Seminarvortrag: „Angriffe auf Tor“

Seminar: „Electronic Identity“
Seminarleiter: Dr. Wolf Müller

Vortragende: Dominique Hüneburg

Angriffe auf TOR

Gliederung

1) Einleitende Bemerkungen

2) Passive Attacken
   2.1) Browser Fingerprinting

3) Aktive Attacken
   → Einschub NSA

4) Directory-Attacken

5) Rendezvous-Point-Attacken

6) Zusammenfassung

7) Quellen

Einleitende Bemerkungen

- Identifizierung auch möglich über Browser, persönliche Accounts
- Tor allein verschlüsselt keine Internetkommunikation
- Nachrichtendienste könnten am Netzwerk beteiligt sein (später: NSA)
- Früher: für jede Anwendung spezifischer Proxy zur Anonymisierung notwendig

Passive Attacken

- Traffic Patterns von Nutzern beobachten
  - Beschreibung: Eingehende und ausgehende Verbindungen werden belauscht, für tatsächliches Profil aber weitergehende Verarbeitung notwendig
  - Verteidigung: -

Passive Attacken

- Inhalt der Verbindungen von Nutzern beobachten
  - Beschreibung: Inhalt beim Nutzer zwar verschlüsselt, aber nicht unbedingt beim Empfänger
  - Verteidigung: u. a. Privoxy

Passive Attacken

- Erkennung individueller Einstellungen
  - Beschreibung: Tor bietet unterschiedliche Konfigurationseinstellungen. Selten benutzte fallen auf.
  - Verteidigung: Benutzung geläufiger Einstellungen

Passive Attacken

- Zeitliche Analyse einer Ende-zu-Ende-Verbindung
  - Beschreibung: Wenn Sender und Empfänger belauscht, durch zeitliche Analyse des Datenverkehrs Verbindung nachvollziehbar
  - Verteidigung: Verbindung zwischen Onion Proxy und erstem Tor-Node geheim halten: Proxy operiert auf dem Tor-Node oder hinter Firewall

Passive Attacken

- Analyse der Datenmengen einer Ende-zu-Ende-Verbindung
  - Beschreibung: Wenn Sender und Empfänger belauscht, durch vergleichen der jeweils ein- und ausgehenden Datenmengen Verbindung nachvollziehbar
  - Verteidigung (begrenzt): bei einem circuit können die Anzahlen der ein- und ausgehenden Pakete unterschiedlich sein

Passive Attacken

- Website Fingerprinting
  - Beschreibung: Mit Hilfe von Datenbank mit Dateigrößen und Zugriffsmustern werden Verbindungen zu den betrachteten Websites erkannt. Eingeschränkt durch Granularität der cells
  - Verteidigung: Vergrößerung der cells
  - Weniger effektiv gegen Tor, aber gegen...
  - SafeWeb: Service zur Identifizierung nicht vertrauenswürdiger Webseiten
  - Nicht zu verwechseln mit...

Browser Fingerprinting

- Diplomarbeit von Henning Tillmann
- 23.709 gesammelte Fingerabdrücke, 93% einmalig
- 86,73% eindeutig durch Plugins, unterstütze MIME-Typen und Schriftarten
- Robust bei kleinen Konfigurationsänderungen
- Gegenmaßnahmen: Javascript und Flash abschalten
- Bietet neben Tracking auch Sicherheit: zusätzliches Identifikationsmerkmal bei Online-Anmeldung

Aktive Attacken

- Ausspionieren und Missbrauchen fremder Schlüssel
  - Beschreibung: Durch Kenntnis vom TLS session key alle control cells und verschlüsselten relay cells auf jedem circuit der Verb. sichtbar. Eine Schicht der Verschlüsselung lässt sich auflösen.
  - OR imitierbar bei Kenntnis seines privaten TLS Schlüssels. Zusätzlich Onion Key bekannt: create cells entschlüsselbar
  - Verteidigung: Regelmäßiger Schlüsselaustausch

Aktive Attacken

- Iteratives Kompromittieren von Tor-Nodes/ORs
  - Beschreibung: Wenn ORs z. B. durch rechtlichen Zwang kompromittierbar, dann auch der ganze circuit. Angriff muss vor Ende des Bestehens des circuit abgeschlossen sein
  - Verteidigung: circuits erstellen, die verschiedene Zuständigkeiten durchqueren (→ Ländergrenzen)

NSA

- Allgemein Handlungsspielraum der NSA in Deutschland sehr groß, keine rechtlichen Konsequenzen zu erwarten
- Auch betroffen: Yahoo und Google
- Ob die NSA Tor-Relays betreibt, ist nicht erwiesen
- Bisher nur einzelne Nutzer deanonymisiert
- Durch (inzwischen behobene) Sicherheitslücke in Firefox wurde Schadsoftware auf den Clients platziert

NSA

- Aber: Tor von den USA zu 60% mitfinanziert
- Gezielter Angriff:
  - Verhaftung des Gründers des Providers Freedom Hosting wegen angeblicher Verbreitung von Kinderpornografie im Tor-Netzwerk
  - Freedom Hosting stellt Server für Hidden Services zur Verfügung
  - Nach der Festnahme liefern Websites der Kunden Schadcode aus
  - Server von Freedom Hosting kompromittiert

NSA

- Angstkampagne, um Nutzer von Anonymisierungsdiensten zu verscheuchen?
- Felix von Leitner: „Benutzt mehr Tor. Denn euer Traffic dient anderen als Cover Traffic. Aber denkt nicht, dass ihr deswegen sicher seid. Je mehr Leute Tor benutzen, desto größer ist das Gleichungssystem. Dennoch ist das prinzipiell lösbar.“

Aktive Attacken

- Einen Webserver betreiben
  - Beschreibung: Betreiber des Servers kann zu ihm aufgebaute Verb. zeitl. Analysieren. Nutzer werden z. B. durch Werbung gelockt. Anwendungsprotokolle könnten Infos über Nutzer preisgeben.
  - Verteidigung: Privoxy

Aktive Attacken

- Einen Onion-Proxy betreiben
  - Beschreibung: Alle durch den Proxy laufenden Verb. können beeinträchtigt werden. Private Nutzer haben eigenen lokalen, für Institutionen manchmal externer notwendig.
  - Verteidigung: -

Aktive Attacken

- DoS-Attacken
  - Beschreibung: Überlaufattacken vermindern Zuverlässigkeit von Nodes, legen sie lahm oder stören das Vertrauen in sie. Datenverkehr lässt sich in andere Teile des Tor-Netzes umleiten.
  - Verteidigung: Robustheit, größere Bandbreite

Aktive Attacken

- Einen (bösartigen) OR betreiben
  - Beschreibung: Einzelner Node müsste zu beiden Endpunkten eines circuit direkt benachbart sein, um seine Anonymität zu beeinträchtigen. Mehrere ORs → höhere Wahrscheinlichkeit.
    Nutzer anlocken durch 'lasche' exit policies und Beeinträchtigung anderer Nodes.
  - Verteidigung: -

Aktive Attacken

- Einflussnahme auf Sende- und Empfangszeiten von Paketen
  - Beschreibung: Stärkere Form der zeitl. Analyse
  - Verteidigung: s. o.

Aktive Attacken

- Markieren von Paketen:
  - Beschreibung: Paket durch Veränderung markieren, Ankunftszeit berechnen, Paket wiedererkennen, Verbindung aufgedeckt
  - Verteidigung: Integritätskontrollen von cells

Aktive Attacken

- Inhalte unter nicht authentifizierten Protokollen verändern
  - Beschreibung: Bösartiger Exit-Node kann adressierten Server imitieren, wenn Nutzer nicht authentifiziertes Protokoll verwendet (z. B. HTTP).
  - Verteidigung: Verwendung von Protokollen mit Ende-zu-Ende-Authentifizierung

Aktive Attacken

- Einen Handshake von einer Seite wiederholen
  - Beschreibung: Bei Wiederholung des Handshakes wird neuer session key ausgehandelt.
  - Verteidigung: Tor nicht anfällig dafür, da neuer session key für bisher beobachtete session unbrauchbar

Aktive Attacken

- Verruf-Attacken
  - Beschreibung: Tor für sozial verurteilte Aktivitäten missbrauchen, Netz in Verruf bringen, Abschaltung erwirken
  - Verteidigung: Entsprechende exit policies, tolerante Nutzer

Aktive Attacken

- Falschen Anonymisierungscode in Umlauf bringen
  - Beschreibung: Software im Namen des Tor-Projektes in Umlauf bringen, die Nutzer deanonymisiert
  - Verteidigung: Jede Software von Tor wird mit offiziellem Schlüssel signiert, in Verzeichnis vertrauenswürdiger Software eingetragen und mit einsehbarem Quellcode verbreitet

Directory-Attacken

- Directory Server außer Gefecht setzen
  - Beschreibung: Wenn nicht alle Directory Server betroffen, werden noch einheitliche Verzeichnisse generiert und gehalten. Wenn über die Hälfte betroffen, Verzeichnis nicht mehr automatisch nutzbar, Vertrauensentscheidung per Hand
  - Verteidigung: -

Directory-Attacken

- Einen Directory Server unterwandern/übernehmen
  - Beschreibung: Korrupter Directory Server kann Aufnahme von ORs in das Verzeichnis per Mehrheitsentscheid beeinflussen und zweifelhafte ORs begünstigen
  - Verteidigung: -

Directory-Attacken

- Die Mehrheit von Directory Servern unterwandern/übernehmen
  - Beschreibung: Hält ein Angreifer über die Hälfte der Directory Server, kann er bel. viele kompromittierte ORs in das Verzeichnis aufnehmen.
  - Verteidigung: Sicherstellung der Unabhängigkeit und Angriffsresistenz der Betreiber von Directory Servern

Directory-Attacken

- Uneinigkeit zwischen Directory Servern erzeugen
  - Beschreibung: Das Directory Agreement Protocol fordert Einverständnis aller Directory Server miteinander. Durch säen von Misstrauen lassen sie sich in verfeindete Parteien aufsplitten. Nutzer müssen sich entscheiden.
  - Verteidigung: -

Directory-Attacken

- Einen kompromittierten OR in das Verzeichnis schmuggeln
  - Beschreibung: Durch täuschen der Directory Server erreichbar.
  - Verteidigung: Im Modell wird angenommen, dass Betreiber der Server die meisten zweifelhaften ORs erkennen können.

Directory-Attacken

- Directory Server von der Korrektheit eines fehlerhaften ORs überzeugen
  - Beschreibung: Directory Server testen Funktionalität von ORs durch korrekten Aufbau einer TLS-Verbind. Ergebnis verfälscht, wenn OR TLS-Verbindungen akzeptiert und cells ignoriert.
  - Verteidigung: Directory Server müssten ORs durch Aufbau von circuits und Senden von Daten testen.

Rendezvous-Point-Attacken

- Introduction Points mit Anfragen fluten
  - Beschreibung: Hidden Service blockieren, indem alle seine introduction points geflutet werden
  - Verteidigung: Introduction points können nicht autorisierte Anfragen abweisen; so lässt sich Anzahl der zu empfangenden Requests begrenzen.

Rendezvous-Point-Attacken

- Einen Introduction Point unfähig machen
  - Beschreibung: Hidden Service wird gestört, Angreifer müssten aber alle (potenziellen) introduction points attackieren, denn:
  - Verteidigung: Hidden Service kann mit seinem festen offiziellen Schlüssel neue introduction points festlegen, auch im Geheimen.

Rendezvous-Point-Attacken

- Einen Introduction Point übernehmen
  - Beschreibung: Kompromittierter introduction point bombardiert den Servicebetreiber mit Anfragen und blockiert legitime requests.
  - Verteidigung: Überlauf erkennbar, circuit schließen. Um Blockierung zu erkennen introduction point regelmäßig mit eigenen requests testen.

Rendezvous-Point-Attacken

- Einen Rendezvous-Point kompromittieren
  - Beschreibung: Rendezvous-points sind für die gleichen Attacken anfällig wie alle anderen ORs eines circuit.
  - Verteidigung: s. o.

Zusammenfassung

- Passive vs. Aktive Attacken
- Infiltration theoretisch möglich
- Angriff auf Directory Server könnte theoretisch das TOR-Netzwerk lahmlegen
- Angriffe oft vermeidbar durch entsprechendes Verhalten des Nutzers

Quellen

Tor: The Second-Generation Onion Router

http://www.spiegel.de/netzwelt/gadgets/raspberry-pi-tor-router-onion-pi-anonymisiert-surfen-im-web-a-907567.html

http://www.golem.de/news/browser-fingerprinting-tracking-geht-auch-ohne-cookies-1310-102253.html

http://kubieziel.de/blog/archives/1559-Betreibt-die-NSA-Tor-Relays.html

http://www.computerbase.de/news/2013-10/nsa-scheitert-bisher-grossflaechig-am-tor-netzwerk/

http://www.zdnet.de/88171545/nsa-arbeitet-sich-an-anonymisierungsdienst-tor-ab/

http://www.zeit.de/digital/datenschutz/2013-08/angriff-tor-netzwerk-nsa/komplettansicht

https://netzpolitik.org/2013/muscular-so-verschafft-sich-die-nsa-zugang-zu-yahoo-und-google/

http://de.nachrichten.yahoo.com/hintergrund-grenzen-strafverfolgung-nsa-aff%C3%A4re-135534877.html