Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis M.Sc.

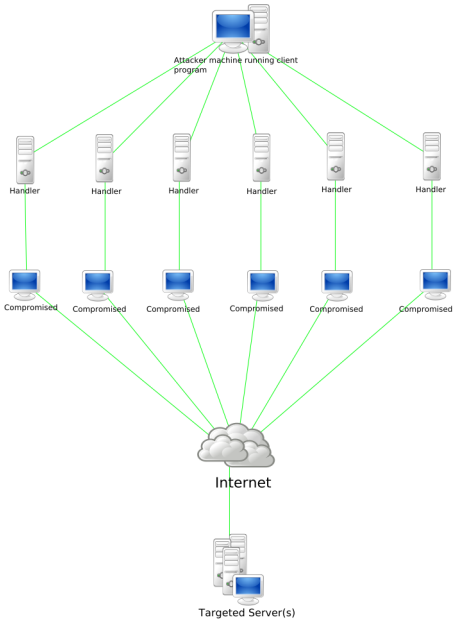
IDP, HiWi

Passive Privacy-Preserving Amplification Attack Detection at Scale

Motivation

Amplification attacks are a special type of DDoS attacks, where the response packet is significantly larger than the request packet. Research has shown [a] [b] that amplification attacks in protocols are widespread. We developed a system [c] to detect amplification attacks in a protocol-agnostic manner.

In this thesis you will build upon previous work which extended the IDS Suricata to allow for protocol-agnostic amplification attack detection. You will implement a privacy-preserving mechanism [d] to pseudonymize private information such as IP addresses. In addition, you will implement a service to notify affected parties upon detection of an ongoing attack. You will evaluate the built software on live traffic of multiple tens of gigabits per second.



[a] Rossow: *Amplification Hell: Revisiting Network Protocols for DDoS Abuse.* NDSS 2014.
[b] Gasser et al.: *The Amplification Threat Posed by Publicly Reachable BACnet Devices.* JCSM 2017.
[c] Böttger et al.: *DoS Amplification Attacks – Protocol-Agnostic Detection of Service Abuse in Amplifier Networks.* TMA 2015.
[d] CryptoPAN: https://github.com/keiichishima/yacryptopan

Requirements

- Interested, motivated, autonomous work ethic
- Experienced in C programming
- You live the GIYF motto

Contact

Oliver Gasser gasser@net.in.tum.de
Simon Bauer bauersi@net.in.tum.de
Stefan Metzger stefan.metzger@lrz.de

http://go.tum.de/306574