Technische Universität München, Department of Informatics



Chair for Network Architectures and Services Prof. Dr.-Ing. Georg Carle



Motivation

Your Task

Bibliography

Understanding the protocol format and the sequence of messages of network protocols gives you the possibility to detect unwanted or malicious behaviour in your network. This protocol inference is possible when done on relatively simple and single-session protocols [1,

Ele Edit View Go Capture Analyze Statistic	cs Telephony Icols (nternals)	кíр				
\$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$	् २ २ 🕹 🖗 🖗 🟦 🗐 🕅	ାର୍ର୍ଚ	L 🖸 🕷 🗹 🥵 🔅 😫			
Filter:	• Spressi	e. Clear App	ily Save			
No. Time Source	Destination	Protocol Le	ngth Info			
1 0.000000000 fe80::89c9:7d53:	f73:clff02::c	SSOP	208 N-SEARCH * HTTP/1.	1		
2 2.999936000 fe801189c917d531	f73:ciff02::c	SSDP	208 M-SEARCH * HTTP/1.	1		-
3 5.840693000 192.168.1.2	255.255.255.255	UDP	82 Source port: 64484	Destination port: sent	inelsrm	
4 6.000009000 fe80::89c9:7d53:	f73:ciff02::c	SSDP	208 M-SEARCH * HTTP/1.	1		
						· ·
Frame 3: 82 bytes on wire (656 bit	s), 82 bytes captured (65	6 bits) on	interface 0			
Interface id: 0						
WTAP_ENCAP: 1						
Arrival Time: Sep 8, 2012 17:21	:20.787839000 Paris, Hadr	1d (heure d	'ete)			
[Time shift for this packet: 0.0	00000000 seconds]					
Epoch 1188: 134/11/680./8/839000	seconds	and all				
[inne deita from previous captur	ed frame: 2.840/5/000 sec	onasj				
Time cipra reference en first f	yea 11 alle: 2,840/5/000 se	Concisi				4
Ersma humbar: 2	1 200 3.010003000 3400103					
prane Length: 82 hytes (656 hits	0					
Capture Length: \$2 bytes (656 bi	(ts)					
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ip:udp:	data]					
[coloring Rule Name: UDP]						
[Coloring Rule String: udp]						
Ethernet II, Src: QuantaCo_48:68:c	6 (60:eb:69:48:68:c6), Ds	t: Broadcas	t (ff:ff:ff:ff:ff:ff)			
B Destination: Broadcast (ff:ff:ff	(ff:ff:ff)					
B Source: QuantaCo_48:68:c6 (60:eb	2:69:48:68:c6)					
Type: IP (0x0800)						
Internet Protocol Version 4, Src:	192.168.1.2 (192.168.1.2)	, DSE: 255.	255.255.255 (255.255.25	.255)		
Version: 4						
Header Tength: 20 bytes						
B Differentiated Services Field: C	and (DSCP 0x00: Default;	ECN: 0000:	NOT-ECI (NOT ECN-Capabi-	(ransport))		-
TOCAT CENDEN: 08		A 104 - 4				
0000 TF TF TF TF TF TF TF 60 60 69 48 0010 00 44 3b 63 00 00 60 11 3d 9c	c0 s4 01 02 ff ff 01c	180				
0020 ff ff fb e6 07 96 00 30 c1 eb	44 71 30 46 55 4c		i.			2
0030 41 58 41 41 42 51 51 56 5a 4a	54 45 6c 50 54 6b AXAA	ADDA SOLATE	rk.			
0040 52 57 4e 67 42 73 62 33 4a 54	61 58 52 42 62 57 RWNg	35b3 JTaxRR	5W			-
	UN CON					

Thesis

IDP, Guided

2, 3, 5] or when manual intervention is done [4]. However, automatic protocol inference with correlation of multiple different protocols (e.g. XMPP and DNS) is still an open challenge. In this thesis you will develop a technique to do protocol inference of multi-session protocols.

- Research state of the art of protocol inference
- Develop a tool to do protocol inference on network traces
- Evaluate your tool with protocols such as WhatsApp
- [1] Joao Antunes, Nuno Neves, and Paulo Verissimo. Reverx: Reverse engineering of protocols. 2011.
- [2] Paolo Milani Comparetti, Gilbert Wondracek, Christopher Kruegel, and Engin Kirda. Prospex: Protocol specification extraction. In *Security and Privacy*, 2009 30th IEEE Symposium on, pages 110–125. IEEE, 2009.
- [3] Weidong Cui, Jayanthkumar Kannan, and Helen J Wang. Discoverer: Automatic protocol reverse engineering from network traces. In *USENIX Security*, pages 199–212, 2007.
- [4] Qun Huang, Patrick PC Lee, Caifeng He, Jianfeng Qian, and Cheng He. Fine-grained dissection of wechat in cellular networks.
- [5] TUM I8. ProtoX GitHub. https://github.com/tumi8/Protocol-Informatics.

Contact

Oliver Gasser gasser@net.in.tum.de







