Overview Honeynet Project
DataFest 2018

München, 2018-03-05
Our reference:

Document Scope

The scope of this document is to give a general overview of the Honeynet project in 2014/15 at TÜV SÜD.

Content

1 Project Description and Scope

The Honeynet project of TÜV SÜD in 2014/15 was intended to simulate the IT infrastructure of a water works in a small Bavarian city. A honeynet is a decoy network designed to attract attacks, allowing detailed analysis of the access and attack methods to be conducted. The deployed structure was a so-called “high interaction honeynet”, consisting of real hard- and software components, as well as simulated ones.
The security measures taken corresponded to the current levels found in industry. To ensure a realistic system structure and authentic security precautions, TÜV SÜD’s experts worked with representatives from the utilities sector during development and implementation.
Industry 4.0 presents companies with the challenging task of having to reconsider their security policy from scratch. Increasing digitization, standardization and interconnectivity makes infrastructures and industrial facilities more vulnerable and opens up new “opportunities” for possible misuse and abuse – from espionage to sabotage.

The main goal was to proof that all industrial and critical infrastructures are prone to cyber-attacks, and to analyse the structure of potential attacks, as well as the behaviour of potential attackers. Network log data was collected between 2014-08-14 and 2015-05-05.

2 Potential Questions

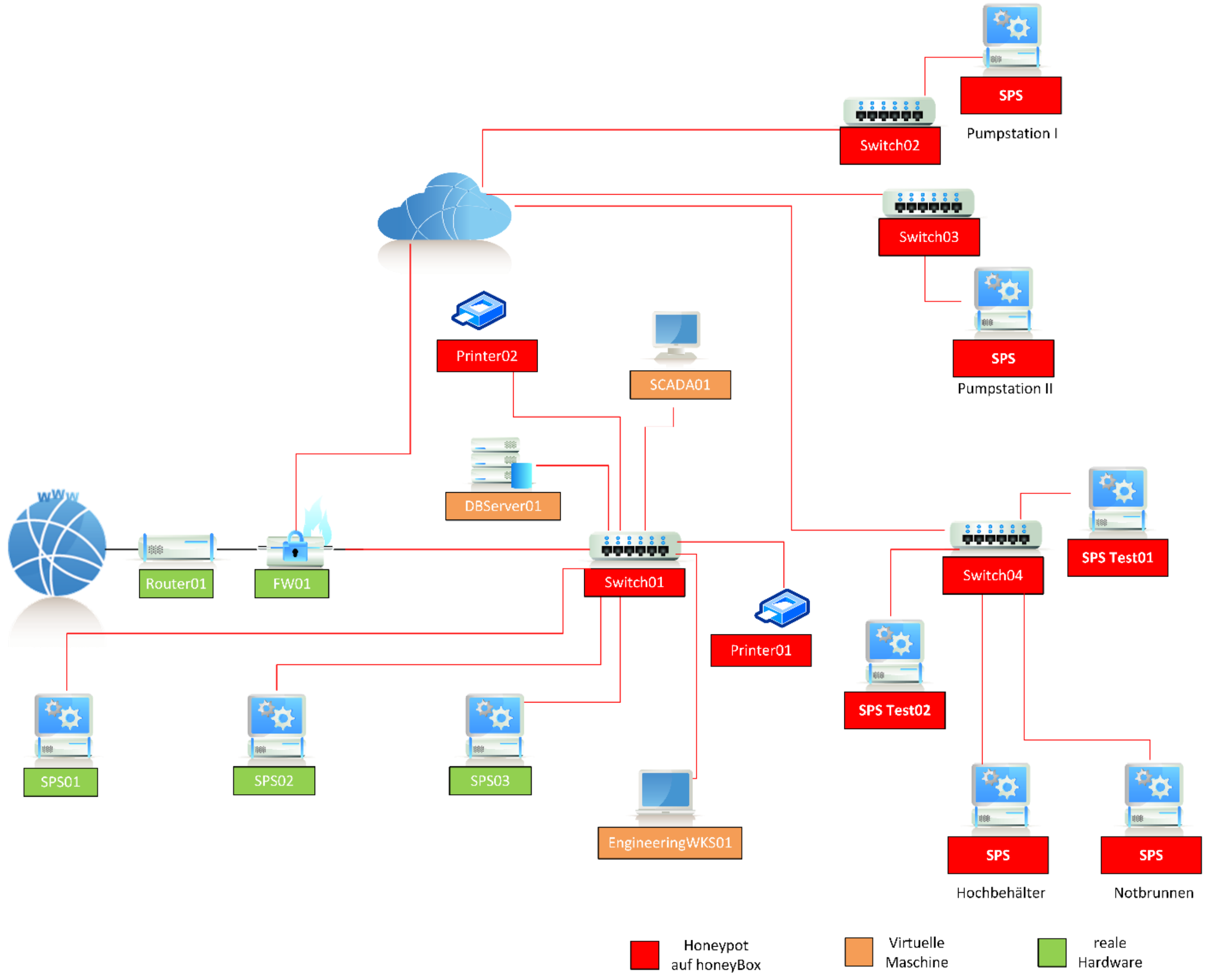
The following questions could be of potential interest:

1) Where do the attacks come from? Can specific patterns over time and/or location be identified?
2) How does the number of attacks develop over time?
3) Can more events like the ones described in Section 4 be found?
4) Can we learn something, taking into account the protocols used?
5) Can methods like some form of outlier detection for instance help us in identifying problematic or dangerous patterns or behaviour?

This list is far from being exhaustive. The purpose of these questions is to provide you with a starting point for your analysis. Please feel free to analyse different aspects – whatever you feel could give some interesting insights.

3 Short Description of the Honeynet Setup

The following figure depicts the architecture of the deployed honeynet.



Datum: 25.11.2014

Figure 1: Architecture of the honeynet for the simulation of a control unit of a water works; without management systems. Red units belong to the honeypot on a honeyBox, orange are virtual machines, and green is real hardware.

The table in the appendix contains some information on components which were accessible from the internet with their respective IP addresses.

3.1 Internet Connection

The honeynet was connected to the internet over a static 2-Mbit connection provided by M-Net. 2 x 16 static public IP addresses were assigned. The intention behind the splitting in two blocks was to let the existence of several locations/sites appear more realistic.

3.2 Victim Network

The upper part shows the victims (honeypots), which are either physical entities, virtual machines, or honeypots on a honeypot-appliance (honeyBox). In order to establish a realistic scenario several victim systems were deployed:

- Siemens S7-1200 SPS (Speicherprogrammierbare Steuerung, real)
- Siemens S7-1200 SPS as Modbus/TCP IO-Devices part of the system (on honeyBox)
- 1 Siemens S7-1200 SPS (honeypot on honeyBox)
- 1 Network switch (real)
- 3 Network switches (honeypots on honeyBox)
- 2 Printing servers (honeypot on honeyBox)
- 1 Windows 7 Workstation (Engineering, virtual)
- 1 Windows 7 Workstation (database for long-term measurements, virtual)
- 1 Windows Server 2008 R2 (SCADA, virtual)

Please note, that Modbus/TCP was used as internal communication protocol. This internal communication is not part of the provided log data.

3.3 Administration Network

An administration network was set up, separate from the victim network and not depicted above. It consisted of the following components:

- Firewalls (Layer-2, Layer-3 and VPN-Gateway for administration)
- Switch
- Server (for collection of log data, data analysis, etc.)
- Server (hosting the virtual machines and connected to the physical emergency switch of the internet connection)
- NAS for data backup of all relevant systems

3.4 Structure of the Water Works

The simulated water works infrastructure consisted of several locations with varying purposes.

3.4.1 Elevated Reservoirs (Hochbehälter)

The simulated structure contained two elevated reservoirs with a capacity of 3000 m^3 each, which were connected to each other, and had a shared pipeline to the general water network. This connection also yields the emergency supply (Notversorgung). In addition, in case of a necessary revision the elevated reservoirs can be emptied using a specific slider (Entleerung). Figure 2 shows the Software UI for this system as an example.
Flow rate, pressure, and conductivity were measured. Pressure and conductivity were also monitored for exceeding threshold values. A security alarm for entering the area of the elevated reservoirs was part of the system, too.

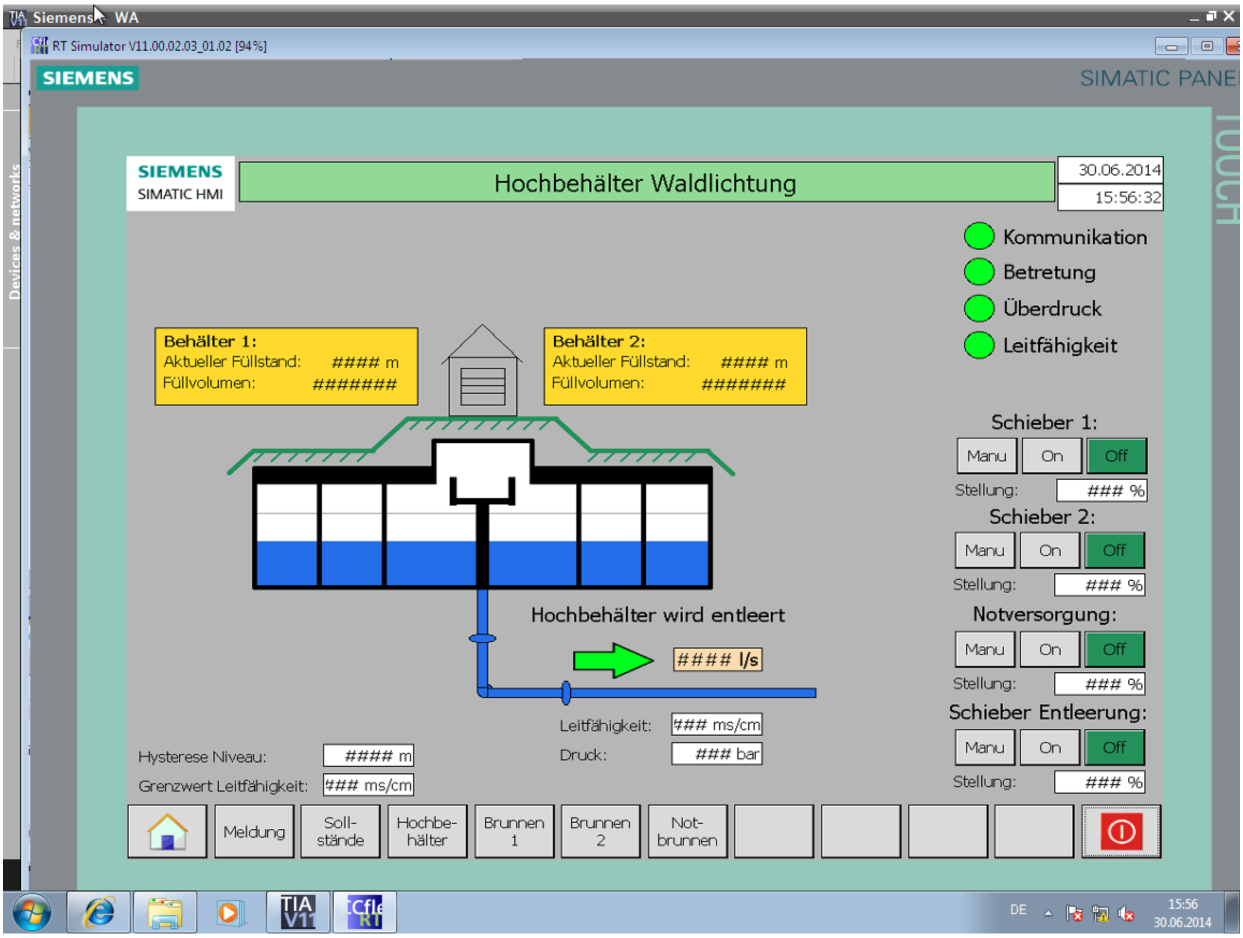


Figure 2: SCADA UI for the elevated reservoirs (Hochbehälter).

3.4.2 Water wells (Brunnen)

Three deep wells (Brunnen 1 and 2 as normal ones, + Notbrunnen as emergency well) were part of the system. Water could be taken from them using a pump and supply it directly into the water network. A slider can separate the respective well from the water network.

Different error situations affecting the pump, and the sliders are monitored. A security alarm for entering the area of the wells was also part of the system.

4 Forensics – Previous Analysis

The purpose of this section is to provide some general insights into the provided traffic data and some examples of previously conducted analysis are given.

4.1 General Remarks

The data contains only external communication of the honeynet, i.e., only incoming connections from external IP addresses are considered.

So-called *port scans* are also part of the data. Some providers do scans on a regular basis to identify open ports of a system. Patterns like having several requests coming from a single IP address targeting several different ports in a short period of time can identify such a scan. The scan itself is not necessarily a problem, but of course exploitation of the gathered information can be.

4.2 Communication Protocols

Standard

Most requests used standard web protocols, such as *HTTP* and *HTTPS*. The following standard protocols are of special interest.
SNMP (Simple Network Management Protocol) is a network management protocol. It allows to monitor and control network units (e.g., routers, switches, etc.) from a central unit. Usually this protocol is not visible from the internet. In our case this protocol was intentionally made accessible to potential attackers to simulate a misconfiguration of the simulated infrastructure. This misconfiguration is a realistic scenario for such control systems.
VNC (Virtual Network Computing) is protocol specific for remote maintenance. Such remote accounts are especially risk-prone and can be abused by potential attackers (which is often the case).

Industrial

Industrial protocols, e.g., *Modbus/TCP*, *S7comm* and *S7Comm+* were also used to access the honeynet.
S7 Communication (*S7 Comm*) is a proprietary protocol from Siemens, which is used for communication to the SPS. It is used for programming these units, as well as for data exchange between different SPS units, and for accessing SPS data from SCADA systems for instance.

4.3 Examples of Critical Accesses

By attempted attack we mean the attempt to manipulate the infrastructure of the honeynet.
By successful attack we mean the successful manipulation of the infrastructure of the honeynet.

4.3.1 Detailed Information Retrival via S7comm+

On 2015-04-03 between 13:25 and 14:03 UTC 20 single connections were recorded coming from the area of Rodalben (Rheinland-Pfalz). The accesses came from an account provided by Kabel Deutschland over a Wifi connection, probably using a notebook manufactured by Lenovo or Dell running Windows (most likely) as operation system. Target in the honeynet was a SPS control unit (192.168.0.12) by using the Siemens software TIA for the connection. A unique identification of the attacker was not possible.

Read as well as write requests were recorded, but they are probably due to the TIA Portal functionality and are not necessarily manipulation attempts. Information regarding the control device as well as the control software were retrieved.

4.3.2 SNMP Denial of Service

There were several attempts (on 2014-12-24, 2014-12-26 until 27, 2015-01-01 until 03, 2015-01-23 until 24) using a set-request to turn off the routing functionality of the honeynet infrastructure. The attackers tried to set the value for ipForwarding in the Management Information Base (MIB) of the respective components to “notForwarding”, and the value of ipDefaultTTL to 1. Targets were the honeynet devices SPS01, SPS02, SPS03, SWITCH02, SWITCH03, and SPS-Test01. Table 1 gives some details on the attacks.

If such an attack is successful the affected routers do no longer forward packages which leads to severe network traffic problems.

IP Address	Country	Host Name
6.123.4.24	United States	Unknown
8.8.4.4	United States	google-public-dns-b.google.com
66.35.59.249	United States	isc.sans.org
194.41.12.17	Poland	sis.sejm.gov.pl

Table 1: SNMP Denial-of-Service attack attempts

Table 1 shows that IP addresses of well-known companies and / or institutions were used to hide the source of the attack (see also the next subsection 4.4).

This recorded attack was part of a world-wide cyber-attack which was recorded around September 2014 for the first time[1]. So, the honeynet was not specifically chosen as target but visible and therefore included in the attack.

4.3.3 S7 Comm Write Access

The attack happened on 2015-03-27 between 13:17 and 13:39 UTC and came from a Ukrainian IP address (213.108.73.187). The long duration of roughly 20 minutes leads to the conclusion that it was not an automated attack. Target was the SPS01 device via the industrial Modbus/TCP protocol. First the attacker accessed the web interface of the SPS device looking at the available sites. After that, he or she tried to overwrite the system variables DB1.DBX 0.0-2 using the function Write Var.

[1] See https://isc.sans.edu/forums/diary/Google+DNS+Server+IP+Address+Spoofed+for+SNMP+reflective+Attacks/18647

4.4 Concealing Techniques

Attackers used various techniques to conceal or hide their behaviour or themselves:

- *Anonymous Hosting Services*, where server hosts promise to not store any data about their clients, i.e., it is hard for prosecutors to find out who rented a specific server in case of an abuse
- *VPN* (Virtual Private Network) services, where providers offer encrypted connections for their client's data
- *Tor*, which is a network for anonymization of connection data; by re-routing the encrypted data it is almost impossible to identify the true source
- *Spoofed IP addresses*

5 Main Project Findings – Management Summary

The following statements are also valid for small, unknown, and mediocre companies operating industrial controlling or automation facilities.

- Accesses to infrastructures of controlling or automation facilities come from all over the world.
- Standard protocols, e.g., HTTP, are used, as well as industrial protocols, like Modbus/TCP, for instance.
- Being accessible from the internet is sufficient to attract potential attacks. Statements like “No one really cares about us.” are therefore not valid.
- Even companies that have not been chosen on purpose can become victims of cyber-attacks. In addition, companies that are under observation can be deliberately attacked at a later point in time.
- Potential attackers employ techniques to cover their true intentions. Available tools or services are used to feign IP addresses of well-known companies or institutions (including public ones). Hence, identified IP addresses cannot be trusted in general.
- Operators of industrial networks are therefore forced to rely on alternative techniques and support of experienced security experts when setting up security monitoring strategies. The security monitoring needs to cover industrial protocols.

Appendix

IP Adresses of Systems Accessible from the Internet

System	Public IP	Internal IP	Type	Model	TCP	UDP	TCP	UDP
Main Location / Hauptstandort								
PROXY01		192.168.0.5	Real (VM)	Apache2 Reverse Proxy for HTTPS to HTTP conversion	8012 8013 8015			
SPS01	212.114.128.132	192.168.0.12	Real	Siemens SPS S71200	80 102 443	161	(80) 443 ANY	ANY
SPS02	212.114.128.133	192.168.0.13	Real	Siemens SPS S71200	80 102 443	161	(80) 443 ANY	ANY
SPS03	212.114.128.135	192.168.0.14	Real	Siemens SPS S71200	80 102 443	161	(80) 443 ANY	ANY
SCADA01	212.114.128.131	192.168.0.20	Real (VM)	Windows Server 2008 R2	80 102 5901		5901	
SVENGINEERINGWKS01	212.114.128.139	192.168.0.25	Real (VM)	Windows 7			5901	
DBSERVER01		192.168.0.30	Real (VM)	Windows 7				
PRINTER01	212.114.128.140	192.168.0.100	HP	tmpl_for_hp_lj	21 23 80 280 515 631 9100	161 427		
PRINTER02	212.114.128.141	192.168.0.101	HP	tmpl_for_hp_lj	21 23 80 280 515 631 9100	161 427		
SWITCH01	212.114.128.142	192.168.0.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024		
Pump Station 1 / Pumpstation 1								

SPS_PUMPSTATION01	212.114.130.99	192.168.13.2	HP	my_tmpl_for_plc_1200_with_modbus Queried by SPS01, Part of the simulation	80 102 443 502	161		
SWITCH02	212.114.130.100	192.168.13.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024	80	ANY
Pump Station 2 / Pumpstation 2								
SPS_PUMPSTATION02	212.114.130.101	192.168.14.2	HP	my_tmpl_for_plc_1200_with_modbus Queried by SPS01, Part of the simulation	80 102 443 502	161		
SWITCH03	212.114.130.102	192.168.14.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024	80	ANY
Elevated Reservoir and Emergency Dwell / Hochbehälter und Notbrunnen								
SPS_HOCHBEHAELTER01	212.114.130.102	192.168.15.2	HP	my_tmpl_for_plc_1200_with_modbus Queried by SPS01, Part of the simulation	80 102 443 502	161		
SPS_TEST01	212.114.130.104	192.168.15.10	HP	my_tmpl_for_plc_1200_with_modbus	80 102 443 502	161	502	161
SPS_TEST02		192.168.15.11	HP	my_tmpl_for_plc_1200_with_modbus	80 102 443 502	161		
SPS_BRUNNEN_NOT	212.114.130.109	192.168.15.12	HP	my_tmpl_for_plc_1200_with_modbus Queried by SPS01, Part of the simulation	80 102 443 502	161		
SWITCH04	212.114.130.110	192.168.15.254	HP	tmpl_for_industrial_switch	23 80	123 161 1024	80	ANY

Legend
Real: real hardware; Real (VM): virtual; HP: honeypot on honeybox