ICN Privacy and Name based Security

Nikos Fotiou, George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Athens, Greece
http://mm.aueb.gr, {fotiou,polyzos}@aueb.gr

http://mm.aueb.gr/presentations/2014-ICN-Privacy-Tutorial.pdf

European Union
European Social Fund
OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY
NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND
Co- financed by Greece and the European Union

Mobile Multimedia Laboratory @ AUEB.GR

George C. Polyzos

AUEB/MMlab Collaborators

Faculty: *Giannis Marias, Vasilios A. Siris, **George Xylomenos**, Stavros Toumpis, Iordanis Koutsopoulos*

PostDocs: ***N. Fotiou**, C.N. Ververidis, K.V. Katsaros, P. Frangoudis*

PhD students: *C. Tsilopoulos, X. Vasilakos, C. Stais, I. Thomas, V. Douros*

+MSc, undergraduate students

Mobile Multimedia Laboratory

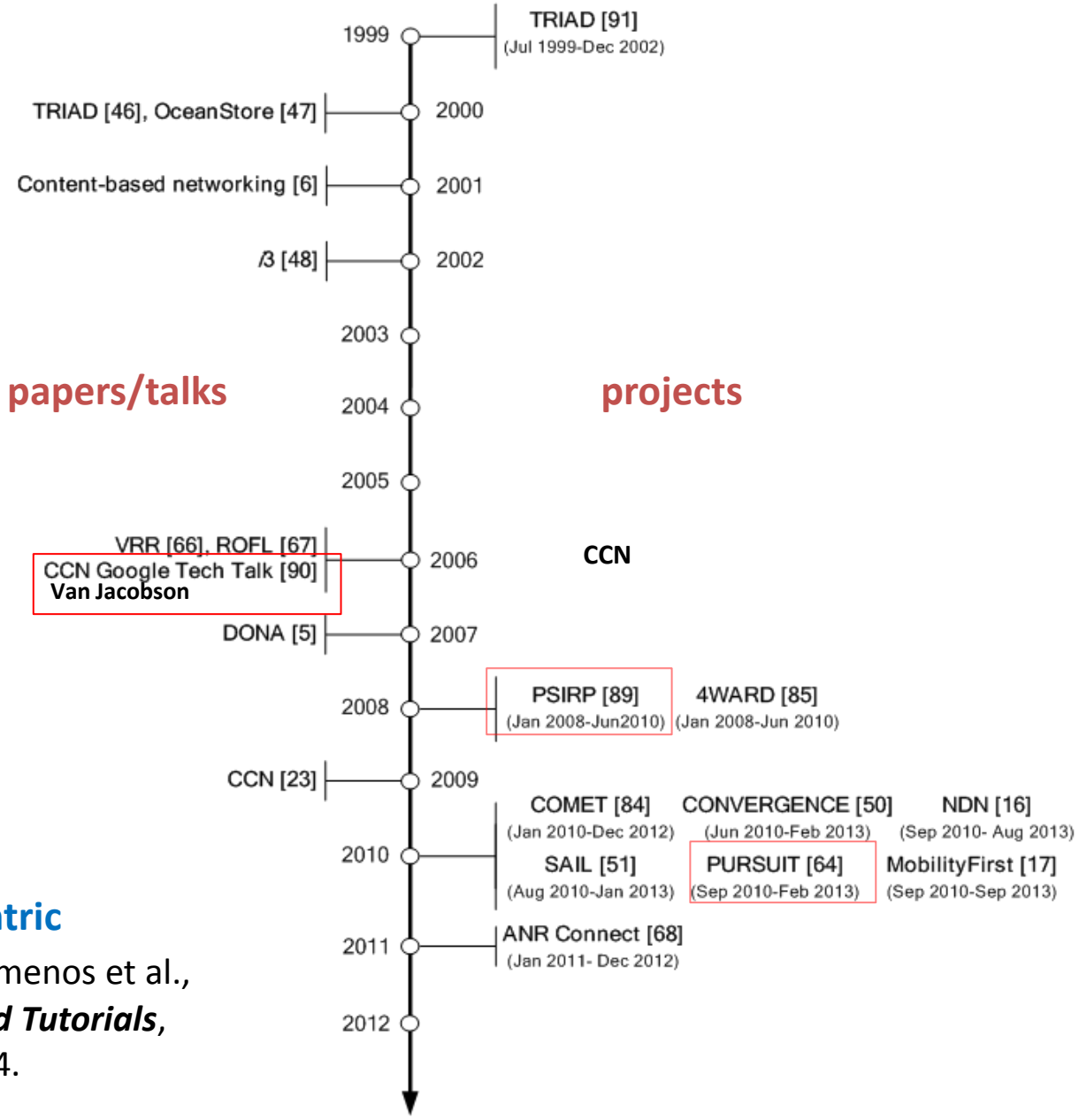
Department of Informatics, School of Information Sciences and Technology

Athens University of Economics and Business

Athens, Greece

http://mm.aueb.gr/ polyzos@aueb.gr

ICN timeline



"**A Survey of Information-Centric Networking Research**," G. Xylomenos et al., ***IEEE Communications Surveys and Tutorials***, vol. 16, no. 2, pp. 1024-1049, 2014.

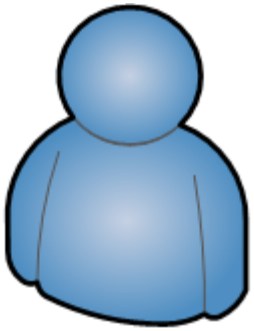
Mobile Multimedia Lab @ AUEB

Relevant Research Projects

- **PSIRP**: Publish Subscribe Internet Routing Paradigm
  - FP7 ICT STREP, 2008-2010
  - **the basis**
- **PURSUIT**: Publish Subscribe Internet Technologies
  - FP7 ICT STREP, 2010-2013
  - revisiting, extending, above and below the internet layer
- **Euro-NF**: Anticipating the Network of the Future—From Theory to Design
  - FP7 ICT NoE, 2008-2012
  - various topics, including network architecture
- **EIFFEL**: Evolved Internet Future For European Leadership
  - FP7 ICT SSA, 2008-2010; Think-Tank continued
  - June 2011 TT: ***Information-Centric Networking***
- ***φSAT***: The Role of Satellite in Future Internet Services
  - ESA (ARTES 1), 2011-2013
- **I-CAN**: Information-Centric Future Access Networks
  - NSRF (Greece), 2014-2015

A REFERENCE ICN MODEL

The data owner entity

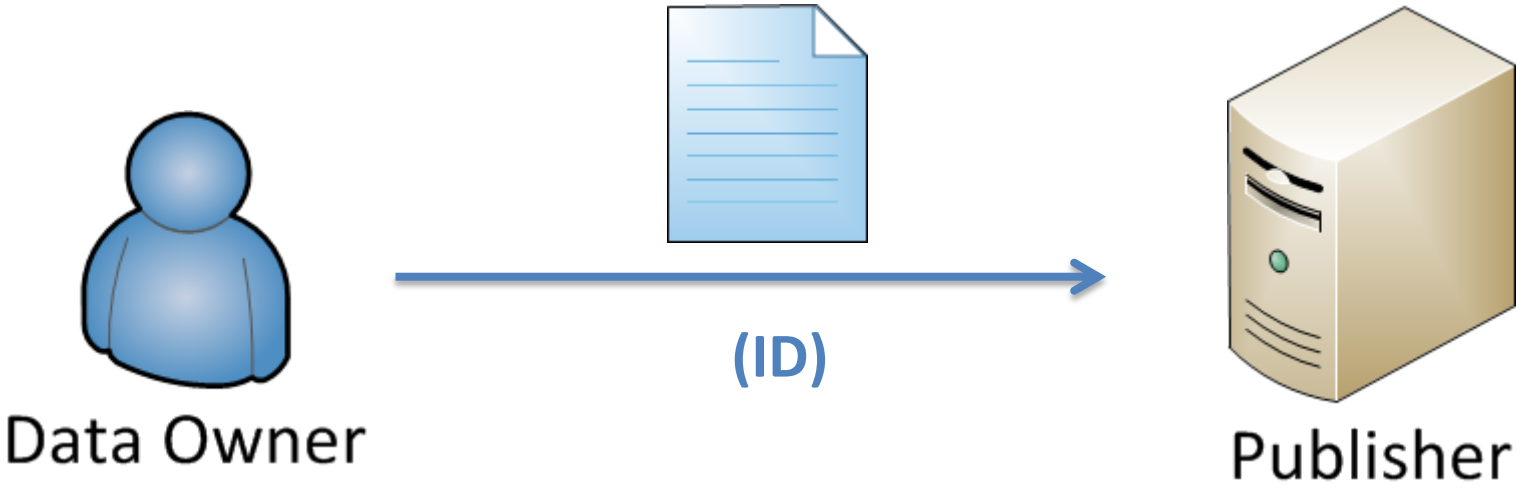


Data Owner

- Real world entity
- Owns a content item that wants to disseminate

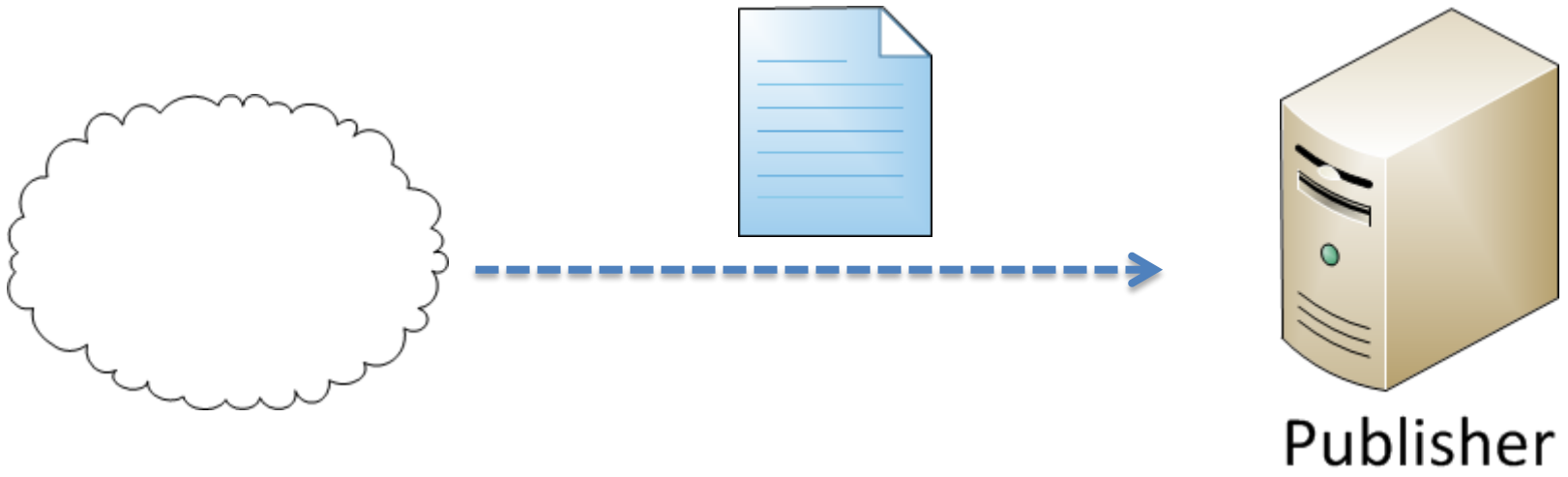
ID assignment and content storage

The data owner assigns a unique identifier to a content item and **Stores** it at a publisher



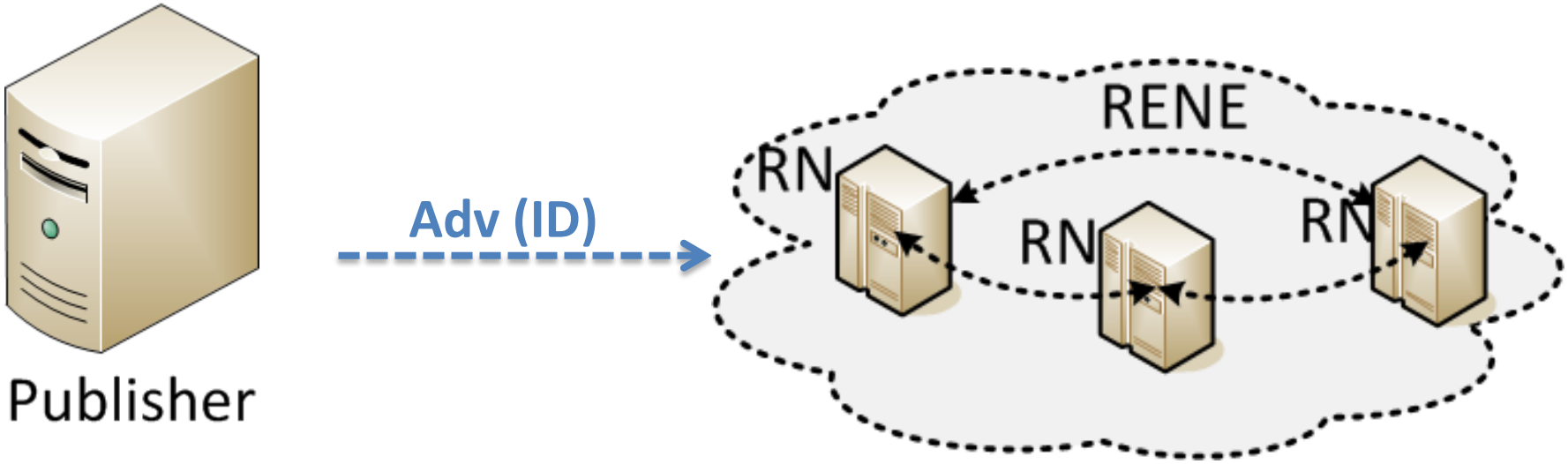
Opportunistic content storage

A publisher may receive an item from multiple sources



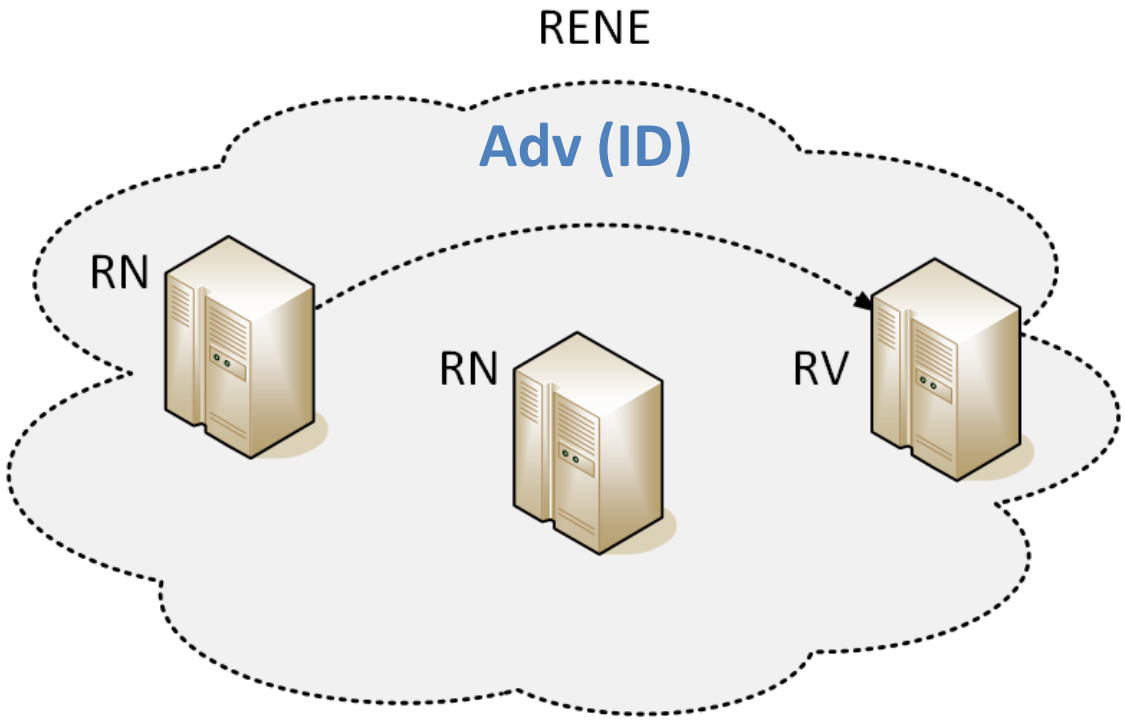
Content advertisement

A publisher **Advertises** a content item to the **Re**ndezvous **Ne**twork

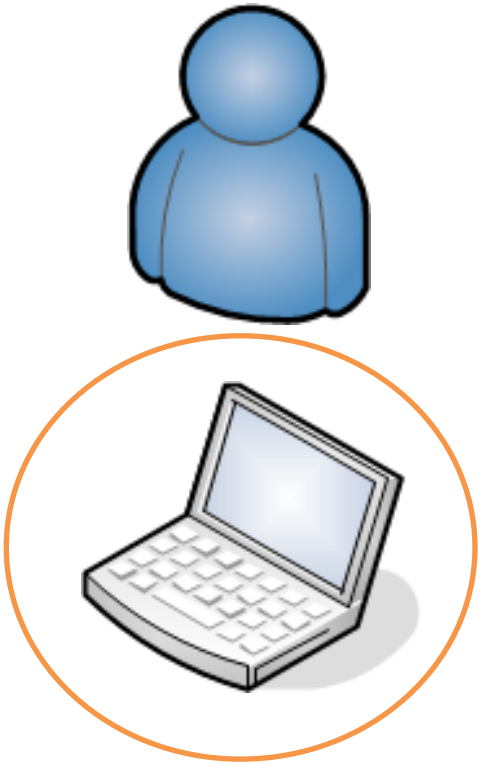


Storing content advertisements

The advertisement is stored in one or more **R**endez**V**ous points



The subscriber entity

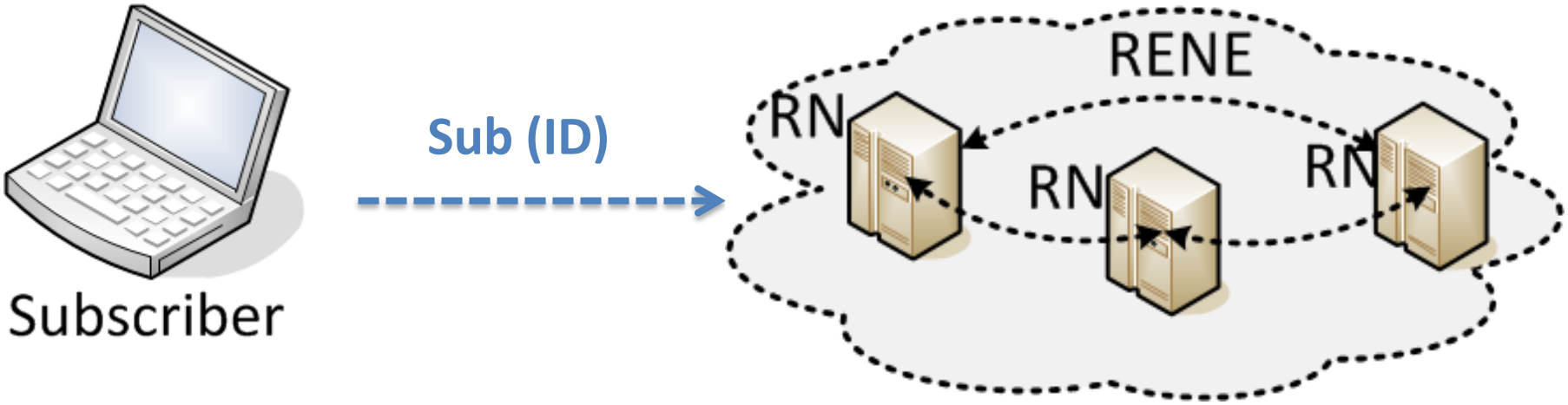


Subscriber

- The device of a real world entity that is interested in a content item

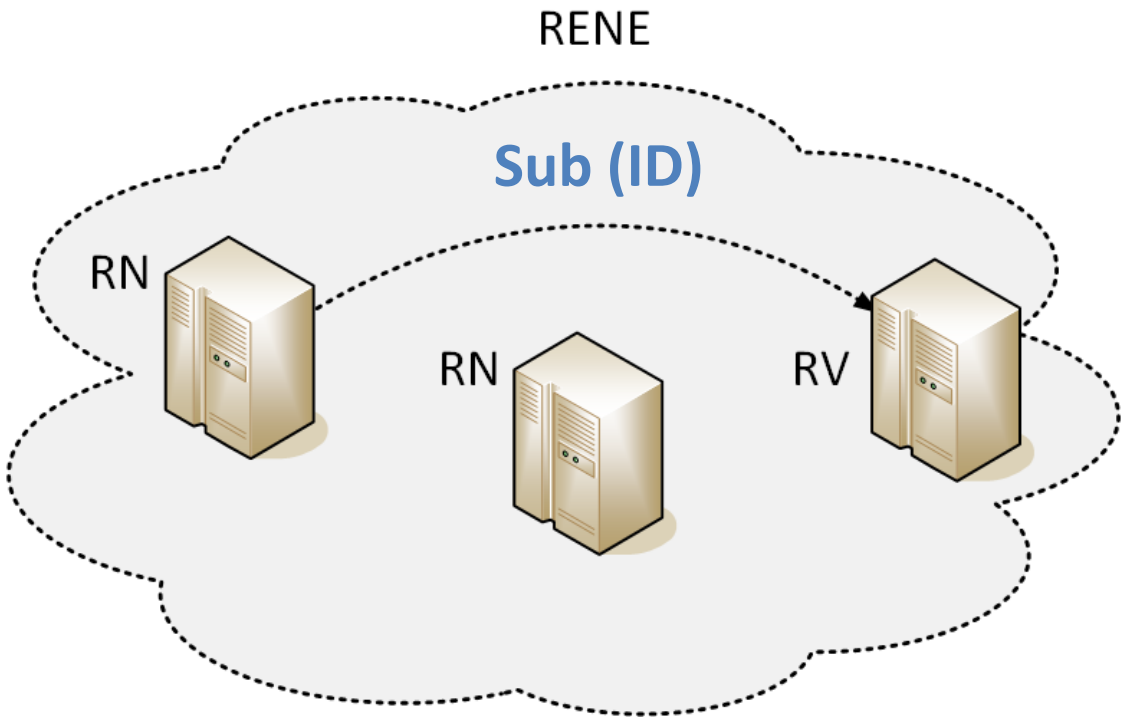
Subscription for content

A subscriber **Subscribes** for a content item



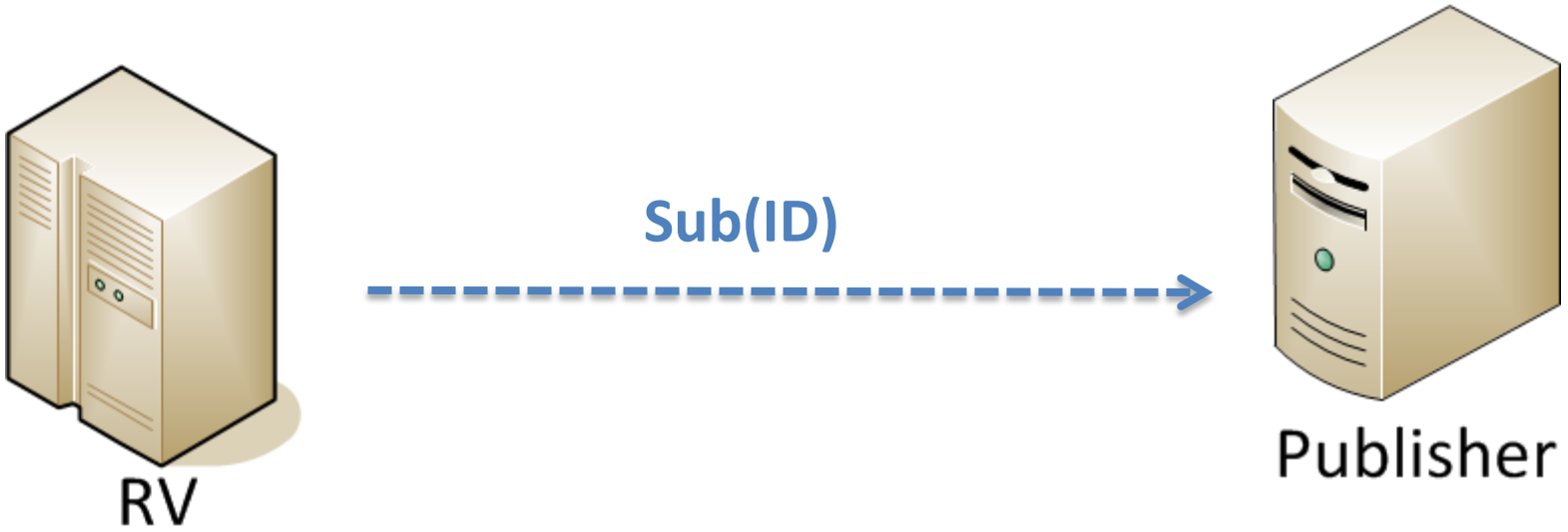
Subscription forwarding

The subscription is rooted at the RENE…



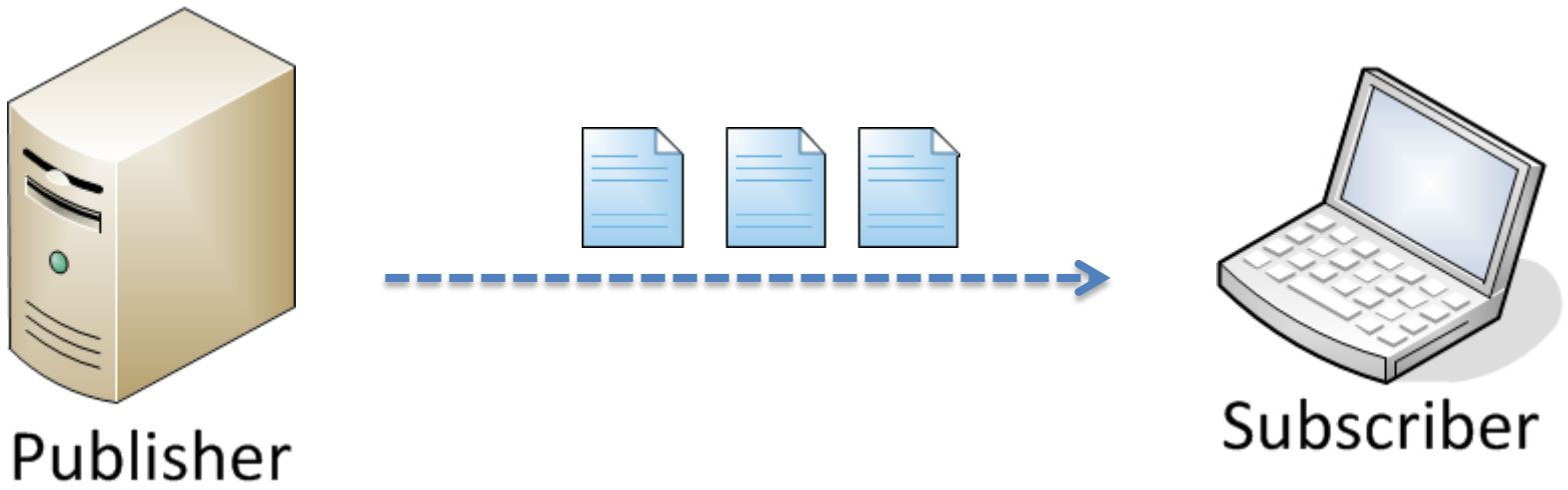
Subscription forwarding

…to a Publisher (after the matching)



Content forwarding

The Publisher **Forwards** the item to the Subscriber



Introduction

ICN PRIVACY

ICN Privacy: a myth to bust (?)

- ICN inherently preserves user's privacy
  - Endpoints are decoupled
  - Subscription and Advertisement messages do not contain sensitive information
  - Forwarding techniques that do not reveal packet destination(s)
    - zFilters (PSIRP/PURSUIT)
    - crumb based(CCN/NDN)

But ICN packets reveal more information…

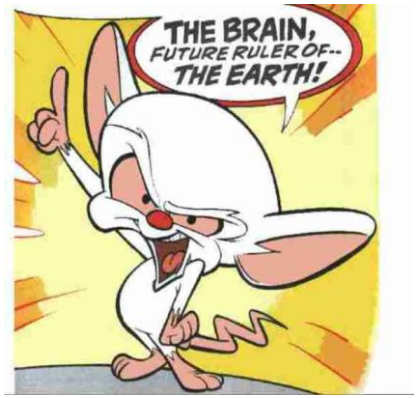
195.251.120.16	210.120.99.88	options

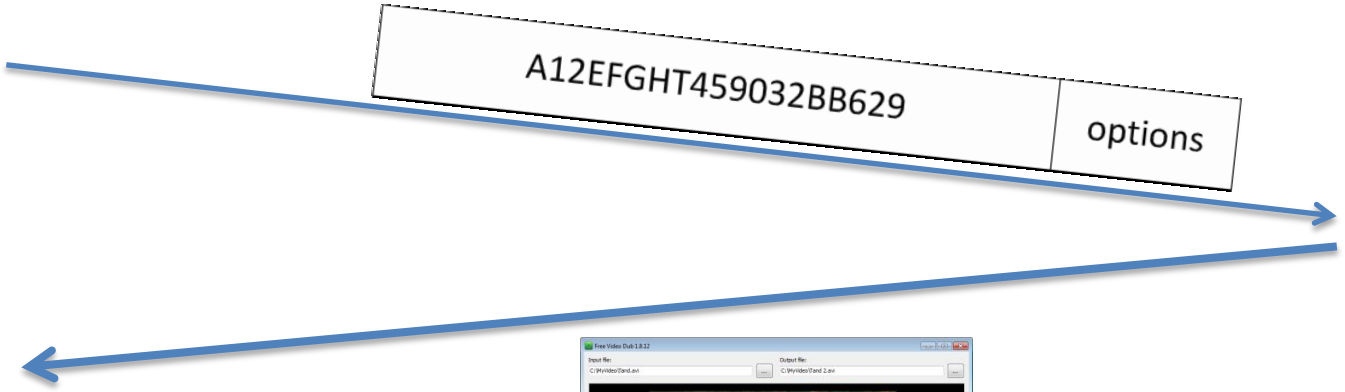
economy/stock/ftse-20/apple/price	options

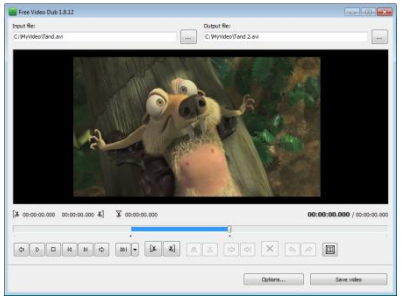
…even if packet header is scrambled…

A12EFGHT459032BB629	options

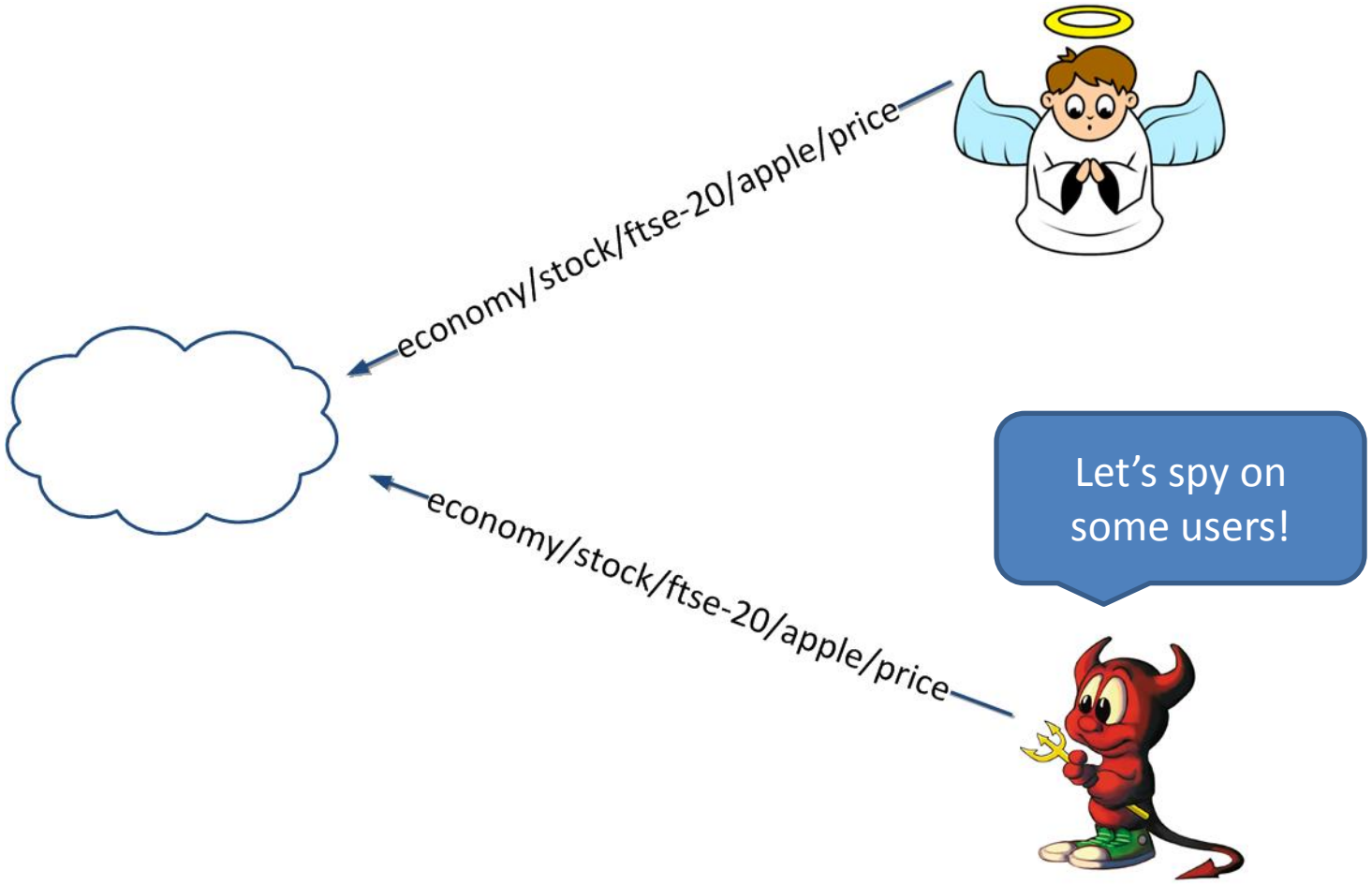
…it is easier to **replay** it and receive the corresponding content



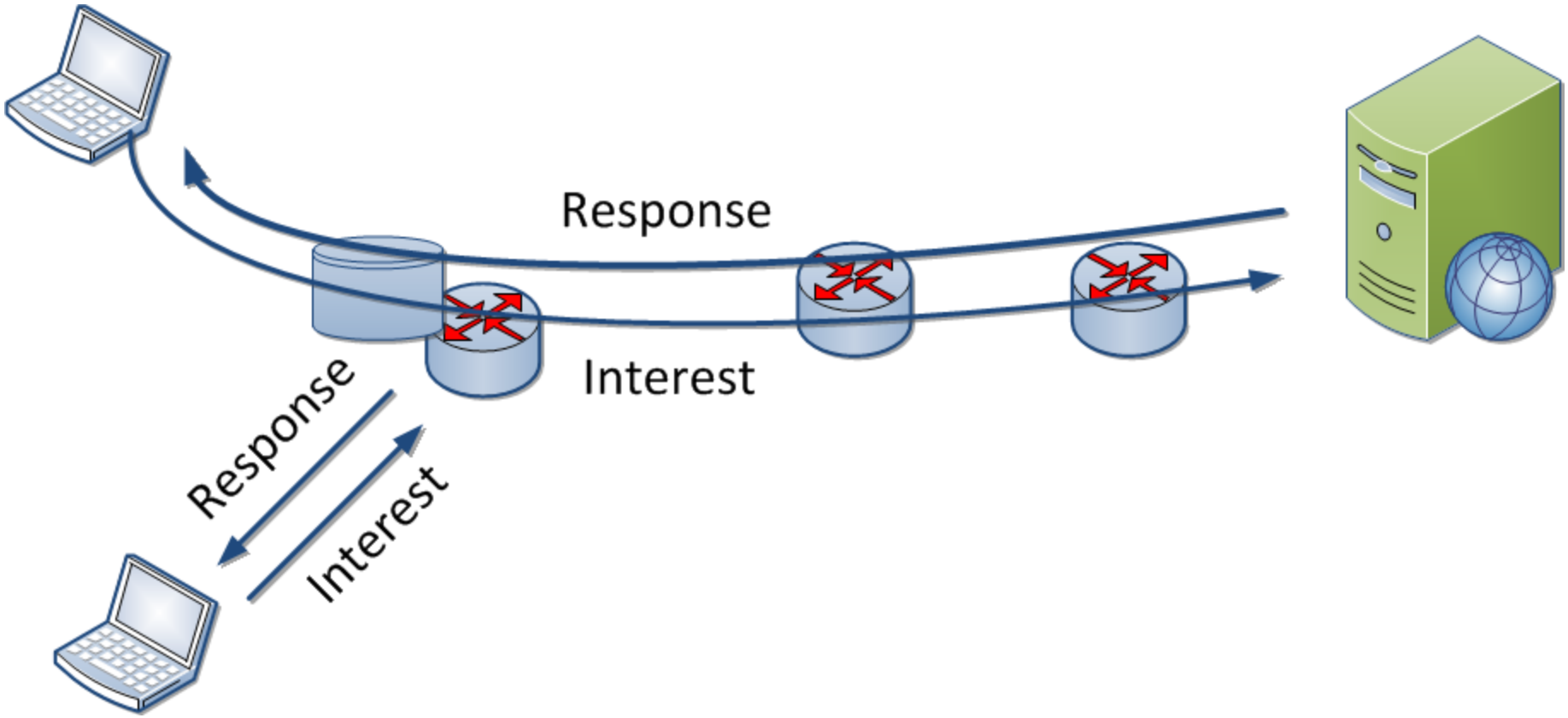




…everybody can be a publisher…

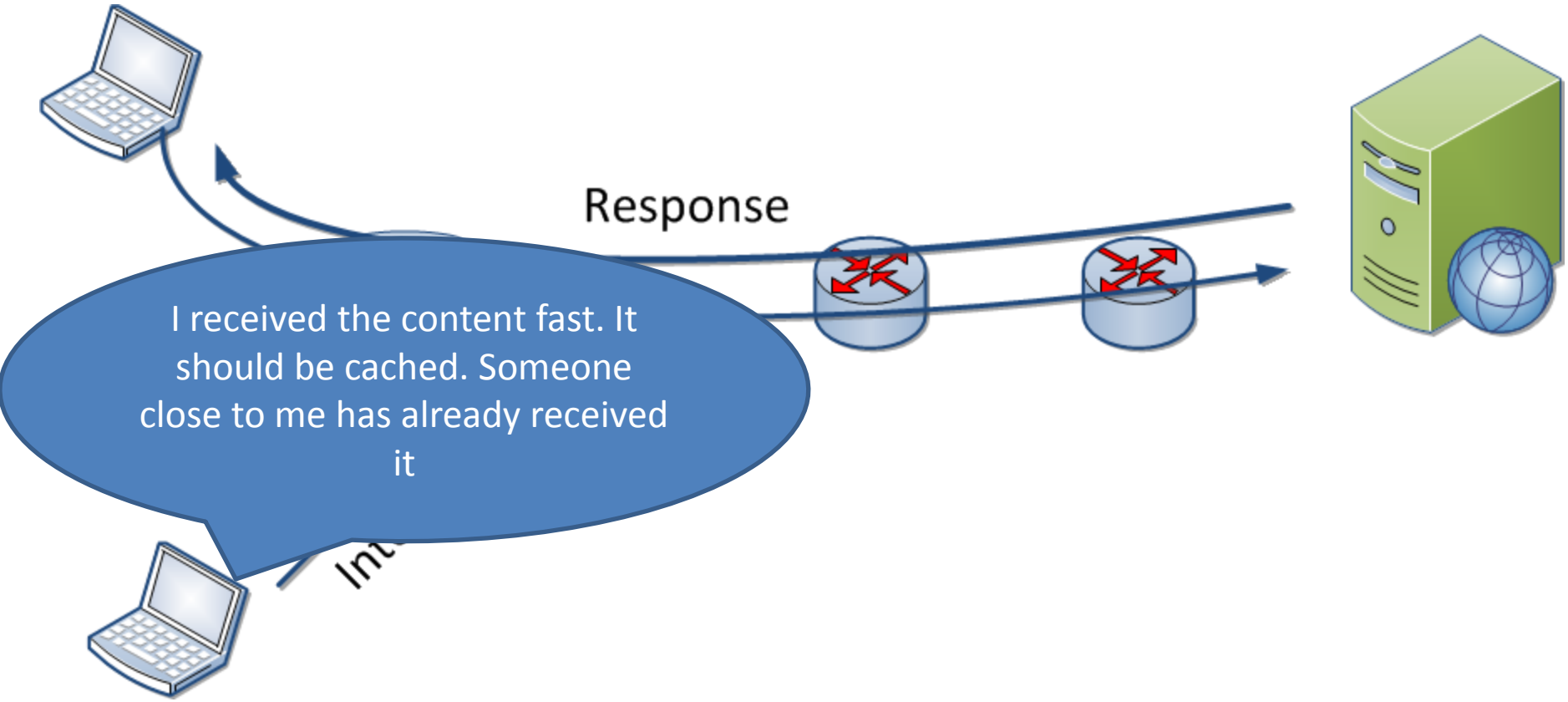


…and some old privacy attacks are upgraded*….



*T. Lauinger et al., "**Privacy risks in named data networking: what is the cost of performance?**," ACM SIGCOMM *Computer Communication Review* 42, no. 5 (2012): 54-57.

…and some old privacy attacks are upgraded*….



*T. Lauinger et al., "**Privacy risks in named data networking: what is the cost of performance?**," ACM SIGCOMM *Computer Communication Review* 42, no. 5 (2012): 54-57.

The devil is in the (implementation) details

- “We represent this by having P(ublisher) digitally sign the mapping from his chosen name”*
- “PLA divides this problem into two distinct parts: binding a user's traffic to that user's cryptographic identity, and binding the user's cryptographic identity to their real identity”**

*D. Smetters, V. Jacobson, “**Securing Network Content**”, PARC Tech Report, October 2009.

** D. Lagutin and S. Tarkoma, “**Cryptographic signatures on the network layer - an alternative to the ISP data retention**,” IEEE ISCC 2010.

The devil is in the (implementation) details

- "We represent this by having P(ublisher) dig[illegible] from his chosen name"*
- "PLA divides this problem into two distinct par[illegible]affic to that user's cry[illegible]nd binding the user's cryptographic identity to their real identity"**

Possibly Censorship

Possibly Surveillance

*D. Smetters, V. Jacobson, "**Securing Network Content**", PARC Tech Report, October 2009.

** D. Lagutin and S. Tarkoma, "**Cryptographic signatures on the network layer - an alternative to the ISP data retention**," IEEE ISCC 2010.

A Threat Model*

ICN PRIVACY

* N. Fotiou, S. Arianfar, M. Särelä, and G.C. Polyzos, "**A Framework for Privacy Analysis of ICN Architectures**," *Privacy Technologies and Policy*, Springer, Lecture Notes in Computer Science, no. 8450 (2014): 117-132.

Adversaries

Location
Local
Arbitrary

Role
Owner
Subscriber
Publisher
Rendezvous Node
Observer
Authority

Mode of operation
Active
Passive
Honest-but-Curious

Privacy attacks*

- 3 Main Categories:
  - Monitoring attacks
    - Aim at learning the preferences of subscribers
  - Decisional interference attacks
    - Censorship
  - Invasion attacks
    - Affect privacy related information of a target in order to cause (not necessarily privacy related) harassment
    - Try to lure a subscriber to subscribe for a content item, or make a RV believe that a subscriber is interested in something

* Based on: D.J. Solove, "**A taxonomy of privacy**," *University of Pennsylvania Law Review* (2006): 477-564.

Monitoring attacks

- Surveillance
  - Collect information about a target
- Interrogation
  - Force a target to give information in order to use a service
    - e.g., a RN that accepts only digitally signed advertisements
- Identification
  - Link collected information to a particular target
- Breach of confidentiality and disclosure
  - Revelation of information by a third party
  - If that party was considered trusted then breach of confidentiality occurs

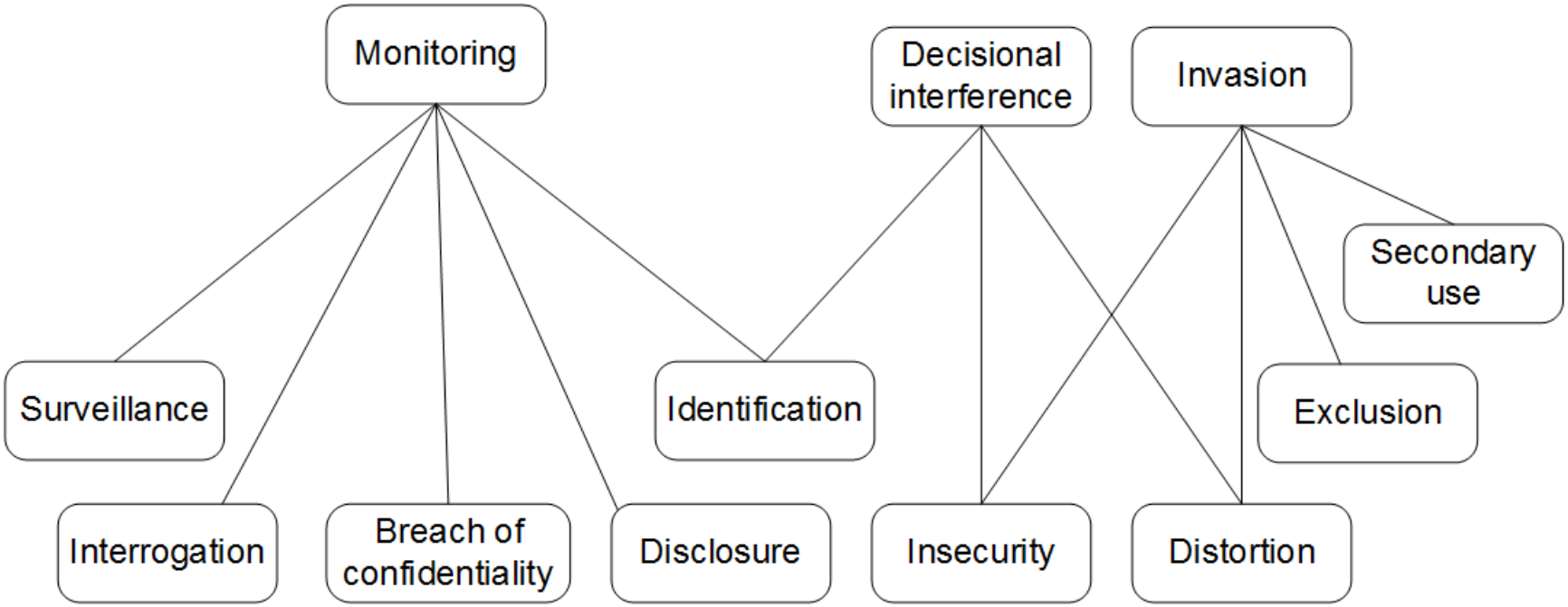
Decisional interference attacks

- Successful Identification is a prerequisite
- Insecurity
  - Manipulation of a “data pool”
    - e.g., manipulation of the state of a RN
- Distortion
  - Manipulate or delete an “information flow”
    - e.g., a subscription message

Invasion attacks

- Insecurity and Distortion
  - Also used for making a subscriber receive something never requested
- Exclusion
  - Prevents a target from removing a record about him in a “data pool”
    - e.g., to prevent a subscriber from withdrawing a subscription
- Secondary use
  - (Re-)Use of previously collected information
    - e.g., repetition of a subscription message

Attacks


Monitoring
Decisional interference
Invasion
Secondary use
Surveillance
Identification
Exclusion
Interrogation
Breach of confidentiality
Disclosure
Insecurity
Distortion

Privacy solutions

ICN PRIVACY

Entropy-based*

- It does not modify underlay architecture
- It makes “hard” for an adversary to guess subscriber preferences
  - Unobservability

* S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, “**On preserving privacy in content-oriented networks**,” Proc. ACM SIGCOMM workshop on Information-Centric Networking (2011): 19-24.

Outline

- Subscriber and Publisher share some knowledge about the content
- Publisher splits the content in chunks and assigns an **Id** to each chunk
- An adversary's goal is to censor content based on its Id

Design

Target File t

- t1
- t2
- t3
- t4
- t5

Design

Target File t	Computed Ids per block
t1	H(t,1)
t2	H(t,2)
t3	H(t,3)
t4	H(t,4)
t5	H(t,5)

Design

Target File t

t1
t2
t3
t4
t5

Cover File c

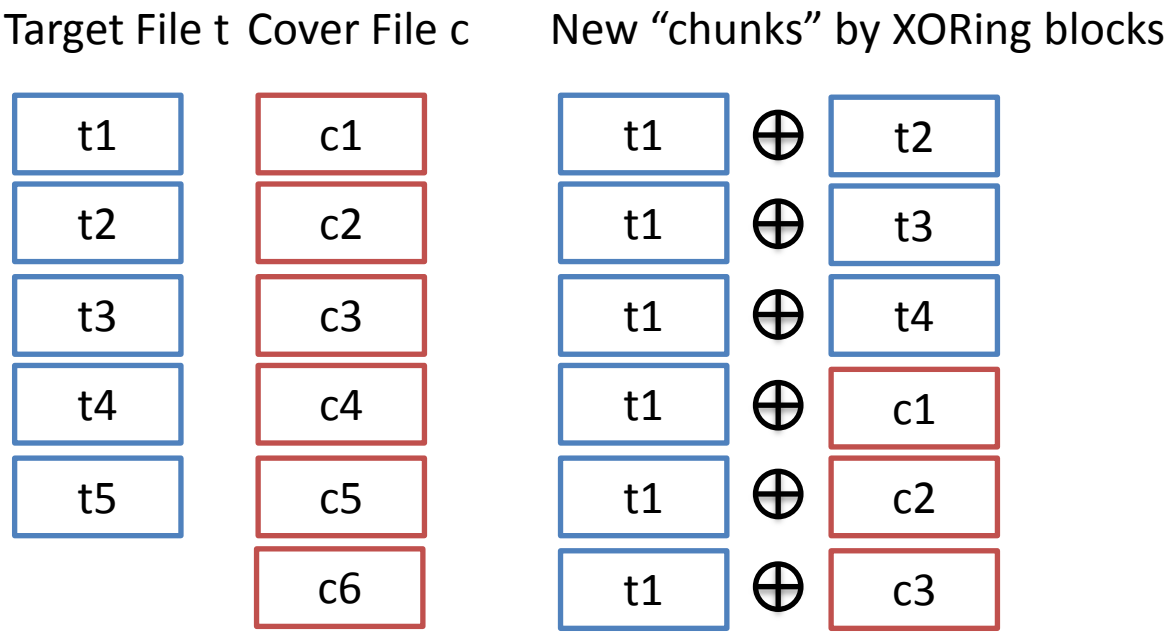
c1
c2
c3
c4
c5
c6

Design

Target File t	Cover File c	Computed Ids per block
t1	c1	H(c,1)
t2	c2	H(c,2)
t3	c3	H(c,3)
t4	c4	H(c,4)
t5	c5	H(c,5)
	c6	H(c,6)

Design

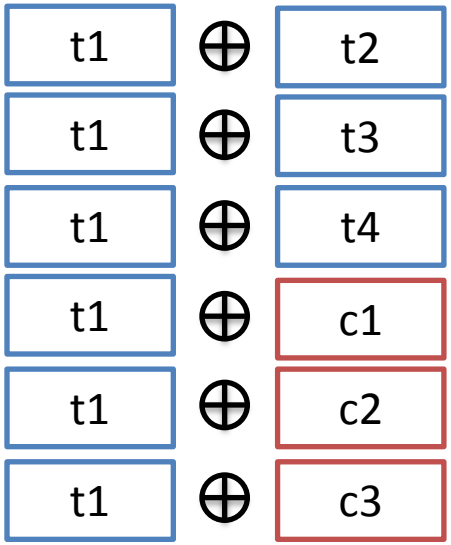

Publisher


Target File t
Cover File c
New “chunks” by XORing blocks
t1
t2
t3
t4
t5
c1
c2
c3
c4
c5
c6
t1 ⊕ t2
t1 ⊕ t3
t1 ⊕ t4
t1 ⊕ c1
t1 ⊕ c2
t1 ⊕ c3

Design

Publisher

New “chunks”



Computed Ids per chunk

H(H(t,1), H(t,2))

H(H(t,1), H(t,3))

H(H(t,1), H(t,4))

H(H(t,1), H(c,1))

H(H(t,1), H(c,2))

H(H(t,1), H(c,3))

Design

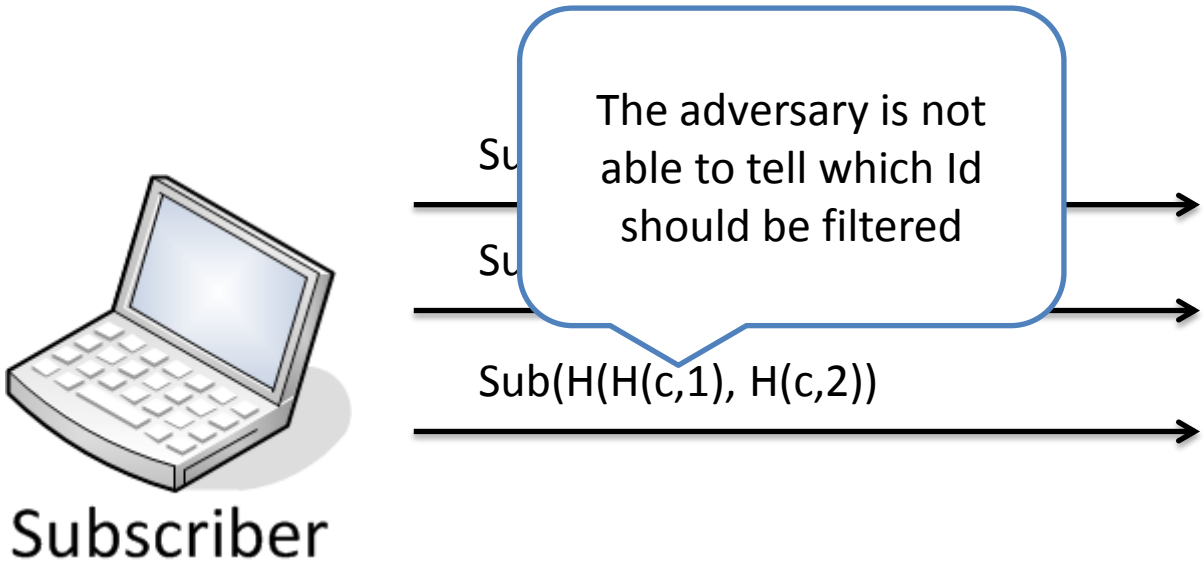
Subscriber

Sub(H(H(t,1), H(c,1))

Sub(H(H(t,1), H(c,2))

Sub(H(H(c,1), H(c,2))

Design


The adversary is not able to tell which Id should be filtered
Su
Su
Sub(H(H(c,1), H(c,2))
Subscriber

Mix networks-based*

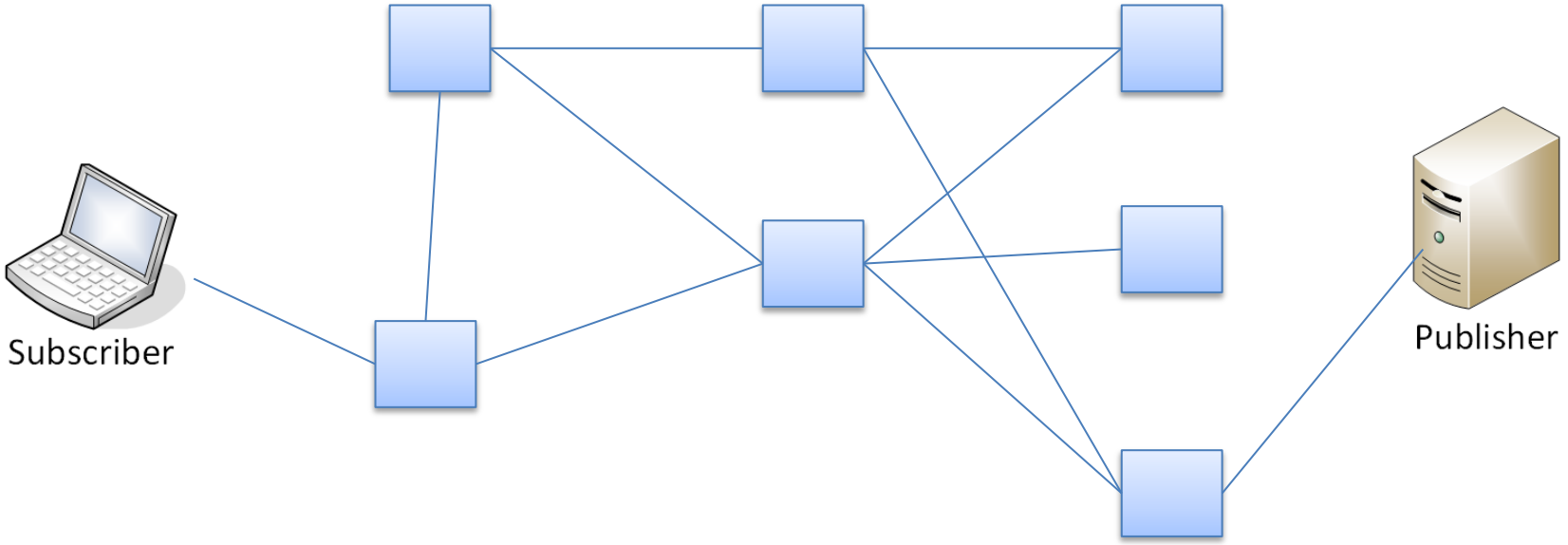
- An adaptation of onion routing for ICN (NDN)
- The identity of the subscriber is hidden
  - Anonymity
- Subscriptions and content packets cannot be "linked"
  - Unlinkability

* S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, "**ANDaNA: Anonymous named data networking application**," Proc. Network and Distributed System Security Symposium (NDSS 2012)

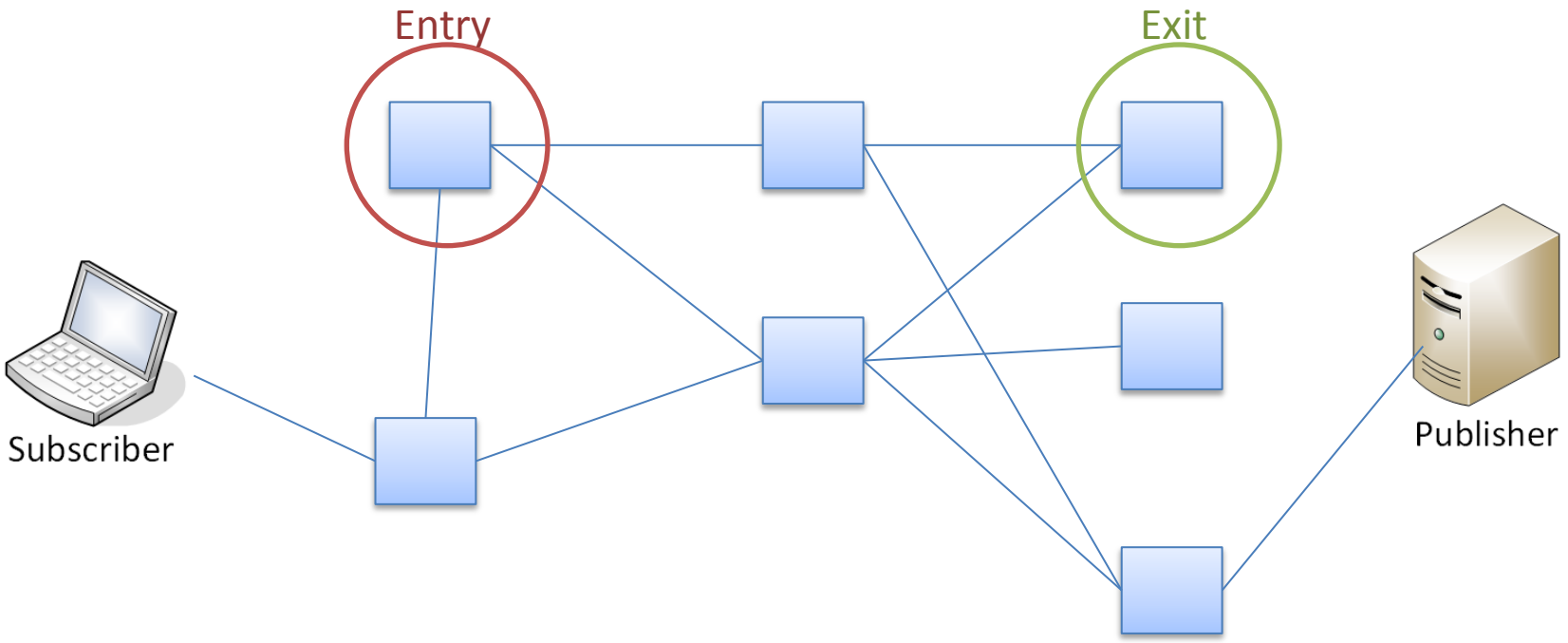
Outline

- Multiple concentric layers of encryption
- Every message is routed through a chain of at least two “anonymizing routers” (ARs)
- Each router removes a layer of encryption and forwards the message to the next hop

Design



Design



Design

- Sub(ID)

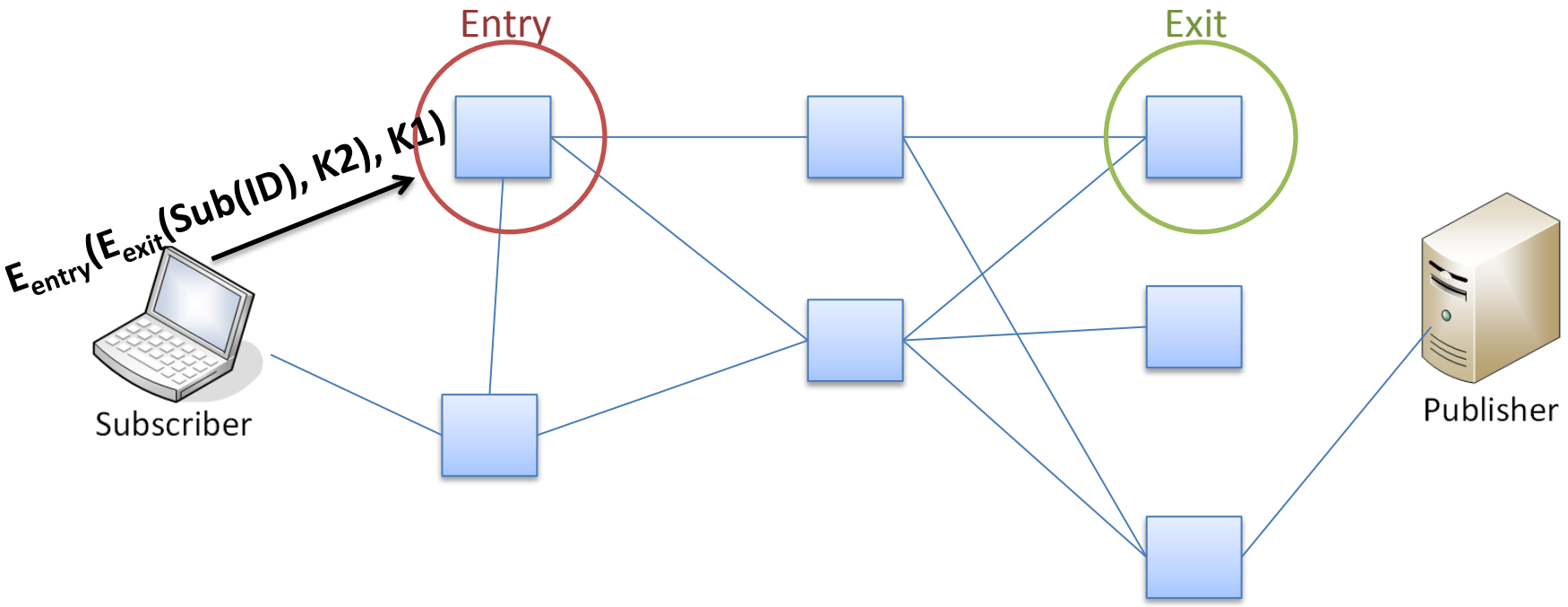
Design

- E_{exit}(Sub(ID), K2)

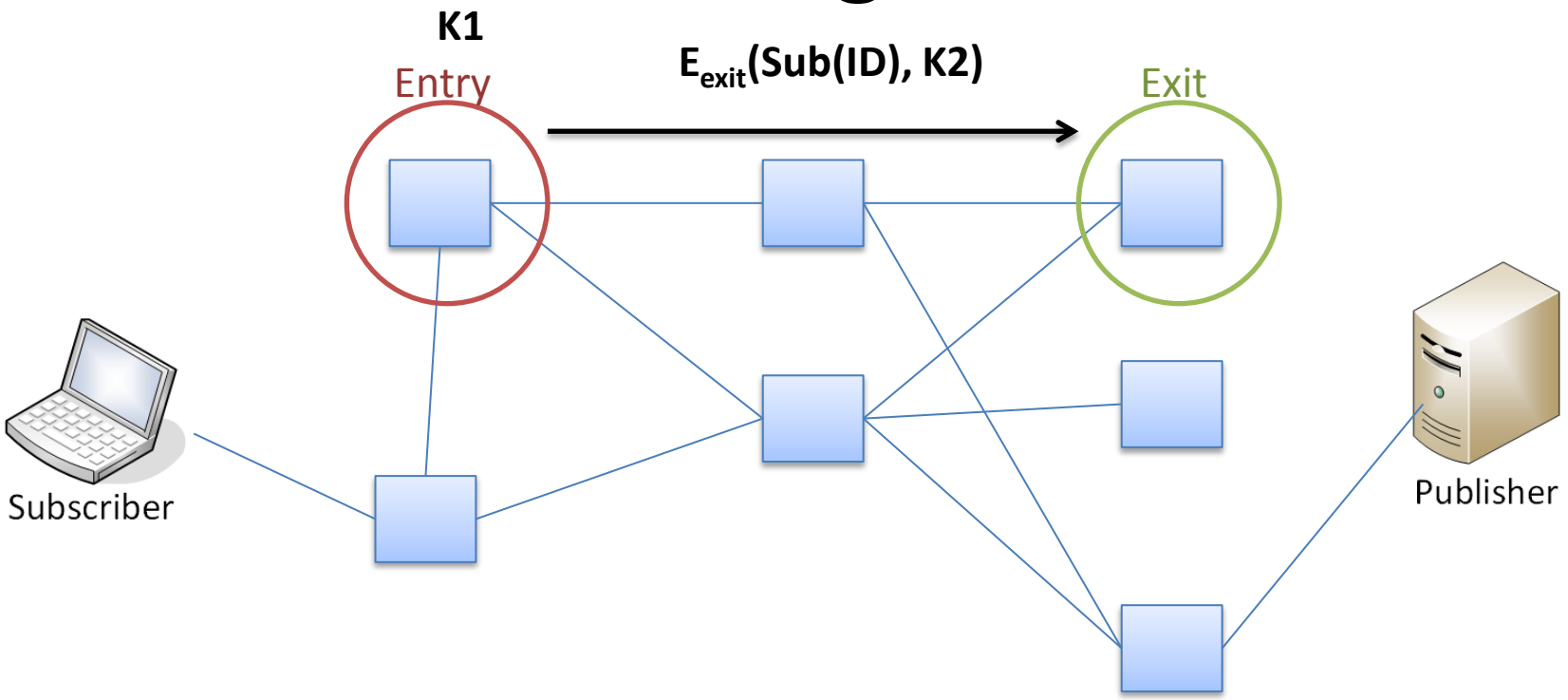
Design

- $E_{entry}(E_{exit}(Sub(ID), K2), K1)$

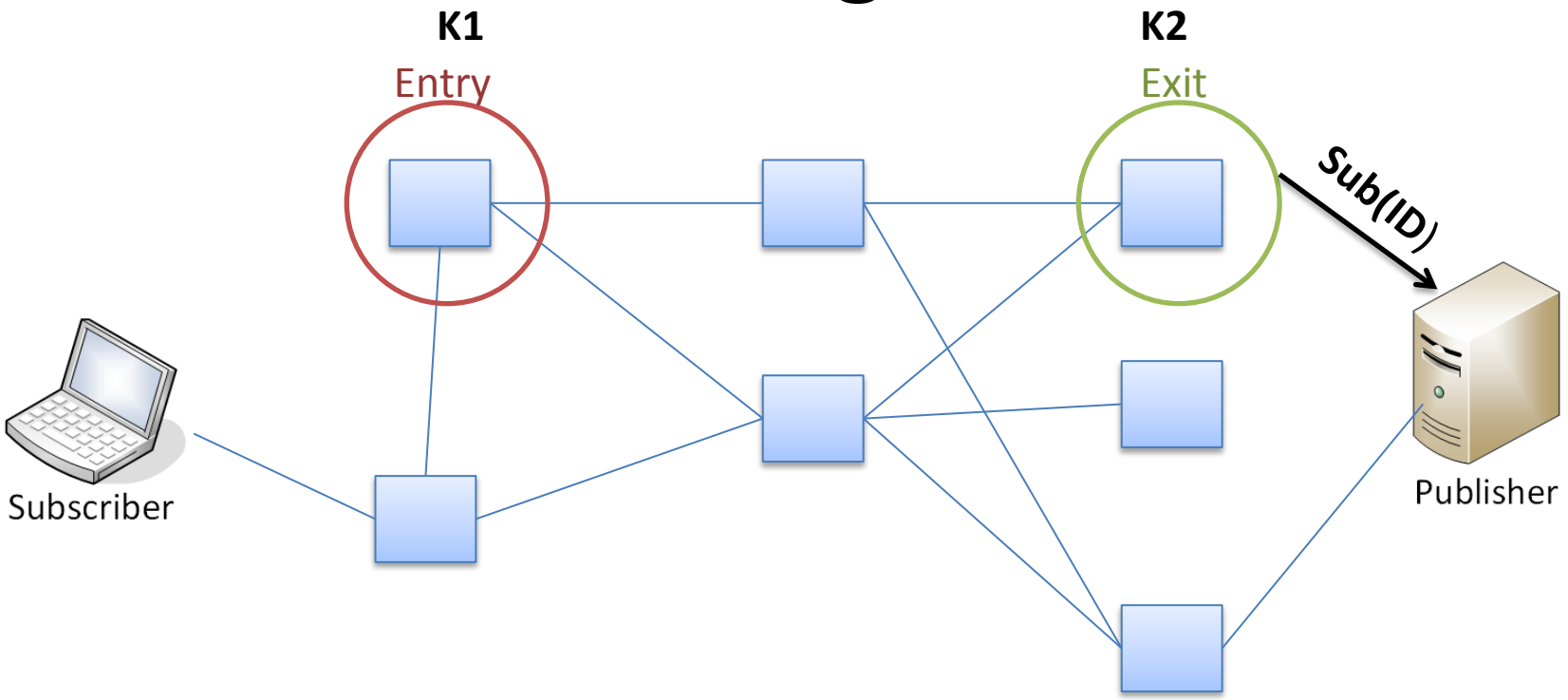
Design



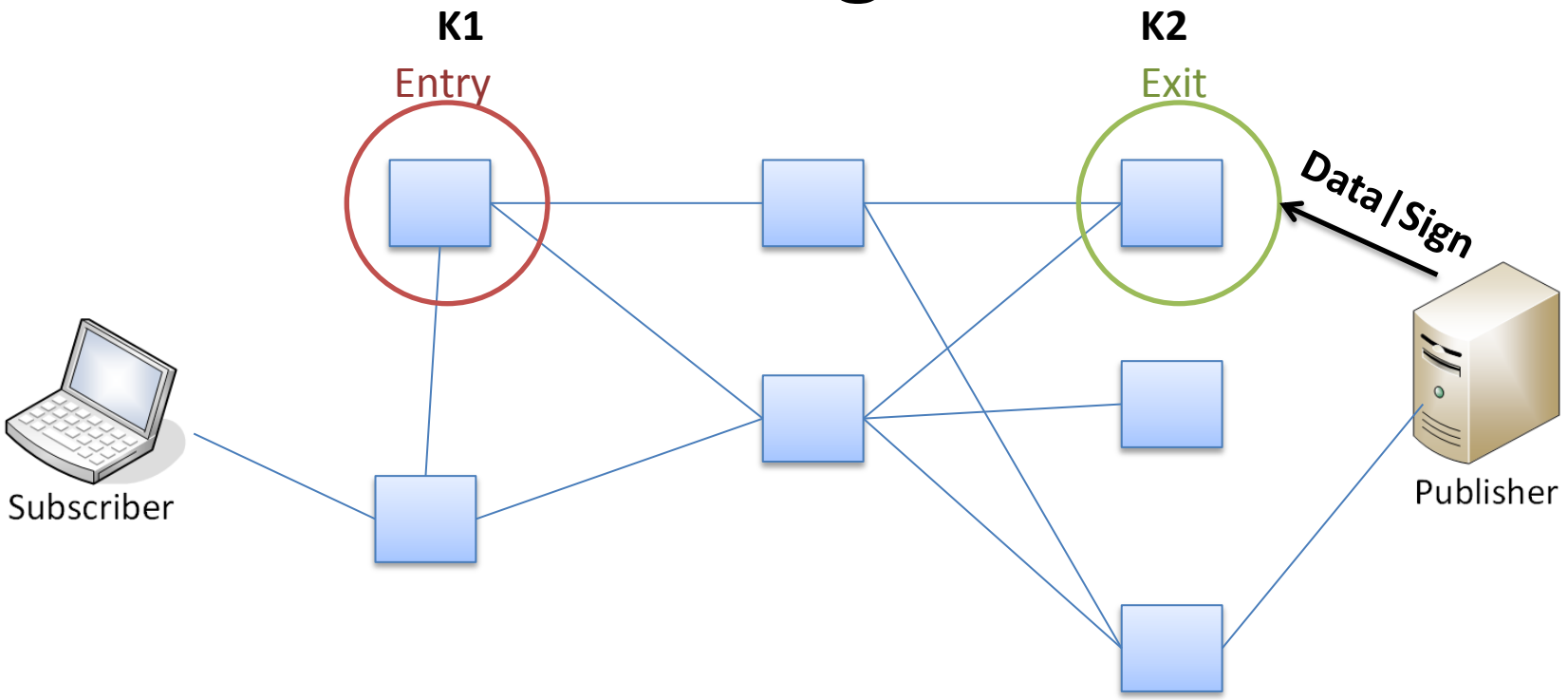
Design



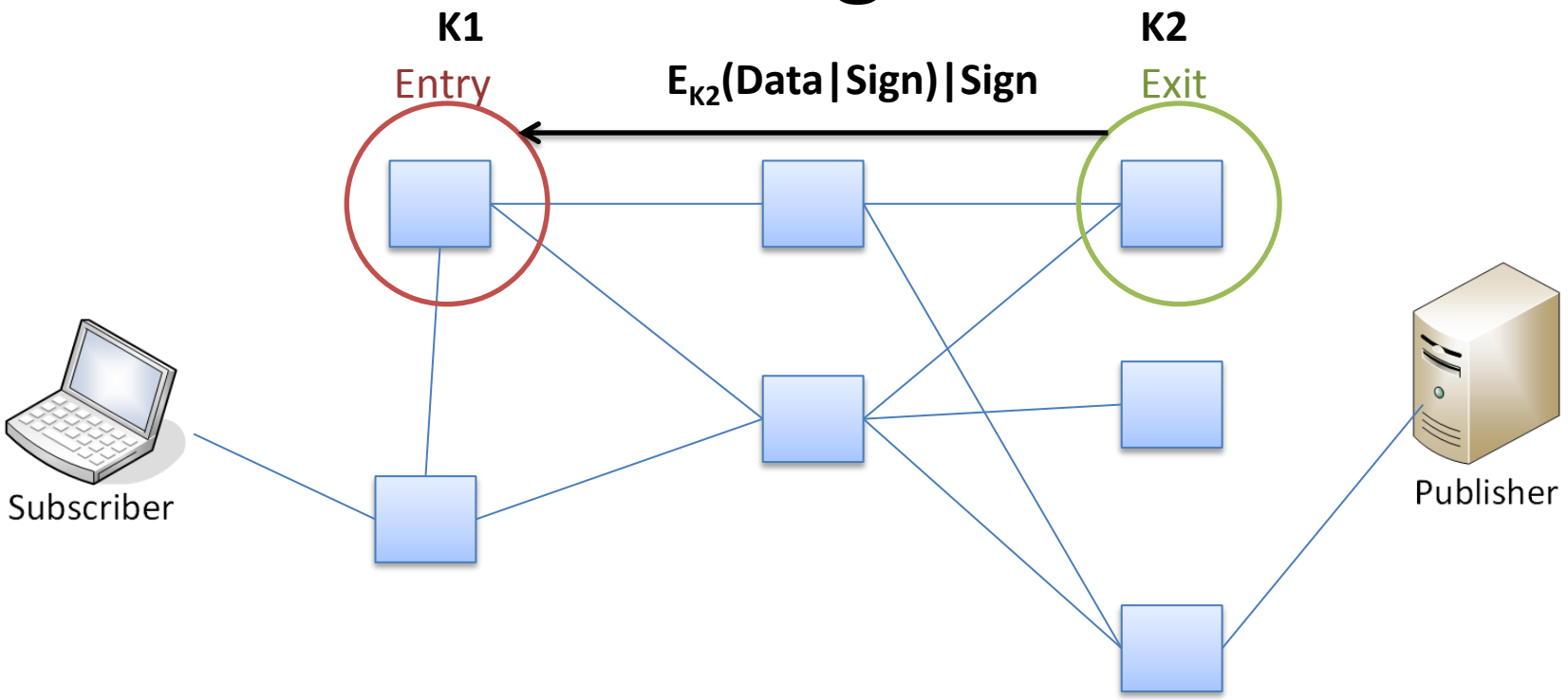
Design



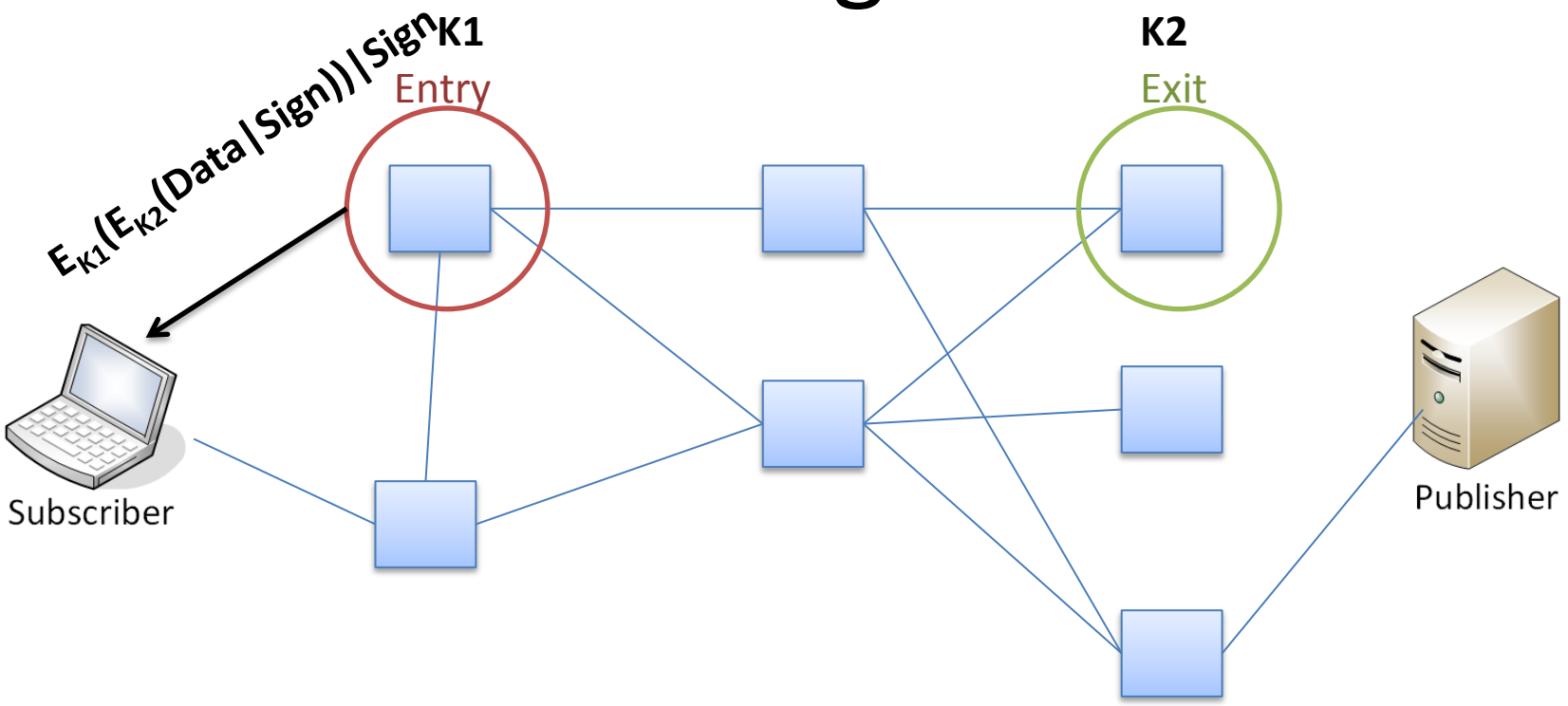
Design



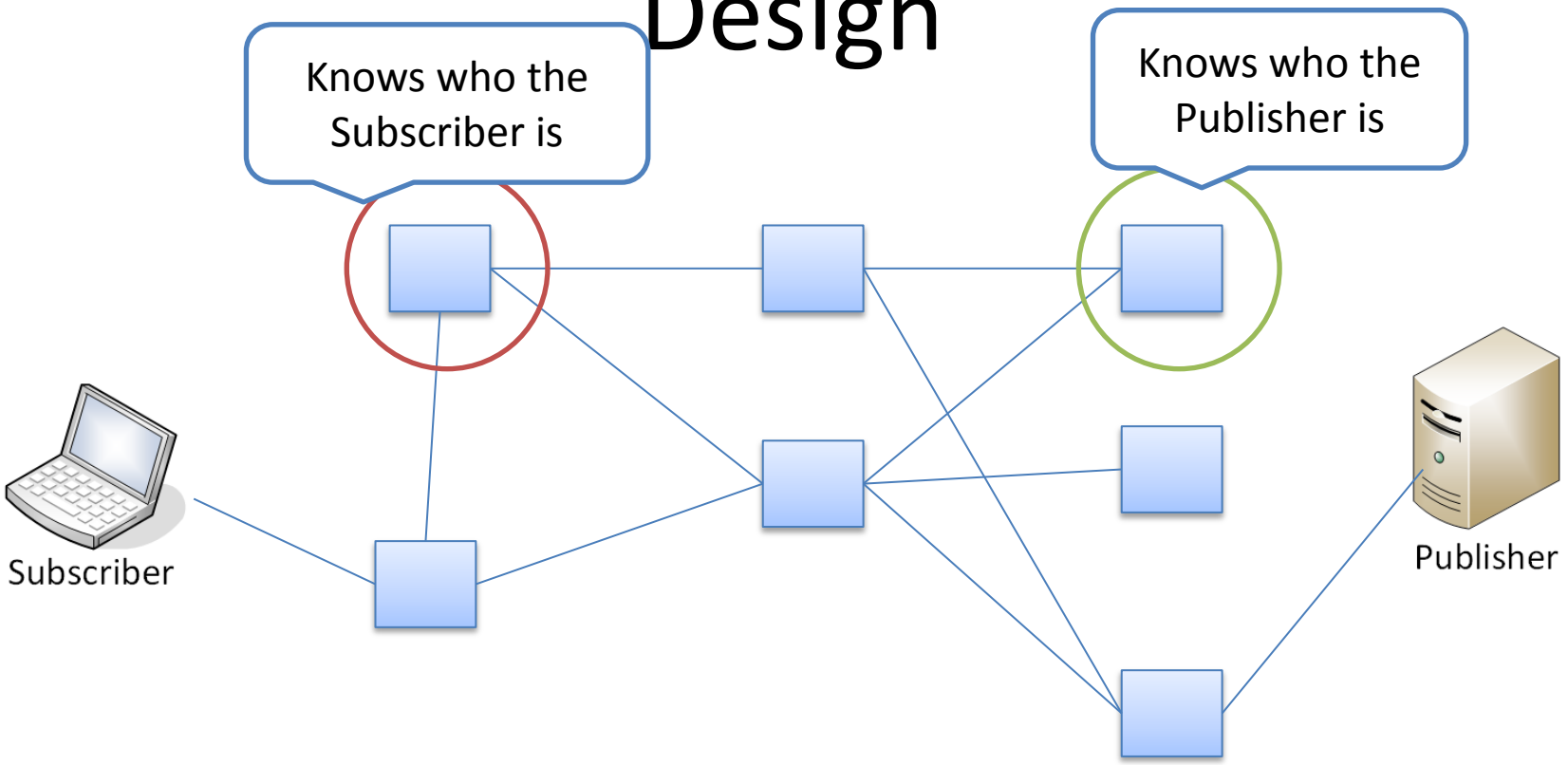
Design



Design


$E_{K1}(E_{K2}(Data|Sign))|Sign_{K1}$
Entry
K2
Exit
Subscriber
Publisher

Design


Knows who the Subscriber is
Knows who the Publisher is
Subscriber
Publisher

Homomorphic encryption-based*

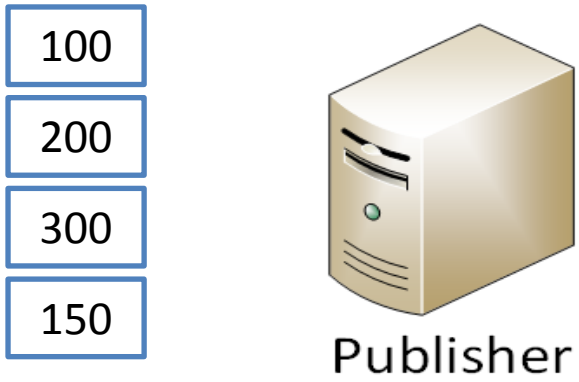
- A subscriber is able to request a content item, a publisher is able to send it, nobody learns what the subscriber asked and what the publisher responded
  - Not even the publisher!
  - Unobservability
- Subscriber identity is not hidden
- Based on the Paillier cryptosystem

* N. Fotiou et al., "**Enhancing information lookup privacy through homomorphic encryption**," *Security and Communication Networks*, Wiley, vol. 7, no. 4, (2014): 700-713

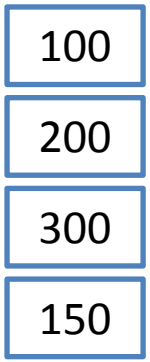
(A very high level) Introduction to the Paillier cryptosystem

- Probabilistic:
  - E(1) != E(1)
- Homomorphism:
  - E(a)*E(b) = E (a + b)
  - E(a)^k = E(a)*E(a)*…(k times)…E(a) = E (k*a)

(A very high level) PIR scheme



(A very high level) PIR scheme



(A very high level) PIR scheme

(A very high level) PIR scheme

Subscriber

E(0)	^	100
E(0)	^	200
E(1)	^	300
E(0)	^	150

Publisher

(A very high level) PIR scheme

Subscriber

E(0 *100)

E(0 *200)

E(1 *300)

E(0 *150)

Publisher

(A very high level) PIR scheme

Subscriber

E(0 *100)

*

E(0 *200)

*

E(1 *300)

*

E(0 *150)

Publisher

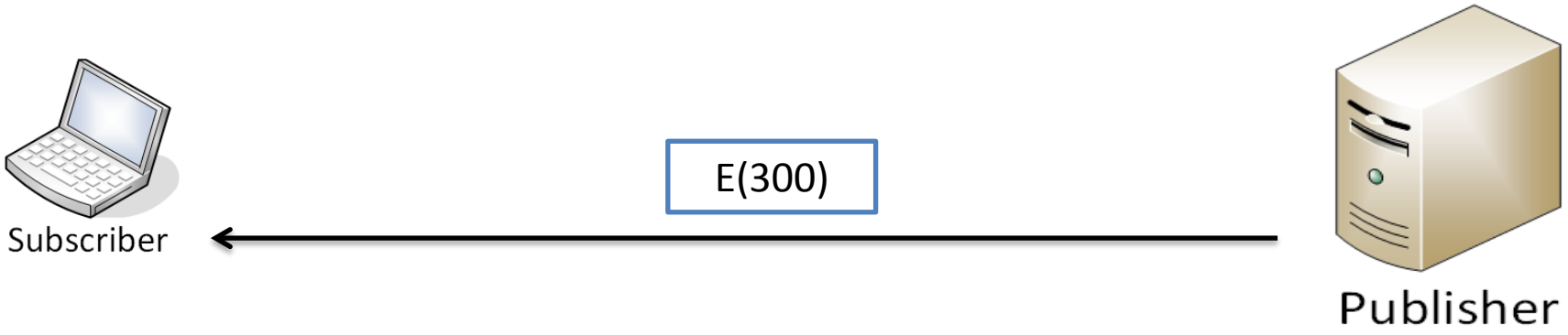
(A very high level) PIR scheme

Subscriber

E(0 *100 + 0*200 + 1*300 + 0*150)

Publisher

(A very high level) PIR scheme



Pros and Cons

- Unobservability is guaranteed by the underlay cryptographic primitives
- Computationally intensive
- Communication overhead

Introduction

NAME-BASED SECURITY

Content-related security requirements

- Confidentiality
  - A content item can be viewed only by the intended recipients
- Integrity
  - A content item has not been modified
- Authenticity
  - A content item is what I asked
- Provenance verification
  - The sender of a content item can be verified

Solutions

NAME-BASED SECURITY

Authenticating Named Content*

- Common ways to satisfy content-related security requirements are:
  - Use content hash as a name
  - Use names of the form “Publisher_key||Label” **
- Authenticating Named Content aims at achieving the same properties by using names of any form

* D. Smetters, V. Jacobson, “**Securing Network Content**,” PARC Tech. Report, (2009).

** Ghodsi et al., “**Naming in Content-Oriented Architectures**,” In Proc. of SIGCOMM ICN Workshop, (2011).

Design

- Content is made available in the network as a mapping triplet (N, C, $Sign_P(N,C)$)
  - N: An arbitrary name chosen by the publisher for a content item
  - C: The hash of the content data
  - $Sign_P(N,C)$: The digital signature of the concatenation of N and C using Publisher's private key

Building a “network of trust”

- N may also include an “indication” about P (e.g., a domain name) which can be mapped to a certificate using PKI
- N may be mapped to a N′ (instead of C)
  - “secure reference”

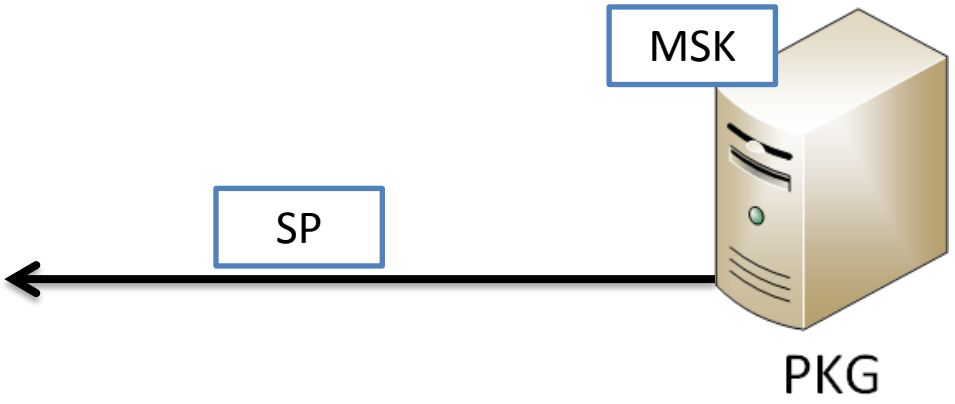
Identity-Based Encryption*

- Public key cryptography, where the public key is an arbitrary string
  - www.example.com, foo@example.com, alice
- Identity-Based Signature schemes also exist

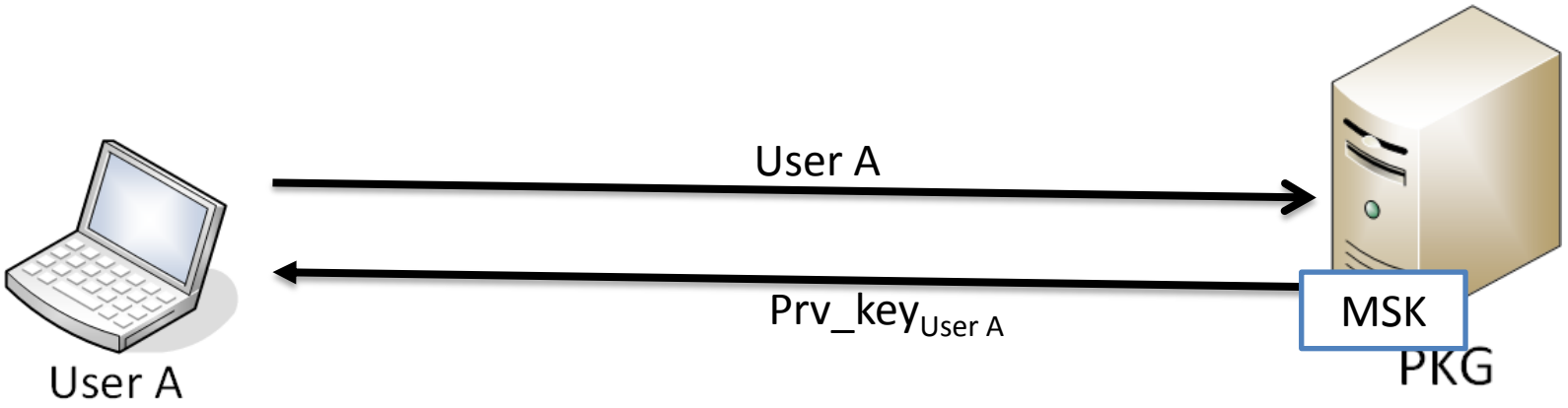
* X. Zhang et al., "**Towards name-based trust and security for content-centric network**," Proc. ICNP 2011

IBE Setup

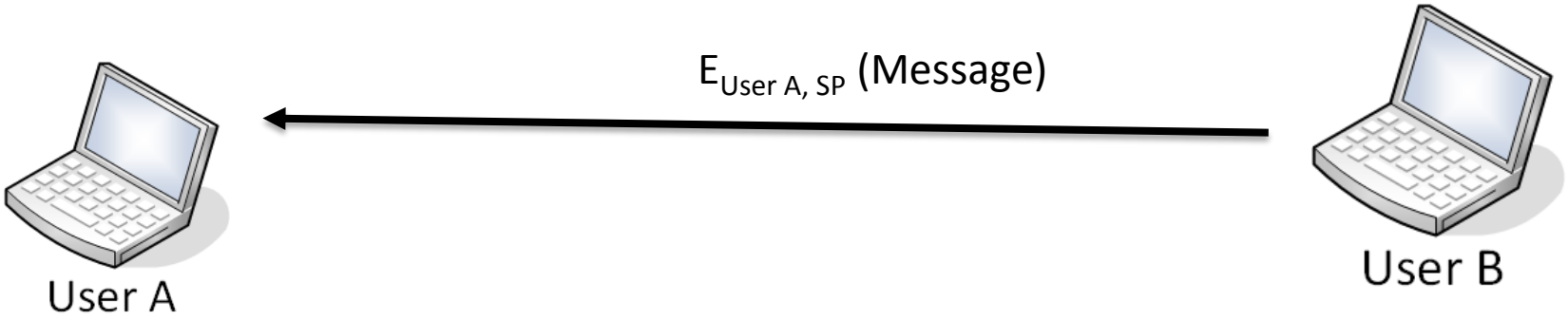
IBE Setup



IBE Key generation



IBE Encryption



Name-based security using IBE

- SP are transmitted using the PKI
- Confidentiality:
  - Encrypt content using as key the identity of the receiver
- Integrity, Authenticity, Provenance verification:
  - Identifiers of the form

    "publisher identity|content identity"
  - Sign the content using IBS and the private key that corresponds to the content identifier

Discussion

- Hierarchical Identity Based Encryption
  - even more possibilities
- Key escrow by PKG
- Key revocation is an issue
  - identities should be “revocable”
  - use as key:

    identity||something
    - where something is: serial number, date,…,

FURTHER READING

Privacy

- H.C. Hsiao et al., "**LAP: Lightweight anonymity and privacy**," Proc. IEEE Symposium on Security and Privacy 2012, pp. 506-520
- G. Acs et al., "**Cache Privacy in Named-Data Networking**," Proc. 33rd IEEE International Conference on Distributed Computing Systems (ICDCS), pp. 41-51, 2013
- A. Chaabane et al., "**Privacy in content-oriented networking: threats and countermeasures**," ACM SIGCOMM *Computer Communication Review*, vol. 43, no. 3, pp. 25-33, 2013
- M. Ion, J .Zhang, and E.M. Schooler, "**Toward Content-centric Privacy in ICN: Attribute-based Encryption and Routing**," ACM SIGCOMM *Computer Communication Review*, vol. 43, no. 4, pp. 513-514, 2013

Access Control

- N. Fotiou, G. F. Marias, and G. C. Polyzos, "**Access control enforcement delegation for information-centric networking architectures**," ACM SIGCOMM Computer Communication Review, vol. 42, no. 4, pp. 497-502, 2012
- V. Jacobson et al. "**Custodian-based information sharing**," IEEE *Communications Magazine*, vol. 50, no. 7, pp. 38-43, 2012
- S. Misra, R. Tourani, and N. E. Majd, "**Secure content delivery in information-centric networks: design, implementation, and analyses**," Proc. 3rd ACM SIGCOMM workshop on Information-Centric Networking , pp. 73-78, 2013
- C.A. Wood and E. Uzun, "**Flexible End-to-End Content Security in CCN**," Proc. IEEE Consumer Communications and Networking Conference, 2014

Content-related security

- C. Dannewitz et al., "**Secure naming for a network of information**," Proc. IEEE INFOCOM Workshops 2010, pp. 1-6, 2010
- W. Wong, and P. Nikander, "**Secure naming in information-centric networks**," Proc. ACM Re-Architecting the Internet Workshop (ReARCH), pp. 1-6, 2010
- C. Ghali, T. Gene, and E. Uzun, "**Needle in a Haystack: Mitigating Content Poisoning in Named-Data Networking**," Proc. NDSS Workshop on Security of Emerging Networking Technologies (SENT), 2014
- N. Fotiou, G. F. Marias, and G. C. Polyzos, "**Fighting spam in publish/subscribe networks using information ranking**," Proc. 6th EURO-NF Conference on Next Generation Internet (NGI), pp. 1-6, 2010

Infrastructure availability

- M. Sarela et al., "**Forwarding anomalies in Bloom filter-based multicast**, " Proc. IEEE INFOCOM, pp. 2399-2407, 2011
- M. Xie, I. Widjaja, and H. Wang, "**Enhancing cache robustness for content-centric networking**," Proc. IEEE INFOCOM, pp. 2426-2434, 2012
- A. Afanasyev et al. "**Interest flooding attack and countermeasures in Named Data Networking**," Proc. IFIP Networking Conference 2013, pp. 1-9, 2013.
- P. Gasti et al. , "**DoS and DDoS in Named Data Networking**," Proc. 22nd IEEE International Conference on Computer Communications and Networks (ICCCN), pp. 1-7, 2013
- Wählisch et al., "**Backscatter from the Data Plane – Threats to Stability and Security in Information-Centric Networking**," *Computer Networks*, Vol. 57, No. 16, pp. 3192-3206, Nov. 2013.

Concluding remarks

- ICN-IP relationship
  - Some of the techniques are adapted for ICN from the existing IP networks
  - More generally, many of techniques are also applicable to the existing IP networks
  - Same for threats and objectives
    - but there are also differences
- Important open issues
  - **Performance trade offs**
    - on a concrete system
    - Caching vs. Privacy vs. Confidentiality
  - **Governance and authorities**
    - On non random identifiers (human readable)
    - e.g., details on naming
  - **Shared responsibility** for important decisions or actions, departure from single TTP models
    - Bitcoin vs Certificates/PKI
    - Byzantine agreement,…
  - **“NSA free” architectures**
    - Global policies
    - Traffic engineering

Thank you

Nikos Fotiou, George C. Polyzos

{fotiou,polyzos}@aueb.gr

Mobile Multimedia Laboratory
Department of Informatics
School of Information Sciences and Technology
Athens University of Economics and Business
Athens, Greece
http://mm.aueb.gr

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY

NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND

Co- financed by Greece and the European Union