Covert Channels

Geheime kanalen binnen computernetwerken

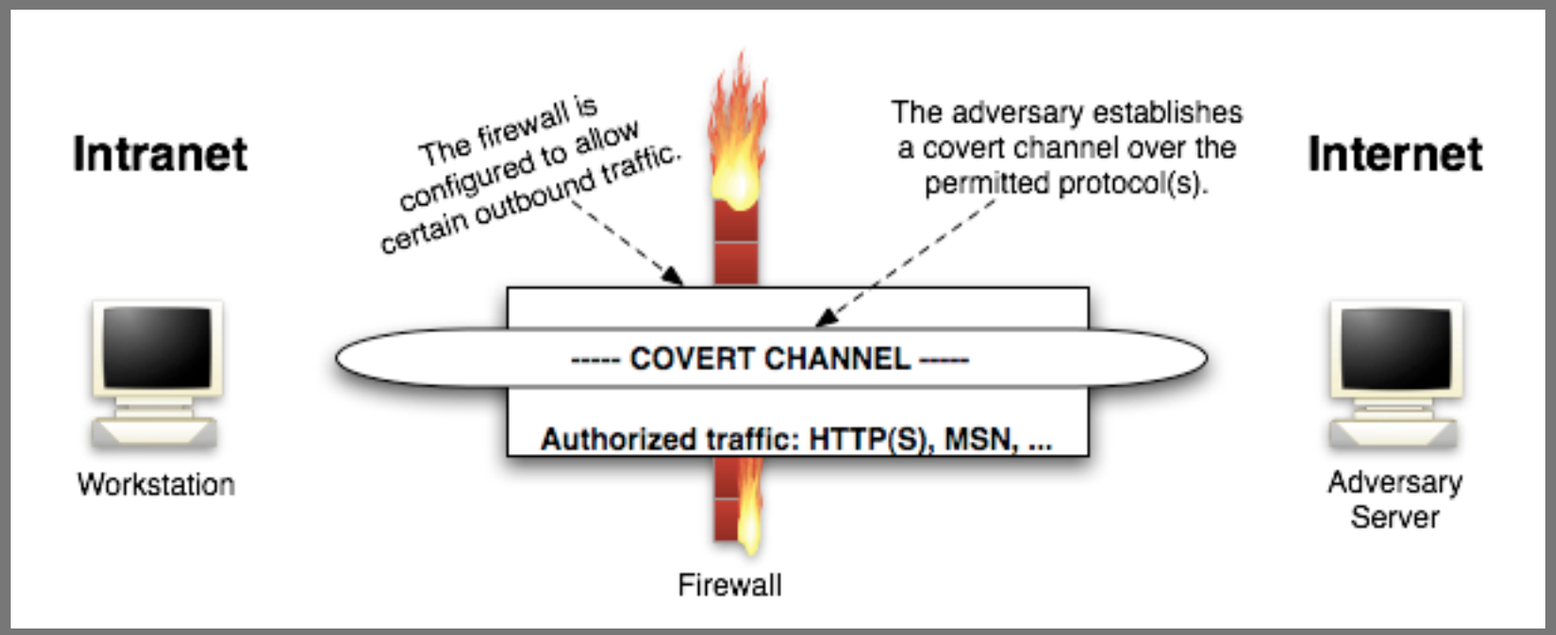
Matthijs Koot & Marc Smeets, 2006-02-08

Agenda

- Vraagstelling
- Aanpak
- Resultaten
- Future work

Vraagstelling

- Vraagstelling van KPMG
- Welke bedreigingen vormen covert channels voor een informatievoorziening?



Aanpak

- Bureau-onderzoek
- Willen we experimenteren? Zo ja:
  - Voorbereiden
  - Meten
  - Interpreteren
  - Concluderen

Bureau-onderzoek

- Academische bronnen
  - portal.acm.org
- Overige bronnen
  - Gray-World.net
  - SecurityFocus
  - ...

Experimenten

- Wat willen we meten / weten?
- #1: Hoe werken covert channels?
- #2: Hoe efficiënt zijn covert channels?
  - Aantal bytes/pakket

Resultaten

- Definitie
- Classificatie
- Kwaliteitscriteria
- Meetresultaten

Definitie

"A covert channel is a communication channel that allows a process to transfer information in a manner that violates the system's security policy."

Bron: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

Voorbeeld

- Carriers in HTTP/1.0 requests:

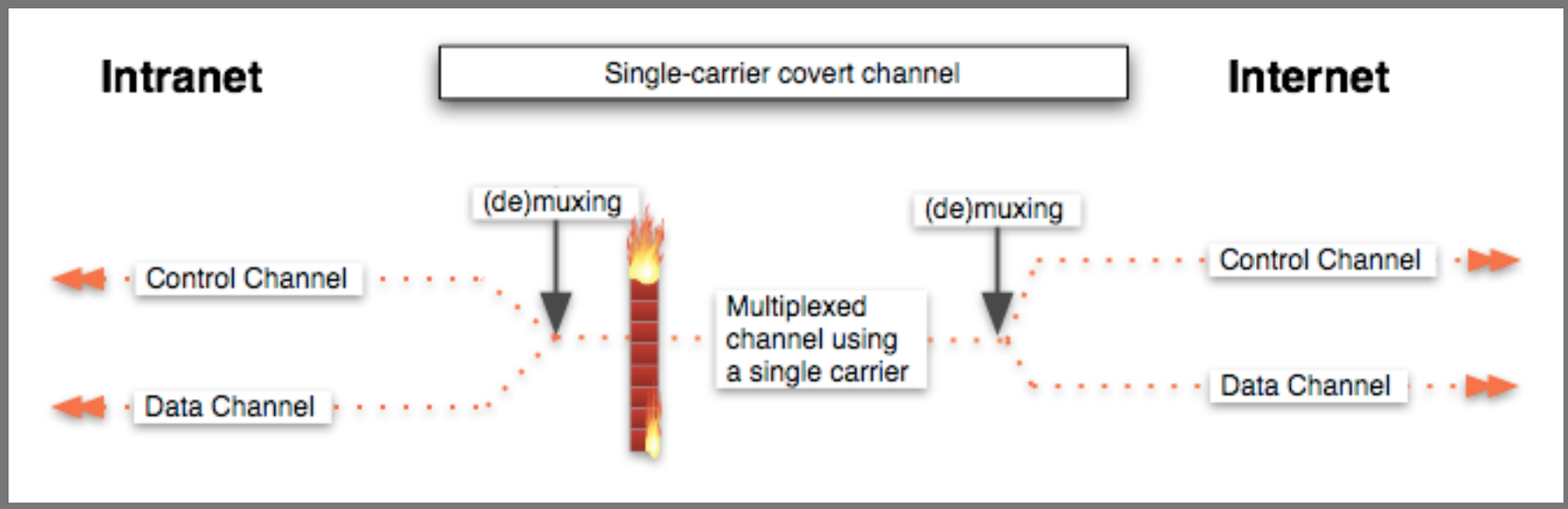
```
Request         = Simple-Request | Full-Request

Simple-Request = "GET" SP Request-URI CRLF

Full-Request    = Request-Line                  ; Section 5.1
                  *( General-Header             ; Section 4.3
                   | Request-Header             ; Section 5.2
                   | Entity-Header )            ; Section 7.1
                  CRLF
                  [ Entity-Body ]               ; Section 7.2
```

Classificatie

- Dimensie (tijd, ruimte)
- Encodering (waarde, transitie)

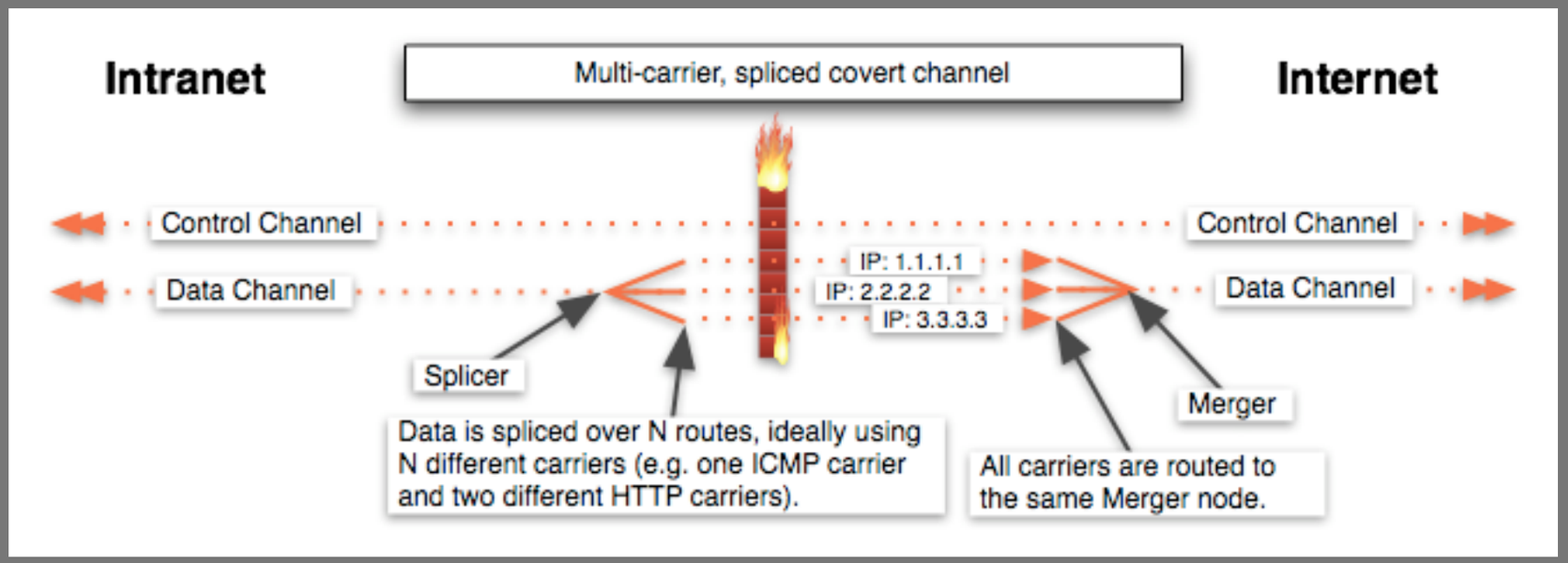
Classificatie (2)

- Gedrag (actief, passief)
- Efficiency
- Path (direct, indirect, spread)



Classificatie (2)

- Gedrag (actief, passief)
- Efficiency
- Path (direct, indirect, spread)

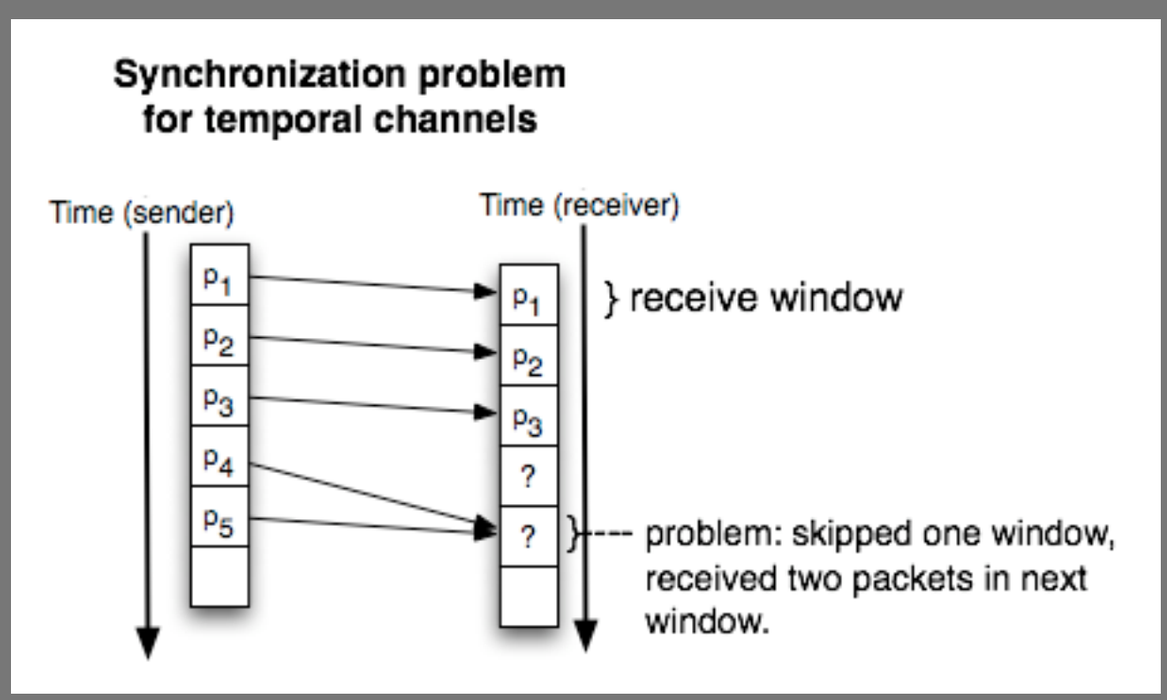


Kwaliteitscriteria

- #1: Robuustheid
  - Transmissiecontrole
  - Synchronisatie

Kwaliteitscriteria

- #1: Robuustheid
  - Transmissiecontrole
  - Synchronisatie



Kwaliteitscriteria (2)

- #2: Aannemelijkheid
  - Geen afwijkend netwerkverkeer
    - Niet in omvang (usage statistics)
    - Niet in vorm (headervalues)
  - Steganografie

Meetresultaten

- Meetmethode
  - Verschillende CC-implementaties
  - Verschillende datasets
    - Alleen 8-bits ASCII
    - Verschillende groottes
- netcat, Ethereal

Meetresultaten (2)

- Objecten
  - covert_tcp (TCP ISN, ...)
  - firepass (TCP-over-HTTP)
  - Ozyman (stdin/out-over-DNS)
  - ptunnel (TCP-over-ICMP)

Meetresultaten (3)

- ptunnel (TCP-over-ICMP)
  - ~66 KB/s, 100% betrouwbaar
- Ozyman (stdin/out-over-DNS)
  - <~1 KB/s, <100% betrouwbaar

Meetresultaten (4)

- Problemen
  - Onvolkomenheden in broncode
  - Veel variabelen (bijv. TCP Window Size)
  - Wat mag je wel/niet vergelijken? (appels vs. peren)

Conclusie

- Reële dreiging
- Moeilijk te bestrijden
- Nieuwe manieren zullen verschijnen

Future work

- Ontologie
- Rowland + Murdoch + Rutkowska
- Channeling over IPv6, Jabber, ...

Vragen?