A Survey of Man in the Middle Attacks

The Man-In-The-Middle (MITM) attack is one of the most well known attacks in computer security, representing one of the biggest concerns for security professionals. MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself. In this paper, we extensively review the literature on MITM to analyse and categorize the scope of MITM attacks, considering both a reference model, such as the open systems interconnection (OSI) model, as well as two specific widely used network technologies, i.e., GSM and UMTS. In particular, we classify MITM attacks based on several parameters, like location of an attacker in the network, nature of a communication channel, and impersonation techniques. Based on an impersonation techniques classification, we then provide execution steps for each MITM class. We survey existing countermeasures and discuss the comparison among them. Finally, based on our analysis, we propose a categorisation of MITM prevention mechanisms, and we identify some possible directions for future research.

General information
Publication status: Published
Organisations: Copenhagen Center for Health Technology, Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark, University of Padova
Contributors: Conti, M., Dragoni, N., Lesyk, V.
Pages: 2027-2051
Publication date: 2016
Peer-reviewed: Yes

Publication information
Journal: IEEE Communications Surveys and Tutorials
Volume: 18
Issue number: 3
ISSN (Print): 1553-877X
Ratings:
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 23.8 SJR 3.494 SNIP 11.505
Web of Science (2016): Impact factor 17.188
Web of Science (2016): Indexed yes
Original language: English
Keywords: Man-In-The-Middle (MITM) attack, MITM classification, MITM defence techniques, Security
DOIs:
10.1109/COMST.2016.2548426
Source: FindIt
Source-ID: 2303156438
Research output: Contribution to journal › Journal article – Annual report year: 2016 › Research › peer-review