Metadata-private Communication

Yossi Gilad

Today, most Internet communication is encrypted. However, it is still difficult to hide the communication metadata, like who communicates with whom and at what time, which usually remains exposed to anyone able to observe network traffic. Metadata reveals a great deal of information. Recent research proposes new systems that hide metadata. However, these solutions usually fall short on performance. Poor performance limits applications to a relatively small user-base, to run on desktop machines, and to means of communication with low requirements on latency such as e-mail exchange and text messaging .

In this talk, we will describe key concepts of the state of the art systems in hiding metadata and discuss whether the above limitations are inherent.