Anonymous Communication in Named Data Networking (NDN)

@PARC: Ersin Uzun, Steven DiBenedetto
@UCI: Gene Tsudik, Paolo Gasti

Named Data Networking (NDN)

- NDN is a collaborative research effort to design a future Internet architecture
- NDN is based on CCNx
- NDN team consists of 9 universities and PARC

Privacy Challenges in NDN

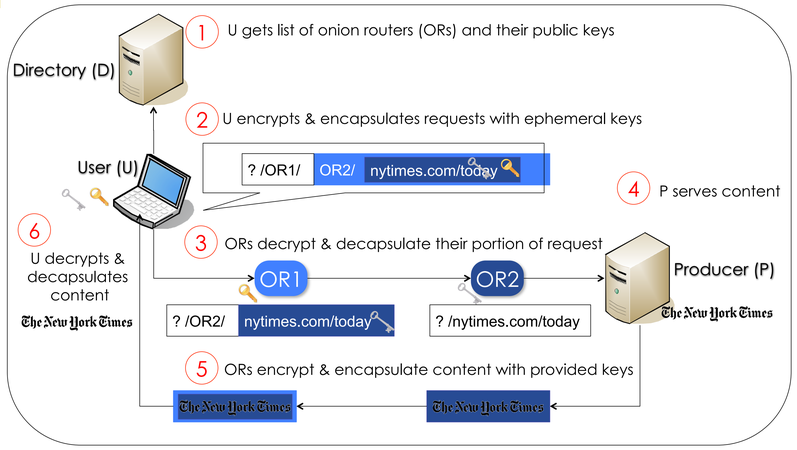
- **Name Privacy**: semantically related names
  - e.g., "/healthonline/STDs/.."
- **Content Privacy**: unencrypted public content.
  - e.g., retrieving and ".mp3" file
- **Signature Privacy**: leaked signer identity
  - e.g., content signed by "match.com"
- **Cache privacy**: detectable cache hits/misses
  - e.g., Alice's interests always miss caches

Question: *How to address them with an easy to deploy solution?*

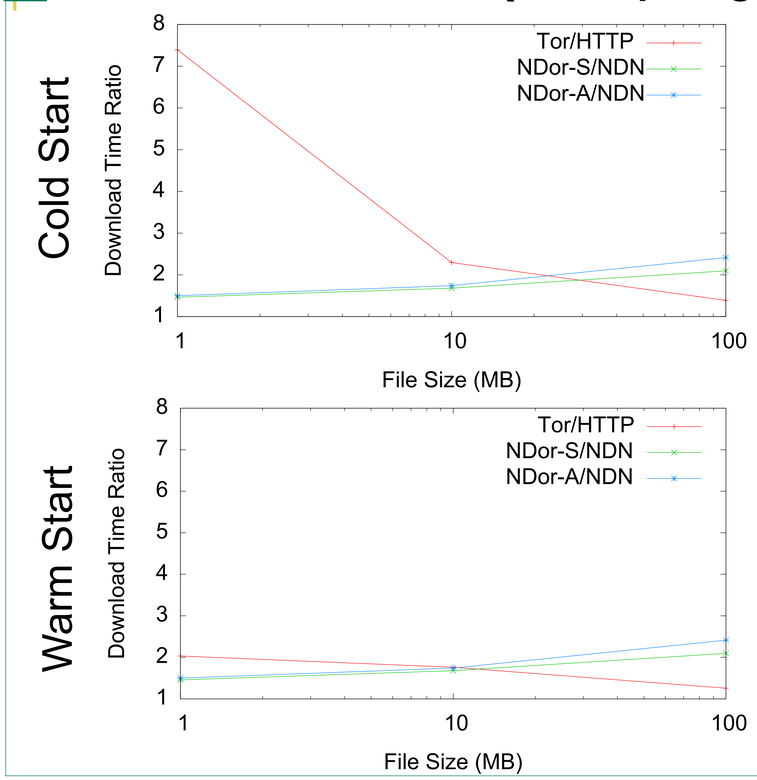
Main Idea

- Use onion routing to hide interests/content
  - Only closer hops can easily identify user
  - Layers of encryptions on interests are peeled off as it travels away from the user.
  - Use the name field on interest packets creatively for interest encapsulation.
  - As content travels back, put layers of encryption around it.
  - Preserve original interest information, content and publisher signature during the process.

Communication Steps



Performance Overhead (line topology)



Implementation

- C application running over CCNx
  - Client transparently encrypts & encapsulate user's traffic
  - Anonymizing routers maintain per-packet state
    - Name mapping & content encryption key
- Support for symmetric/asymmetric crypto for ephemeral/session-based operation
- Source code will be available to public soon.

NDor Results

- Robust, flexible, distributed architecture
- Verifiable privacy and anonymity guarantees with less nodes than its IP based analogs (2 vs. 3)
- Comparable per node computational overhead with existing solutions
- Expected to outperform its IP analogs in real life

Security Topics in NDN

- More efficient security primitives
  - Faster signature generation/verification
- New library functionalities for security
  - Access control, security protocols, key management
- Trust Management framework/solutions
- Privacy and anonymity

For more information about the Named-Data Networking Project: http://www.named-data.net/