Wenn DPI nicht tief genug ist

Steffen Ullrich, genua mbH, BMBF-Projekt Padiofire

1 Zusammenfassung

Ein aktueller Trend bei Perimeterfirewalls ist die Nutzung von *Deep-Packet-Inspection (DPI)* zur Applikationserkennung, und darauf aufbauend der Blockierung von unerwünschten Protokollen oder Inhalten. Mit Begriffen wie *Next Generation Firewall (NGFW)* oder *Unified Threat Management (UTM)* werden Lösungen angeboten, die eine volle Kontrolle über das Netzwerk bei dennoch hoher Performance versprechen.

Wir betrachten, wie gut diese Produkte wirklich sind, welche Probleme man mit DPI prinzipiell angehen kann und wann eine über existente Lösungen hinausgehende Inspektion und Manipulation der Daten notwendig ist. Unser Fokus liegt dabei auf der Absicherung von Clients durch Perimeterfirewalls innerhalb des Web 2.0.

Um tiefergehende Analysen zu vereinfachen, haben wir im Forschungsprojekt Padiofire eine Schnittstelle entwickelt, die bei Analysesystemen, wie z.B. *Intrusion Detection System (IDS)*, *Intrusion Prevention System (IPS)* oder Firewall, eine Trennung zwischen Datenextraktion und Datenanalyse schafft. Das erlaubt es, sich auf die zügige Umsetzung neuer Ideen zu konzentrieren und gleiche Analysen in verschiedenen Systemen zu verwenden.

2 Deep Packet Inspection

Ursprünglich war DPI der Versuch, durch Signaturanalyse einzelner Datenpakete Angriffe zu erkennen. Später wurden für Signaturvergleiche in streambasierten Protokollen wie HTTP die Daten mehrerer Pakete aggregiert. Moderne Systeme können auch tiefere Aggregierungen, wie z.B. einzelne Requests innerhalb einer HTTP-Verbindung, vornehmen. Aktuell werden unter dem Namen DPI auch Lösungen angeboten, die in der Lage sind, SSL- oder SSH-Verbindungen aufzubrechen (d.h. Man In The Middle), um so verschlüsselte Kommunikation zu analysieren.

Allen Interpretationen des Begriffs ist aber gemein, dass man sich auf die Inspektion der Daten beschränkt, sie also nicht verändert.

2.1 Anwendungsfälle

Aktuelle DPI Produkte lassen sich grob nach ihrer Nutzung in Lösungen zur Netzwerkoptimierung und Sicherheitslösungen unterteilen. Bei der Netzwerkoptimierung geht es um eine applikationsspezifische Bevorzugung (z.B. VoIP) oder Behinderung (z.B. P2P) von Daten in Real-time. Daher müssen hier Applikationen möglichst schnell erkannt werden, selbst wenn das zu Lasten der Genauigkeit geht.

Im Bereich der Netzwerksicherheit hingegen wird die Applikationserkennung zum Monitoring und zur Durchsetzung von Policies benutzt. Auch wenn die Geschwindigkeit weiterhin wichtig ist, so ist die Präzision kritisch, da Fehlklassifikationen sicherheitsrelevant sein können. Aufbauend auf die Applikationserkennung findet zusätzlich oft eine Malwareerkennung oder *Data Leakage Prevention (DLP)*, d.h. Schutz gegen unerwünschten Abfluß von Informationen, statt, ebenfalls unter Nutzung von DPI.

2.2 Möglichkeiten und Grenzen von DPI

Um bessere Durchsatzzahlen präsentieren zu können, werden in der Praxis öfter Optimierungen eingesetzt, die zu Lasten der Sicherheit gehen.

Ein Beispiel ist der standardmäßig aktive App-Cache bei Palo Alto Networks. Wenn zwischen zwei Endpunkten stets die gleiche Applikation (z.B. SIP oder Google) genutzt wird, wird nach einiger Zeit davon ausgegangen, dass dieses auch in Zukunft der Fall sein wird. Die erkannte Applikation wird dann in den App-Cache eingeführt um so zukünftige Analysen zu ersparen. Zusammen mit der schwachen initialen Applikationserkennung kann man dadurch applikationsspezifische Policies umgehen.

Ähnlich problematisch ist die standardmäßige Begrenzung der analysierten Datenmenge bei Fortinet. Ein Angreifer kann mit einem sehr großen HTTP-Response-Header dieses Limit überschreiten und eine im HTTP-Body befindliche Malware am IPS vorbeischmuggeln.

Auch wenn man diese Probleme auf Kosten der Performance lösen könnte, so bleibt, dass bei DPI die Daten nur inspiziert, aber nicht verändert werden. Daten mit mehreren Interpretationsmöglichkeiten (z.B. unterschiedliche Content-length bei HTTP), Stückelung (z.B. Range-Header bei HTTP), Einsatz von neueren Kompressionsalgorithmen (sdch) oder Transportprotokollen (SPDY) erlauben einen Bypass des IPS, wenn dieses die Inhalte nicht oder anders als das Zielsystem interpretiert, oder im Gegensatz zum Zielsystem keine vollständige Sicht auf die Daten hat.

Wenn man die Daten hingegen modifizieren kann, so ermöglicht das neben der Normalisierung ambivalenter Inhalte und Durchsetzung gewünschter Protokolle oder Protokollteile auch weitere sicherheitsrelevante Anpassungen, wie z.B. Entfernen von Cookies bei Cross-Site HTTP-Requests als Schutz gegen CSRF oder Einfügen einer Content-Security-Policy in HTTP-Response-Header, um XSS zu erschweren.

3 Deeper Data Inspection and Modification

Im Forschungsprojekt Padiofire beschäftigen wir uns damit, wie mit Hilfe von Perimeterfirewalls eine sichere Nutzung des inherent unsicheren Web ermöglicht werden kann. Reines DPI ist auf Grund der beschriebenen Limitierungen nicht in der Lage, aktuelle Attacken wie z.B. *Cross-Site-Scripting (XSS)*, *Cross-Site-request-Forgery (CSRF)* oder Malvertising, effektiv zu verhindern. Daher werden Lösungen gebraucht, die sowohl tiefer und zuverlässiger analysieren, wie auch in der Lage sind, Daten zu verändern.

Um effizient eine Vielzahl von Ideen für tiefere Analysen evaluieren zu können und diese einfach in verschiedenen Analysesystemen nutzbar zu machen, haben wir eine Schnittstelle zur Trennung von Datenextraktion und Analyse entwickelt, die sowohl Inspektion wie auch Modifikation der Daten ermöglicht.

3.1 Inspection and Modification Protocol - IMP

Während bei Protokollen wie ICAP die kompletten Daten erst gesammelt und dann im Gesamten verarbeitet werden, analysiert IMP die Daten inkrementell und gibt die Ergebnisse so früh wie möglich zurück. Dieses Vorgehen ermöglicht es auch, gezielt Daten vorab von der Analyse auszuschließen. Das ist z.B. interessant, wenn man nur bestimmte Antworten bei HTTP analysieren will. Da über eine TCP-Verbindung mehrere HTTP-Requests erfolgen können, kann man einfach die uninteressanten Daten überspringen, und damit die Performance des Systems deutlich erhöhen.

Die Schnittstelle ist bereits in der Firewall *genugate* der Firma genua enthalten und wird dort zur Analyse von (auch mit SSL verschlüsselten) TCP-Verbindungen genutzt. Es existiert eine freie Implementation in Perl, welche neben der Schnittstelle auch bereits diverse Analysen und Analysesysteme beinhaltet.

3.2 Resultate

Unter Nutzung der IMP Schnittstelle wurden verschiedene Ideen zur Verbesserung der Sicherheit im Web als Proof Of Concept implementiert. So analysiert eine Komponente den HTTP-Verkehr und erstellt automatisch site-spezifische Profile, welche dann über eine in den Response-Header injizierte Content-Security-Policy von modernen Webbrowsern durchgesetzt werden. Eine weitere Analysekomponente entfernt Autorisierungsinformationen aus Cross-Site-Requests, um so CSRF zu unterbinden. Auch wird über IMP die im Forschungsprojekt Padiofire entwickelte Bibliothek libpadiofire angebunden, welche mit Hilfe von Website-spezifischen Profilen versucht abnormales Verhalten (z.B. XSS) zu erkennen und zu unterbinden. Weitere Ideen, wie die Nutzung von Google Safebrowsing und Anzeigenblockern gegen Malware und Malvertising, liessen sich ebenfalls einfach umsetzen.

Wir implementieren IMP auch in weitere Analysesysteme. Für das *genugate* sind u.a. Analysen von HTTP und von SSH-Forwardings geplant. Weitere Forschungsprojekte beschäftigen mit der Anbindung an den OpenBSD *relayd* Proxy und mit dem Einsatz in *Software Defined Networks (SDN)* innerhalb eines *OpenFlow*-Controllers.