits provided by the NDN architecture, including the structured naming shared among network and application layers, stateful data retrieval with name-based interest forwarding, in-network caching, data-centric security model, and others. The proposed work will capitalize on the PI's existing experience as part of the NDN project, part of the NSF Future Internet Architecture program, and the resulting developed codebases. We also expect to learn new lessons from this proposed research that can be fed back into the NDN research effort to refine the architecture and

	implementation to meet real application and networking management requirements.

Support:	Current
Project/Proposal Title:	RET in Engineering and Computer Science SITE: Research Experience for Teachers on Cyber-Enabled Technologies
Source of Support:	NSF
Total Award Amount:	600,000, 08/01/18 – 07/31/21
Person-Months Per Year Committed to the Project:	Summer: 0.03
Brief Overview:	This project aims to engage teacher in the research to drive new wireless edge network architecture design through exercise of two distinct application scenarios to integrate with augmented reality (AR) mechanisms: AR-enriched campus daily life and disaster recovery. Leveraging the research results from Named Data Networking (NDN) project, the project proposed the design that aims to enable intrinsic security, scalable content caching and discovery, in-network hardware acceleration, and unique time-saving features enabled by NDN's direct use of application data names at network layer.

Support:	Current
Project/Proposal Title:	ICN-WEN: Collaborative Research: ICN-Enabled Secure Edge Networking with Augmented Reality
Source of Support:	NSF/Intel
Person-Months Per Year Committed to the Project:	Cal: 0.50
Total Award Amount:	750,000, 06/01/17 – 08/31/21
Brief Overview:	Technological advances have moved the society into an exciting wireless mobile computing era, where people's daily life is enhanced by new applications of ever increasing sophistication. However, today's Internet operates using the TCP/IP protocol architecture that was developed 40 years ago, which limits the utilization of these technology advances to their full potential. In this project, we propose to remove the architectural limitations by applying the results from our six-year research efforts on Named Data Networking, a realization of the Information Centric Networking (ICN) vision, to develop a new wireless network architecture.

Support:	Current
Project/Proposal Title:	CI-NEW: Collaborative: Building the Core NDN Infrastructure to Advance Information-Centric Networking Research
Source of Support:	NSF
Total Award Amount:	950,000, 09/01/16 – 08/31/20
Person-Months Per Year Committed to the Project:	Cal: 0.50
Brief Overview:	The main goal of this project is to expand Named Data Networking architecture beyond typical workstations and servers to support a wide range of platforms including mobile devices, Internet of Things (IoT) devices, and embedded systems, supporting research in these emerging areas. It will also provide performance enhancement to support research in big-data science where NDN is already being explored and high throughput is an important requirement. As we believe data-centric security is the foundation for trustworthy future Internet, security features will be implemented throughput the libraries and made an integral part of NDN application development to support security-related research. We will also implement various toolkits to enable the community performing large-scale demonstrations over the NDN testbed and cloud services.

Current and Pending Support

Investigator: Wei Ding

Support:	Pending
Project/Proposal Title:	Applying Named Data Networking Principles for REST Object Authentication in IoT
Source of Support:	FC2
Total Award Amount:	75,000, 07/01/2018 – 06/30/2019
Person-Months Per Year Committed to the Project:	Summer month: 0.50
Brief Overview:	The project proposes to address IoT security problems by developing a content-based security architecture that directly secures RESTful information exchanges end-to-end. By applying principles of Named Data Networking architecture, clients will send secured requests to retrieve uniquely named secured request and receive secured responses, without dependency on the underlying connection, group channel, or data storage security. We will explore both application of the content-based security within the existing IP/HTTP and IP/CoAP infrastructure, as well build a prototype of the native NDN- based IoT framework that provides security directly at the network level. The latter is especially important in constrained environments of many IoT applications, where IP stack cannot function effectively.

Support:	Current
Project/Proposal Title:	Aging in Place Smart Home Design Kit for Fall Prevention and Sleep Enhancement
Source of Support:	Internal Seed Grant by Florida Poly
Total Award Amount:	$21,000, 02/01/2016 – 03/312018
Person-Months Per Year Committed to the Project:	Cal month: 0.01
Brief Overview:	In this project, a general purpose (disease agnostic) infrastructure for fall prediction, detection, and prevention, will be prototyped, designed, implemented, and evaluated. The infrastructure will enable researchers and clinical practitioners to test and prototype various treatments and technologies for fall prevention, prediction, and treatments, particularly sleep related fall at regular aging in place settings. The infrastructure aims at low and middle income families in all social-economical settings, including urban, suburb, and rural surroundings. The infrastructure will follow general modeling scheme for cyber-physical systems.

Facilities and Equipment

Florida International University (FIU), School of Computing and Information Sciences

Investigator: Alexander Afanasyev

The School of Computing and Information Sciences (SCIS) maintains a data center, research and instructional labs, and computer classroom facilities. These facilities are housed in the Engineering and Computer Science (ECS) and PG6 Tech Station (PG6) buildings on the Modesto A. Maidique Campus located in Miami, Fl. The facilities are maintained by a dedicated professional IT support staff as noted in the staffing section below.

The School provides computing services such as file, compute, web, email, messaging, backup, print, and other computing services. Our networking services include a 10 Gigabit Ethernet core network that interconnects rack mounted switches and servers. All school desktop systems are connected by 1 Gigabit switched ports. Our network is highly redundant with multiple fiber and copper paths and is designed with routing fail-over capacity. We provide automated monitoring of our network and servers 24x7. The building subscribes to the university 802.11 WiFi network and SCIS maintains a legacy research WiFi network. Our network interconnects at 10GBs to the campus backbone, which provides a 10GBs connection to the NAP of the Americas to provide for connections to Internet, Internet2, Florida and National Lambda Rail, and CLARA (South American Research) networks.

Our systems feature a variety of open source, commercial development and scientific software products from numerous vendors including IBM, Microsoft, ESRI, MathWorks, etc. We provide middleware technologies to support web services. Our environment takes advantage of hundreds of open source software solutions including Apache with full mods, PHP, Perl, and many others. Many of our shared infrastructures provide virtualization services.

Notable Shared Computing Infrastructure

- File Server 1 (faculty, grad students, researchers): Silicon Mechanics Storform 2x Opteron 6320 proc, 128GB ram, Intel X520 10Gb NIC, 24x4TB 7.2k hdd (80TB after RAID), Linux ZFS system.
- File Server 2 (undergrad students): Silicon Mechanics Storform 2x Opteron 6320 proc, 128GB ram, Intel X520 10Gb NIC, 36TB (30TB after RAID), Linux ZFS system.
- Mail Server: Silicon Mechanics 1U server, 128gb ram, 2x Intel Xeon E5-2620 proc, 2x 600gb hdd, 384gb SATA Solid State Disk, gigabit nic,
- Active Directory Domain Controllers: (2) Dell Poweredge R210, 8gb ram, Intel Xeon X3430 2.4ghz proc, raid 1, gigabit nic, 2x 250gb 7.2k hdd
- Computing Server: (1) Dell Poweredge R210, 8gb ram, Intel Xeon X3430 2.4ghz proc, raid 1, gigabit nic, 2x 250gb 7.2k hdd
- Webserver and Learning Management System:
    - Silicon Mechanics Storform, 96gb ram, 2x Intel Xeon E5-2407 2.93ghz proc, raid 15, gigabit nic, 2x 2TB 15k hdd, 2x 480GB SSD

    - Dell Poweredge 2900 III, 32gb ram, 2x Intel Xeon 5410 proc, 4x 300gb hdd, gigabit nic.
    - Dell Poweredge R310, 16GB ram, 2x Intel Xeon X3470, 2TB mechanical storage.

Dedicated Shared Research and Instructional Infrastructure

- Virtual Machine Servers: (3) Dell Poweredge R410, 64gb ram, 2x Intel Xeon E5620 2.4ghz proc, gigabit nic, 1.8TB raid 5 storage, (3) Dell Poweredge R420, 96gb ram, 2x Intel Xeon E5-2450L @ 1.8GHz, gigabit nic, 1TB raid 5 storage
- General Compute Servers:
    - (2) Dell Poweredge 29xx, 64gb+ ram, Intel Xeon proc,
    - (3) Dell Poweredge R410, 64gb ram, 2x Intel Xeon X5650, gigabit nic, 3x 600gb hdd
    - (2) Dell Poweredge R710, 72gb ram, 2x Intel Xeon X5570, gigabit nic, 8x 300gb hdd
    - (2) Dell Poweredge R815, 512gb ram, 4x AMD Opteron 6380 @ 2.5GHz, 10gb nic, 1.5TB disk

Business Continuity Infrastructure

- General Compute Server: Dell Poweredge R410, 64gb ram, 2x Intel Xeon E5620 2.4ghz proc, raid 5, gigabit nic, 4x 600gb 15k hdd
- (2) 80TB Online Backup server for File Server 1 (one off-site, one in ECS Building): Silicon Mechanics Storform 2x Opteron 6320 proc, 128gb ram, Intel X520 10Gb NIC, 24x4TB 7.2k hdd (80TB after RAID). Linux ZFS system.
- (2) 80TB Online Backup server for File Server 2 (one off-site, one in ECS Building). Silicon Mechanics Storform 2x Opteron 6320 proc, 128GB ram, Intel X520 10Gb NIC, 36TB (30TB after RAID), Linux ZFS system.
- (2) 80TB Online Backup server for General Backup and Standalone systems (one off-site, one in ECS Building): Silicon Mechanics Storform 2x Opteron 6320 proc, 128gb ram, Intel X520 10Gb NIC, 24x4TB 7.2k hdd (80TB after RAID). Linux ZFS system.

Staffing

The school maintains all its computing facilities (total research and instruction: 26 labs, 350+ desktops, 100+ servers, layer 2 and 3 networking) via a dedicated Technology Group. The SCIS Technology Group consists of 5 FTE of permanent professional staff assigned to all of the school's research and instructional laboratories management. In addition, there are at least 2 FTE of temporary students specifically assigned to laboratory assistance. The SCIS Technology Group staff is organized into three groups: Engineering Services, including Networking, Systems, Desktop, and Help Desk Support, and Business Services including Technology Procurement, Asset Management, and Budget/Contract Management, and a Marketing Technology group that promotes the school via digital and social media outlets.

Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication

FACILITIES AND OTHER RESOURCES

Florida Polytechnic University

Investigator: Wei Ding

The Co-PI, Dr. Wei Ding, will provide following devices from his own collection obtained through previous faculty equipment requests.

- One frequency generator
- One sensor network kit
- One RFID kit

Besides these devices, participating students can also access devices and equipment in following university resources.

Supercomputer: The supercomputer at Florida Poly is a shared high performance computing environment serving needs in education, research, and industrial collaboration. Besides specific research usage, the supercomputer is typically used in big data analytics, cloud computing, simulation, and visualization. Two former undergraduate students who worked with the Dr. Ding utilized 64 G memory virtual computer for a simulation to generate preliminary data for his 2016 NSF CPS grant application. For this project, the supercomputer will be used rapid simulation and prototype testing and deployment.

Visualization and Robotics Lab: This lab features two lab rooms and advanced hardware and software resources, such as 20+ 3D printers, various robots, drones, and other embedded devices. The lab has considerably helped Poly's application-oriented research in engineering, AI, automation, robotics, remote sensing/control, computer graphics, gaming, and visualization. Following devices in this lab may be used for this project

- Raspberry Pi
- Humanoid NAO robot
- 3D printers

In addition, the Co-PI and his students may use the network intrusion detection kit in networked environment from the Cyber Security Lab.

FIU | Research & Economic Development
FLORIDA INTERNATIONAL UNIVERSITY

November 27, 2018

Florida Center for Cybersecurity
University of South Florida
4202 E. Fowler Avenue, Tampa, FL 33620

Proposal Title: **Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication**
Period of Performance: **07/01/2018 – 06/30/2019**
Requested Amount: **$75,00.00** (FIU $37,500.00 and FL Polytech $37,500.00)

To Whom It May Concern:

On behalf of Florida International University and Dr. Alex Afanasyev, I am pleased to support the enclosed proposal for funding. The proposal has been reviewed and approved by our office. This letter also serves as confirmation, that Dr. Afanasyev's base salary is $97,440.00. One Graduate student will be hired for the Fall 2019 and Spring 2020 semesters at a $27,600.00 annual salary.

Any negotiations related to an award should be directed to Robert Gutierrez, Assistant Vice President for Research, who can be reached at (305) 348-2494 or gutierrr@fiu.edu.

Award documents resulting from this submission should be sent to the above-named representative at the Office of Research & Economic Development, Florida International University, 11200 SW 8 Street, MARC 430, Miami, FL 33199.

Thank you in advance for your consideration.

Sincerely,

Ludmilla Etienne

Ludmilla C. Etienne
Associate Director, Pre-Award Administration

LE/MA

OFFICE OF RESEARCH AND ECONOMIC DEVELOPMENT
11200 SW 8th Street · MARC 430 · Miami, FL 33199 · Tel 305-348-2494 · Fax 305-348-4117 · research.fiu.edu

FLORIDA POLYTECHNIC UNIVERSITY

November 26, 2018

Dear FIU Officials:

I am the Provost and the Execute Vice President for Academic Affairs of Florida Polytechnic University (FPU). I am writing to support Dr. Wei Ding as Co-PI for his effort to apply for the seed grant from Cyber Florida through the proposed project entitled "Applying Named Data Networking and Blockchain Principles for RESTful IoT Authentication." The total requested budget for Florida Polytechnic's portion is $37,500.

FPU will support the collaboration between Dr. Ding and Dr. Afanasyev from the School of Computing and Information Sciences (SCIS) at Florida International University (FIU) for the above mentioned research project. FPU will devote necessary resources, such as student time, supplies, labs, and equipment, etc., to this research project and this collaboration.

Sincerely,

Terry Parker, Ph.D.
Provost and the Vice President
Academic Affairs

4700 RESEARCH WAY
LAKELAND, FL 33805-8531

FLORIDAPOLY.EDU