

Vergleich von datenschutzfreundlichen Übertragungstechniken hinsichtlich ihres Schutzes vor Datenverkehrsanalysen im Internet

oder:

Wie schützt man sich am besten gegen Traffic-Analyse-Angriffe?

Dominik Herrmann
16.08.2007

1st Convention on Privacy Enhancing Technologies, Frankfurt am Main

This talk is something like the kick-off presentation for my diploma thesis, so please do not expect lots of insightful content or results on the next slides. Ask me for that in 6 months!

Traffic Analyse? Wovon?

- Verschlüsselte Übertragung von Inhalten
- Was kann man dann noch beobachten?
 - Paketgröße
 - Inter-Arrival-Time
 - „Durchsatz“
 - Senderichtung

Das soll funktionieren?

Ja.

- Bereits erfolgreich durchgeführte Angriffe
 - Erkennung der Anwesenheit von getunneltem Traffic
 - Tracken von anonymisierten VoIP-Verbindungen
 - Erkennung des getunnelten Protokolls in VPN-Tunneln
 - Bestimmung des Hosts in SSH-Tunnel anhand Frontpage
 - Bestimmung der abgerufenen Seite in SSL-Traffic

Und wie?

- Machine Learning, Pattern Recognition:
(Naive Bayes, Hidden Markov Chains, ...)
- Antrainieren eines Modells
- Versuche in unbekanntem Traffic einen
Treffer zu finden

Einschränkung bisheriger Ansätze

- Verschlüsselter Traffic wird „simuliert“
- Protokoll-Spezifika werden vernachlässigt
- Wie gut funktionieren existierende Angriffe bei unterschiedlichen verschlüsselnden Übertragungsmethoden?
- Oder: Welche verschlüsselte Übertragungsmethode schützt am besten?

Methoden wirken in verschiedenen Layern

- XML Encryption
- HTTPS
- SSH-SOCKS-Tunnel
- Tor, AN.ON/Jondonym
- VPN Tunnel, VPN Bridge
- WEP, WPA

Forschungsfragen

- Bieten Methoden, die auf niedrigeren Layern wirken, mehr Schutz?
- Schutz durch HTTP-Proxy?
- Schutz durch Jitter eines Anon-Dienstes?
- Schutz durch Burst-Proxy?
- (Schutz durch Dummy Traffic?)

Fragen zur Methodik

- Welches Traffic-Analyse-Verfahren geeignet?
(Welche Merkmale wie auswerten?)
- Welche Übertragungsmethoden zu testen?
- Verbindungsbeginn-Erkennung in Tunneln?

Was ist zu tun?

- Traffic-Analyse Messung bei unverschlüsseltem Traffic
- Vergleich mit OpenSSH-Tunnel, OpenVPN, Proxy-Traffic, SSL, AN.ON
- Burst-Proxy implementieren und Erkennungsrate vergleichen