State-of-the-art security and privacy attacks and mitigations in Information Centric Networking

Contact Info: Mohamed Rashad (m.Rashad@student.tudelft.nl) , Chhagan Lal (c.lal@tudelft.nl), Mauro Conti (m.conti@tudelft.nl)

1 Background information on ICN

- Future Internet architecture
- Content routing
  - Location-independent
- Suitable for high internet activity:
  - Ubiquitous caching
  - Efficient content retrievals
  - Low latency
- Scalable
- Content centric security
- Security and privacy issues

2 Main Research Question

What are the security and privacy attacks and defence mechanisms in ICN and how do these attacks impact different functionalities of ICN?

3 Research methodology

- Literature review on topics:
  - ICN architecture
  - State-of-the-art security and privacy attack in ICN
- 2 security attacks and 2 privacy attacks:
  - Impacted entities and network metrics
  - Attacker requirements
  - Relation between attack and network config
  - Violated security and privacy parameters
- Improve existent the timing attack defence mechanism.

4 Investigation Results

	Associated adversarial model (attacker requirements)	Entities impacted by the attack/attackers	Network metrics impacted by the attack/attackers	Security & Privacy parameters violated due to the attack	Attack-network configuration relation
Interest flooding (Fig. 1) [2][3]	Hijacked users / owned devices to preform large amount of interest requests, request non-existent content	Users, Routers, Content providers	Pending Interest Table (PIT) space overloaded, bandwidth reduction, increase in latency, decrease in network throughput, increase network traffic	Availability, Access control, Content Authentication, Non-repudiation	Small size of PIT, large interest requests expiration time, no use of rate limiting algorithms
Cache pollution [2]	Hijacked users / owned devices to request interest, Set of unpopular content	Routers, Users, Content providers	Bandwidth reduction, increase in network traffic, increase in response delays and latency, disrupted/falsified cache locality, decrease in cache hit-ratio	Integrity, Availability	LRU caching algorithm, no use of public/subscribe architecture, absence of popularity evaluation on content
Timing attack (Fig. 2) [1][2]	Precise time measurements of cache hits/misses	Users, Edge routers	-	Confidentiality, Request Secrecy, Unlinkability	Non-randomized time delays for cache hit/miss
Censorship (Fig. 3) [2]	Blacklist of content to censor, ability to drop/censor content based on content name	Users, Routers	-	Anonymity, Availability	Non-encrypted content names, No proxy usage

5 Limitations of existing defence mechanisms for timing attacks

- Time delay additions **[4]**:
  - Deteriorates user experience
  - Increases response delays
- State tracking for cache privacy **[4]**:
  - Hard to debug
  - Resource inefficient

6 Improved defence mechanism for timing attacks

- Time delays:
  - Balance between performance and user privacy
  - High enough to counteract timing attacks

$$td(n) = \begin{cases} 0, & h = 1 \\ 0.5 * td_0 \leq td(n) \leq 0.75 * td_x, & h > 1 \end{cases}$$

- Dedicated state nodes:
  - Better resource distribution
  - Allow state information replication
  - Easier debugging and logging

7 Conclusion and Future work

- Misconfigured network, choice of architecture and absence of critical countermeasures cause ICN to be more vulnerable for security and privacy attacks.
- The improved defence mechanism lacks stateless state tracking which can eliminate the need for active state tracking and additional infrastructural nodes.

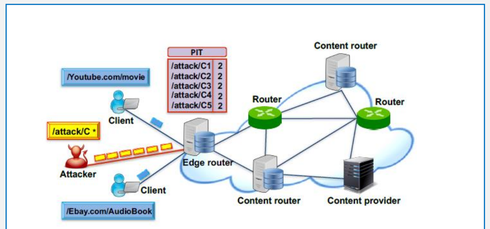

Fig. 1: DoS scenario

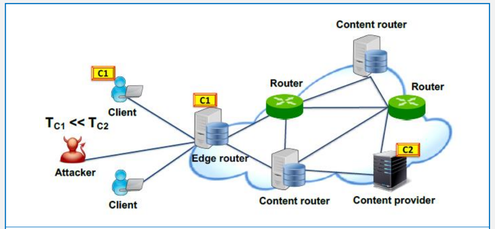

Fig. 2: Timing attack scenario

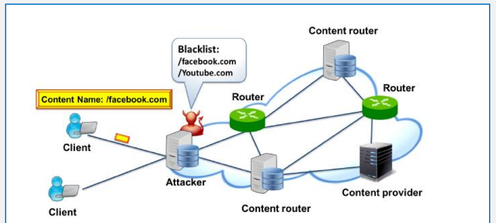

Fig. 3: Censorship risk scenario

References:

[1] Gergely Acs, Mauro Conti, Paolo Gasti, Cesar Ghali,and Gene Tsudik. Cache privacy in named-data net-working. In2013 IEEE 33rd International Conferenceon Distributed Computing Systems, pages 41–51, 201

[2] Eslam G. AbdAllah, Hossam S. Hassanein, and Mohammad Zulkernine. A survey of security attacks ininformation-centric networking.IEEE CommunicationsSurveys Tutorials, 17(3):1441–1454, 201

[3] Alexander Afanasyev, Priya Mahadevan, Ilya Moi-seenko, Ersin Uzun, and Lixia Zhang. Interest floodingattack and countermeasures in named data networking.In2013 IFIP Networking Conference, pages 1–9, 201

[4] Abedelaziz Mohaisen Verisign Labs, Abedelaziz Mo-haisen, Verisign Labs, Xinwen Zhang Huawei Tech-nologies, Xinwen Zhang, Huawei Technologies, MaxSchuchard University of Minnesota, Max Schuchard,University of Minnesota, Haiyong Xie Huawei Tech-nologies, and et al. Protecting access privacy of cachedcontents in information centric networks, May 20