
- Bachelor- / Masterarbeit -

Effiziente Speicherung von Netzwerk-Flowdaten

CASED	Das neue Forschungs- und Entwicklungszentrum für IT-Sicherheit CASED (Center for Advanced Security Research Darmstadt) stellt sich mit seinen starken Partnern – der Technischen Universität Darmstadt, dem Fraunhofer Institut für Sichere Informationstechnologie und der Hochschule Darmstadt – einer immensen Herausforderung: In einer einzigartigen Kooperation von Informatikern, Ingenieuren, Physikern, Juristen und Betriebswirten, mit internationalen Forschungszentren und Industriepartnern, werden zukunftsweisende IT-Sicherheitslösungen erforscht, entwickelt und in die Anwendung und wirtschaftliche Verwertung gebracht.	
Motivation	Netzwerk-Flowdaten stellen eine abstrakte und aggregierte Beschreibung in einem IP-Netzwerk stattfindender unidirektionaler Kommunikationsflüsse dar. Kommunikationsflüsse werden in der Regel eindeutig durch das 5-Tupel (Quell-IP, Ziel-IP, Quell-Port, Ziel-Port, Layer 4 Protokoll) charakterisiert und um Intensitätsinformationen (ausgetauschte Byte/s und Pakete/s) erweitert. Netzwerk-Flowdaten werden in unterschiedlichen Dateiformaten von Netzkomponenten (Routern, Switches) exportiert (z.B. Cisco NetFlow, IPFIX) und werden häufig zum Netzmonitoring, Accounting und Billing sowie zur Angriffs-Erkennung verwendet.	
Aufgabenstellung	Wenngleich die Verwendung von Netzwerk-Flowdaten im Vergleich zu rohen Netzdaten eine enorme Datenreduktion darstellt, werden in Hochgeschwindigkeits-Netzwerken sehr viele Flows erzeugt, die je nach Anwendungszweck unterschiedlich lang gespeichert und anhand variierender Charakteristika zur späteren Verarbeitung abgerufen werden können müssen. Im Rahmen dieser Arbeit sollen daher effiziente und flexible Verfahren zur Speicherung, Indexierung und zum Abruf von Netzwerk-Flowdaten entwickelt werden. Die Lösung soll dabei in der Lage sein, unterschiedliche Flowdaten Formate zu harmonisieren. Optional kann ergänzend die Fragestellung der automatischen Datenkorrelation (Clustering) thematisiert werden.	
Voraussetzungen	<ul style="list-style-type: none">• Kreatives, eigenständiges und engagiertes Arbeiten• Kommunikationsbereitschaft• Gute Programmierkenntnisse (z.B. C, Perl, Ruby)• Gute Kenntnisse gängiger Internetprotokolle• Linux-Kenntnisse sind vorteilhaft• Sehr gute deutsche und/oder gute englische Sprachkenntnisse	
Starttermin	Ab sofort	
Kontakt	Sebastian Abt sebastian.abt@h-da.de 06151.16-8416	CASED Mornwegstraße 32 64293 Darmstadt