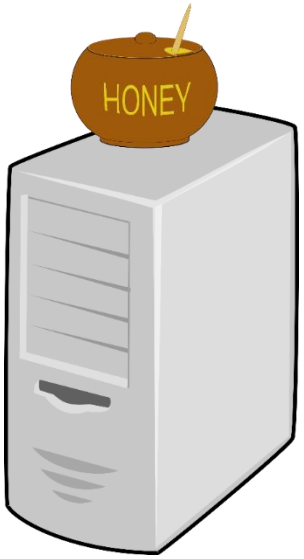
Introducing Falcom: A Multifunctional High-Interaction Honeypot Framework for Industrial and Embedded Applications

Daniel Fraunholz, **Daniel Krohmer**,
Carolina Nogueira and Hans Dieter Schotten

Cyber Security 2018

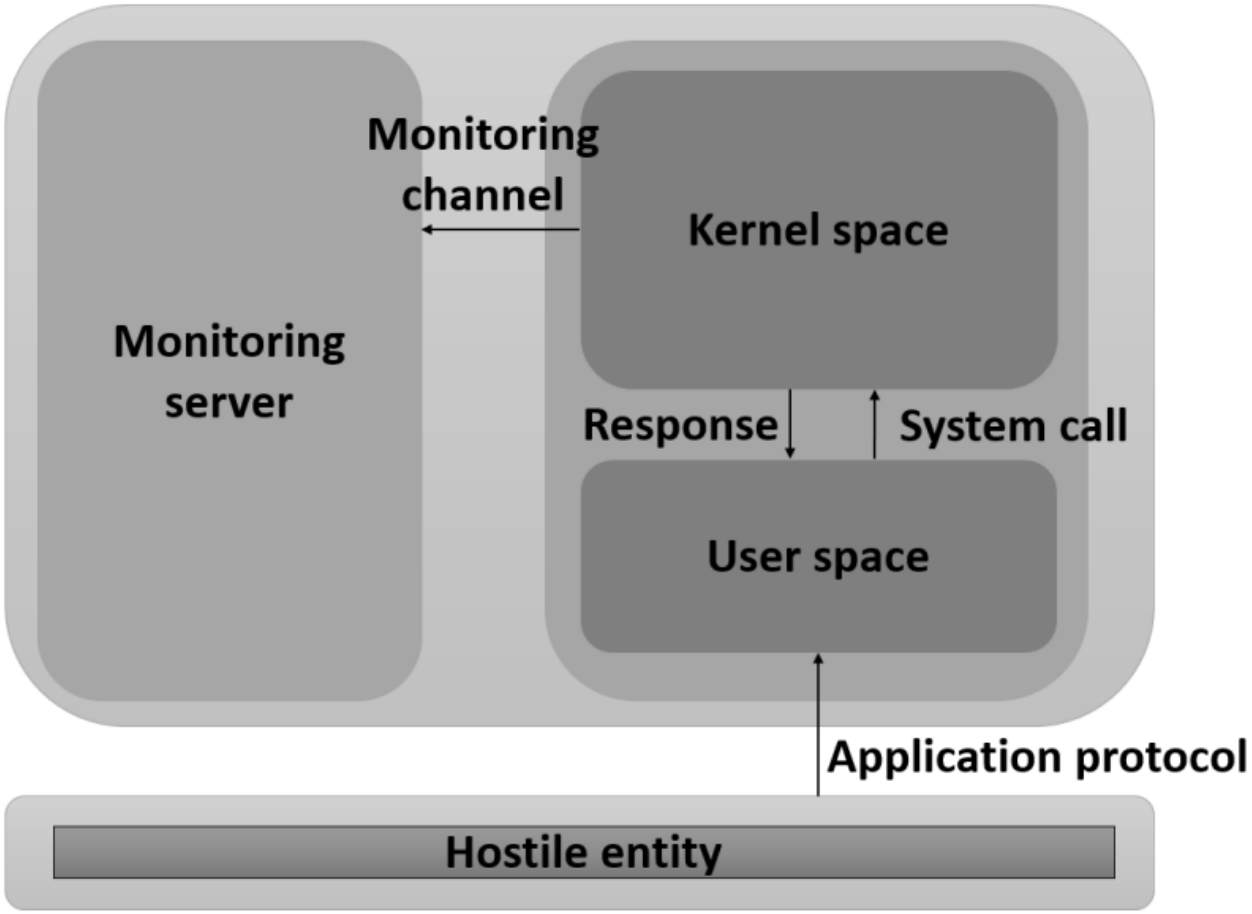
What is a Honeypot?

Source: techviral.com



"A honeypot is in general a computing resource, whose sole task is to be probed, attacked, compromised, used or accessed in any other unauthorised way"
– *ENISA, 2012*

System Design

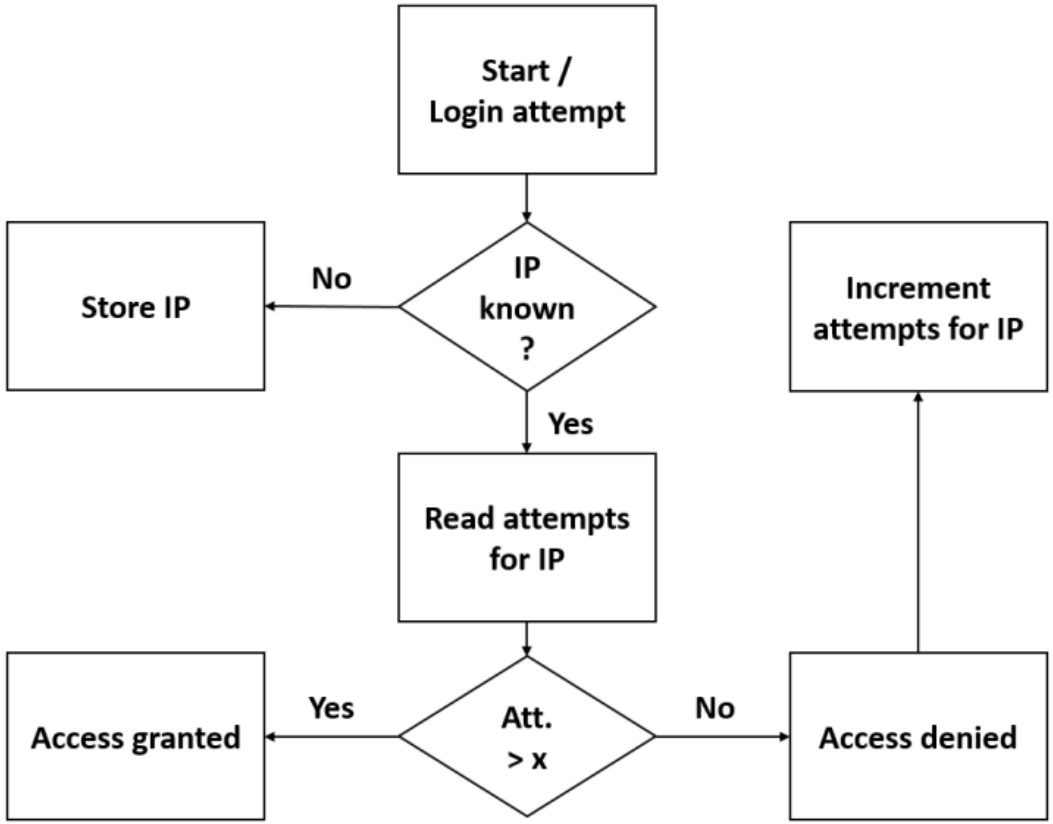


Observation Methods

Activity type	Example	Monitoring method
Authentication	*SSH* login attempt	
Terminal creation	Successful *SSH* login	*open*-system call
User input	Write commands in terminal	*read*-system call
Networking	Download file	Socket creation
Execution	Run downloaded binary	*execve*-system call

Port Collision Probability $p(ep, cc) = 1 - e^{(\frac{-cc^2}{2ep})}$

Intended Vulnerabilities



Application Scenarios

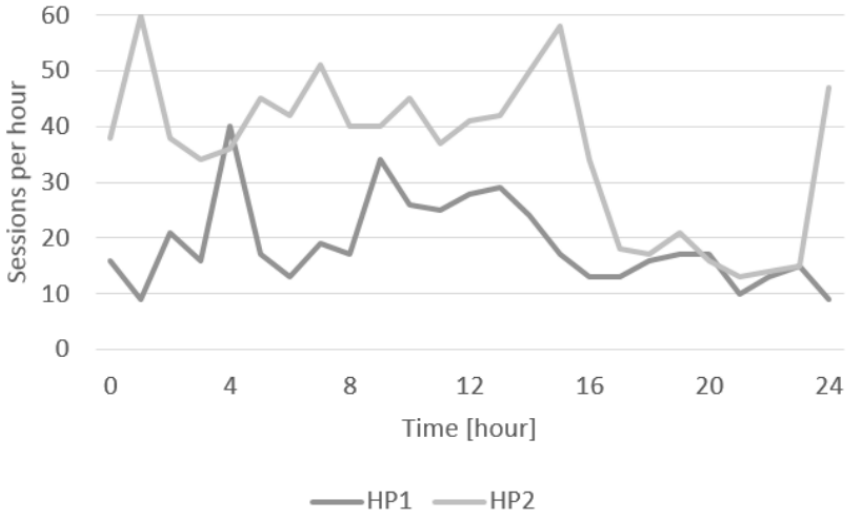
Falcom can be deployed as:

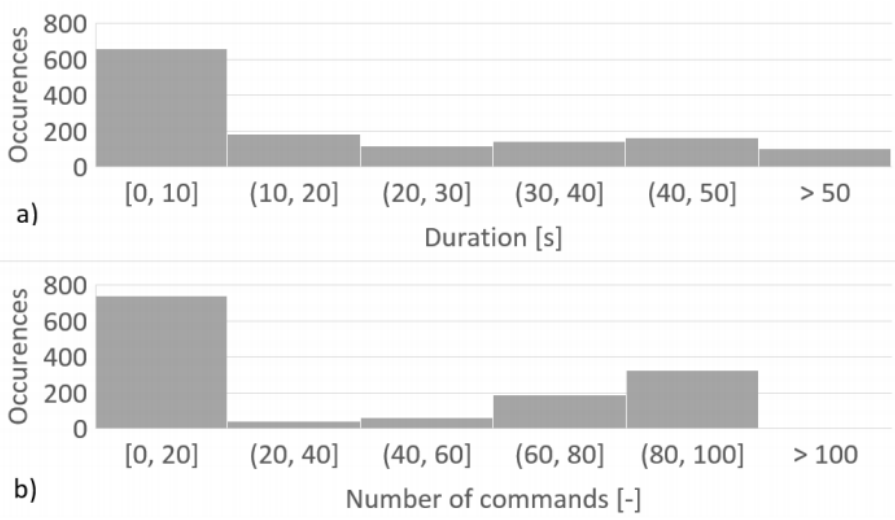
- Research Honeypot
  - Deployment with public IP address
  - Allows active research on observed activities
- Production Honeypot
  - Intrusion Detection and Monitoring
  - Capturing
- Malware Analyser
  - Packet Sniffing of traffic between attacker and C&C-Server

Experimental Study Overview (I)

Attribute	Value
Communication protocol	Telnet
Vulnerability	Weak password authentication
Deployment	University (HP1), web hosting (HP2)
Experiment duration	25 hours
Overall number of attacks	1366

Experimental Study Overview (II)





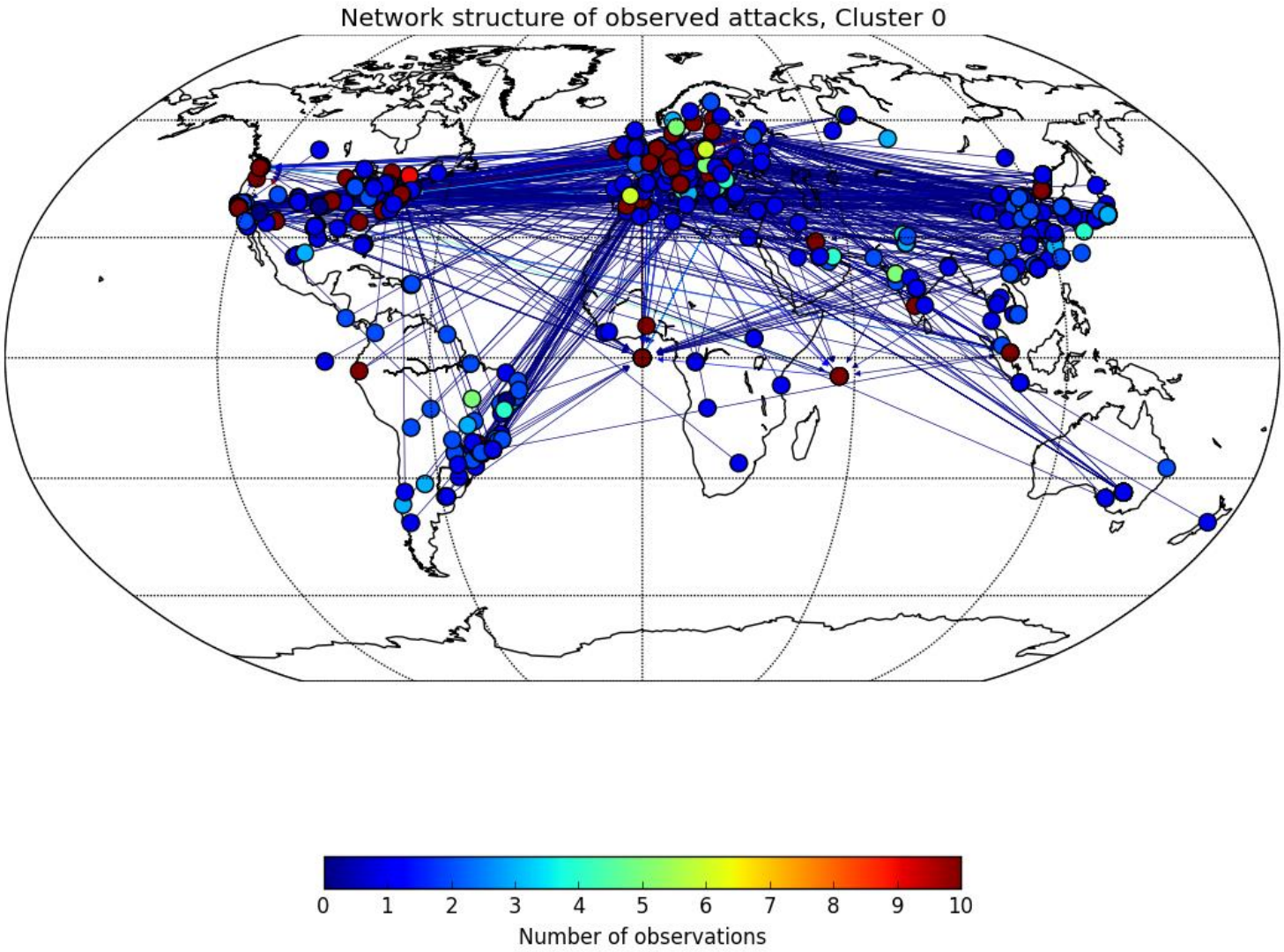
a) Distribution of durations

b) Number of issued commands

Experimental Study Overview (III)

Country	# sess.	By sess. [%]	By pop. [%]	By GDP [%]
Spain	665	57.38	2.16	2.16
US	110	9.49	14.28	33.37
China	89	7.68	61.52	33.37
Brazil	67	5.78	9.14	5.50
Hungary	65	5.61	0.43	0.46
Japan	65	5.61	5.55	8.95
Italy	43	3.71	2.66	3.68
Romania	21	1.81	0.86	0.78
Canada	17	1.47	1.54	3.02
Ukraine	17	1.47	1.86	0.61

Clustering


Network structure of observed attacks, Cluster 0
0
1
2
3
4
5
6
7
8
9
10
Number of observations

Summary

- Implementation and deployment of a high-interaction honeypot
- Novel approach with OpenWrt and Kernel Manipulation
- Deployment on 2 servers with different use cases
- Data evaluation, i.a. with various clustering algorithms

Future Work

- Improvement of obfuscation techniques
- Bug Fixes
- Integration in deceptOS

Thank you!

Daniel.Krohmer@dfki.de