Privacy-Aware Caching in Information-Centric Networking

ABSTRACT

Today's Internet has become a de facto public utility with a large percentage of the world's population relying on it for numerous activities. However, despite its unparalleled success and popularity, the current IP-based architecture is rapidly aging. As a consequence, a number of research efforts have recently started in preparation for the next-generation Internet architecture. One key motivator for a new Internet architecture is the fundamental shift in the nature of traffic. What was once mainly low-bandwidth interactive (e.g., remote log-in) and store-andforward (e.g., email) communication in the early days of the Internet is now web- and content-dominated traffic. At the same time, massive and ever-increasing amounts of content continue to be produced and consumed (distributed) over the network. This phenomena is manifested over file sharing services such as Dropbox and media sites such as YouTube and Netflix.

EXISTING SYSTEM

Information-Centric Networking (ICN) is an emerging network architecture in which the focal point is named and routable data (content), rather than hosts and addresses. In ICN, a consumer requests content by name (i.e., expresses interests for the content) and the network takes care of finding and returning the data. The ICN approach moves hosts into the background by treating named content as a first-class object. One important ICN feature is opportunistic in-network content caching. Its goal is to reduce congestion while improving throughput and latency for popular content. In contrast to IP, ICN routers can often satisfy interests using previously forwarded content. Consequently, content might be served from a router's cache rather than its original producer.

Disadvantages

- Cross-site timing attack is more dangerous as it can reveal information about private sections of websites.
- Not safe against cache privacy attacks.

PROPOSED SYSTEM

This paper explored cache privacy in ICN (and CCN) and identified several important privacy threats. We then introduced some plausible and effective counter-measures. First, we suggested that consumers and producers should indicate which content is privacy-sensitive. Then, we proposed several techniques that provide certain tradeoffs between privacy and latency. These techniques were assessed with respect to local and distributed adversaries. We also introduced a formal model that allows us to quantify the degree of privacy offered by various caching algorithms. We believe that proposed techniques are general and may be of interest beyond caching.

Advantages

- Cache privacy in ICN, with NDN.
- The attacker sends a Java applet to the victim and detects cache hits with respect to the user's browsing cache.

SOFTWARE REQUIREMENTS

Front-end	:	JSP
Back-End	:	MySQL
Server	:	Tomcat Server
OS	:	WINDOWS 7/above

HARDWARE REQUIREMENTS

PROCESSOR	:	CORE i3
RAM	:	512MB-2GB
HARD DISK	:	40GB