

=====

**Title : Privacy in Router-Side Caching: the Case of Named-Data Networking**

**Gene Tsudik**

Content-Centric Networking (CCN) is an alternative to host-centric networking exemplified by today's Internet. CCN emphasizes content distribution by making content directly addressable. Named-Data Networking (NDN) is an example of CCN being considered as a candidate next-generation Internet architecture. One key NDN feature is router-side content caching that optimizes bandwidth consumption, reduces congestion and provides fast fetching for popular content.

Unfortunately, the same feature is also detrimental to privacy of both consumers and producers of content. As we show in this paper, simple and difficult-to-detect timing attacks can exploit NDN routers as ``oracles" and allow the adversary to learn whether a nearby consumer recently requested certain content.

Similarly, probing attacks that target adjacent content producers can be used to discover whether certain content has been recently fetched. After analyzing the scope and feasibility of such attacks, we propose and evaluate some efficient countermeasures that offer quantifiable privacy guarantees while retaining key features of NDN.

Joint work with Gergely Acs (INRIA), Cesar Ghali (UCI), Paolo Gasti (NYIT) and Mauro Conti (UPD)

**BIO:**

Gene Tsudik is a Chancellor's Professor of Computer Science at UC Irvine (UCI). He received his PhD in Computer Science from USC in 1991. Before coming to UCI in 2000, he was at IBM Zurich Research Laboratory (1991-1996) and USC/ISI (1996-2000). Over the years, his research interests included many topics in security, privacy and applied cryptography. He serves as the Editor-in-Chief of ACM Transactions on Information and Systems Security (TISSEC).

=====