Hochschule
Augsburg University of
Applied Sciences

Abschlussarbeit

Fakultät für Informatik

Titel

Implementierung und Evaluation eines SNMP Scanners

Autor: Christian Weiß
Prüfer: Prof. Dr. Winter

Datum: 29. Juni 2015

Einleitung

Das Internet ist ein weltweiter Verbund von Rechnernetzwerken. Physikalisch besteht das Internet im Kernbereich aus einzelnen Netzwerken von Providern, Firmen und Universitäts- und Forschungsnetzwerke. Router verbinden diese Netzwerke miteinander.
Das Internet im Ganzen ist unbekannt. Selbst Netzbetreiber kennen nur einen kleinen Teil. Eine Verwaltung findet nur in den Subnetzen statt. Das macht eine Erfassung und Überwachung schwierig. Um den Zustand des Internet zu messen, sind viele Messstellen notwendig. Gut geeignet als Messstellen sind Endgeräte die sich regelmäßig Pakete durchs Internet schicken. Dieser Datenverkehr aus den Messungen kann Aufschluss über das Internet geben. Dafür wurde in der Hochschule eine App namens „Glimpse“ entwickelt, die auf allen erdenklichen Endgeräten installiert werden kann. Glimpse verfügt über verschiedene Messmethoden, wie z.B. ein Bandbreitentest. Die Endgeräte sollen aus den Subnetzen, in denen sie sich befinden, die Bandbreite des Netzwerks zum Internet messen. Doch das Ergebnis einer solchen Messung kann keinen direkten Aufschluss zur Bandbreite geben. Waren zum Zeitpunkt der Messung noch andere Verbindungen aktive, so kann der gemessene Wert von der Bandbreite des Netzwerks stark Abweichen. Um nun eine bessere Einschätzung machen zu können, müsste man wissen, wie viele Verbindungen während der Messung bestanden haben. Diese Information hält ein Router in seinen Statistiken.
Es gibt verschiedene Protokolle mit denen Administratoren ihre Geräte im Netzwerk verwalten können. Darunter fallen Netconf und SNMP (Simple Network Management Protocol). Das Simple Network Management Protocol ist bereits weit verbreitet. Auf vielen Geräten wie Routern, Switches und Druckern ist vom Hersteller die Software bereits installiert. Ausgeliefert werden sie mit Standardpasswörtern, die von den Administratoren oft nicht geändert werden. Das bietet mir die Möglichkeit diese Geräte zu finden und auszulesen. Findet sich im Subnetz von einem Glimpse-Client ein Gateway-Router, der mit den Standardpasswörtern läuft, können die Statistiken ausgelesen werden.

Geschichte

„Die Geschichte des SNMP hängt stark mit der Geschichte des Internets zusammen.[...] So entstand im Jahre 1987 das SGMP (Simple Gateway Monitoring Protocol), da zu damaliger Zeit das Verbinden der Gateways das Hauptproblem war. Gleichzeitig entstand noch ein anderes Protokoll mit dem Namen HEMS (High Level Management Entity System), dessen Entwicklung schon länger zurückreichte. Allerdings fand dieses keine breite Unterstützung im Gegensatz zu dem SGMP, das schon zu dieser Zeit anfing, sich durchzusetzen. Ein weiterer Ansatz lag in einem OSI basierten Protokoll CMIP (Common Management Information Protocol) das auf TCP Protokoll aufgesetzt werden sollte und somit den Namen CMOT erhielt (CMIP over TCP). Aufgrund der geringen Durchsetzung von HEMS wurden nur SGMP und CMOT weiterentwickelt, ersteres, weil es schon weit verbreitet war und zweiteres, weil es auf einem langen ISO-standardisierten Untergrund aufbaute. Später sollten beide zu einem Protokoll verschmelzen. 1988 brachten die Entwickler um SGMP das RFC 1065 Structure of Managment Information [MR88b], RFC 1066 Managment Information Base [MR88a] und RFC 1067 Simple Network Managment Protocol [CFSD88] heraus, was dann 1989 zu recommended erklärt wurde, welches einem quasi-Standard entspricht und ab hier auch schon den Namen SNMP trägt. [...] SNMPv2 war allerdings von seinem Sicherheitsstandard her zu komplex, so dass dies keine breite Zustimmung fand und so wurde 1996 SNMPv2 nur mit dem Sicherheitsmanagement aus SNMPv1 noch mal als RFC eingereicht, was dann SNMPv2c genannt wurde. Doch auch diese Lösung wurde nicht als zufriedenstellend empfunden und so entstanden die beiden Standards SNMPv2u und SNMPv2*, die das Sicherheitsproblem lösen sollten. Als letztes ist noch SNMPv3, RFC 2272-2275, zu erwähnen, das als Nachfolger von SNMPv2 zu verstehen ist, aber zusätzlich noch die Vereinigung von SNMPv2u und SNMPv2* bewirken soll [Bla97]. Diese wurde 1998 zum Proposed Internet Standard und dann 1999 zum Draft Internet Standard.“ [**?**]

Literatur

[1] http://www-i4.informatik.rwth-aachen.de/content/teaching/proseminars/sub/2003$_s s_p roseminar_d ocs/snmp.pdf$