Flow-based Detection of IPv6-specific Threats

RIPE71, Bucharest

Luuk Hendriks
Design and Analysis of Communication Systems

UNIVERSITY OF TWENTE.

*”Absence of evidence
is no evidence of absence”*

We don't have proper v6 security appliances

<==>

We don't see any threats on v6

<==>

We don't need to spend resources on this

USENIX WOOT '14
Workshop On Offensive Technologies:

IPv6 Security: Attacks and Countermeasures in a Nutshell, Ullrich et al.:
42 threats, allmost all L3

We want ...

To define flow-level signatures of
IPv6 L3-specific threats

in order to enable detection in a
easily deployable, scalable fashion

We don't want ...

To turn our flow exporters
into full-blown packet-based
IDS/IPS/...

doing anything but
exporting quality flow records

Almost everything we need is almost there almost-ish

IANA IPFIX Information Elements:
e0id31: **flowLabelIPv6**
e0id5: **ipClassOfService** (Traffic Class)
e0id139: **icmpTypeCodeIPv6**

Q: how many of these fields were exported by our probe?

“we never have had such request yet”

– $vendor support guy

Time to enjoy IPFIX

Currently focussing on exporting **fragmentation** information:

e785id401: **v6fragNxtProto**
e785id402: **v6fragNxtSrc**
e785id403: **v6fragNxtDst**
e785id404: **v6fragMinOffset**

Where to now?

Right now,

generate and test with synthetic attacks

Soon,

deploy online detection at two NRENs

In the long run,

characterize the v6 security landscape

Discussion

How v6-ready are your flow exporters?

What IPFIX Information Elements should we define and standardize?

Which other possible uses of these IEs can we think of?

Flow-based Detection of IPv6-specific Threats

As presented at RIPE71, Bucharest

Luuk Hendriks

luuk.hendriks@utwente.nl
IRC: dRiek/DriKE/dRk/dr<tab><tab><tab>

UNIVERSITY OF TWENTE.