



Bram C.M. Cappers
b.c.m.cappers@tue.nl

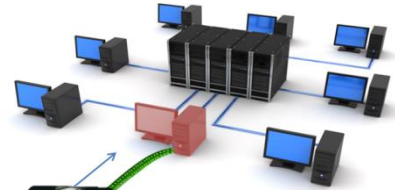


Jarke J. van Wijk
j.j.v.wijk@tue.nl

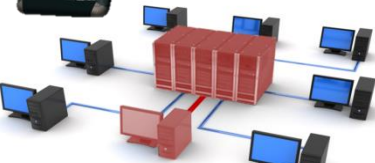
SEMANTIC NETWORK TRAFFIC ANALYSIS USING DEEP PACKET INSPECTION AND VISUAL ANALYTICS

Advanced Persistent Threats (APTs)

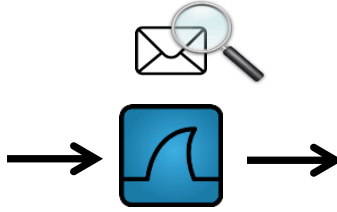
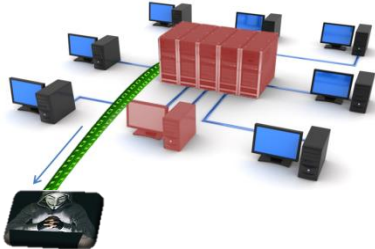
Infiltration



Expansion



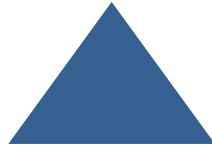
Sabotage



Wireshark
Protocol
Analyzer

ip.version	ip.src	ip.dst	tcp.srcport	tcp.flag	tcp.flag.SYN	tcp.flag.ACK	smb.header	smb.cmd	smb.type	smb.file	smb.bytestream	dcerpc.call_id	dcerpc.opnum
4	192.168.0.1	192.168.0.2	80	2	true	false	smb	5	readFile	a.txt			
⋮													
4	192.168.0.3	192.168.0.2	91	1	false	true	smb	3	IOControl		20	0	3

Alerts



Messages

Attributes

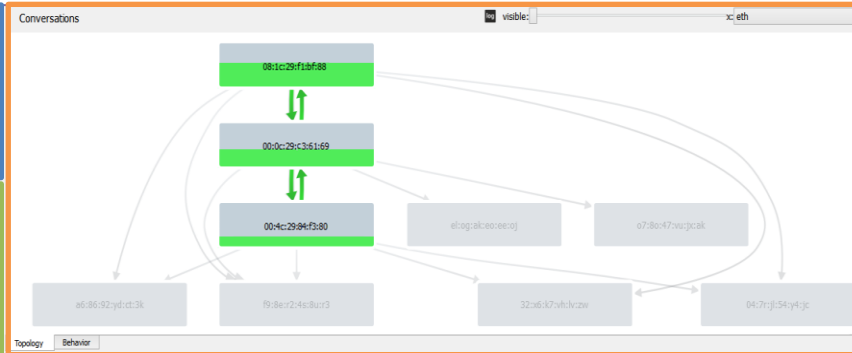
Overview

Filtering

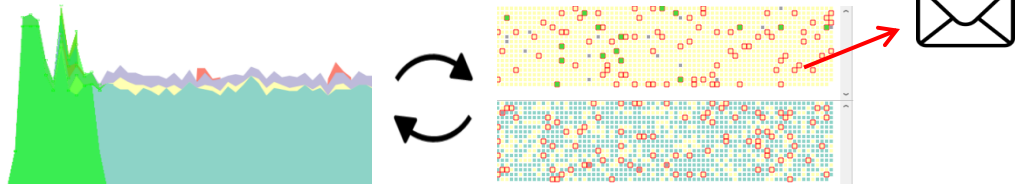
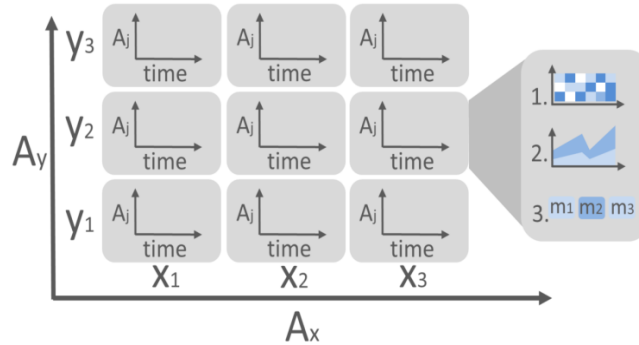
The interface is divided into two main sections. The top section, titled "Context", shows a table with columns for "Status", "Context", "#Packets", "#Alerts", "Coverage", and "Alerts". It lists three categories: "all" (84209 packets, 2475 alerts), "alert burst" (22292 packets, 1171 alerts), and "suspicious connection modbus" (55215 packets, 2101 alerts). The bottom section, titled "Attributes", displays a grid of 12 small bar charts for various attributes, including "mbtcp.group0.reference_num", "mbtcp.group0.register_uint16", "mbtcp.group0.seconds-since-duplica", and "mbtcp.trans_id".

Attributes

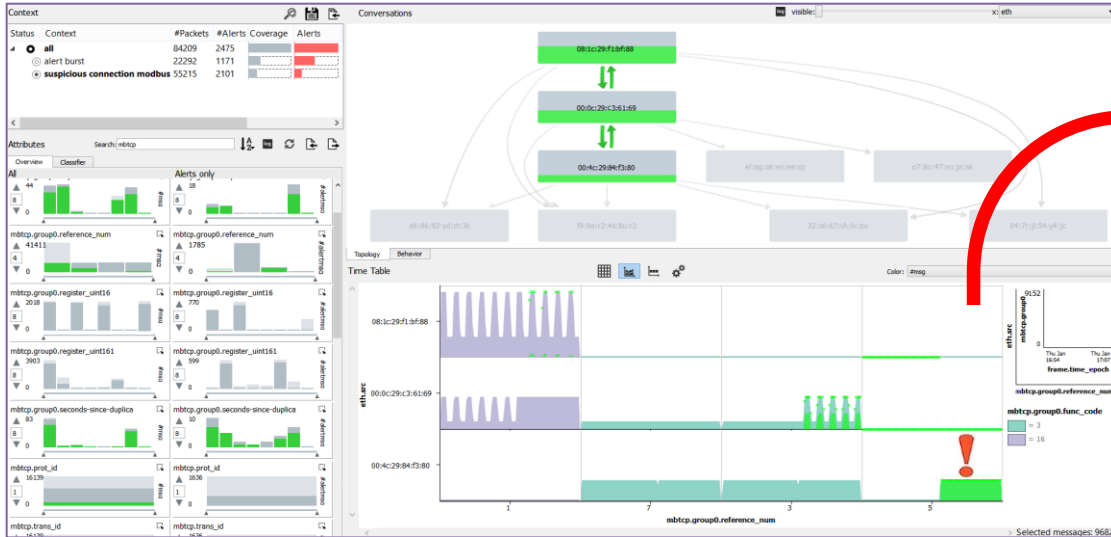
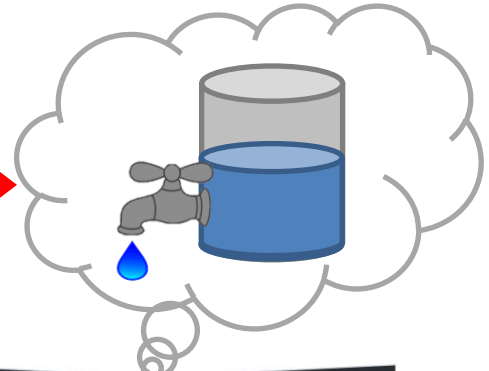
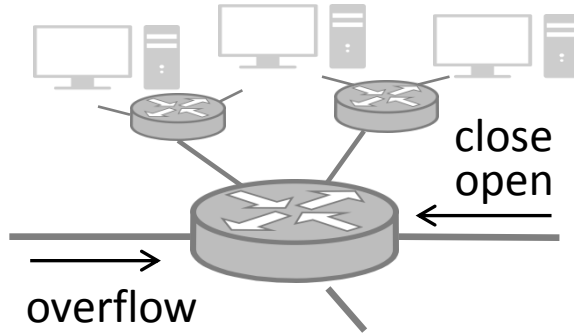
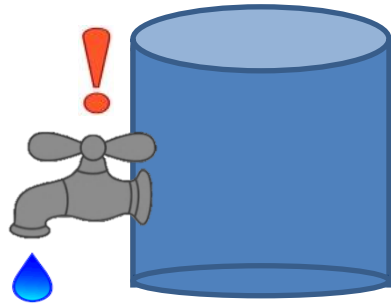
Conversations



Messages
+
Alerts



Results





Bram C.M. Cappers
b.c.m.cappers@tue.nl



Jarke J. van Wijk
j.j.v.wijk@tue.nl

THANKS FOR YOUR ATTENTION!



SpySpot
Seeing is believing