Covert Channel Protocol

Ein adaptives Protokoll zur verdeckten Übertragung von Informationen mittels existierender Covert-Channel

---

Florian Preinstorfer

http://nblock.org/about

Security Insights, 18.04.2012

Agenda

1. **Grundlegendes**
2. **Covert Channel Protocol**
   - Idee
   - Evaluierung von Trägerprotokollen
   - Entwicklung des Covert Channel Protocols
   - Proof of Concept
3. **Status & Fazit**

Begriff I

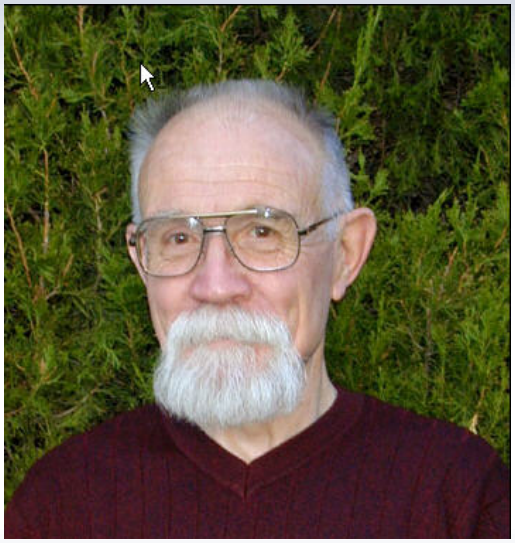
- Butler W. Lampson
- A note on the confinement problem, 1973
- 1. Definition des Begriffs „Covert Channel“:

  „Covert Channels, i.e. those not intended for information transfer at all, such as the service program's effect on the system load.“

Quelle: acm.org

Begriff II

- Gustavus J. Simmons
- The Prisoners' Problem and the Subliminal Channel, 1983
  - Zwei Gefangene in getrennten Zellen
  - Kommunikation nur über Wärter möglich
  - Wärter kann Nachrichten weiterreichen, verändern, unterdrücken, erstellen, ...
  - Ziel: Ausbruch aus dem Gefängnis



Quelle: iacr.org

Begriff III

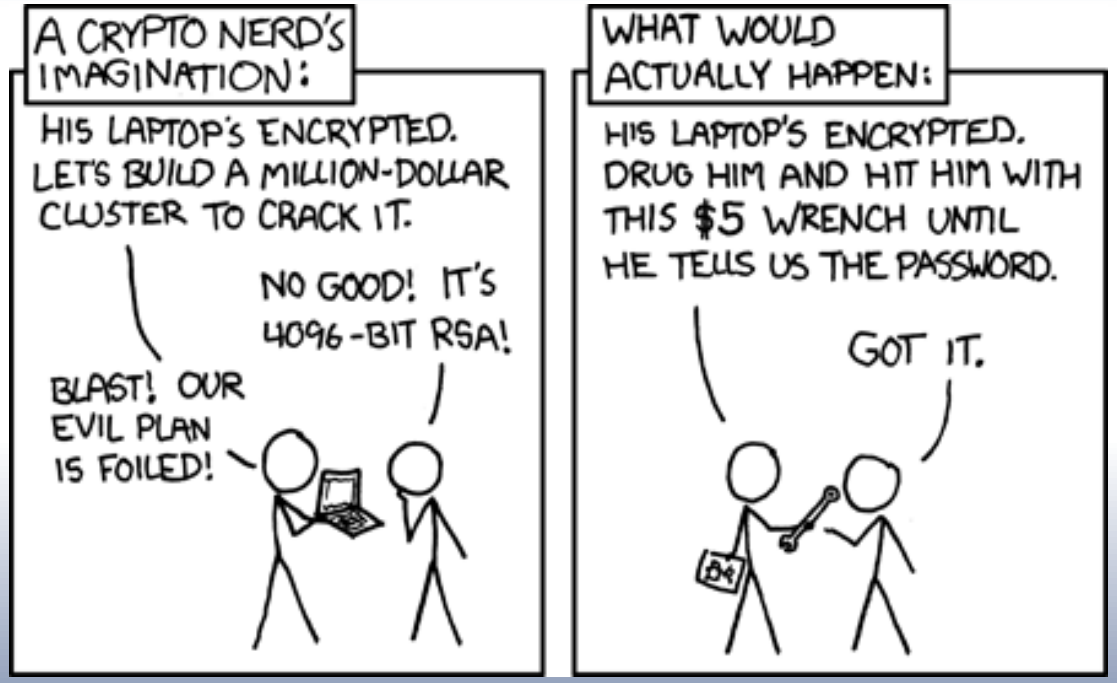
- Matt Bishop
- Computer Security: Art and Science, 2002

„A covert channel is a path of communication that was not designed to be used for communication.“

Quelle: nob.cs.ucdavis.edu/bishop

Motivation I

- Schutz der eigene Freiheit:



Quelle: xkcd.com/538

Motivation II

- Unterwanderung von Zugriffskontrolle und Überwachung
- Anti-Zensur → Tor (obfsproxy) vs. Iran
- Leaking von Dokumenten

Quellen: torproject.org, en.wikipedia.org

Klassifikation I

- Storage vs. Timing Covert Channel
- Active vs. Passive Covert Channel

Klassifikation II

- Storage Covert Channel
  - Anpassung von Paketen zur Informationsverschleierung
  - ID-Felder, Sequenznummern, Cookies, ...
- Timing Covert Channel
  - Anpassung der Reihenfolge oder des Zeitverhaltens von Paketen zur Informationsverschleierung
  - 1-Bit Kanal: Webserver
    - Bit 1: Webserver unter Vollast $\rightarrow$ langsame Antwort
    - Bit 0: Webserver unter geringer Last $\rightarrow$ schnelle Antwort
    - Messung der Antwortzeiten

Klassifikation III

- Active Covert Channel
  - Erzeugt selbst den Netzwerkverkehr, der zur Verschleierung von Nutzdaten benötigt wird
  - häufigste Variante
- Passive Covert Channel
  - Nutzt und verändert bereits existierenden Netzwerkverkehr zur Übertragung von Nutzdaten
  - Erstmals implementiert in NUSHU (Joanna Rutkowska)

Beispiele für Covert Channel I

- IPv4
  - Type of Service
  - Time to Live
  - Identification
- ICMPv4
  - ID
  - Data

Beispiele für Covert Channel II

- HTTP
  - URL
  - Header (ETag, Cookies)
  - Schreibweise, Reihenfolge von Header
- DNS
  - QNAME
  - NULL
  - TXT
  - Slackspace im Protokoll

Tools

- Viele öffentlich verfügbare Implementierungen
- Meist als Tunnel realisiert
- Ziel: Durchsatzmaximierung
- Beispiele:
  - PingTunnel (ICMP)
  - LOKI (ICMP)
  - httptunnel (HTTP)
  - Corkscrew (SSH über HTTP)
  - iodine (DNS)
  - psudp (DNS)
  - ...

Limitierungen von Covert Channel

- Geringe Kapazität/Bandbreite
- Sinkende Tarnfähigkeit bei steigender Bandbreite
- Variable Verlässlichkeit

Idee/Lösungsansatz

- Kombination von Covert Channel unterschiedlicher Trägerprotokolle
  - Gesteigerte Bandbreite
  - Verbesserte Resistenz
  - Abstraktion
  - ...
- Umsetzung durch ein eigenes Covert Channel Protocol

Herangehensweise

1. Anforderungen an Trägerprotokolle festlegen
2. Bestehende Covert Channel evaluieren
3. Geeignete Trägerprotokolle auswählen
4. Paketformat spezifizieren
5. Protokoll entwickeln
6. Testen & verbessern mithilfe von Proof of Concepts

Anforderungen an Trägerprotokolle

- Verbreitung
- Vorhandene Covert Channel
- Verdecktheit
- Kapazität
- Latenz

Auswahl der Trägerprotokolle

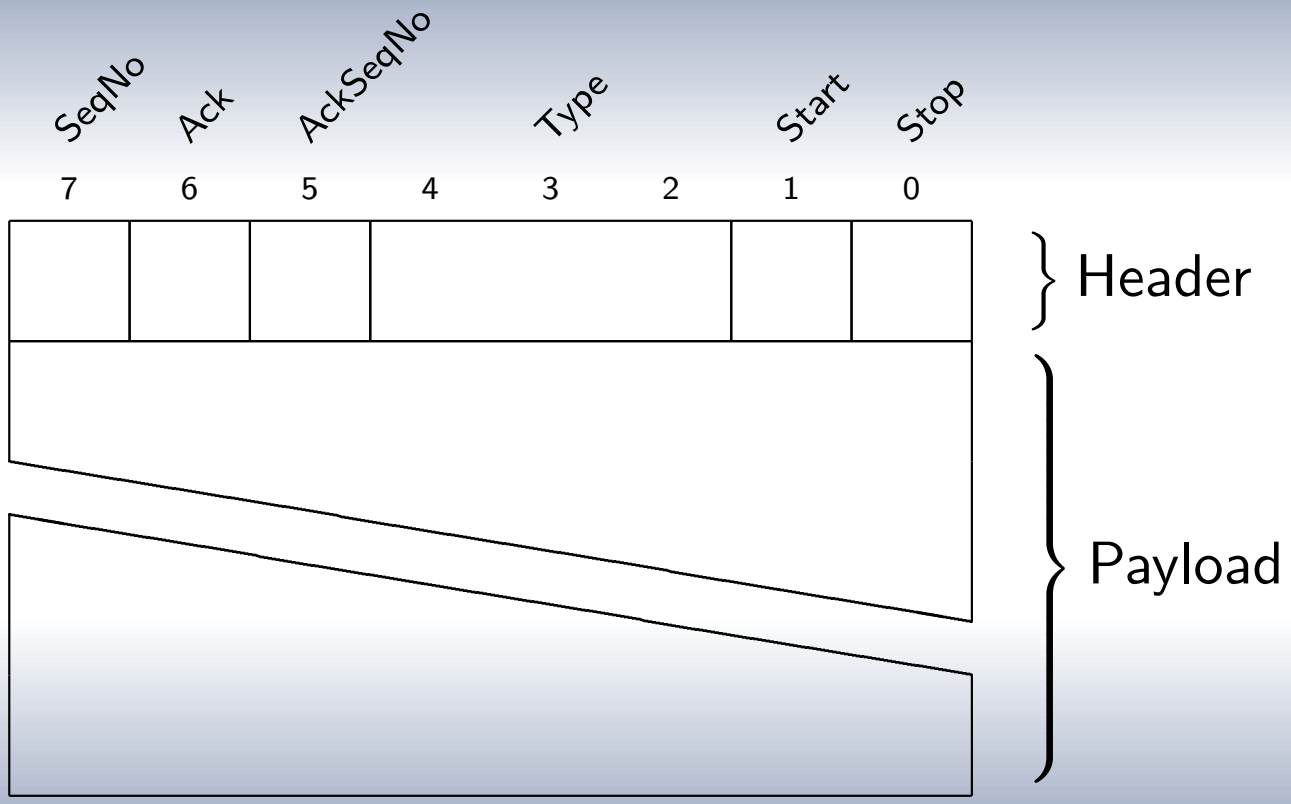
- HTTP
- DNS
- ICMP

Anforderungen

- Gesicherte Datenübertragung
- Beliebige Nutzdaten
- Möglichst kleiner Header
- Verbindungsorientiertes Protokoll
- Freie Wahl des Trägerprotokolls

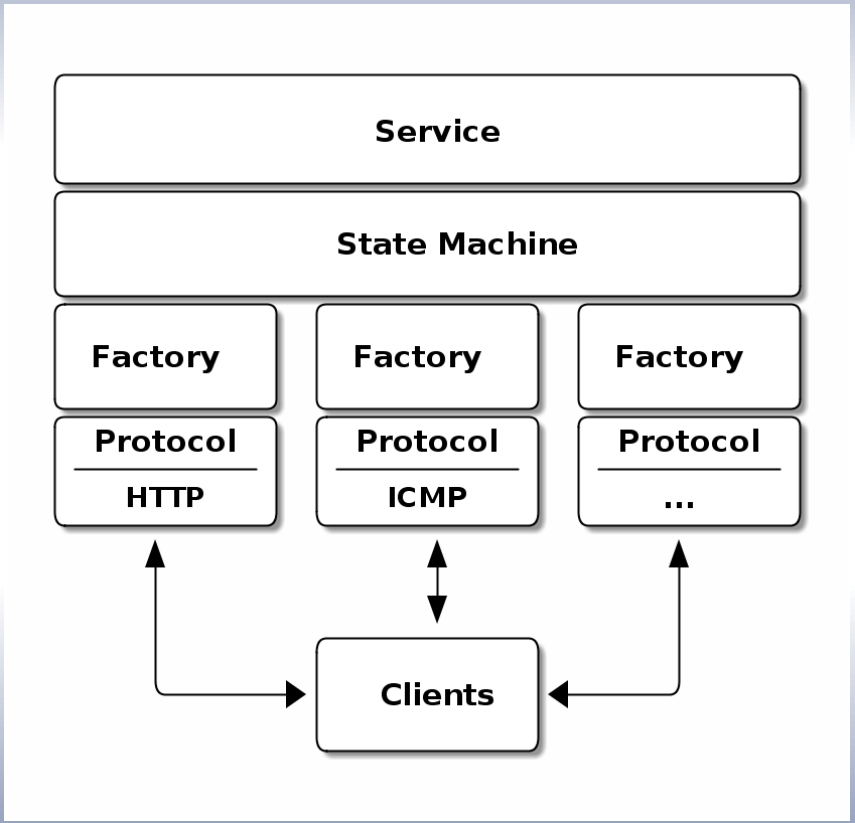
→ Eigenes Paketformat nötig

Paketformat



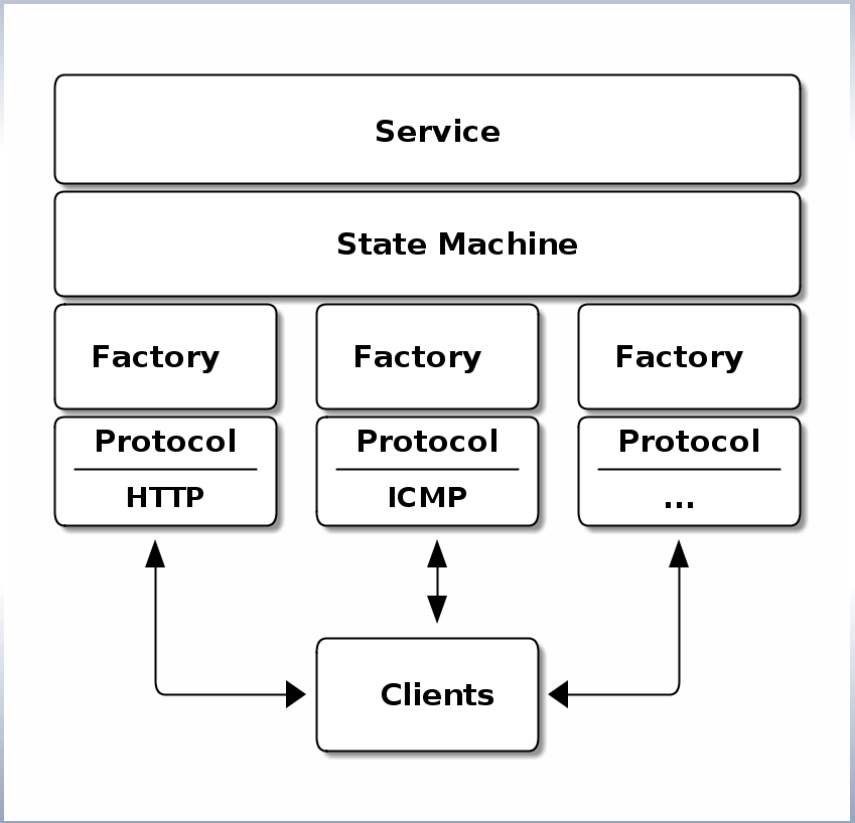
Proof of Concept

- Umsetzung mit Python & Twisted
- Mehrere Trägerprotokolle
- Verschiedene Services
- Active & Passive Covert Channel

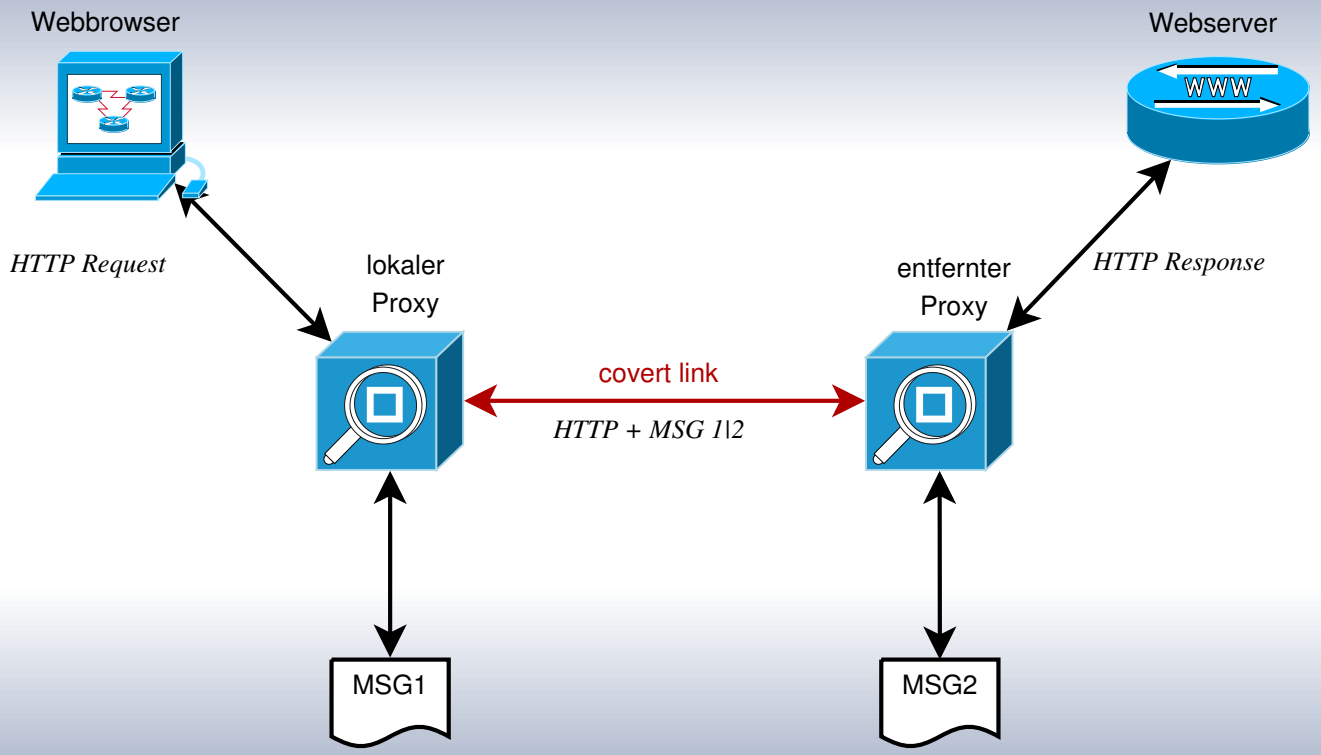


Proof of Concept

- Implementierte Services
  - Verdeckte Übertragung von Dateien
  - Verdeckter Chat
  - Transparenter Proxy ...



Transparenter Proxy



Die nächsten Schritte ...

- Weitere Trägerprotokolle und Covert Channel implementieren
- Stabilität der Implementierung verbessern
- Messungen & Tests durchführen
- Masterarbeit schreiben :)

Covert Channel Protocol

Ein adaptives Protokoll zur verdeckten Übertragung von Informationen mittels existierender Covert-Channel

Florian Preinstorfer

http://nblock.org/about

Security Insights, 18.04.2012