Cache-Induced Privacy Risks in Named Data Networking

What is the Cost of Performance?

Tobias Lauinger
toby@ccs.neu.edu

Northeastern University

Overview

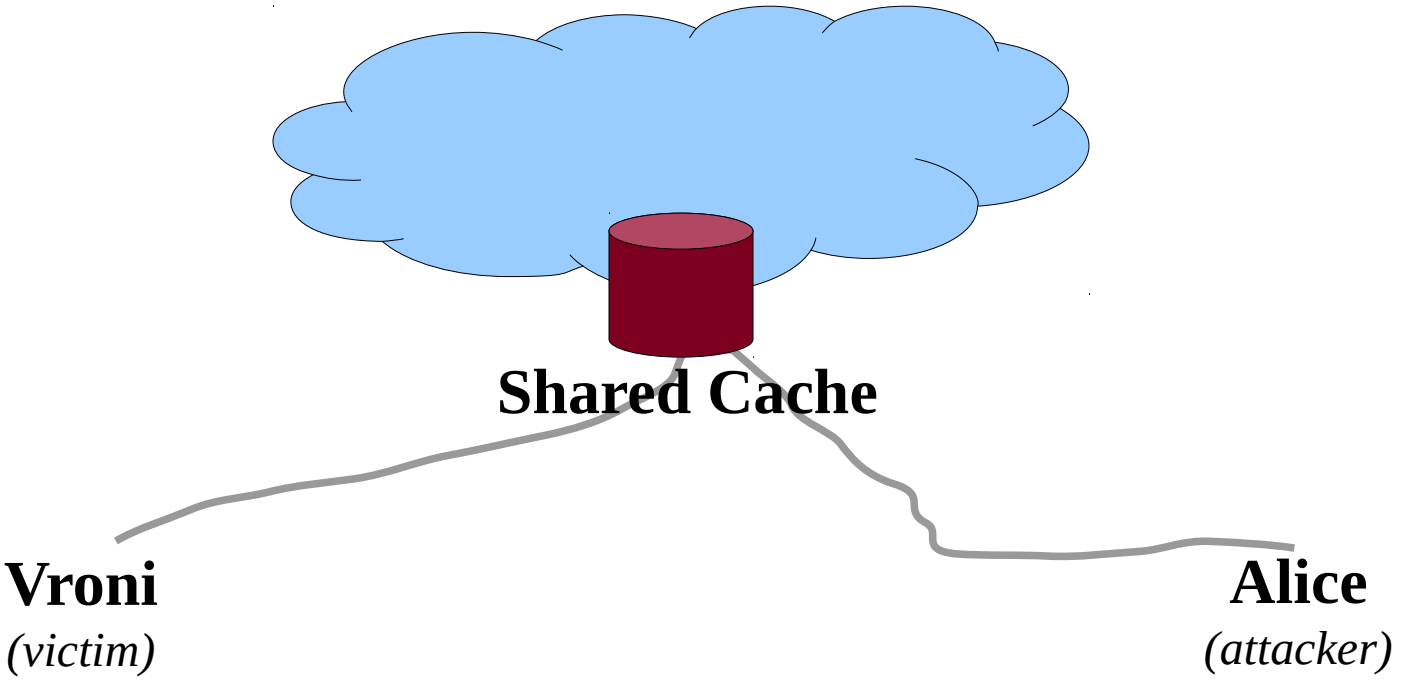
- Privacy Leaks in NDN/CCN
- Attack Model for Cache-Based Attacks
- Simple Cache Probing Attack
- Performance XOR Privacy?
- Alternative Approaches

Privacy Leaks in NDN

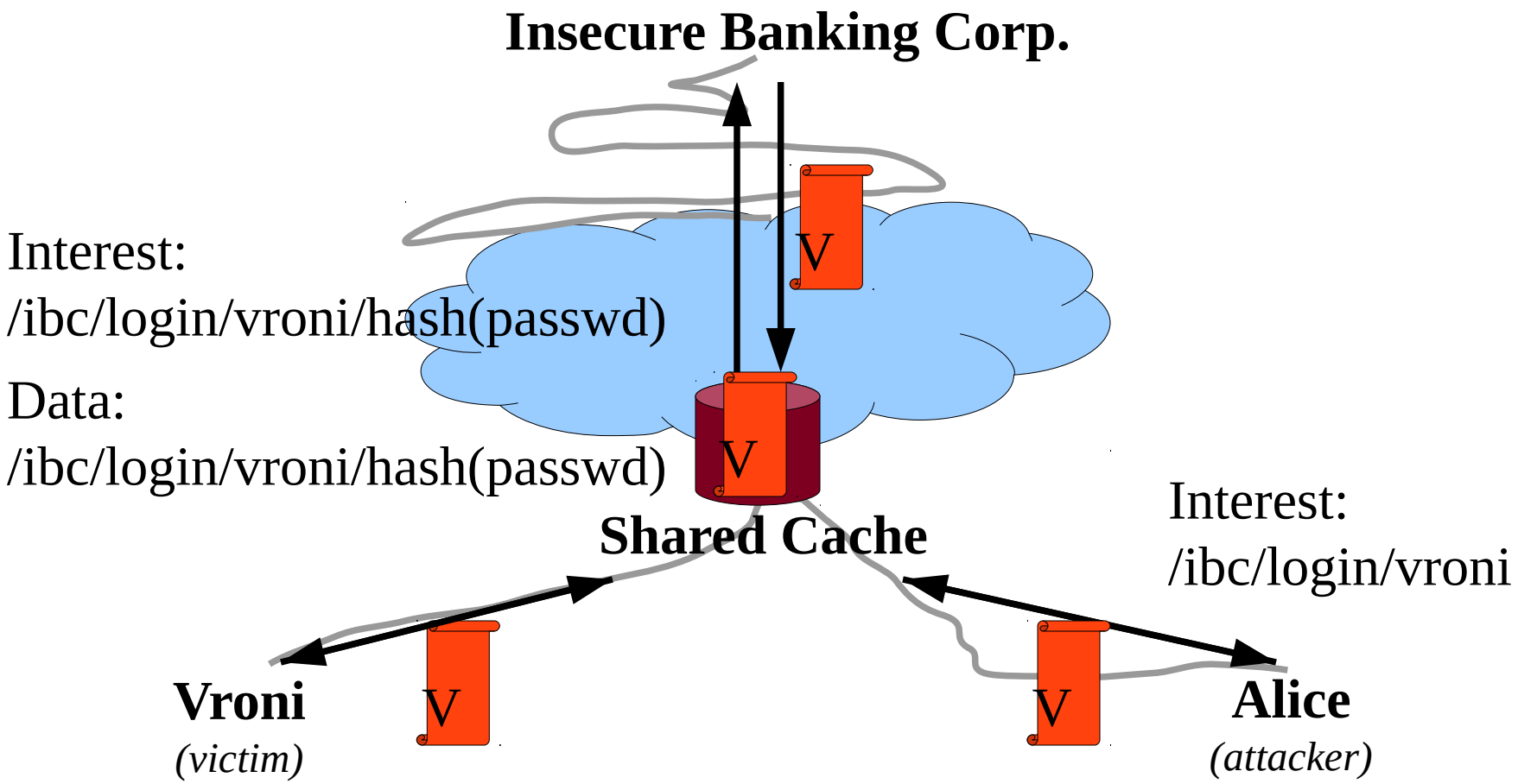
- NDN: Self-Contained Content Objects
  - Location-independent (content names)
  - Caching “easy”
- Privacy Leaks
  - Object name
  - Signature
  - Cache hit/miss (not a “new” problem)
  - ...

Attack Model

- Trusted ISP
- “Unprivileged” attacker



Simple Cache Probing Attack



Performance XOR Privacy?

- “Any” user can spy on other users connected to the same cache
- End-to-end solution: Tunneling (Andana)
  - Performance decreases
  - No more caching
- Users must risk privacy to get performance
- For privacy, they must “break” NDN

Alternative Approaches

- Better use an in-network approach?
  - Detect if privacy-sensitive and don't cache
  - Improve privacy *and* performance
- Hybrid approaches
  - “Don't-cache flag” (Interest or Data-driven)
  - Compartmentalisation
- … or “advanced” end-to-end approaches
  - Selective tunneling

Conclusion & Outlook

- Attack (probably) feasible by “every” user
- Other privacy attacks conceivable (PIT)
- Solutions should not purely rely on users
  - if not “properly” used, bad for performance
  - if not used, bad for privacy

- Can we “reconcile” privacy and performance?