Verdeckte Kanäle

Neuland für freie Software

Open-Source-Treffen München, 22. Juli '11

Steffen Wendzel

Zwei Jahre Open Source Treffen München

Herzlichen Glückwunsch zum Geburtstag! ;-)

Agenda

- Kurze Einführung in das Thema
- OpenCCD
- Freie PoC-Codes
- Exemplarisch: Detektion
- Preview Fachbuch

Covert Channel

- dt. *verdeckter Kanal*
  - *bspw. Dateiname, IP TTL*
- *Hacking-Community: Tunneling, teilweise auch „Side Channel“ (beides falsch)*
- B. Lampson: *A Note on the Confinement Problem, Comm. ACM 16(10),pp. 613–615,* 1973:

  „*not intended for information transfer at all*“
- Multilevel Security (NRU, NWD)

Relevanz

- Journalisten
- Unternehmen

  Fisk et. al.: 4 GByte/Tag möglicher, verdeckter Information Leakage eines Unternehmens über größere Webseite mit 500 Mio. Pkts/Tag möglich (2003).
- Würmer etc.
- evtl. Geheimdienste

Womit ich mich beschäftige …

- Seit 2007 (Diplomarbeit, Masterarbeit, einige Fachartikel, PoC-Codes, jetzt Doktorarbeit)
- Es gibt bereits unzählige Techniken für verdeckte Kanäle.
  - Spezialisten in der Hacking-Community vorhanden
  - neue Covert Channels sind langweilig → kann jeder
- Mein Fokus:
  - Detektion (Leakage Protection → OpenCCD und Forschung)
  - Protocol Engineering (Protokolle innerhalb der verdeckten Daten) → Ph.D. Thesis

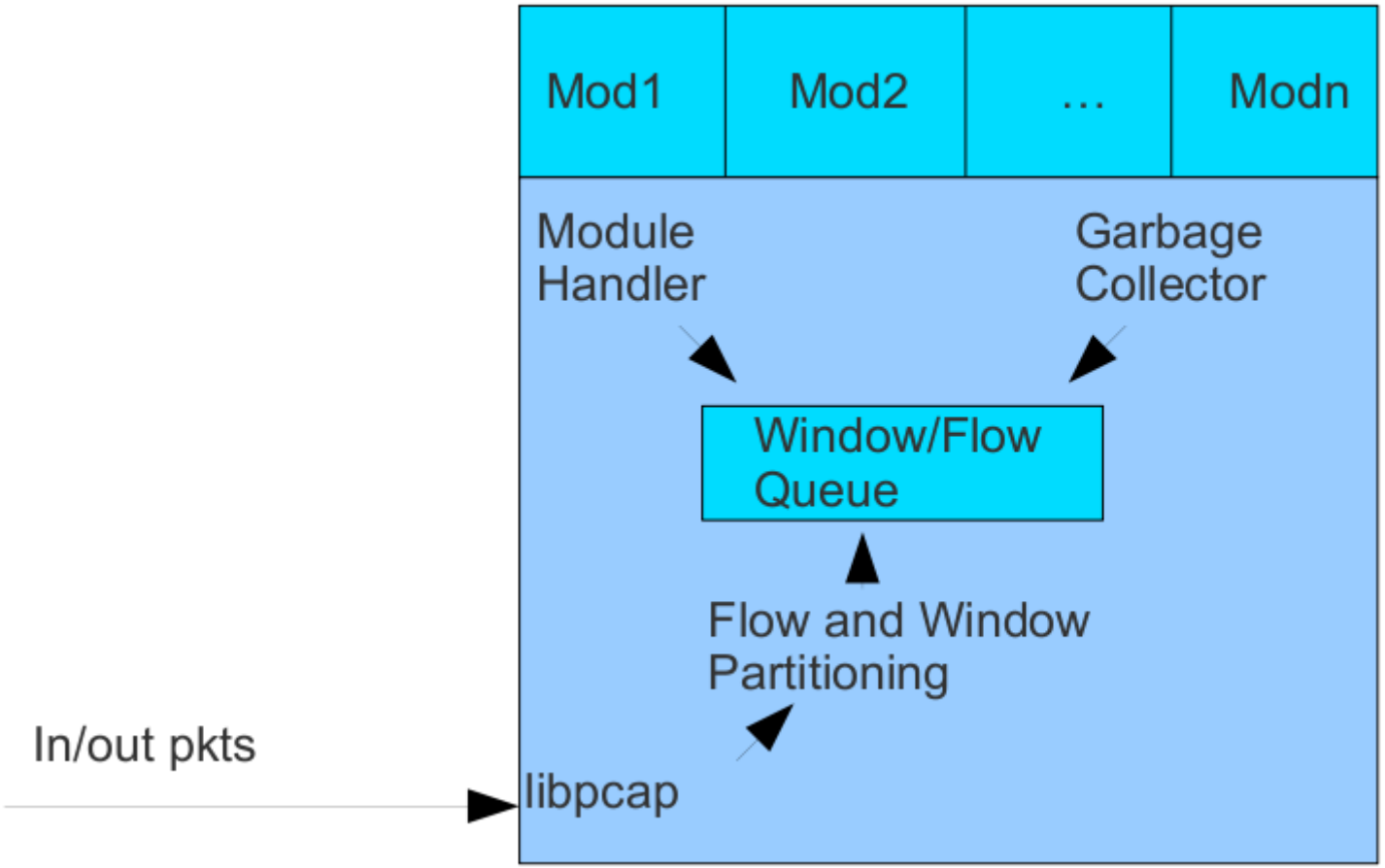
Was ist sinnvoll?

- Leakage Protection für Unternehmen:
  - Szenario: MA lädt Tool herunter und nutzt es.
  - Algorithmen sind bekannt (Jahrzehnte an Forschungsarbeit)
    - Siehe Google Scholar (CC+{elimination,detection,...})
    - Nur mäßig befriedigende Detection-Resultate
  - Tasks:
    - Neue Algorithmen erfinden
    - Neue und bekannte Algorithmen verifizieren/optimieren
    - … und implementieren

OpenCCD

- Erst kürzlich gegründet!
- www.openccd.org
- Ziel: Covert Channel Detection implementieren (Open Source)
- Wenige Spezialisten, Mangel an Entwicklern

Funktionsweise



Wird OpenCCD nützlich sein?

- Nur der Praxistest wird es zeigen!
- Wie würden Sie Daten leaken?
  - E-Mail?
  - Steganografie in Bildern, Videos etc.?
  - Covert Channels sind auch „nur“ Steganografie.
- Covert Channel-Detection/-Prevention kann nur **einen** Aspekt der Leakage Protection darstellen, sollte aber nicht außer Acht gelassen werden!

Warum erst jetzt?

- Oder: *Warum können eigentlich Snort und Co. noch keine Covert Channel-Detection?*
- Thema kaum bekannt
  - es kommt erst auf!
- Risiko kaum bekannt
  - es muss erst Beispielfälle geben!
- Fast ausschließlich ein Forschungsthema
  - Die Detection-Algorithmen sind fast alle noch nicht für den Praxiseinsatz nützlich!

Freie (Proof-of-Concept-)Codes

- pingtunnel
- LOKI2
- NUSHU
- phcct und pct

Protokollwechsel

- Ziel: Detektion und Aufdeckung übertragenen Inhalts erschweren
- Erste Implementierung
  - „LOKI2“, Phrack Mag. Vol. 7/51, 1997
  - Autor: ”daemon9”

LOKI 2

- Tunneling via UDP und ICMP
  - Manueller Protokollwechsel via '/swapt'

"Swapping protocols is broken in everything but Linux. (...) This is why this feature is 'beta'."

(Auszug aus dem LOKI2-Artikel im Phrack Mag.)

swendzel@steffenmobile: ~

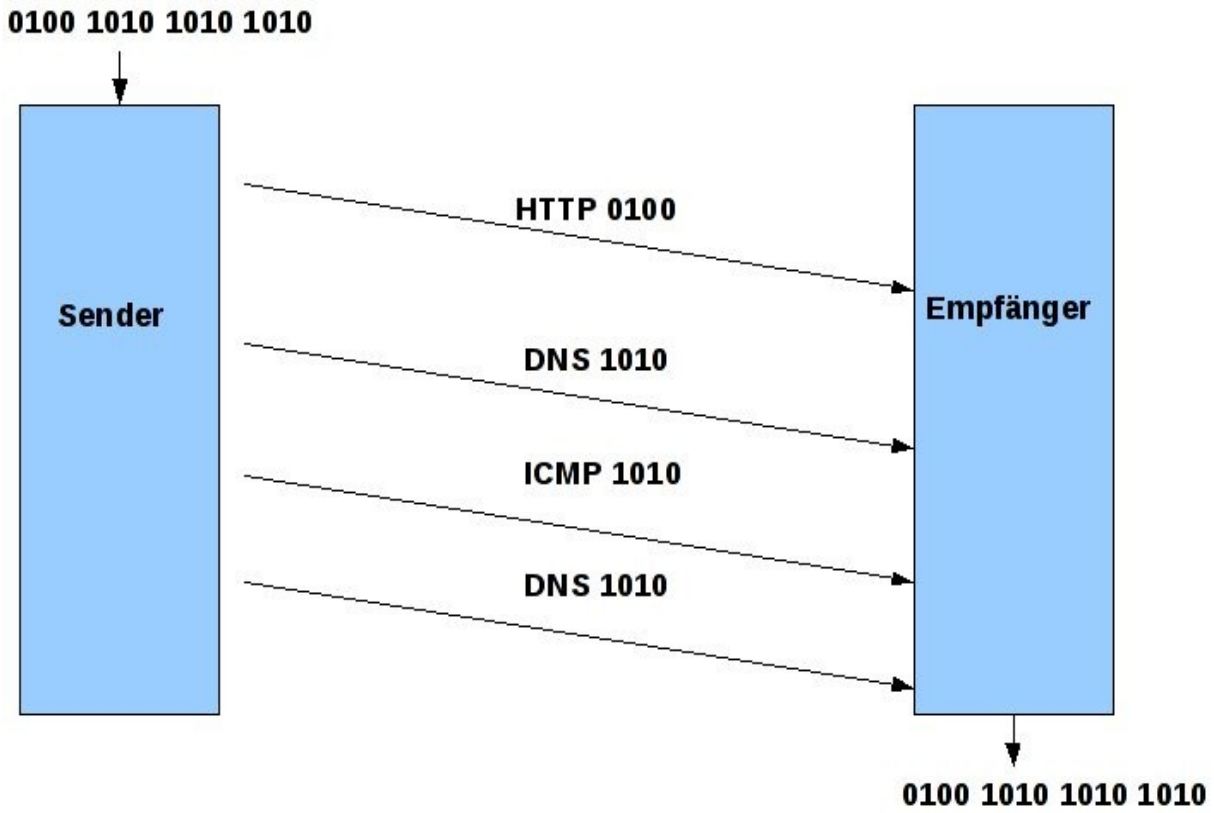
```
#define SWAP_T      "/swapt"        /* Swap protocols  */
...
    if (signal(SIGUSR1, swap_t) == SIG_ERR)
        err_exit(1, 1, verbose, L_MSG_SIGUSR1);
...

void d_parse(u_char *buf, pid_t pid, int ripsock) {
    ....
    if (!strncmp(buf, SWAP_T, sizeof(SWAP_T) - 1))
    {
        if (kill(getppid(), SIGUSR1))
            err_exit(1, 1, verbose,
                "[fatal] could not signal parent");
        clean_exit(0);
    }
...
void swap_t(int signo) {
    ...
    close(tsock);

    prot = (prot == IPPROTO_UDP) ? IPPROTO_ICMP : IPPROTO_UDP;
    if ((tsock = socket(AF_INET, SOCK_RAW, prot)) < 0)
        err_exit(1, 1, verbose, L_MSG_SOCKET);
    pprot = getprotobynumber(prot);
    sprintf(buf, "lokid: transport protocol changed to %s\n",
        pprot -> p_name);
    fprintf(stderr, "\n%s", buf);
                                                    24,1        Anfang
```

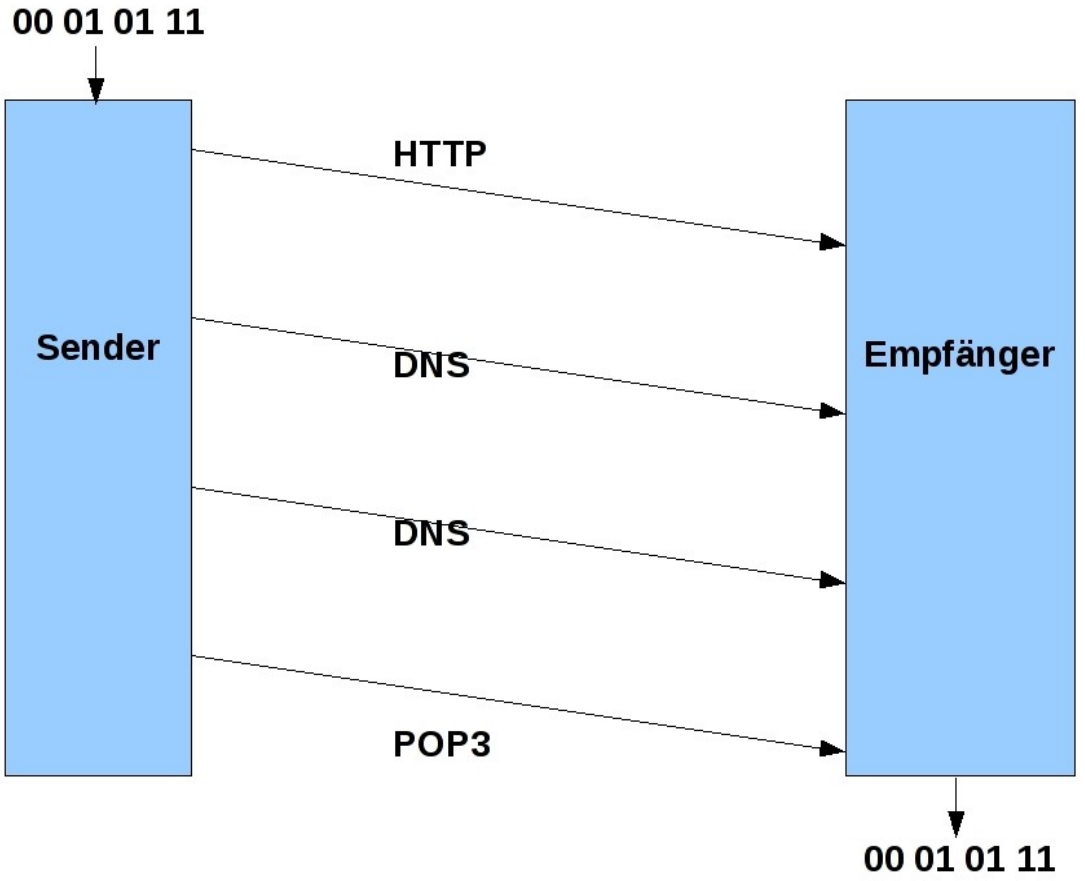
Protocol Hopping Covert Channels

- Sind Covert Storage Channels
- Wechsel des verwendeten Protokolls *jederzeit* und auch *zufällig* möglich. → Transparenz!
- Detektion und Analyse erschweren.
- Mikroprotokoll empfehlenswert (Sortierung)



Protocol Channels

- Signalisierung der zu übertragenden Informationen *ausschließlich* durch die Information des verwendeten Protokolls.
- Nur statistisch detektierbar



Kurzer Überblick
Covert Channel-Detection

Detektion in Geschäftsprozessen

- Accorsi & Wonnemann:
  - *Detective Information Flow Analysis for Business Processes*, 2009
  - *Informationsfluss-Mechanismen zur Zertifizierung von Cloud-basierten Geschäftsprozessen*, 2011
  - Leaking confidential business data

Normalisierung

- Typische Felder wie DF-Flag, Reserved Flag im IP-Header → decken nur bekannte Bits ab!
- Could-Start Problem
- Inconsistent TCP-Transmissions (Handley et.al.'01) → „nice“ || „root“
- pf scrub, Snort, norm

Timing Channel Detection

- Diverse Verfahren zur Auswertung von Inter Packet Gaps (Inter-Arrival Times)
- Epsilon-Similarity (Cabuk et. al.)
- Compressibility (Cabuk et. al.)
- P_{CovChan} (Berk et. al.)

Passive ISN-Cov. Chan. Detection

- Murdoch/Lewis '05: Detektion von Rutkowskas TCP-ISN PCC „Nushu“
- Unterschiedliche Verteilung der ISNs
  - Current ISN → next ISN
- Unterschiedliche Wertebereiche der ISNs

Wie können Sie beitragen?

- Selber im Bereich Covert Channel-Detection forschen/sich einlesen

- Algorithmen in OpenCCD implementieren und testen

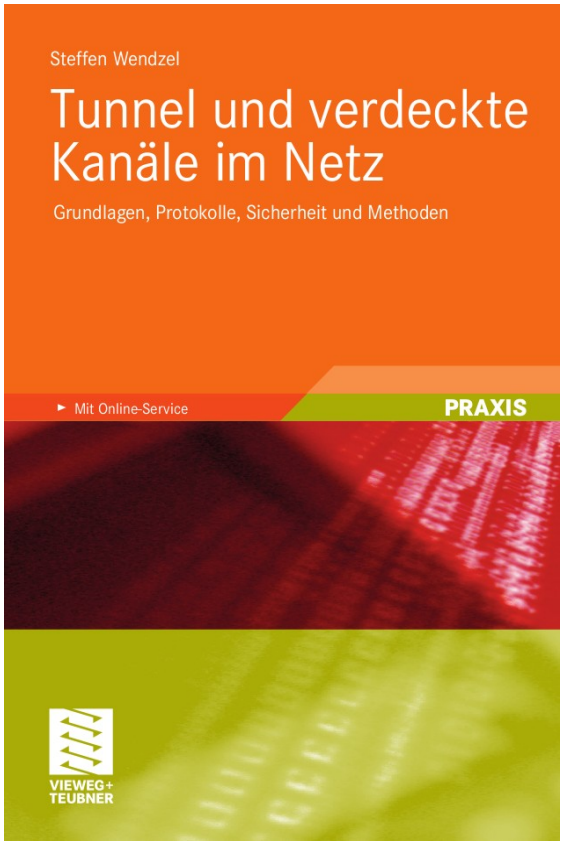
Werden Sie ein Pionier ;-)

Das waren natürlich nicht alle Verfahren!

- VoIP based Detection
- Entropy based Approach
- Diverse Präventions- und Limitierungs-Ansätze
  - Fuzzy Time (Hu)
  - Shared Resource Matrix Methodology (Kemmerer)
  - Covert Flow Trees (Kemmerer/Porras)
  - (Network) Pump (Moskowitz et. al.)/Quantized Pump, Upwards Channel, Store and Forward Protocol, …
  - Detection von TTL-Channels
  - Detection von Timing Channels im Generellen
  - Multiplayer Covert Channel-Detection
  - …

Vorschau

- Tunnel und verdeckte Kanäle im Netz
  - Einführung, Detection/Prevention, Techniken der verdeckten Kanäle etc. ausführlich beschrieben.
  - Vieweg+Teubner, 2012
  - www.linux-openbook.de
  - Noch dieses Jahr:
    - Linux. Das umfassende Handbuch, 5. Aufl.
      >1300 Seiten 4 free als Download!
    - Evtl. auch noch Einstieg in Linux, 5. Auf.



- Open Covert Channel Detector
  - Erstes Covert Channel-NIDS
  - www.openccd.org
  - Call for Developers!