Automatic Detection of potential Attackpoints in Computernetworks

Alexander Motzek, M.Sc.
Institute for Information Systems
31. Oktober 2014

Summary
As part of an EU project in the field of computer security, we need to detect potential entry points of attackers into a network.

Such potential attack points deal as entry points of so called attack paths. Our approach is to identify such entry points as partners of a network who have direct internet access or are directly accessible from the outside. The approach is based on traffic captures, which are analysed in respect to an abnormal high in- and outbound traffic towards the outside of an encapsulated network. The evaluation is based on publically available data sets, spanning hundred of Gigabytes. Basic principals of Big Data and complexity theory is welcomed.

This Master’s thesis is open for all study fields. Basic knowledge of computer security is a benefit, but is also easily acquirable.

Example
Traffic captures, so called PCAPs, contain every single packet transmitted over a physical line. A recording and analysis environment is given by a popular tool „Wireshark“. A package, e.g., might show up a TCP-IP connection from a port of an IP towards another port of a different IP, in which another HTTP request is encapsulated. It becomes interesting, once a node of the network has a high inbound traffic from outside the network (e.g. the Internet), or, if, e.g., a node sends high amounts of HTTP requests to a partner not located inside the company’s network (read, he surfs the Internet and might catch a trojan).

The thesis is very open to independent, self-organized work and can be freely shaped. Study of current publications (papers) is advised.

Prerequisites
• Solid programming skills in Java
• Understanding of computer networks, protocols, etc.
• You know that Wiresharks don’t bite

Goals
• Excellent thesis
• Free, independent, self-organized work
• Literature research
• Publication at a scientific conference
• Use of your implementation in an EU project

Contact
ALEXANDER MOTZEK
Institute of Information Systems
Fon +49 451 500 5716
motzek@ifis.uni-luebeck.de
http://www.ifis.uni-luebeck.de/~motzek/