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

Thesis B.Sc.

Thesis M.Sc.

Scanning for TCP SYN proxy implementations

Motivation

TCP SYN flooding is an effective Denial-of-Service attack. A common example for a mitigation strategy are TCP SYN cookies, shifting the attack from targeting the memory to a CPU exhaustion attack. Other approaches exist which are less computational expensive, but come with the tradeoff of less security or user friendlyness (e.g. SYN authentication). These techniques are not well documented, as they are usually only available as commercial black boxes.

http://tinyurl.com/hdcp4vh

In the wild, SYN flood mitigation techniques are deployed as a proxy. Only if the connection attempt is whitelisted using one of the mitigation techniques, a real connection with the target server is established. Finding these proxy implementations is not straight forward because of two reasons: First, the mitigation mechanism is only activated during an ongoing SYN flood. Second, depending on the used mitigation mechanism, the effect on the client is different, ranging from missing TCP options or strange packet sizes to connection resets.

The goal of this thesis is to find suitable active measurement approaches that are able to identify deployed SYN proxies in the Internet. Based on periodic measurements, different implementations have to be identified and their behavior over time analyzed. The data has to be analyzed in real time, so that in case a potential active proxy is detected, additional detailed measruements for the identified target can be performed.

Your Task

- Research mitigation methods: SYN cookies, SYN authentication, ...
- Conduct periodic Internet-wide scans
- Detect proxy deployments in real-time
- Analyse your findings

Contact

Dominik Scholz scholz@net.in.tum.de
Paul Emmerich emmericp@net.in.tum.de
Quirin Scheitle scheitle@net.in.tum.de

http://go.tum.de/215562