parc
A Xerox Company

# Anonymous Named Data Networking Application

## NDN Security Group

Ersin Uzun, Steven DiBenedetto, Gene Tsudik, Paolo Gasti

# Privacy Challenges in NDN

- Name Privacy: semantically related names
  - Interested in “/healthonline/STDs/..”
- Content Privacy: unencrypted public content.
  - Retrieved content is an “.mp3” file
- Signature Privacy: leaked signer(publisher) identity
  - Retrieved content is signed by “match.com”
- Cache privacy: detectable cache hits/misses
  - Interests from this user usually misses caches -- it is for Russian content.

# Objective

- Design a practical system for NDN that enables
  - user privacy and anonymity
  - censorship resistance

- Implement and evaluate its performance and anonymity guarantees

# Threat Model

- Passive:
  - Traffic observation & fingerprinting
  - Timing & size correlation

- Active:
  - Moving attacker
  - Compromised routers & content producers

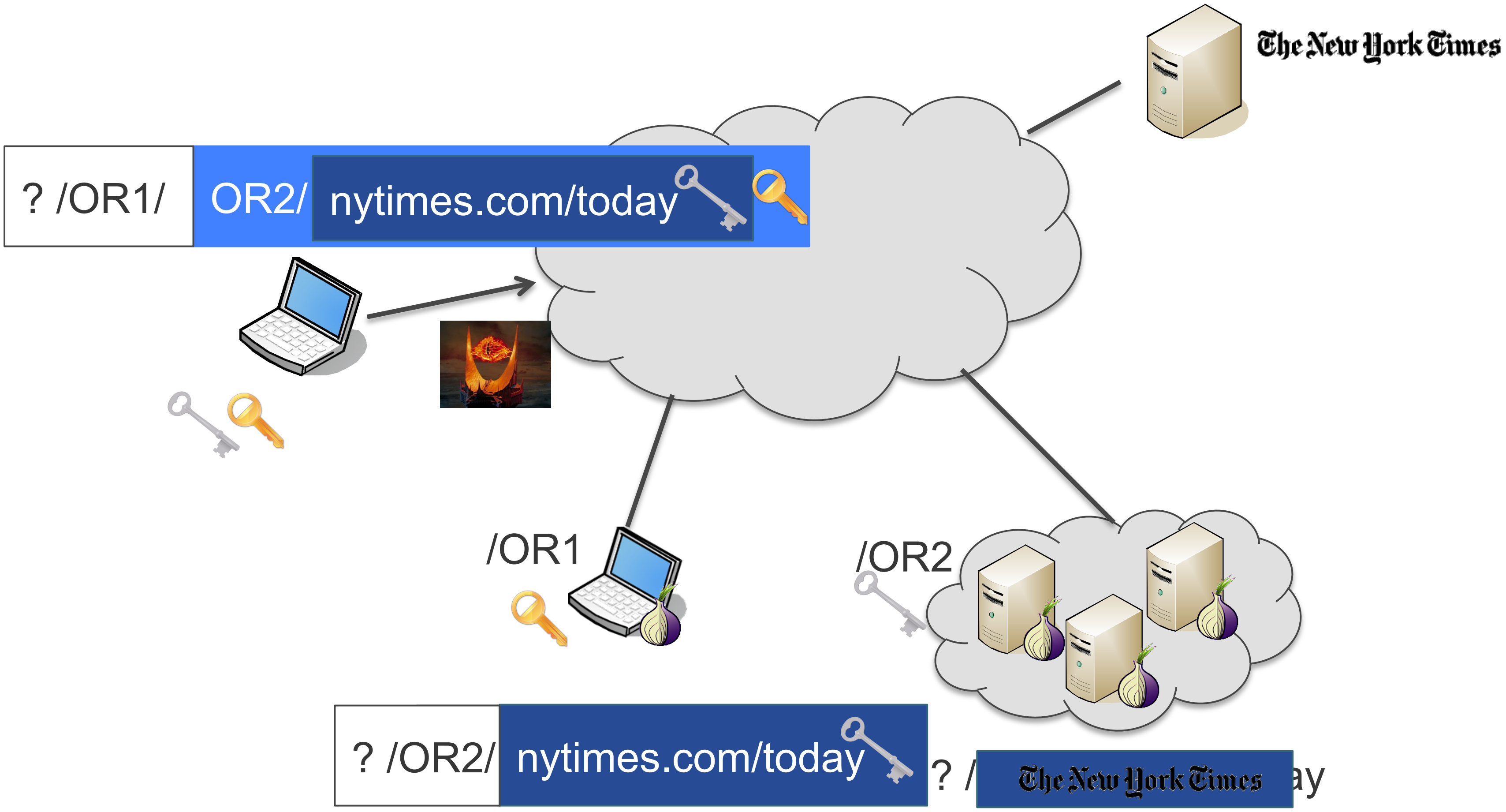
# Named Data Onion Routing (NDor)

- Consists of client and anonymizing router (AR) software
- Supports two modes
  - Ephemeral : Asymmetric encryption of interests
  - Session: Symmetric encryption of interests
- Client:
  - Encrypt & encapsulate interests
  - Decrypt & decapsulate data
- Anonymizing Routers:
  - Decrypt & decapsulate interests
  - Encrypt & encapsulate data

# Interest & Content Format

- Layers of encrypted Interests reside inside the name component of interests
  - E.g.,: */anonymizer/Enc(Timestamp* || *key* || *Interest)*
- Content is encrypted with the client-provided key on its way back
  - Encapsulation is published under the requested name and signed by ARs.

# NDor Example



? /OR1/

OR2/

nytimes.com/today

/OR1

/OR2

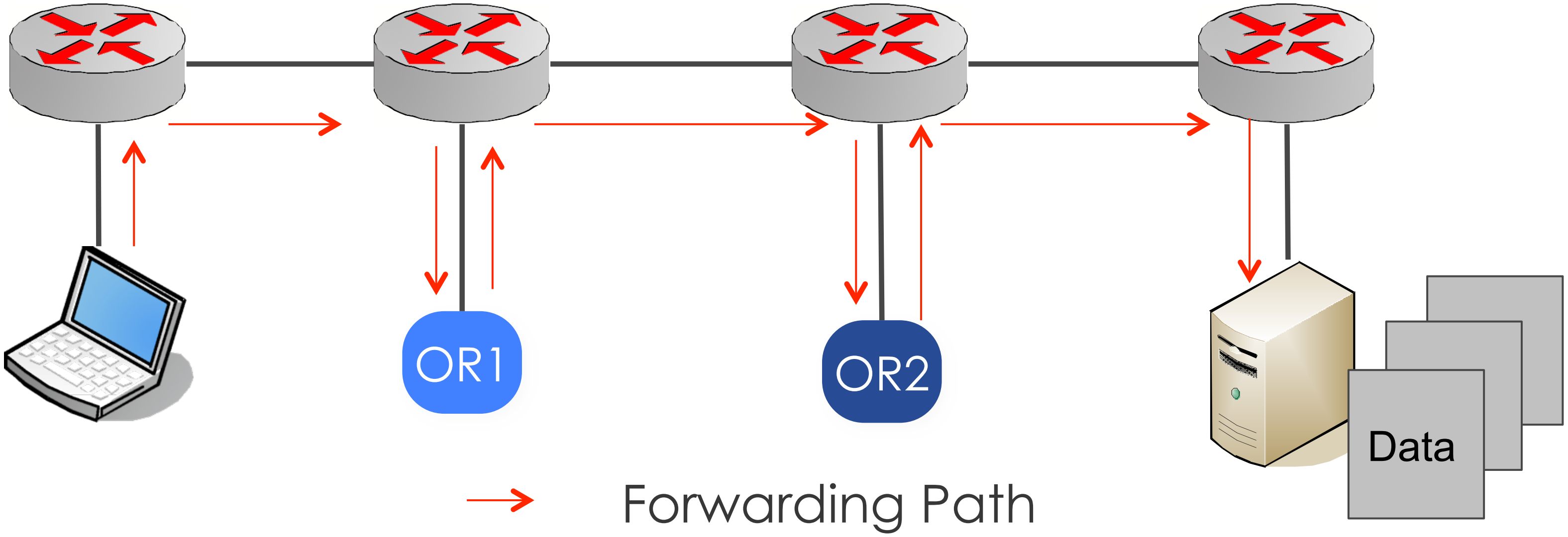
? /OR2/

nytimes.com/today

? /

ay

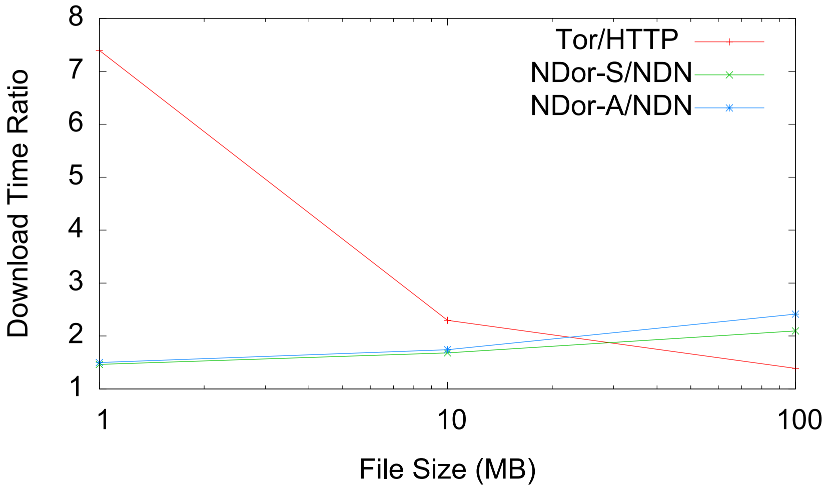
# Experimental Setup



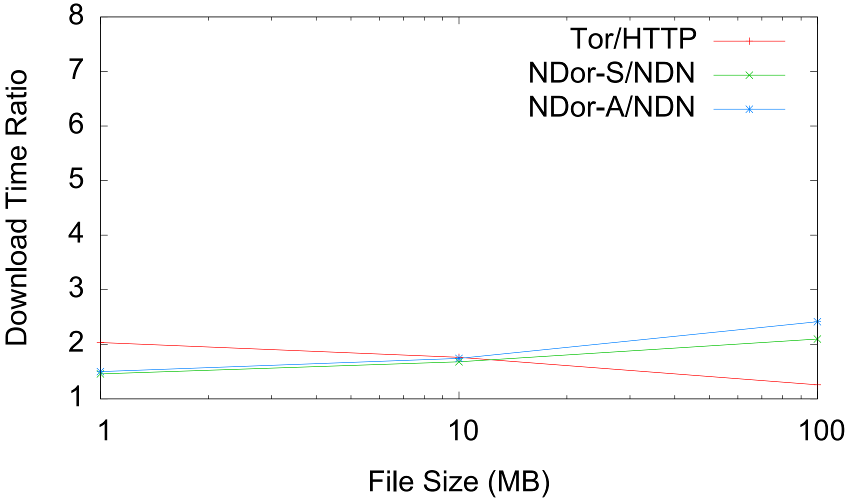
- Experiments on ONL
  - Line topology
  - Comparison with TOR (for comparable privacy)

# Initial Results

Cold Start:
Including Initial setup time



Warm Start:
Omitting the setup time



- Computational relative overhead is comparable to Tor...
- Expected real-life overhead is less than Tor
  - NDor requires less hops (2 ARs only compared to 3 in Tor and others)
  - Dynamic caching on and around exit nodes

# Other Security topics in NDN project

- More efficient security primitives
  - Esp. signature schemes
- New library functionalities
  - e.g., access control, key mgnt, signed interests…
- Trust management research
  - Alternatives for PKI

# Thanks!

- NDN website:
  - http://www.named-data.net
- Contact information:
  - euzun@parc.com