Some Notes on the Present and Future of Internet Monitoring

Panel contribution at ICISP 2006

Arno Wagner

arno@wagner.name

Communication Systems Laboratory

Swiss Federal Institute of Technology Zurich (ETH Zurich)

Background: The DDoSVax Project

`http://www.tik.ee.ethz.ch/~ddosvax/`

- Collaboration between SWITCH (www.switch.ch, AS559) and ETH Zurich (www.ethz.ch)
- Aim (long-term): Near real-time analysis and countermeasures for DDoS-Attacks and Internet Worms
- Start: Begin of 2003
- Funded by SWITCH and the Swiss National Science Foundation

DDoSVax Data Source: SWITCH

The Swiss Academic And Research Network

- .ch Registrar
- Links most Swiss Universities and CERN
- Carried around 5% of all Swiss Internet traffic in 2003
- Around 60.000.000 flows/hour
- Around 300GB traffic/hour
- Unsampled flow archive since May 2003
  $\sim$ 20TB compressed

Packet Level Monitoring

The ”natural” solution

- + Gives you all payload and header-data
- + Gives you precise packet timing
- - More transfer bandwith than monitored network
- - ”Storage limited”, e.g, SWITCH: 300GB/h
- - Legally problematic, (also liability!)

⇒ Very expensive. Legally problematic.

Packet Headers

The ”smaller” solution

- What/how long is a header?

+ No payloads, smaller.
+ Usually needs far less bandwith than monitored network to transfer
- No payloads
- Still a lot of data

⇒ Expensive. May be legally problematic.

Flows

The ”available” solution

+ Sensor often ”for free”
+ Small (on average)
+ Can often be transfered intra-network
+ Shows most of what headers give you
- Worst-case: Can be more than network traffic!
- Not even packet headers....

$\Rightarrow$ Cheap. Usually legal.

Predictions I

We will see more encrypted traffic

- Driven by P2P filesharing
- Also relevant to MMORG to make cheating more difficult (WoW: 6 million subscribers!)
- At some point everything may be encrypted...

Impact:

- Packet capturing: Reverts to (partial) headers
- Header capturing: Less information
- Flow capting: Less information.

Dealing with Encryption

- Legal countermeasures? ⇒ Forget it
- Social countermeasures? (”Only criminals use encrytion”)
  ⇒ Forget it
- Legalised hacking? Extremely dangerous and doubtful with regard to effectiveness.

⇒ Learn to live with it

Predictions II

We will see more anonymisation

- P2P (filesharing):
  Countermeasure to ”hacked” clients
- Other anonymisation: Less relevant

Impact:

- Even more P2P traffic than already there
- Lots of opaque and possible cover traffic
- Traffic will become meaningless

Dealing with Anonymisation

- Basically the same as with encryption

⇒ Learn to live with it

Thank You!