Understanding the TCP Expert

Jasper Bongertz, Senior Consultant
Airbus Defence & Space CyberSecurity

Topics

- Motivation
- The TCP Expert module
- TCP Expert messages

Motivation

- Questions on http://ask.wireshark.org like:
  - „why does my server say the window is full?“
- The TCP expert is not alway right:
  - Classic „segment lost, out-of-order, retransmission“ messages in a row

The TCP Expert Module

- The TCP expert is a software module that verifies TCP packets
  - Tracked per TCP connection
- Packets that are „bad“ or „in the wrong“ place are marked
  - Packet Loss, Out-of-order,...
- Also, some packets with important characteristics will be marked
  - Window Full, Window Update,...

TCP Expert messages

- We will look at these messages:
  - TCP Window
    - „Window Full“
    - „Window Update“
    - „Zero Window“, „Zero Window Probe“, „Zero Window Probe ACK“
  - Packet Loss:
    - „Previous Segment not captured“
    - „Out-of-Order“
    - „Retransmission“ (Normal, Fast, Spurious)


SHARKFEST'14
WIRESHARK DEVELOPER AND USER CONFERENCE
JUNE 16-20 2014 · DOMINICAN UNIVERSITY
Live Demos

Thanks! Questions?

eMail: jasper@packet-foo.com
Blog: blog.packet-foo.com
Twitter: @packetjay