BDSec - Big Data Security

Body:

Motivation
No one is safe from criminal attacks and data breaches, motivated either by industrial espionage, politically motivated hacking, or broad surveillance by agencies. In addition, attackers can cause immense damage without the need for many resources. Because of the complexity and enormity of code, software, and traffic contributing to the internet, the detection of malicious attacks but also configuration errors or bugs takes time, or is impossible altogether. Thus, research and development is urgently needed to make Big Data accessible for IT-Security.

Challenges & Highlights
To protect hosts and clients from attacks in real time, we develop analytical tools that allow for the continuous analysis of Big Data. These will make the timely deployment of countermeasures possible. Specifically, in the field of infrastructure attacks, we aim to identify targeted attacks against client systems as well as DDoS attacks and improve protection against these kind of attacks. In the field of client threats, we plan to improve protection against SSL attacks as well as malware infection in end user clients.

Potential Applications & Future Issues
Since this project encompasses members from the German economy, namely DE-CIX Management GmbH and SAP SE, the results of this project will be deployed and installed in their current systems. Scientific publication in cooperation with our industry partners as well as with the research partners Ruhr-Universität Bochum and Fraunhofer AISEC will be published on the relevant conferences. In addition, we plan to contribute our general results and implementations into open source projects.

Project abstract:

BDSec aims to utilize Big Data technologies to protect Web infrastructure as well as client systems against a variety of threats like Distributed Denial of Service (DDoS) attacks or attacks against the end users of web applications. In the past, these attacks have been caused by botnets, but also exploits of configuration errors. The project identifies attack vectors with the use of Big Data tools on real-time data flows while following the "privacy by design" approach, and aims to suggest countermeasures to the identified problems.

Logo:

Project manager:
Prof. Dr. Matthew Smith

Project duration:
2015 - 2016

URL:
http://bdsec.de

Research Area:
E-Science

Status of the Project:
Bibsonomy show project publications:
1
Bibsonomy use tabs to list publications: 1