A Novel Name-Based Security Mechanism for Information-Centric Networking

Balkis Hamdane[1,2], Sihem Guemara El Fatmi[1], and Ahmed Serhrouchni[2]

[1]Digital Security Research Unit, Higher School of Communication of Tunis (Sup'Com), Tunisia
[2]Télécom ParisTech, Paris, France
{balkis.hamdane, Ahmed.Serhrouchni}@telecom-paristech.fr
sihem.guemara@supcom.rnu.tn

***Abstract*—The Information-Centric Networking (ICN) approach represents a prominent future Internet research activity. It aims to ensure a large-scale content distribution while supporting mobility and security natively. In this approach, named content represents the central element and it is independent from its delivering host. Security can no longer be tied to a particular location. It is built-in the content and it strongly depends on names. There are mainly two naming approaches: (1) hierarchical and human readable, (2) flat and self-certifying. Each one provides certain security services. The other services are ensured using additional mechanisms. In this paper, we propose the adaptation of the naming system in order to provide a robust security model built-in the name. The proposed solution combines the benefits of the two existing naming system and it is built on top of Identity-Based Cryptography (IBC). A formal security analysis is provided to confirm the safety of the new proposal.**

***Index Terms*—Information-Centric Networking, security, naming, Named Data Networking, Network of Information, Identity-based cryptography, AVISPA**

I. Introduction

Information-Centric Networking (ICN) [1] [2] approach constitutes a prominent direction for the future Internet research activities. It aims to provide an Internet architecture that is more suited to today's use. Its goal is to ensure a large-scale content distribution while supporting mobility and security natively.

In ICN, the named information represents the central element rather than IP addresses. Indeed instead of establishing communication channels between hosts as in the current Internet, the network focuses on information delivery to consumers regardless of their locations. The content source can be any node possessing a copy of this data through caching. The security in ICN can no longer depend on the delivering host [3] [4]. That's why a content-centric security model is adopted. In this model, security aspects are built-in the content and they strongly depend on the adopted naming system.

There are two main naming approaches. The first one provides hierarchical and human-readable names. It has been defined in the Content Centric Networking (CCN) [3] and Named Data Networking (NDN) [5] projects. The second one proposes flat and self-certifying names. It has been adopted by various ICN projects as Network of Information (NetInf) [6]. Each naming system provides certain security services. The other services are not ensured or they are provided by using additional and more costly mechanisms.

978-1-4799-3083-8/14/$31.00 © 2014 IEEE

There is an ongoing debate on the most appropriate naming approach in ICN [7] [8]. In this paper we analyze the impact of the name structure and its semantic on security in order to prove that these two approaches are complementary. We propose then the adaptation of the naming system to provide a robust security model built-in the name. The proposed solution combines the characteristics and benefits of the two existing naming approaches. It uses the identity-based cryptography (IBC) [9] [10] and it is integrated into the naming system of the two representative projects NDN and NetInf. A formal security analysis is provided to confirm the safety of our proposal.

The rest of this paper is structured as follows. In section II, we define the security services in the ICN approach and we present the NDN and NetInf projects with a special focus on security. In section III, we analyze the impact of naming on security. In section IV, we propose a new name-based security mechanism. In Section V, we provide a formal validation of our proposal and finally we conclude in section VI.

II. Security in Information Centric Networks

In Information Centric Networking approach, a content-centric security model is adopted. This model relies on the following security services [7] [4][6]:

- Data integrity: received data are in their original form, generated by a legitimate producer.
- Name authenticity: received content correspond to the name given by the requester.
- Data provenance: content are published by an appropriate producer. This combines the authentication and the identification of the producer.
- Relevance: data represents the answer to a question the receiver asked.
- Confidentiality: only authorized entities can read content.
- Availability: data are available to authorized entities.
- Access Control: access to content is restricted to authorized entities.

The naming structure and its semantic play a critical role to ensure these security services. There are mainly two naming approaches: (1) hierarchical and human readable, (2) flat and self-certifying. In the rest of this section, we present Named Data Networking (NDN) and Network of Information (NetInf) projects with a special focus on security. We feel that these projects are representative of the two naming system and cover the diverse research efforts toward naming and security in ICN.

A. Named Data Networking

1) General presentation: Content Centric Networking (CCN) [3] has been proposed since 2006 by Van Jacobson in the Palo Alto Research Center (PARC). In September 2010, it was selected as one of the four projects of the National Science Foundation's. In this new context, its name becomes Named Data Networking (NDN).

There are two packet types in NDN: Interest and Data. The Interest packet is sent to the network by consumer to request data. It carries a name identifying the required content. The Data packet represents the response to the Interest. It is composed of a name, a signed info field and a signature calculated on the entire packet. This packet satisfies an Interest if the name in the Interest packet is the same or represents the prefix of its name.

Names in NDN are hierarchical and human-readable. They are mainly composed of three parts: a globally routable name, an organizational name and a versioning and segmentation part.

2) Security: In order to achieve security, NDN implements several mechanisms. To ensure data integrity, name authenticity and producer authentication, each chink of data is signed together with its name, securely binding them. The signature verification requires the public key of the producer. This key can be recovered as an NDN data, based on information provided in the field signed info. To build trust in this key, a traditional public key infrastructure (PKI) can be deployed. However, besides the elevated cost and the high number of issued certificates, the use of PKI is vulnerable to a potential attack that we indentified in [11]. As shown in figure 1, to request a data, the user sends an Interest packet. By hearing this packet, an attacker produces and sends a fake Data packet containing the same name, false data, information about his public key and the associated digital signature. This packet seems legitimate and bears a legitimate signature. Therefore, the requester does not perceive the false data. The requester initially only knows the name of the desired content. A link between the name and the public key is then required to prevent an attacker to forge a Data packet with a valid signature.

To guarantee producer identification, his identity must be bound to the received data. This can be ensured if the signature in the Data packet can be verified and the content name contains valid information about the producer identity.

Since the content name in Interest packet is meaningful and it is equal to the content name in Data packet, the relevance service is explicit in this name [7].

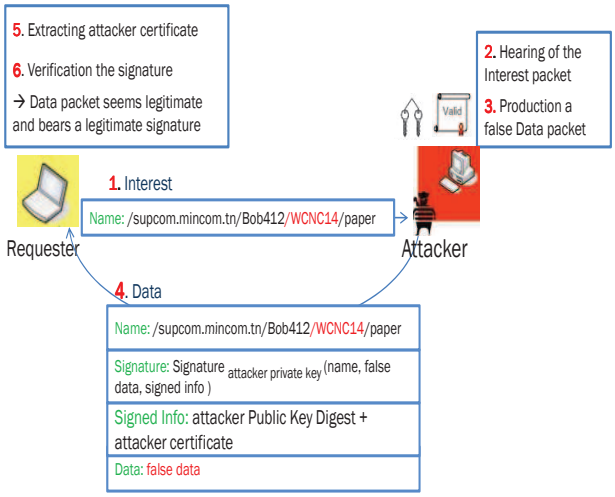


Fig. 1. Identified attack in NDN

B. Network of Information

1) General presentation: Network of Information (NetInf) [6] is a European ICN project that was initially conceived in 2008 in the project 4WARD. In 2010, it was prolonged within the project SAIL.

In NetInf, pieces of information are called Named Data Object (NDO). They are globally identified by unique names. They also carry metadata which are composed of attributes describing the NDO, information necessary to perform the security functions and the signature of data.

Names are flat, composed of two parts: the authenticator A and the label L. A is the cryptographic hash of the producer's public key K_{pub}. L uniquely identifies the NDO.

2) Security: The naming system in Netinf plays an important role in security [12]. It ensures the self-certification of the data integrity. For static content, the label L is equal to the hash of the content. The secure link established between the name and the contents makes then possible the checking of the data integrity, by simply calculating the hash and comparing it to the received one. This link ensures also name authenticity.
For dynamic NDO, metadata include the signature of content and the authenticator part of the content name is equal to the hash of the public key K_{pub} necessary to verify this signature. The secure link established between the name and the public key allows the receiver to verify the signature and to validate consequently the integrity of the data. However, this link doesn't ensure the association between a given name and a given piece of data what threatens the name authenticity. Indeed, a data can be undetectably substituted by any other data signed using the same key K_{priv} [7].

To ensure producer authentication, the metadata include a signature of the data and the hash of the producer public key using the associated private key. The binding established between the contents and the public key of the producer makes then possible the checking of the producer authentication, by simply verifying the signature.

To check producer identification, the metadata include:

- A signature calculated on content, the producer public key and its identity using the associated private key.
- A certificate issued by a PKI to ensure the association between the public key and the producer identity.

Thereby, the link established between the content, the identity of the producer and his public key allows his identification.

Finally, relevance is not ensured because a consumer uses a non human-readable name to request a NDO. He can easily accept to use a false name to retrieve desired data. He receives a valid NDO but that doesn't correspond to his request [7].

III. Impact of naming structure on security

Each ICN project proposes its own mechanisms to ensure security. These mechanisms strongly depend on the naming system adopted and the data signature.

In the NDN project, the significance of the names ensures the relevance. Their flexibility allows the introduction of information about the real identity of the producer and therefore guarantees his identification.
Also the link established with content through signature insures data integrity, name authenticity and producer authentication. However, a link between these names and the producer's public keys is missing. Yet it is necessary for the protection of the attack described in figure 1.

In the NetInf project, the self-certification of the names ensures the data integrity and even the name authenticity for the static NDO. However, the authentication and the identification of the producer are independent of the naming system and the relevance is not taken into consideration.

There is an ongoing debate on the most appropriate naming approach in ICN [7] [8]. We view that these two approaches are complementary. A hybrid naming scheme combining the characteristics and benefits of each approach will improve the content-centric security model. In this scheme, the name must contain valid and human-readable information on the producer identity and on the associated content. It must establish a link with this content through a signature. Finally, it must be self-certifying ensuring a direct link with the producer public key.

IV. A new name-based security mechanism for ICN

To provide a robust security model built-in the name, the requirements on the naming system, identified in the previous section, must be satisfied. To meet these requirements, we propose an adaptation of the naming system based on IBC [9] [10], where the producer public keys are directly derived from content names.

Other solutions based on IBC have been proposed to improve the security in the project NDN [11][13] [14]. They focus on the specific project NDN and they differ from the proposed solution in many specificities.

The proposed solution provides a generic naming system enhancing security. It can be integrated into all ICN projects and it keeps the same name structure to fit in perfectly with all other aspects of the architecture.

We present in the following the identity-based cryptography. To prove the possibility of integration of our proposal into both naming approaches, we detail the adaptation of the naming system in the two representative projects NDN and NetInf. We summarize the advantages of using IBC in NDN and NetInf in table I.

A. Identity-Based Cryptography

In an IBC cryptosystem, any string can form a valid public key. The associated private key is generated from the public key, the secret key (S) and the public parameters (params) of a server named Private Key Generator (PKG). The latter distributes securely private keys to users. The figure 2 illustrates the steps necessary to a signature generation and verification using IBC.

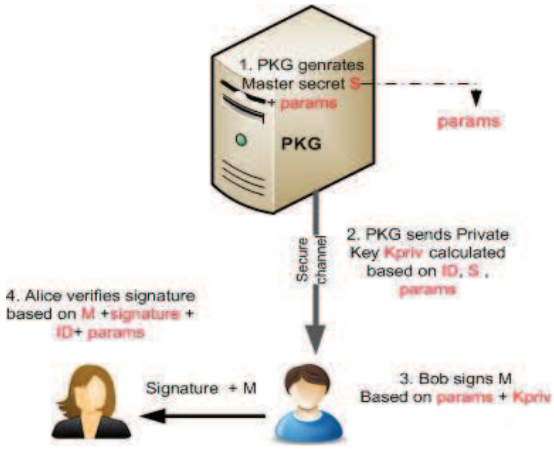


Fig. 2. Identity-Based Signature

B. A new name-based security mechanism for NDN

In the proposed solution, the name retains its hierarchical and human-readable structure. It is still composed of a globally routable name, an organizational name and a versioning and segmentation part. The organizational name includes information about the published data and the identity of the producer. The obtained name identifies as well the contents as its producer. It acts as an IBC public key for this content.
The private key K_{priv} is generated by the PKG associated with the globally routable name. This server is responsible for the secure sending of K_{priv} to its owner. It can send it encrypted with the producer identity. The PKG ensures also producers authenticating and names uniqueness under its domain.
To publish a content, the producer requests the K_{priv} key and receives it from the PKG. He uses this key to calculate the signature and finally produces a Data packet, illustrated in figure 3. This packet contains the calculated signature and the PKG public parameters params in the field signed Info. By receiving such a packet, a requester retrieves params and uses them with the name to verify the signature.

Names meet all requirements listed in Section III. They are human-readable and they contain valid information on the producer identity and on the associated content.

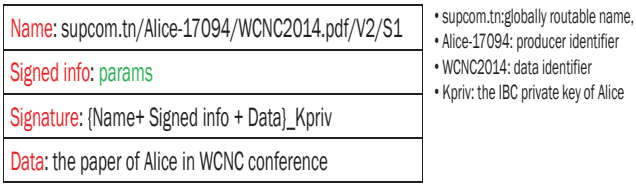


Fig. 3. Data packet in NDN with IBC

They also establish a link with the content through the signature and they are self-certifying since they act as public keys. These properties ensure the relevance, the integrity and the provenance of data and the name authenticity. Finally, they mitigate the attack described in figure 1 because a link between the name and the producer public key is provided

C. A new name-based security mechanism for NetInf

In the proposed solution, the NetInf name structure is retained. The label L is composed of the producer identifier and information on the published data. This part acts as an IBC public key. The authenticator A is equal to the cryptographic hash of the Label L for dynamic data and it is equal to the hash of the content and the PKG public parameters for static content.

The private key K_{priv} is generated by the PKG associated with the Name Resolution Service (NRS) used in routing [6]. As in NDN, this server sends securely the K_{priv} to producers and validates the information about their identities.

To publish a NDO, the producer retrieves the K_{priv} and he uses it to calculate the signature of the name, the content and the PKG public parameters params. This signature is put with params in metadata. By receiving a desired NDO and the associated metadata, a requester uses params and the label to verify the signature.

Since the name contains valid information on the producer identity and the metadata include a signature securely binding this name to the content, the integrity and the provenance of data and the name authenticity are ensured. They are built-in the naming system. In addition, the human-readable information in the name guarantees relevance. All the requirements on names listed in Section III are satisfied and the security in NetInf is improved.

V. Formal validation

In order to prove the vulnerability of the actual security model in the NDN and NetInf projects and to verify the robustness of our proposals, we use the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [15]. AVISPA represents an automatic and formal security analyzer. It takes as input the modular and expressive formal language HLSPL (High Level Protocols Specification Language) to describe security protocols and to verify their security properties.

TABLE I
NDN and NetInf comparison with and without IBC

	NDN	NDN with IBC	NetInf	NetInf with IBC
Data integrity	Requires a link between the public key and the name	Ensured	Ensured	Ensured
Name authenticity	Requires a link between the public key and the name	Ensured	Not ensured for dynamic content	Ensured
Producer authentication	Requires a link between the public key and the name	Ensured	Ensured: independent of the naming system	Ensured: built-in the naming system
Producer identification	Requires a link between the public key and the name + valid information about the producer identity in the name	Ensured	Ensured: independent of the naming system	Ensured: built-in the naming system
Relevance	Ensured	Ensured	Not ensured	Ensured

Protocol specifications in HLPSL are based on roles. Basic roles represent the actions of one principal in a run of the protocol. Composed roles instantiate basic roles and define the entire protocol [16].
To validate the security of the specified protocol, security properties are modeled as security goals in HLPSL.

AVISPA incorporates four different back-ends tools: OFMC, CL-ATSE, SATMC and TA4SP [15]. It also offers a graphical interface called Security Protocol Animator for AVISPA (SPAN) [17] that animates the HLPSL specification.

A. Formal validation of NDN

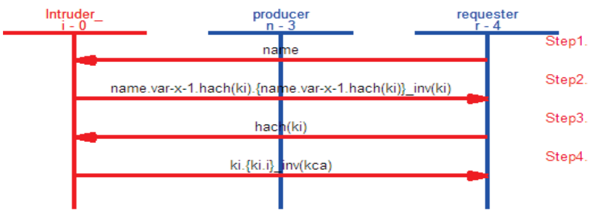
NDN with an without IBC are specified in requester and producer model using the HLPSL language. Their partial specifications are respectively given in figures 4 and 6.

For NDN without IBC, the expressions "wrequest(R,P, publickeyeditor, Name.Data')" in the role requester, "witness(P,R, publickeyeditor,Name'.Data)" in the role producer and "weak_ authentication_ on publickeyeditor" in the goal section, shown in figure 4, verify that the requester receives the exact values of the content name and the data generated by the producer. This checks data integrity, the name authenticity and the producer authentication.
The expressions "wrequest(R,P, identity, P')" in the role requester ," witness(P, R, identity,P)" in the role producer and "weak_ authentication_ on identity" in the goal section check that the requester retrieves the exact producer identity. This verifies the producer identification.

```
role requester (...
   1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Name)
   2. State=1 /\ RCV(Name.Data'.H(Kproducer').
   {Name.Data'.H(Kproducer')}_inv(Kproducer'))
   /\ Name' =Name
   =|> State':=2 /\ SND(H(Kproducer'))
   3. State=2/\ RCV(Kproducer.{Kproducer.P'}_inv(Kca))
   =|>State':=3/\wrequest(R,P,publickeyeditor,Name.Data')
   /\ wrequest(R,P, identity, P')
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role producer(...
   1. State=0 /\ RCV(Name') /\ Name' =Name
   =|> State':=1 /\ SND(Name'.Data.H(Kproducer).
   {Name'.Data.H(Kproducer)}_inv(Kproducer))
   2. State=1 /\ RCV(H(Kproducer))
   =|>State':=2/\SND (Kproducer.{Kproducer.P}_inv(Kca))
   /\ witness(P,R, publickeyeditor,Name'.Data)
   /\ witness(P, R, identity,P)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role session(...
   composition
   producer(P,Name,Data,H,Kproducer,Kca,SND2,RCV2)
   /\ requester(R,Name,H,Kca,SND1,RCV1)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role environment()...
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
goal
weak_authentication_on publickeyeditor
weak_authentication_on identity
end goal
environment()
```

Fig. 4. Extract of HLPSL specifications for NDN without IBC

The AVISPA execution proves that NDN is vulnerable to the attack described in figure 1. The animation of this attack with SPAN is shown in 5.



var-x-1: false data; ki: attacker public key; kca: certification authority public key

Fig. 5. Visualization of an attack in NDN with SPAN

For the proposal in NDN, the expressions "wrequest(R,P, publickeyeditor, Name.P.Data')" in the role requester, "witness(P,R,publickeyeditor,Name'.P.Data)" in the role producer and "weak_ authentication_ on publickeyeditor" in the goal section verify that the requester receives the exact values of the producer identity, the content name and the data generated by that producer. This checks data integrity, the name authenticity and the authentication and the identification of the producer. The execution of our proposal exhibits safe results.

B. Formal validation of NetInf

To verify NetInf with and without IBC, we defined them using the HLPSL language. Parts of their specifications are respectively illustrated in figures 7 and 8.

As in NDN the expressions "wrequest" in the requester role, "witness" in the producer role and weak_ authentication_ on on the goal section, framed in figures 7 and 8, allow the

```
role requester (...
   1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Name.P)
   2. State=1 /\ RCV(Name.P.Data'.{Name.P.Data'}_inv(Name))|
   /\ Name' =Name
   =|> State':=2/\wrequest(R,P, publickeyeditor,Name.P.Data')
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role producer(...
   1. State=0 /\ RCV(Name'.P') /\ Name' =Name /\ P' = P
   =|> State':=1 /\SND(Name'.P.Data.{Name'.P.Data}_inv(Name))
   /\ witness(P,R,publickeyeditor,Name'.P.Data)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role session(...
   composition
   producer(P,Name,Data,H,SND2,RCV2)
   /\ requester(R,Name,H,SND1,RCV1)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role environment()...
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
goal
weak_authentication_on publickeyeditor
end goal
environment()
```

Fig. 6. Extract of HLPSL specifications for NDN with IBC

```
role requester(...
   1. State=0 /\ RCV(start)  =|> State':= 1
   /\ Authenticator':= H(KPa)/\SND(Label.Authenticator')
   2. State=1/\RCV(Label.Authenticator.Data'.{Data'}_inv(KPa))
   =|> State':=2 /\ wrequest(R,P,publickeyeditor,Label
      .Authenticator.Data')
                /\SND(Metadata.Label.Authenticator)
   3. State=2 /\RCV ({Data'.H(KPa)}_inv(KPa).
   {Data.KPa.P'}_inv(KPa).KPa.{KPa.P'}_inv(Kca))
   =|> State':=3
   /\ wrequest(R,P, producerauthenticity,Data.H(KPa))
   /\ wrequest(R,P, produceridentification,P)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role producer(...
   1. State=0/\ RCV(Label'.Authenticator') /\ Label'=Label
   /\ Authenticator'= H(KPa)
   =|> State':=1 /\ SND(Label.Authenticator'.Data.{Data}_inv(KPa))
                /\witness(P,R,publickeyeditor,Label.Authenticator.Data')
   2. State=1/\ RCV (Metadata'.Label'.Authenticator')
   /\ Label'=Label /\ Authenticator'= H(KPa)
   =|> State':= 2 /\ SND({Data.H(KPa)}_inv(KPa).
   {Data.KPa.P}_inv(KPa). KPa.{KPa.P}_inv(Kca))
   /\ witness(P,R,producerauthenticity,Data.H(KPa))
   /\ witness(P,R,produceridentification,P)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role session(...
   composition
   producer(P,Data,H,KPa,Kca,Label, Metadata,SND2,RCV2)
   /\requester(R,Label,Metadata,H,KPa,Kca,SND1,RCV1)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role environment()...
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
goal
weak_authentication_on publickeyeditor
weak_authentication_on producerauthenticity
weak_authentication_on produceridentification
end goal
```

Fig. 7. Extract of HLPSL specifications for NetInf without IBC

```
role requester(...
   1. State=0 /\ RCV(start)
    =|> State':= 1/\SND(Label.P.H(Label))
   2. State=1 /\RCV(Label.H(Label).P.Data'
    .{Label.H(Label).P.Data'}_inv(Label))
   =|> State':=2 /\wrequest(R,P, publickeyediteur,
    Label.H(Label).P.Data')

end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role producer(...
   1. State=0/\ RCV(Label'.P'.H(Label'))
   =|> State':=1 /\ SND(Label.H(Label).P.
   Data.{Label.H(Label).P.Data} inv(Label))
   /\ witness(P,R,publickeyediteur,Label.H(Label).P.Data)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role session(...
   producer(P,Data,H,Label, SND2,RCV2)
   /\ requester(R,Label,H,SND1,RCV1)
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
role environment()...
end role
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
goal
weak_authentication_on publickeyediteur
end goal
```

Fig. 8. Extract of HLPSL specifications for NetInf with IBC

checking of the data integrity, the name authenticity and the authentication and the identification of the producer.

The AVISPA execution proves that the name authenticity isn't ensured in NetInf without IBC. The animation of the possible attack is illustrated with SPAN in figure 9.

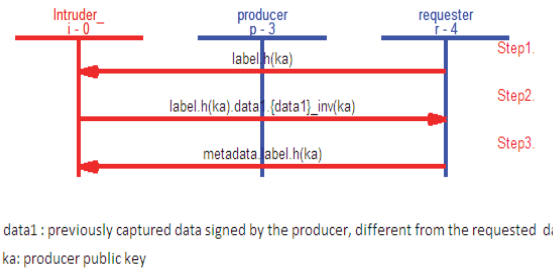


Fig. 9. Visualization of an attack in NetInf with SPAN

The execution of our proposal indicates safe results and it doesn't detect any vulnerability.

VI. Conclusion

In the Information-Centric Networking approach, the named information represent the central element in the network and they are independent from its location. Security can no longer be tied to the delivering host and a data-centric security model is adopted. This model relies on the content and especially on the adopted naming system. There are hierarchical, human readable and flat, self-certifying naming approaches.

Names in the first approach ensure the relevance but they require a link with the public key of the producer to guarantee the authentication and the identification of the producer, the data integrity and the name authenticity. One the other hand, names in the second approach ensure the data integrity and the name authenticity for static data. They don't take relevance into consideration. Also, the authentication and the identification of the producer are independent of the naming system.

To provide a better name-based security model, we proposed the use of a hybrid naming system combining the benefits of the two existing naming approaches. The proposed solution is based on the IBC and it ensures intrinsically most security services. The adaptation of the naming system in the two representative projects NDN and NetInf are also provided to prove the possibility of integration of our proposal into both naming approaches. Finally, a formal security analysis using the AVISPA tool proved the vulnerability of NDN and NetInf without IBC and the safety of our proposal.

References

[1] M. Bari, S. Rahman Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu, "A survey of naming and routing in information-centric networks," *Communications Magazine, IEEE*, vol. 50, no. 12, pp. 44–53, 2012.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *Communications Magazine, IEEE*, vol. 50, no. 7, pp. 26–36, 2012.

[3] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*. ACM, 2009, pp. 1–12.

[4] B. Ahlgren, M. D'ambrosio, C. Dannewitz, A. Eriksson, J. Golic, B. Grönvall, D. Horne, A. Lindgren, O. Mämmelä, M. Marchisio *et al.*, "Second netinf architecture description," *4WARD EU FP7 Project, Deliverable D-6.2 v2. 0*, 2010.

[5] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos *et al.*, "Named data networking (ndn) project," *NDN Technical Report NDN-0001, Xerox Palo Alto Research Center-PARC*, 2010.

[6] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, and H. Karl, "Network of information (netinf)–an information-centric networking architecture," *Computer Communications*, 2013.

[7] D. Smetters and V. Jacobson, "Securing network content," *PARC Tech Report TR-2009-1, Xerox Palo Alto Research Center-PARC*, 2009.

[8] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *Proceedings of the ACM SIGCOMM workshop on Information-centric networking*. ACM, 2011, pp. 1–6.

[9] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology—CRYPTO 2001*. Springer, 2001, pp. 213–229.

[10] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. of Australian Unix Users Group Annual Conference*, 2004, pp. 95–102.

[11] B. Hamdane, A. Serhrouchni, A. Fadlallah, and S. G. El Fatmi, "Named-data security scheme for named data networking," in *The 2012 Third International Conference on the Network of the Future (NoF)*. IFIP - IEEE, 2012, pp. 1–7.

[12] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in *INFOCOM IEEE Conference on Computer Communications Workshops, 2010*. IEEE, 2010, pp. 1–6.

[13] X. Zhang, K. Chang, H. Xiong, Y. Wen, G. Shi, and G. Wang, "Towards name-based trust and security for content-centric network," in *Network Protocols (ICNP), 2011 19th IEEE International Conference on*. IEEE, 2011, pp. 1–6.

[14] B. Hamdane, A. Serhrouchni, and S. G. E. Fatmi, "Access control enforcement in named data networking," in *International Conferece For Internet Technology And Secured Transactions, 2013*. IEEE, 2013.

[15] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *Computer Aided Verification*. Springer, 2005, pp. 281–285.

[16] B. Hamdane, A. Serhrouchni, A. Montfaucon, and S. Guemara, "Using the hmac-based one-time password algorithm for tls authentication," in *Network and Information Systems Security (SAR-SSI), 2011 Conference on*. IEEE, 2011, pp. 1–8.

[17] Y. Glouche, T. Genet, and E. Houssay, "Span–a security protocol animator for avispa–user manual," *IRISA/Université de Rennes*, vol. 1, p. 20, 2006.