Website-Fingerprinting mit dem multinomialen Naïve-Bayes-Klassifizierer

Dominik Herrmann
Lehrstuhl Management der Informationssicherheit
Universität Regensburg, Deutschland
dh@exomail.to

Zusammenfassung

In diesem Arbeitspapier wird ein verbessertes Verfahren zur Identifizierung von Webseiten anhand des charakteristischen Datenverkehrs, der bei ihrem Abruf entsteht, vorgestellt und mit Testdaten evaluiert. Es basiert auf dem multinomialen Naïve-Bayes-Klassifizierer, der auf die normalisierte Häufigkeitsverteilung der IP-Paketgrößen angewendet wird. Das Verfahren ist bereits bei einer einzigen Trainingsinstanz mit einer Erkennungsrate von 89 % genauer als bislang vorgestellte Methoden. Darüber hinaus werden eine Reihe von Forschungsfragen formuliert, die zur Evaluierung der Praktikabilität von Website-Fingerprinting zu untersuchen sind.

1 Einleitung

Datenschutzfreundliche Übertragungsverfahren (z. B. Protokolle zur verschlüsselten Kommunikation in drahtlosen Netzen, VPNs sowie Anonymisierungssysteme wie JonDonym[1] und Tor[2] sollen die Inhalte der übermittelten Nachrichten sowie u. U. die Identitäten von Sender und/oder Empfänger vor Außenstehenden verbergen.

Beim Abruf einer Webseite über solche Systeme ist dieser Schutz jedoch möglicherweise schwächer als angenommen. Die zur Übermittlung der einzelnen HTTP-Anfragen und -Antworten ausgetauschten IP-Pakete ergeben ein charakteristisches Profil, das auch durch den Einsatz von Verschlüsselung nicht eliminiert wird. Anhand von einzelnen Netzwerk-*traces*, die zu *Fingerabdrücken* kombiniert werden, lässt sich dann die Identität (URL) einer Webseite ermitteln.

Dieses Arbeitspapier hat zwei Ziele: Zunächst soll ein verbessertes Verfahren zur Erstellung von Website-Fingerabdrücken vorgestellt werden, das die Häufigkeitsverteilung der beim Abruf einer Website beobachteten IP-Paketgrößen mit einem multinomialen Naïve-Bayes-Klassifizierer

[1] `http://www.jondonym.de/`; vormals AN.ON bzw. JAP
[2] `http://tor.eff.org/`

analysiert. Da die Genauigkeit der Klassifizierung von Webseiten unter Idealbedingungen inzwischen sehr hoch ist, ist zukünftig neben der Untersuchung von Gegenmaßnahmen vor allem von Interesse, inwiefern sich Website-Fingerprinting *in der Praxis* durchführen lässt. Hierzu werden im zweiten Teil Forschungsfragen formuliert, deren Untersuchung zu einer besseren Einschätzung des Gefahrenpotentials, das von Website-Fingerprinting-Angriffen ausgeht, führen soll.

Abschnitt 2 gibt einen Überblick über verwandte Arbeiten. Abschnitt 3 präsentiert das unterstellte Angreifermodell, während Abschnitt 4 auf den Versuchsaufbau eingeht, der zur Erstellung von Website-Fingerabdrücken verwendet wurde. In Abschnitt 5 werden das verbesserte Verfahren zum Vergleich von Fingerabdrücken erläutert sowie erste Ergebnisse präsentiert. Die offenen Forschungsfragen werden in Abschnitt 6 beschrieben.

2 Verwandte Arbeiten

Bissias et al. [BLJL05] verwenden den Korrelationskoeffizienten, um Webseiten anhand ihres charakteristischen Datenverkehrs zu identifizieren. Die Autoren betrachten dabei die auftretenden IP-Paketgrößen sowie die zeitlichen Abstände zwischen den Paketen *(packet inter-arrival time)*, wobei die Reihenfolge der Pakete berücksichtigt wird. Die Genauigkeit des Verfahrens wird durch den Abruf von 100 populären Seiten über einen OpenSSH-Tunnel getestet. Der dabei entstehende Datenverkehr wird mit *tcpdump* aufgezeichnet. Zur Erzeugung der Fingerabdrücke kombinieren die Autoren die Merkmale, die sie aus den *tcpdump-traces* extrahiert haben. Bei Verwendung von 24 *traces*, die innerhalb eines Tages aufgenommen wurden, werden nach einer Stunde nur 23 % der Seiten richtig identifiziert. Immerhin befinden sich etwa 60 % der Seiten jeweils unter den zehn ähnlichsten Profilen.

Liberatore et al. [LL06] stellen ein verbessertes Verfahren vor, das sie ebenfalls mit einem OpenSSH-Tunnel evaluieren. Zur Erstellung der Fingerabdrücke verwenden sie ausschließlich die beobachteten IP-Paketgrößen während der Übertragung einer Webseite. Die Fingerabdrücke werden mit dem *Jaccard-Koeffizienten*, einer Ähnlichkeitsmetrik für Mengen, die die Häufigkeiten vernachlässigt, sowie einem *Naïve-Bayes-Klassifizierer* miteinander verglichen. Die Genauigkeit der beiden Verfahren ist vergleichsweise hoch: Von 1000 zu identifizierenden Seiten werden bei Verwendung von Fingerabdrücken, die lediglich aus einem einzigen *trace* bestehen, mit dem Jaccard-Koeffizienten nach 24 Stunden noch 60 % der Seiten korrekt erkannt. Der Naïve-Bayes-Klassifizierer erzielt im direkten Vergleich lediglich eine Genauigkeit von 40 %. Erst bei Fingerabdrücken, die aus acht *traces* bestehen, erreicht der Naïve-Bayes-Klassifizierer eine zufrieden stellende Performance (ca. 75 % der Seiten werden korrekt erkannt). Beide Verfahren tolerieren die typische Änderung von Webseiten im Zeitverlauf. Selbst vier Wochen nach der Aufnahme der Fingerabdrücke sinken die Erkennungsraten nur um etwa 10 %.

Darüber hinaus zeigen die Autoren, dass die Effektivität beider Verfahren durch den Einsatz von Padding erheblich reduziert werden kann: Werden etwa alle IP-Pakete auf die MTU (1500 Byte) aufgefüllt, fallen die Erkennungsraten auf weniger als 10 %. Der Naïve-Bayes-Klassifizierer schneidet zwar erheblich besser ab als der Jaccard-Koeffizient, die niedrigen Erkennungsraten machen den Angriff jedoch unpraktikabel. Die Kosten des Paddings sind allerdings hoch: Das übertragene Datenvolumen nimmt dabei um mehr als 140 % zu.

3 Angreifermodell und Ziele des Angreifers

Für die nachfolgenden Betrachtungen wird von einem passiven lokalen Angreifer ausgegangen, der Zugriff auf das Netzwerk seines Opfers hat. Das Opfer verwendet zum Surfen ein datenschutzfreundliches Übertragungsverfahren (z. B. einen OpenSSH-Tunnel, ein VPN, Tor oder JonDonym). Der Angreifer will ermitteln, welche Webseiten das Opfer abgerufen hat bzw. ob eine ganz bestimmte Webseite abgerufen wurde. Es wird weiterhin unterstellt, dass die Pakete nicht entschlüsselt werden können. Der Angreifer ist lediglich in der Lage, den verschlüsselten Datenverkehr (gegebenenfalls auch über einen längeren Zeitraum) mitzulesen und auszuwerten.

Das Angreifermodell vieler datenschutzfreundlicher Techniken lässt einen solchen *lokalen Angreifer* durchaus zu. Nur ein stärkerer (verteilter) Angreifer, der z. B. den Datenverkehr vor und hinter einem Anonymisierer korreliert, kann bei diesen Systemen die Sender- bzw. Empfängeridentitäten ermitteln und verknüpfen. Durch Website-Fingerprinting kann diese Fähigkeit auch ein schwächerer (lokaler) Angreifer erlangen.

Je nach Zielsetzung werden unterschiedliche Anforderungen an ein Website-Fingerprinting-Verfahren gestellt. Zum einen kann ein Angreifer auf die Gewohnheiten und Interessen eines Benutzers schließen, obwohl dieser datenschutzfreundliche Techniken verwendet. Für eine solche Totalüberwachung muss der Angreifer Fingerabdrücke für eine möglichst große Anzahl von Webseiten aufzeichnen, die dann im abgehörten Datenverkehr des Opfers zu suchen sind. In Summe sind möglichst viele Webseiten zu identifizieren. Im Rahmen der Strafverfolgung kann jedoch auch eine andere Fragestellung auftreten: Es ist zu ermitteln, ob ein bestimmter Benutzer eine ganz bestimmte (möglicherweise inkriminierende) Webseite abgerufen hat. Im Vergleich zur Totalüberwachung ist die Anzahl der vorzuhaltenden Fingerabdrücke gering – diese wenigen Seiten sollen dann jedoch möglichst zuverlässig identifiziert werden.

4 Versuchsaufbau

Zur Analyse von Website-Fingerabdrücken wird folgender Versuchsaufbau verwendet: Auf einem Linux-Rechner wird mit Hilfe eines Skripts eine Instanz von Firefox automatisiert, so dass sie nacheinander eine Reihe von Webseiten abruft. Wie bei bisherigen Untersuchungen ist zur Absicherung der Kommunikation im Browser ein OpenSSH-SOCKS-Proxy eingetragen.

Die Konfiguration des Browsers folgt den Beschreibungen in [BLJL05] und [LL06] (u. a. deaktiviertes Caching, keine automatischen Updates), wobei zusätzlich alle aktive Inhalte (Java, JavaScript, Flash, usw.) deaktiviert wurden. Die daraus resultierende Konfiguration ist mit der des JonDoFox-Browsers[3], der für datenschutzfreundliches Surfen optimiert wurde, vergleichbar.

Bei jedem Abruf werden mit *tcpdump* die Header der übertragenen IP-Pakete protokolliert, um deren Paketgrößen zu ermitteln. Die Multimenge der auftretenden Paketgrößen wird im folgenden als *trace* bezeichnet. Abbildung 1 zeigt das Paketgrößen-Histogramm, das aus einem *trace* von `www.google.com` erstellt wurde.

[3] `https://www.jondos.de/en/jondofox`

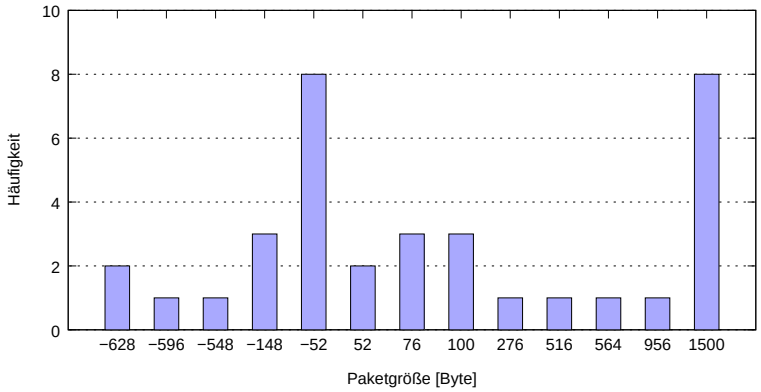

Abbildung 1: Paketgrößen-Histogramm für den Abruf von `www.google.com` (Pakete in Senderichtung – vom Client zum Server – sind durch negative Pakegrößen gekennzeichnet.)

Zur Analyse der Genauigkeit des Klassifizierungsverfahrens wurden 775 URLs verwendet, die sich unter den populärsten Seiten befinden, die im Zeitraum von 12 Monaten über den vom Autor betriebenen Internet-Filter FilterSurf[4] abgerufen wurden. Die URLs wurden manuell ausgewählt, um eine hohe Datenqualität sicherzustellen. Zur Analyse des Klassifizierungsverfahrens wurden die Webseiten im Zeitraum vom 09.01.2008 bis 19.01.2008 ohne Unterbrechung nacheinander heruntergeladen, wobei jede Webseite etwa zehnmal pro Tag abgerufen wurde.

5 Klassifizierung von *traces* mit Text-Mining-Techniken

Die Identifizierung von Webseiten anhand ihrer Fingerabdrücke erfolgt mit Hilfe von Weka[5], einer Data-Mining-Software der University of Waikato. Zur Auswertung der Genauigkeit werden die beim Abruf erstellten *tcpdump-traces* in *Trainingsinstanzen*, mit denen der Klassifizierungsalgorithmus den Fingerabdruck einer Seite lernt, und *Testinstanzen*, deren Identität der Klassifizierer ermitteln soll, aufgeteilt. Die im Folgenden vorgestellten Ergebnisse wurden jeweils mit 10 Testinstanzen ermittelt. Für jeden Versuch wurden aus der Grundgesamtheit 25 Stichproben gezogen und der Mittelwert der Ergebnisse gebildet.

Während in [LL06] der *NaïveBayes*-Klassifizierer von Weka (mit *Kernel-Density-Estimation*) verwendet wird, setzt das in diesem Arbeitspapier vorgestellte Verfahren den *Naïve-Bayes-Multinomial*-Klassifizierer (vgl. [MRS07]) in Verbindung mit dem *StringToWordVector*-Filter von Weka ein – eine Kombination, die klassischerweise im Text-Mining bei der Klassifizierung von Text-Dokumenten verwendet wird. Ein *trace* wird dabei als String repräsentiert, der aus den aufgetretenen Paketgrößen (durch Leerzeichen getrennt) besteht (z. B. „-628 956 -52 1500 1500 -52 -52 1500 . . . “). Der StringToWordVector-Filter ermittelt aus einem solchen Dokument die Termhäufigkeiten, also die Auftretenshäufigkeiten der einzelnen Paketgrößen. Für jedes Dokument (also für jeden *trace*) ergibt sich dann ein Häufigkeitsvektor, dessen Elemente den jeweiligen Termhäufigkeiten (oder 0, falls der Term nicht vorkommt) entsprechen.

[4] `http://www.filtersurf.de/`

[5] `http://www.cs.waikato.ac.nz/ml/weka/`

Der multinomiale Naïve-Bayes-Klassifizierer schätzt die Wahrscheinlichkeit, dass ein Dokument *(trace)* d, zu einer Klasse *(Webseite)* c gehört, nach folgender Formel:

$$\hat{P}(c|d) = \frac{\hat{P}(c)\hat{P}(d|c)}{\hat{P}(d)} \quad \propto \quad C_{\text{multi}} \cdot \prod_{t \in V} \left(\frac{f_{t,c}}{\sum_{t' \in V} f_{t',c}} \right)^{f_{t,d}} \tag{1}$$

Zur Klassifizierung eines Dokuments werden für alle Klassen $c \in C$ die Wahrscheinlichkeiten $\hat{P}(c|d)$ geschätzt. Das Dokument wird dann der Klasse mit der größten Wahrscheinlichkeit zugeordnet. Bei Bedarf lässt sich auch die Wahrscheinlichkeit dieser Zuordnung bestimmen.

Zur Klassifizierung ist die exakte Wahrscheinlichkeit nicht von Interesse. Daher lässt sich der mittlere Term in Formel (1) wie dort abgebildet vereinfachen. Sind alle Klassen (Webseiten) in der Grundgesamtheit gleichverteilt, kann die (dann einheitliche) Auftretenswahrscheinlichkeit der Klassen $\hat{P}(c)$ vernachlässigt werden. Die Auftretenswahrscheinlichkeit des Dokuments $\hat{P}(d)$ ist zur Ermittlung der wahrscheinlichsten Klasse ebenfalls bedeutungslos (da konstant) und muss nicht berücksichtigt werden. Der Term auf der rechten Seite der Gleichung ist dann immer noch proportional zur tatsächlichen Wahrscheinlichkeit; die Rangfolge der Wahrscheinlichkeiten $\hat{P}(c|d)$ bleibt dadurch erhalten.

In Formel (1) ist V das Vokabular aller vorkommenden Terme, $f_{t',c}$ die Auftretenshäufigkeit von Term t' in allen Dokumenten, die zur Klasse c gehören und $f_{t,d}$ die Auftretenshäufigkeit von Term t im Dokument d. Ein Dokument wird dabei als „bag of words“ aufgefasst, aus der die einzelnen Terme gezogen werden. Der zugehörige Multinomialkoeffizient $C_{\text{multi}} = \frac{L_d!}{f_{t_1,d}! \cdots f_{t_n,d}!}$ ist für ein gegebenes Dokument d mit Länge L_d eine Konstante – er muss zur Ermittlung der wahrscheinlichsten Klasse gar nicht berechnet werden.

Dem „bag of words“-Modell liegen zwei naive Annahmen zugrunde, die bei Textdokumenten üblicherweise verletzt sind: (1) Die Reihenfolge der Terme (bzw. Paketgrößen) spielt keine Rolle und (2) das Vorkommen der einzelnen Terme ist voneinander unabhängig. Es ist davon auszugehen, dass diese Annahmen auch bei *tcpdump-traces* verletzt werden – der multinomiale Naïve-Bayes-Klassifizierer erzielt jedoch auch unter solchen Umständen in der Regel gute Erkennungsraten.

Die Interpretation eines Fingerabdrucks als Text-Dokument ermöglicht die Verwendung von einschlägigen Optimierungsmöglichkeiten aus dem Text-Mining. Durch geeignete Transformation der Häufigkeitsvektoren $\mathbf{f}$ lassen sich die Erkennungsraten erheblich verbessern. Abbildung 2 zeigt die Klassifizierungsergebnisse für verschiedene Transformationen mit und ohne Normalisierung für den Fall, dass lediglich eine einzige Trainingsinstanz verwendet wird und zwischen Training und Test mindestens 6 Tage liegen.

Im Versuch zeigte sich, dass sich durch Verwendung der TF-Transformation $f_i^* = \log(1 + f_i)$ [MRS07] und die Normalisierung der Häufigkeitsvektoren auf die durchschnittliche euklidische Länge $f_i^{\text{norm}} = \frac{f_i^*}{\left\| (f_1^*, \ldots, f_n^*)^T \right\|}$ [MRS07] die besten Ergebnisse erzielen lasen. Die IDF-Transformation, die beim Text-Mining denjenigen Termen ein höheres Gewicht zuordnet, die in einem Dokument besonders häufig vorkommen, in den anderen Dokumenten hingegen sehr selten sind, hat sich hingegen als kontraproduktiv erwiesen.

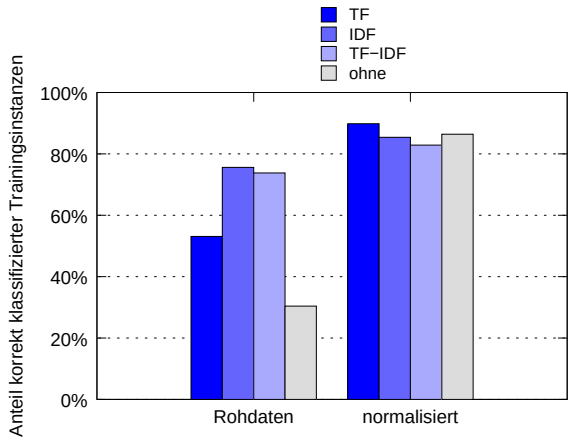

Abbildung 2: Einfluss verschiedener Transformationen auf die Genauigkeit der Klassifizierung bei 6 Tagen Zeitdifferenz zwischen Training und Test (bei einer einzigen Trainingsinstanz).

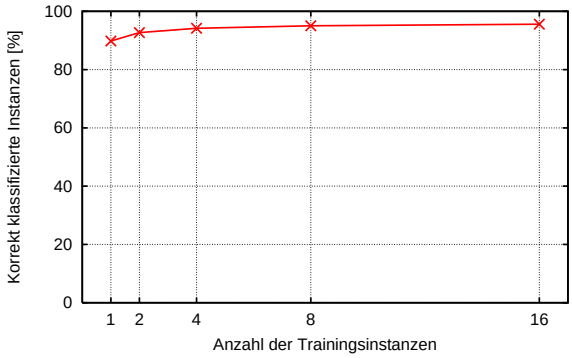

Abbildung 3: Einfluss der Anzahl der Trainingsinstanzen auf die Genauigkeit des Klassifizierers

Der multinomiale Naïve-Bayes-Klassifizierer erreicht bei einer Trainingsinstanz im besten Fall eine Erkennungsrate von 89,89 %. Erhöht man die Anzahl der Trainingsinstanzen, nehmen die Erkennungsraten weiter zu. Abbildung 3 zeigt die Ergebnisse für verschiedene Varianten dieses Experiments. Bei vier Trainingsinstanzen werden bereits 94,18 % der Testinstanzen korrekt identifiziert; bei mehr als vier Trainingsinstanzen sind die Zuwächse hingegen sehr gering.

Der multinomiale Naïve-Bayes-Klassifizierer übertrifft damit die Genauigkeit der bisher vorgestellten Verfahren. Zum Vergleich: in [LL06] wurden bei einer Grundgesamtheit von 1000 Seiten nach einer Woche nur ca. 70 % der Seiten korrekt identifiziert. Die Aussagekraft eines solchen Vergleichs wird durch die unterschiedlichen Webseiten zwar leicht eingeschränkt, die Unterschiede sind jedoch angesichts der vergleichbaren Untersuchungsbedingungen nicht zu vernachlässigen.

Da sich das gezeigte Verfahren genauso wie seine Vorgänger auf die charakteristische Häufigkeitsverteilung der IP-Paketgrößen stützt, ist davon auszugehen, dass die Erkennungsleistung beim Einsatz von Padding deutlich sinkt. Eine erste Implementierung wurde unter dem Namen *Traffic Flow Confidentiality* für IPsec gerade erst von Kiraly et al. [KTB+07] vorgestellt.

6 Weiterer Untersuchungsbedarf

Im Folgenden werden verschiedene Forschungsfragen formuliert, deren Untersuchung einen Beitrag zur Evaluation von Website-Fingerprinting in der Praxis liefern könnte.

Skalierbarkeit Website-Fingerprinting kann zum Erstellen von Benutzerprofilen verwendet werden, wenn Fingerabdrücke für eine große Anzahl von Webseiten erstellt werden. Es ist zu klären, inwiefern das vorgestellte Klassifizierungsverfahren im Hinblick auf die Anzahl der Instanzen skaliert.

Einsatzmöglichkeiten Neben der Erstellung von Benutzerprofilen sind weitere Einsatzmöglichkeiten für Website-Fingerprinting denkbar. Zur strukturierten und zielgerichteten Analyse ist es erforderlich, potentielle Anwendungen zu kennen und explizit zu beschreiben.

Vergleich verschiedener datenschutzfreundlicher Techniken Die meisten Analysen widmen sich SSH-Tunneln, die praktisch kein Padding implementieren. Ein Vergleich mit anderen datenschutzfreundlichen Übertragungstechniken (z. B. SSL- und IPsec-VPNs) steht noch aus. Unter Umständen bieten die heute bereits verfügbaren Anonymisierungssysteme bereits genügend Schutz gegen Website-Fingerprinting.

Untersuchung effizienter Gegenmaßnahmen Bislang konzentriert sich die Entwicklung von Gegenmaßnahmen auf verschiedene Padding-Schemata. Wirkungsvolles Padding erhöht jedoch das übertragene Datenvolumen erheblich. Effizientere Gegenmaßnahmen (z. B. ein Burst-Proxy, der selbständig die in HTML-Seiten eingebetteten Objekte herunterlädt und in einem zusammenhängenden Datenstrom zum Client sendet) wurden zwar vorgeschlagen, jedoch noch nicht implementiert und auf ihre Wirksamkeit hin untersucht.

Gezielte Erleichterung von Website-Fingerprinting Es ist zu untersuchen, inwiefern der Betreiber einer Webseite bzw. der ISP deren Identifizierung mutwillig erleichtern kann. Solchermaßen modifizierter Traffic könnte mit Hilfe von Website-Fingerprinting auf dem Weg durch das Netzwerk verfolgt werden, um einem Nutzer den Besuch der manipulierten Webseite nachzuweisen. Darüber hinaus ist zu klären, ob es wirksame Gegenmaßnahmen zur Unterbindung dieses aktiven Angriffs gibt.

Überbrückung von Anonymisierungssystemen Möglicherweise lassen sich Anonymisierer wie Tor und JonDonym, die den Datenverkehr über mehrere Stationen weiterleiten, durch Website-Fingerprinting vor der ersten und nach der letzten Station überbrücken.

Erkennung von Website-Abrufen in getunneltem Traffic In den bisherigen Veröffentlichungen wird unterstellt, dass Beginn und Ende eines Seitenabrufs im verschlüsselten Datenverkehr wegen der Denkpausen des Benutzers leicht zu ermitteln sind. Aktuelle Studien [CCW+07, KAA06] deuten jedoch darauf hin, dass diese Annahme unzutreffend ist. Es ist demnach völlig ungewiss, ob Website-Fingerprinting in der Praxis (etwa wenn der Tunnel parallel auch von anderen Diensten genutzt wird) überhaupt durchführbar ist.

Robustheit Unterschiedliche Browser, Plugins (z. B. Ad-Blocker) und Internetverbindungen beeinflussen Art und Größe der übermittelten Pakete. Es wurde noch nicht untersucht, wie robust Website-Fingerabdrücke gegen solche äußeren Einflüsse sind.

Website-Fingerprinting beim Einsatz von Caching In bisherigen Studien war der Cache im Browser stets deaktiviert, um sicherzustellen, dass bei jedem Abruf einer Webseite alle eingebetteten Elemente übertragen werden. Es ist zu erwarten, dass die Erkennungsraten durch Caching erheblich sinken. Eine Analyse der Effektivität von Website-Fingerprinting beim Einsatz von Caching erlaubt Rückschlüsse auf die Einsetzbarkeit in der Praxis.

Bedeutung der False-Positive-Rate Bislang lag der Fokus bei der Analyse von Website-Fingerprinting auf Basis von IP-Paketgrößen auf den *True Positives* (Anzahl der korrekt identifizierten Webseiten). In [SSW+02] wird jedoch auf die hohe Relevanz der Minimierung der *False Positives* (fälschlich identifizierte Webseiten) hingewiesen. Eine Analyse des Klassifizierungsverhaltens für Webseiten, die nicht antrainiert wurden, steht noch aus.

Literatur

[BLJL05] Bissias, George, Marc Liberatore, David Jensen, and Brian Neil Levine: *Privacy Vulnerabilities in Encrypted HTTP Streams.* In *Proceedings of the 5th Privacy Enhancing Technologies Workshop (PET 2005)*, pages 1–11, May 2005. http://prisms.cs.umass.edu/brian/pubs/bissias.liberatore.pet.2005.pdf.

[CCW+07] Coull, S.E., M.P. Collins, C.V. Wright, F. Monrose, and M.K. Reiter: *On Web Browsing Privacy in Anonymized NetFlows.* In *Proceedings of the 16th USENIX Security Symposium*, Boston, MA, August 2007.

[KAA06] Koukis, D., Spyros Antonatos, and Kostas G. Anagnostakis: *On the Privacy Risks of Publishing Anonymized IP Network Traces.* In Leitold, Herbert and Evangelos P. Markatos (editors): *Communications and Multimedia Security*, volume 4237 of *Lecture Notes in Computer Science*, pages 22–32. Springer, 2006, ISBN 3-540-47820-5.

[KTB+07] Kiraly, Csaba, Simone Teofili, Giuseppe Bianchi, Renate Lo Cigno, Matteo Nardelli, and Emanuele Delzeri: *Traffic Flow Confidentiality in IPsec: Protocol and Implementation.* In *Preproceedings Third IFIP/FIDIS Summer School "The Future of Identity in the Information Society"*, August 2007.

[LL06] Liberatore, Marc and Brian Neil Levine: *Inferring the source of encrypted HTTP connections.* In *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*, pages 255–263, New York, NY, USA, 2006. ACM Press, ISBN 1-59593-518-5.

[MRS07] Manning, C. D., P. Raghavan, and H. Schütze: *Introduction to Information Retrieval (preliminary draft printed on November 17, 2007).* Cambridge University Press, 2007. http://nlp.stanford.edu/IR-book/pdf/irbookprint.pdf.

[SSW+02] Sun, Qixiang, Daniel R. Simon, Yi Min Wang, Wilf Russell, Venkata N. Padmanabhan, and Lili Qiu: *Statistical Identification of Encrypted Web Browsing Traffic.* In *SP '02: Proceedings of the 2002 IEEE Symposium on Security and Privacy*, page 19, Washington, DC, USA, 2002. IEEE Computer Society, ISBN 0-7695-1543-6.