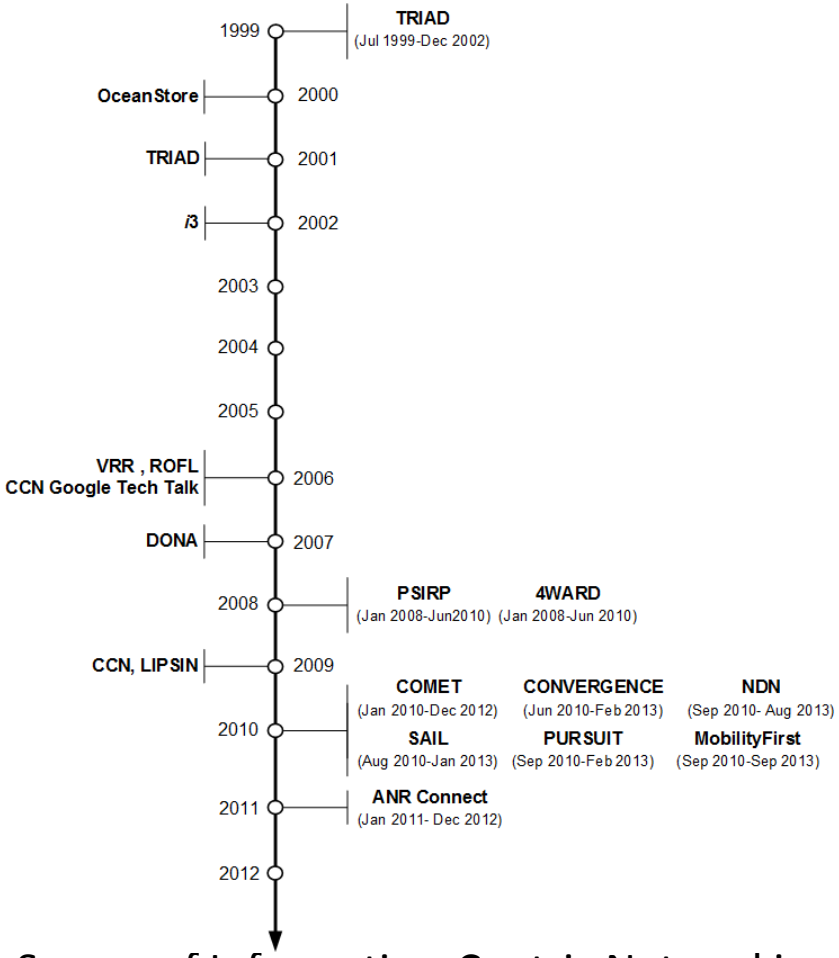
A framework for privacy analysis of ICN architectures

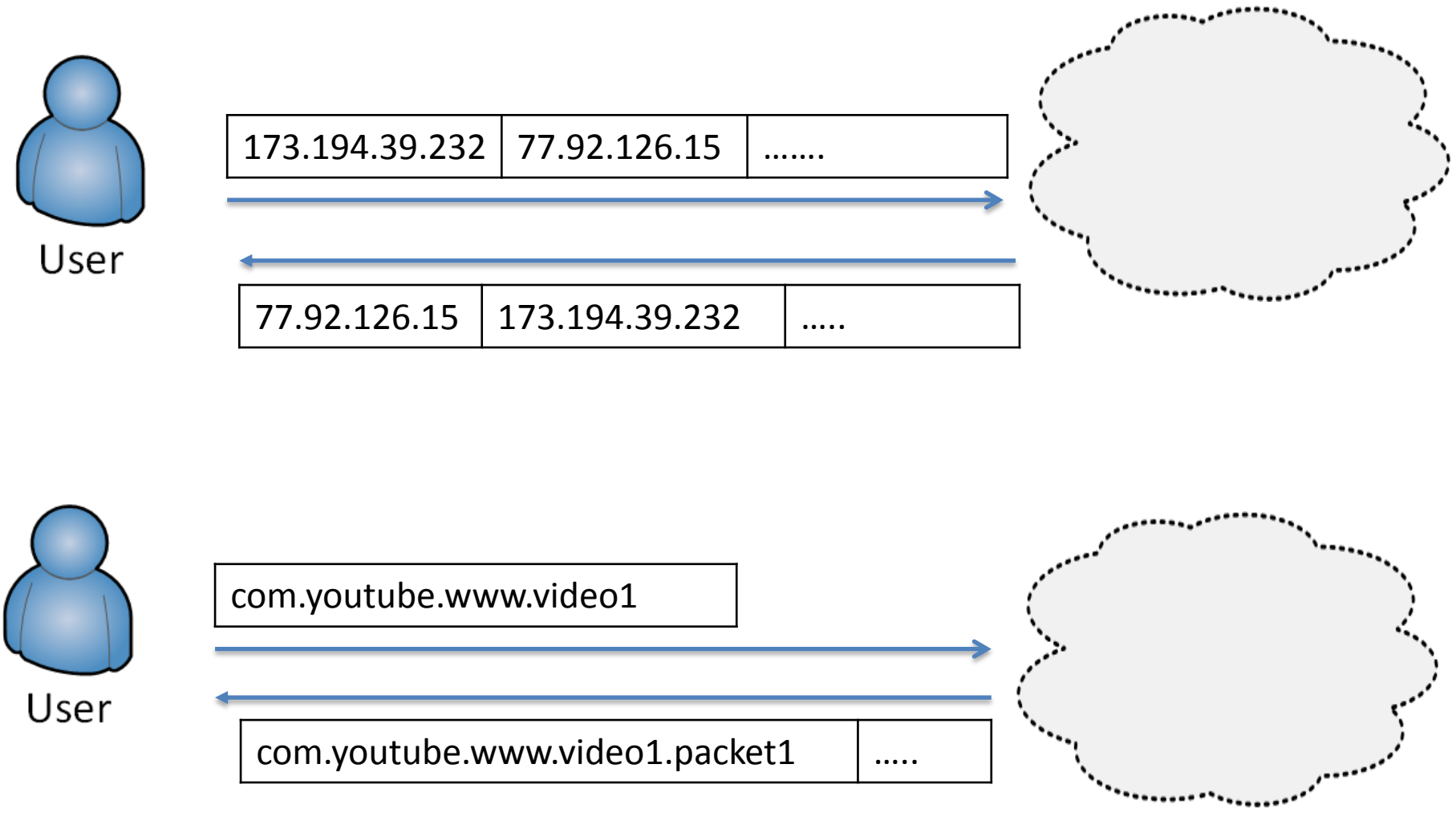
Nikos Fotiou, Somaya Arianfar, Mikko Sarela and George C. Polyzos

ICN Networking Research



G. Xylomenos et al. “A Survey of Information-Centric Networking Research,” IEEE Communications Surveys and Tutorials, 2013

ICN 101


User
173.194.39.232
77.92.126.15
…….
77.92.126.15
173.194.39.232
…..
User
com.youtube.www.video1
com.youtube.www.video1.packet1
…..

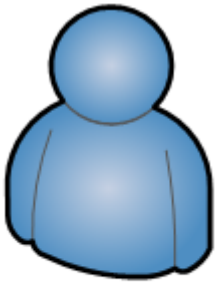
Why the fact that “the network knows” is important?

- Requests can be aggregated -> multicast
- Reponses can be cached
- It should be easier to isolate malicious information (malware, spam, (D)DoS)
- It should be easier to support multisource
- But what about user privacy?

Why privacy analysis of ICN is challenging?

- Many diverse ICN proposals
- Different forms of communication
  - Decoupled, Asynchronous, Indirection points, One-to-many
- New network functions
  - Information lookup, in-network storage

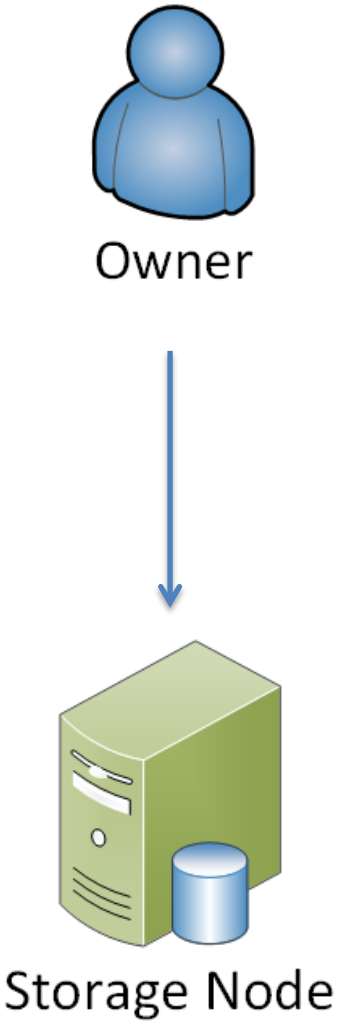
A common reference ICN model



Owner

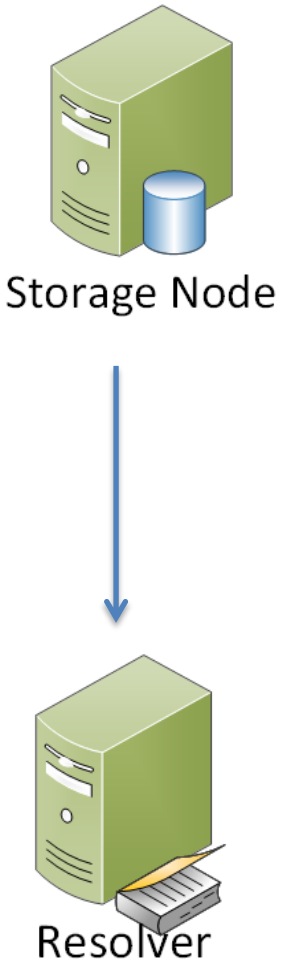
- Real world entity
- He **owns** a **content item** that wants to disseminate

A common reference ICN model



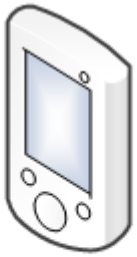
- The owner **stores** the content item in a **storage node**

A common reference ICN model



- The storage node **advertises** the content item in a **resolution network**

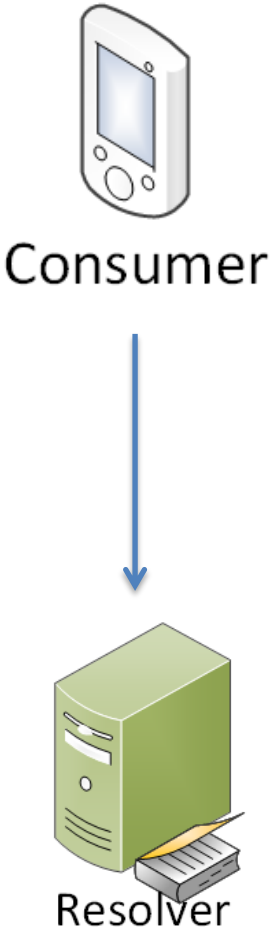
A common reference ICN model



Consumer

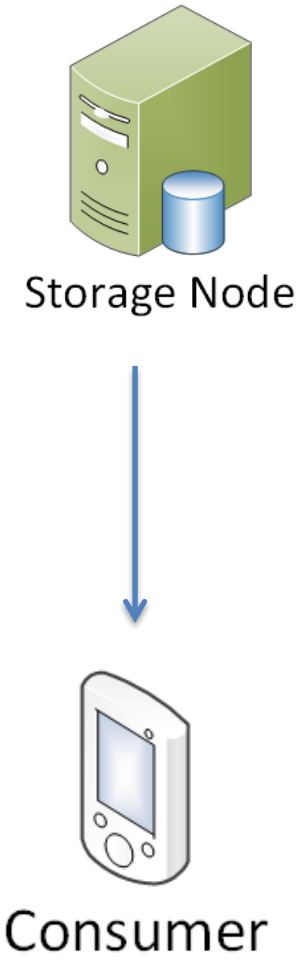
- The device of a user that is **interested** in receiving a content item

A common reference ICN model



- The consumer performs a content **lookup** in the **resolution network**

A common reference ICN model



- The desired content item is **forwarded** from the storage node to the consumer

A common reference ICN model

- Design choices for:
  - Naming
  - Advertisement
  - Lookup
  - Forwarding
- Each design choice has different impact on privacy

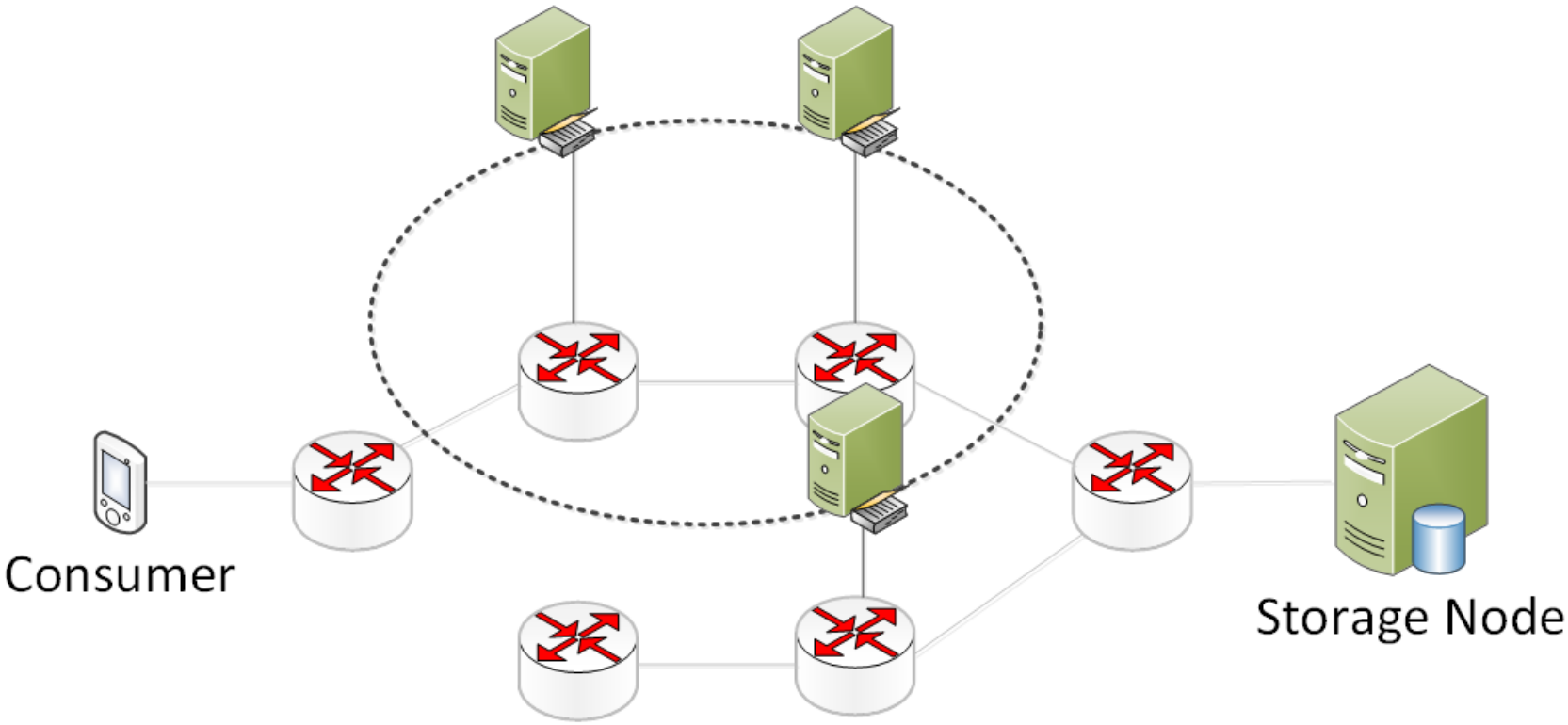
An example

- Design choice: Advertisement and lookup are (de)coupled to the routing layer
- Threat: Surveillance of consumers of a particular item
- Threat ranking (1-5) based on:
  - Damage
  - Reproducibility
  - Exploitability
  - Affected users
  - Discoverability

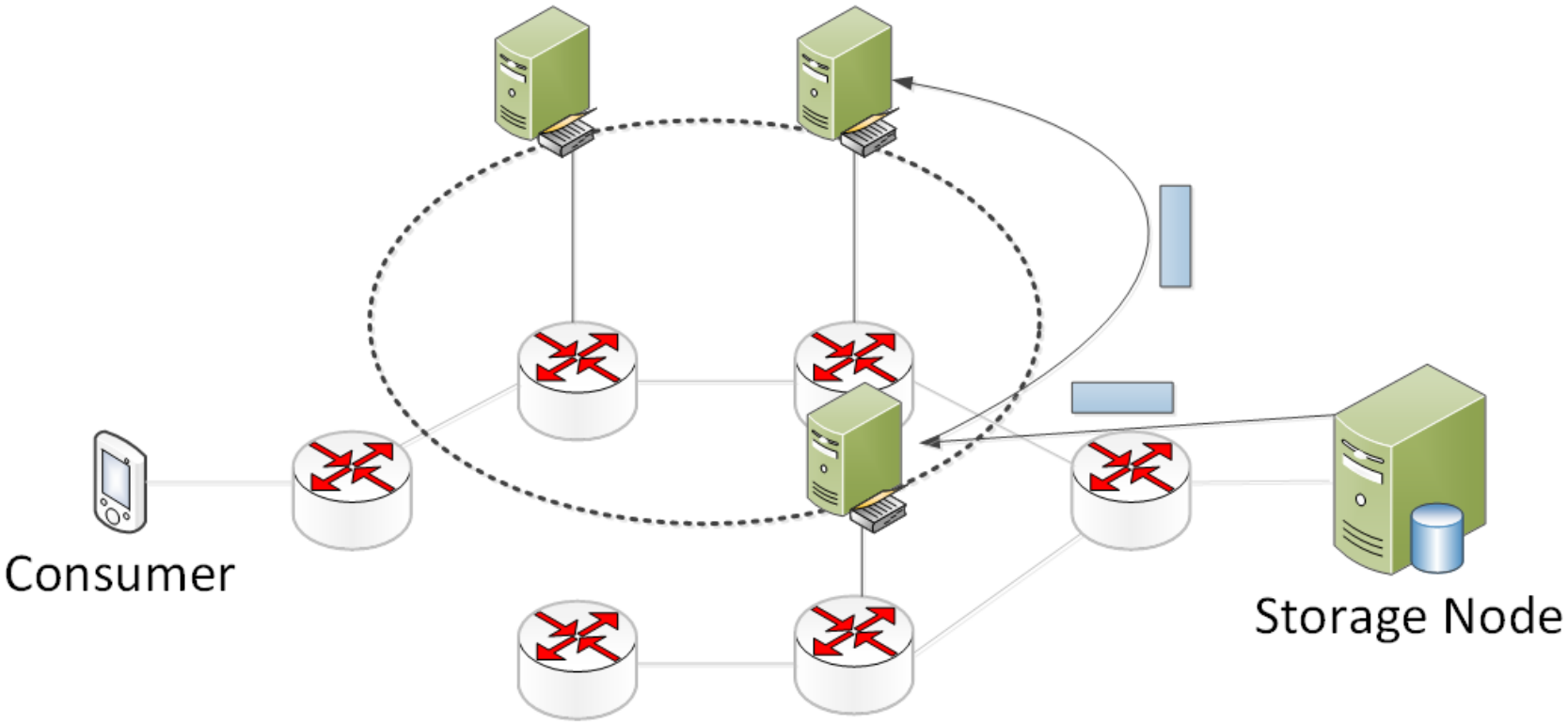
Adversary

Location	Role	Mode of operation
Local	Owner	Active
Arbitrary	Consumer	Passive
	Storage node	Honest-but-Curious
	Resolver	
	Observer	
	Authority	

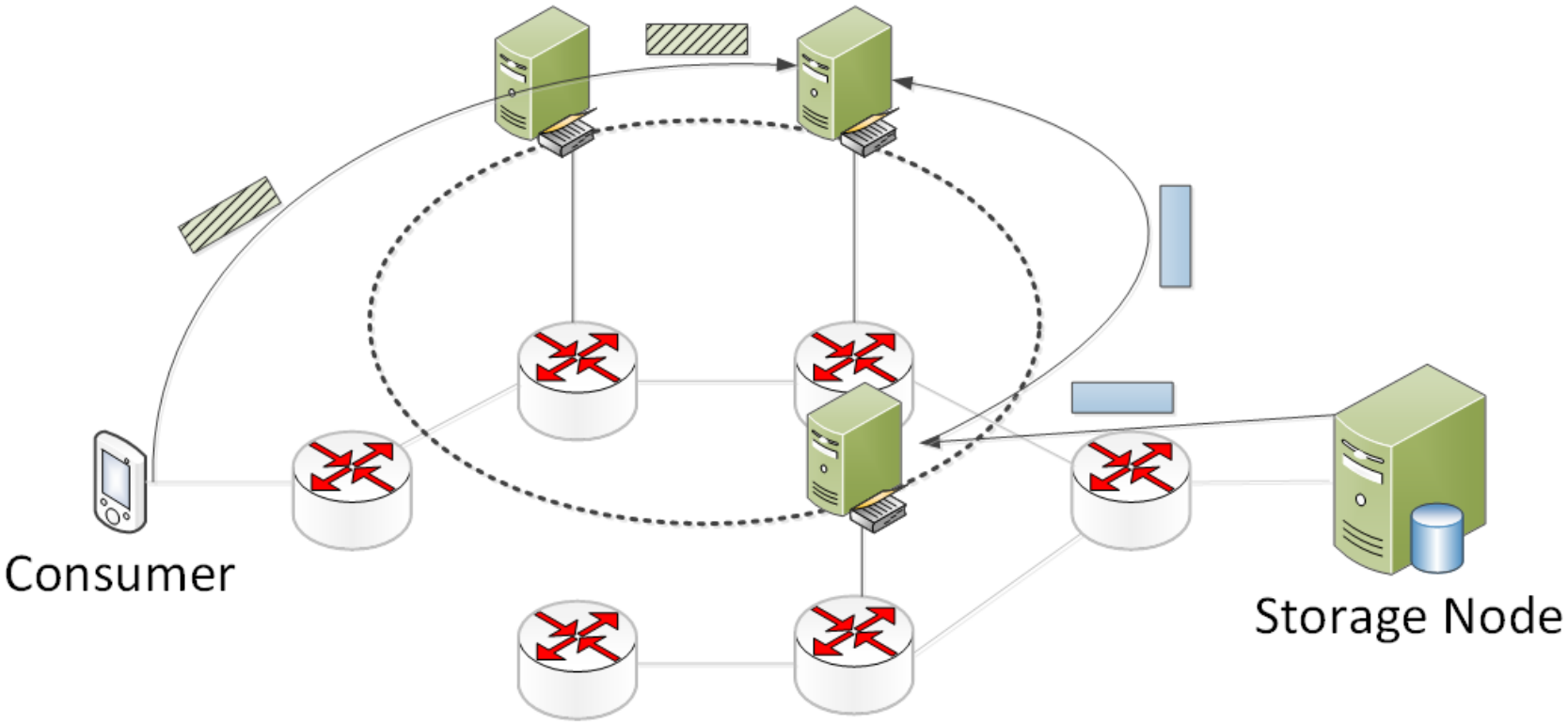
Design choice 1: Advertisement and lookup are decoupled to routing



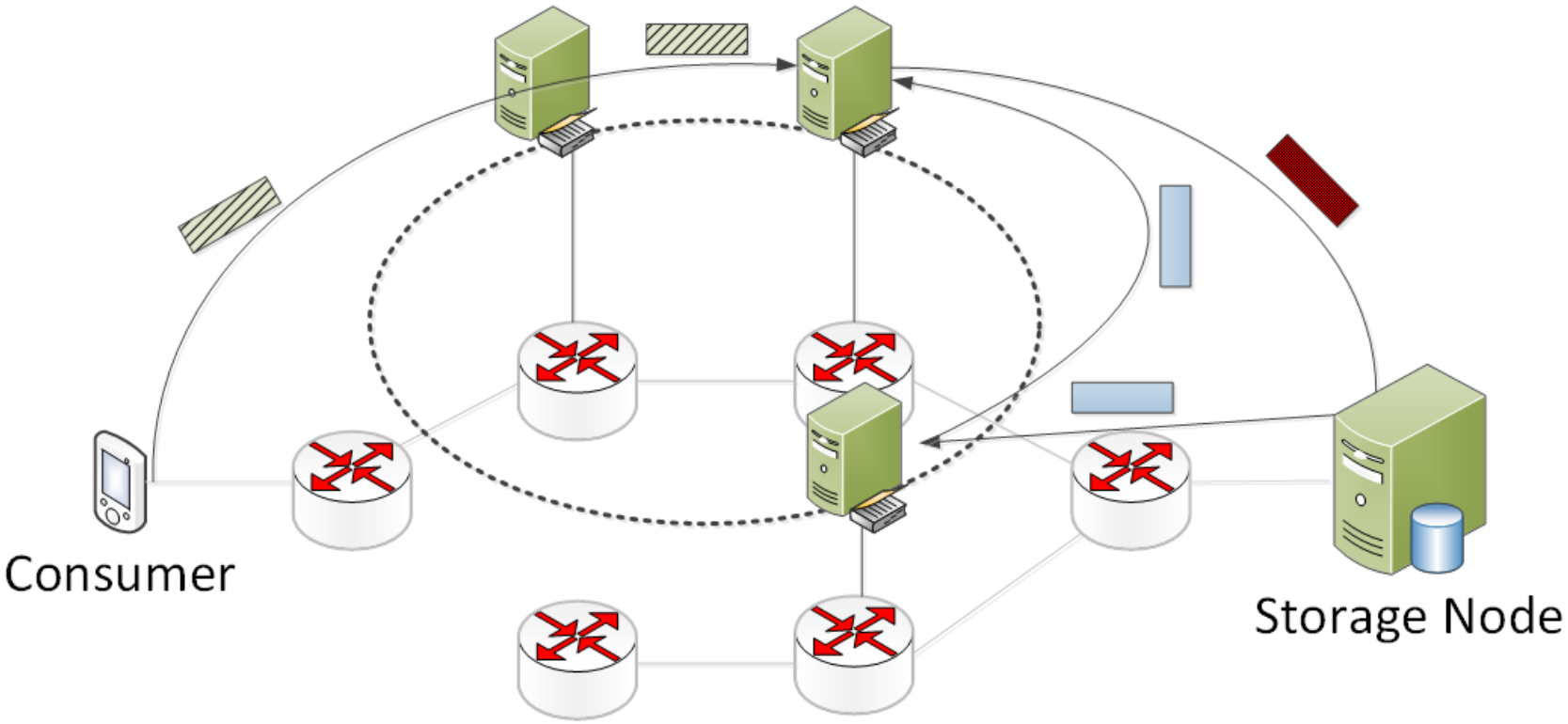
Design choice 1: Advertisement and lookup are decoupled to routing



Design choice 1: Advertisement and lookup are decoupled to routing



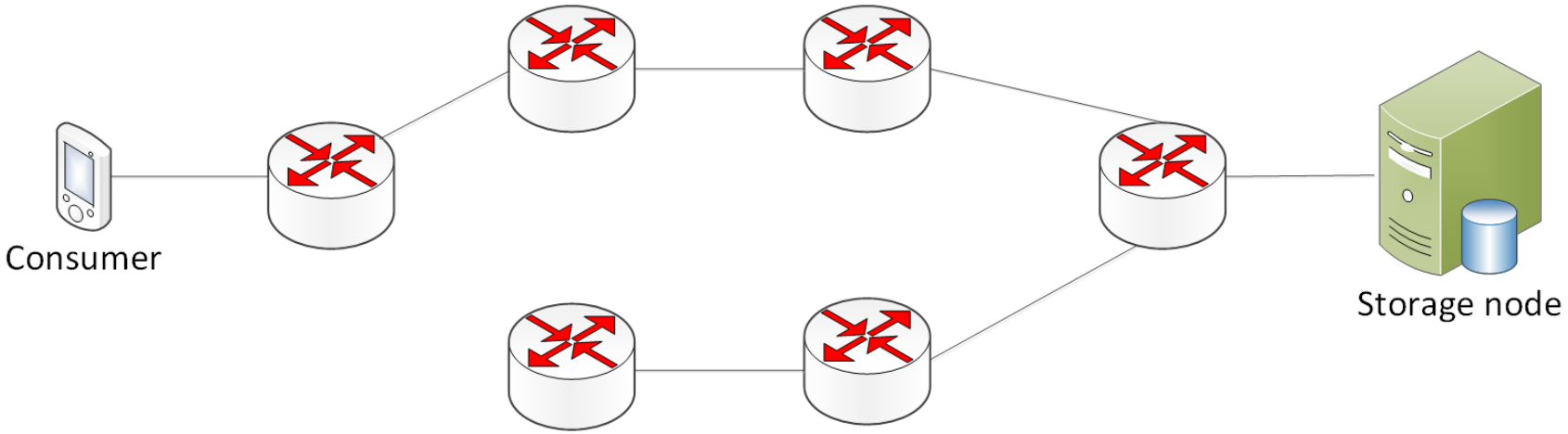
Design choice 1: Advertisement and lookup are decoupled to routing



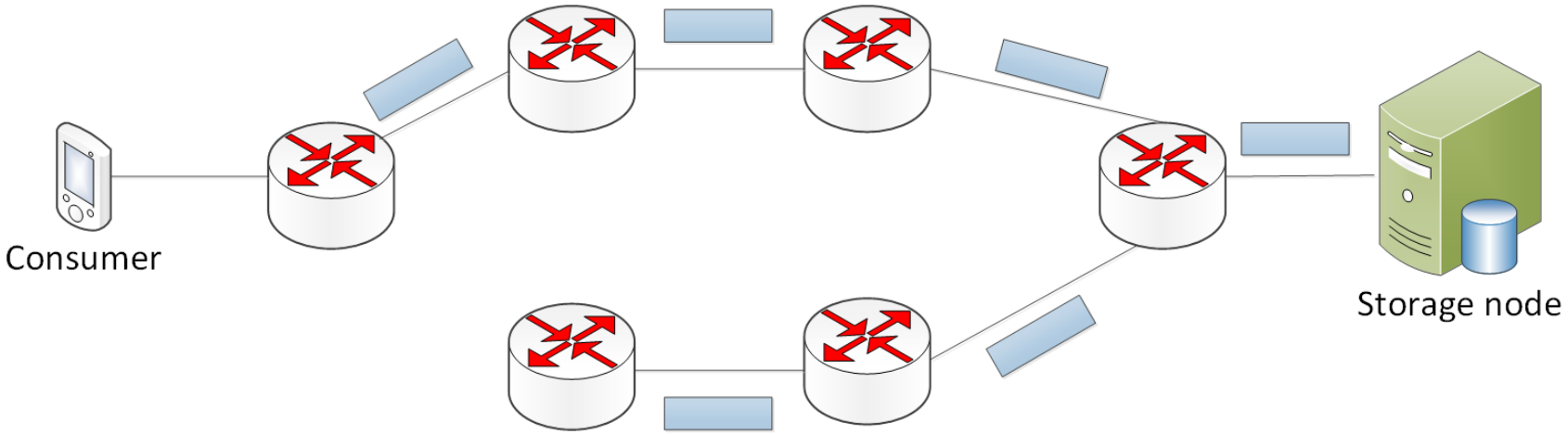
Threat ranking for design choice 1

Damage	Reproducibility	Exploitability	Affected users	Discoverability
5	1	4	3	2

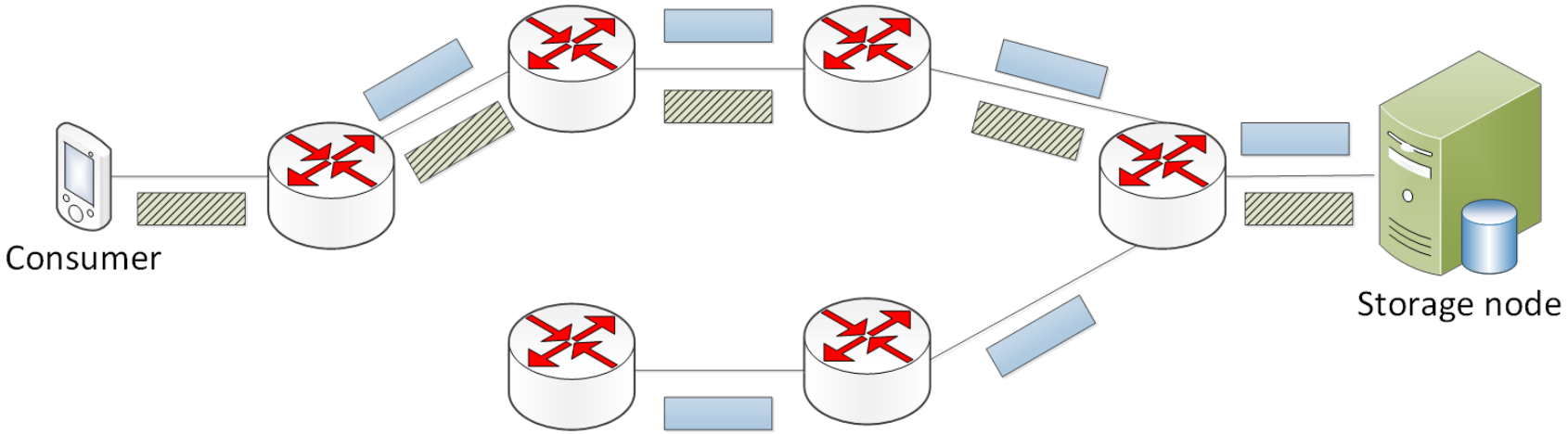
Design choice 2: Advertisement and lookup are coupled to routing



Design choice 2: Advertisement and lookup are coupled to routing



Design choice 2: Advertisement and lookup are coupled to routing



Threat ranking for design choice 1

Damage	Reproducibility	Exploitability	Affected users	Discoverability
5	1	4	3	2

Threat ranking for design choice 2

Damage	Reproducibility	Exploitability	Affected users	Discoverability
2	3	3	3	3

Final remarks

- We consider more design choices, adversaries and threats in the paper
- Our approach can be used to compare solutions, to choose design choices and to propose new privacy solutions

Thank you

fotiou@aueb.gr