Abstract

The present strategies that reduce the delay associated with multicast authentication, make more efficient usage of receiver-side buffers, make delayed key disclosure authentication more resilient to buffer overflow denial of service attacks, and allow for multiple levels of trust in authentication. Throughout this base paper, the main focus of discussion will be on the popular
Multicast Routing Authentication System using Advanced Tesla

multicast authentication scheme Timed Efficient Stream Loss-tolerant Authentication (TESLA) based upon the delayed key disclosure principle. Similar to other schemes based upon delayed key disclosure, TESLA is susceptible to Denial-of-Service (DoS) attacks and is not well suited for delay-sensitive applications.

Reference

- D. Bolenron, D. McGrew, and A. Sheimom, "Keyhkgement for Large Dynamic Groups: One-way Function Trees and Amortized Initialization," IETF Internet droft (work in progrrerr], Feb. 1999
- P. Q. Judge and M. H. Ammar, “WHIM: Watermarking Multicast Videowith a Hierarchy of

Index Terms

Computer Science    Network Security

Key words

Denial-of-Service (DoS) attacks
forge – capable area
Message Authentication Code (MAC)
multigrade source authentication
Timed Efficient Stream Loss-tolerant Authentication (TESLA)
Packet Interleaving
trust