Deployable Anonymity System: Introducing Sparta

Tech ID: 33657 / UC Case 2024-798-0

BACKGROUND

Metadata is used to summarize basic information about data that can make tracking and working with specific data easier. Today's communication systems, like WhatsApp, iMessage, and Signal, use end-to-end encryption to protect message contents. Such communication systems do not hide metadata, which is the data providing information about one or more aspects of such contents, like messages. Such metadata includes information about who communicates with whom, when, and how much, and is generally visible to systems and network observers. As a result, cyber risk associated with metadata leakage and traffic analysis remains a significant attack vector in such modern communication systems. Previous attempts to address this risk have been generally seen as not secure or prohibitively expensive, for example, by imposing inflexible bandwidth restrictions and cumbersome synchronous schedules globally, which cripples performance. Moreover, prior approaches relied on distributed trust for security, which is largely incompatible with conventional organizations hosting or using such apps.

TECHNOLOGY DESCRIPTION

To help address the growing cyber risks related to metadata leakage and traffic analysis, investigators at UC Santa Cruz (UCSC) have researched and reported on a new traffic analysis model named Sparta with a research goal of safeguarding users' messages against correlations made by an observer of a network and its system infrastructure. UCSC's key approach is prevent metadata from leaking who is communicating with whom, even if a bad actor or system is able to observe all parts of the network and can compromise the system itself. The demonstrated UCSC system uses original software code, novel oblivious algorithms, and configured hardware enclaves to pass messages between users without disclosing information about who is talking to whom. Sparta further achieves its goal by custom leakage "risk profiles" based on long-term statistical attacks, which allows end-users certain performance tunability. Sparta can be implemented by a single organization (as compared to others require multiple collaborating parties) without violating trust assumptions, which reduces the operational challenges of deploying a real instance. Experiments evaluating the long-term performance of Sparta under real workloads resulted in sub-minute latencies with less network overhead than streaming music.

APPLICATIONS

- Network/Cloud security software

FEATURES/BENEFITS

- Preliminary results show sub-minute latencies with low overhead
- Implementable by a single organization without violating trust assumptions
- Flexible architecture for different environments requiring low-latency, multithread implementation, or distributed setting

RELATED MATERIALS

CONTACT

Marc Oettinger
marc.oettinger@ucsc.edu
tel: 831-502-0253.

INVENTORS

- Demertzis, Ioannis
- Fredrickson, Kyle
- Long, Darrell D.E.

OTHER INFORMATION

KEYWORDS

messaging, instant messenger, end-to-end encryption, metadata, cyber risk, cyberrisk, cybersecurity, traffic analysis attacks, traffic analysis, communication systems, telecommunications, oblivious sorting algorithm, oblivious sorting

CATEGORIZED AS

- **Communications**
  - Internet
  - Networking
- **Computer**
  - Security
  - Software
- **Security and Defense**
  - Cyber security

RELATED CASES

2024-798-0