Accepted Manuscript

Title: Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies

Author: Ismail Melih Tas, Bahar Ugurdogan, Selcuk Baktir

PII: S0167-4048(16)30098-0
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2016.08.007
Reference: COSE 1032

To appear in: *Computers & Security*

Received date: 26-10-2015
Revised date: 12-8-2016
Accepted date: 31-8-2016

Please cite this article as: Ismail Melih Tas, Bahar Ugurdogan, Selcuk Baktir, Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies, *Computers & Security* (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.08.007.

Novel Session Initiation Protocol-Based Distributed Denial-of-Service Attacks and Effective Defense Strategies

Ismail Melih Tas[a], Bahar Ugurdogan[b], Selcuk Baktir[c]

[a]*Department of Computer Engineering, Bahcesehir University, Istanbul, Turkey*

[b]*Department of Applied Mathematics, Bahcesehir University, Istanbul, Turkey*

[c]*Department of Computer Engineering, Bahcesehir University, Istanbul, Turkey*

*Corresponding author

Email address: selcuk.baktir@bahcesehir.edu.tr (Selcuk Baktir)

Abstract

Voice-over-IP (VoIP) and its underlying session initiation protocol (SIP) techniques have become popular in recent years. VoIP/SIP techniques are used widely in unified communication systems and next generation networks, and there is no doubt they will play increasingly important roles in the future of communication techniques. However, unlike transmission control protocol (TCP)-based applications, the user datagram protocol (UDP)-based VoIP/SIP applications are not as mature and they have some security vulnerabilities. Therefore, it is crucial to study VoIP/SIP-related security issues. In this study, we investigated the existing vulnerabilities in the SIP protocol and identify new vulnerabilities in the SIP retransmission mechanisms, which could be exploited by denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks. We prepared a VoIP/SIP security laboratory environment and a DDoS attack simulator. We developed two advanced attacks by exploiting the vulnerabilities identified in the SIP retransmission mechanism and we implemented these attacks in our laboratory environment using the DoS/DDoS attack simulator. Our intelligent attacks could bypass black-lists as well as IP-based rate limiting, packet count-based rate limiting, session/transaction-based rate limiting, and automatic message generation detection systems in the existing state-of-the-art security perimeters, such as firewalls, intrusion detection systems, intrusion prevention systems, and anomaly detection systems. Furthermore, we developed a novel defense mechanism to effectively combat the proposed attacks and we implemented it successfully in our VoIP/SIP security laboratory environment. We showed that our defense mechanism reduced the CPU load