HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

P2P-Detektionsverfahren

Name der Diplomandin / des Diplomanden	Vincent Dorsch	Tobias Schoch
Examinator / Experte	Prof. Dr. P. Heinzmann	Dr. Th. Siegenthaler
Industriepartner		
Diplomausstellungs-Raum	1.258	

Unter einem Peer-to-Peer (P2P) Netzwerk versteht man einen Verbund von gleichberechtigten, miteinander kommunizierenden Computern. Gegenwärtig wird P2P vor allem unter jüngeren Internetbenutzern als Datenaustauschsystem genutzt. In Europa wird mehr als die Hälfte der übertragenen Datenmenge P2P-Verkehr zugeschrieben und in Asien sogar mehr als 80 Prozent. Vor allem im Privatbereich ist die P2P-Technologie von grosser Bedeutung. Bei Unternehmen und Internet Dienstanbieter hingegen ist die Technologie sehr umstritten, da häufig illegale Daten verbreitet werden, und die P2P-Clients zunehmend für Sicherheitsprobleme verantwortlich gemacht werden. Weiter führen die grossen Datenmengen zu grosser Belastung der vorhandenen Netzinfrastruktur.
Aufgrund dieser Argumente wünschen sich viele Unternehmen und Internet Dienstanbieter eine bessere Kenntnis zur P2P-Verbreitung in ihren Netzen.

Im Rahmen dieser Diplomarbeit wurde ein Detektionsverfahren entwickelt, dank welchem P2P-Verkehr nicht nur anhand spezifischer P2P-Protokolle, sondern durch P2P-typische Charakteristiken erkannt werden kann. Dieses universelle Detektionsverfahren ist wichtig, da die P2P-Protokolle und die P2P-Client einem rasanten Wandel unterlegen sind.

Anhand einer detaillierten Analyse konnten P2P-typische Verhaltensweisen identifiziert werden und es wurden passive Detektionsstrategien entwickelt, welche P2P-Verkehr mit einer sehr geringen Fehlerquote erkennen können. Als gute und universelle Detektionsstrategien erwiesen sich die Anzahl der Verkehrspartner, die übertragene Datenmenge, die Gleichmässigkeit der Aktivität des Datenverkehrs, die Anzahl und Art der ICMP-Meldungen, die Überprüfung verdächtiger P2P-Web-Portale, welche der Benutzer angesteuert hat sowie die Untersuchung der bezogenen Meta-Dateien.

Die entwickelten Erkennungsstrategien wurden in einem Prototypen implementiert. Erste Test zeigen, dass mit Hilfe des Verfahrens P2P-Verkehr erzeugende Rechner mit grosser Sicherheit identifiziert werden können, auch wenn diese keine allgemein bekannte, spezifisch für P2P-Verkehr vorgesehene Protokolle und Portnummern verwenden. Bei der realisierten P2P-Detektion werden - ähnlich wie bei der SPAM-Detektion - bestimmte Verkehrsparameter ausgewertet in gewichteter Form addiert.

Durch den implementierten Prototyp konnten die entwickelten Detektionsstrategien bestätigt werden. Anhand dieser neuartigen Detektionsstrategien ist es nun möglich, einen beispielsweise im ISP-Umfeld einsetzbaren Detektor zu entwickeln, welcher zwischen dem Internet und dem zu überprüfenden Netzwerk eingesetzt wird und den Netzwerkadministrator alarmiert, sobald eine P2P-Verbindung erkannt wurde.