http://dx.doi.org/10.14236/ewic/ICS2018.8

Investigating Current PLC Security Issues Regarding Siemens S7 Communications and TIA Portal

Henry Hui, Kieran McLaughlin
Centre for Secure Information Technologies (CSIT)
Queen's University Belfast
{hhui01,kieran.mclaughin}@qub.ac.uk

Programmable Logic Controllers (PLCs) are the essential components in many Industrial Control Systems that control physical processes. However, in recent years the security flaws of these devices have come under scrutiny, particularly since the widely discussed Stuxnet attack. To help the industry state-of-the-art to move forward and to provide information required to improve the security for these controllers, this work investigates potential exploits of the Siemens S7-1211C controllers and the Totally Integrated Automation (TIA) engineering software. Using Windbg and Scapy, the anti-replay mechanism of the Siemens proprietary communication protocol, S7CommPlus, and the Profinet Discovery and Basic Configuration Protocol are found to be vulnerable. Attacks like session stealing, phantom PLC, cross connecting controllers and denial of S7 connections are demonstrated. The lack of authentication and consequent exploitation of the S7-ACK packet, an application layer packet for the S7CommPlus protocol, is highlighted as a key issue in this investigation.

Keywords: Programmable Logic Controllers, PLC, cyber security

1. INTRODUCTION

Industrial control systems (ICS) control important physical processes in critical infrastructures and various industrial environments. Programmable Logic Controllers (PLC) are one of the most crucial components in many such systems, as PLCs are the point of interaction between the cyber and physical world. Well known previous attacks that targeted PLCs, like Stuxnet, have demonstrated the security challenges faced by these devices. The industry has since attempted to improve the security of PLCs but the impact of these measures is often not widely understood, despite various attacks that took place post-Stuxnet. Moreover, there is a relatively small amount of information available in the research community on the security of state-of-the-art PLCs, firmware and programming environments. Therefore, to help improve the security of PLCs, and thereby ICS more generally, a study has been done to understand the vulnerabilities of current generation PLC technologies. Various experiments and testing has been conducted, from manual testing to reverse engineering using different tools. This paper presents a number of possible exploits against PLCs that were discovered and discusses future work that can be done to enhance security in the area. As Siemens is one of the leading vendors in the industry, the widely used S7-1211C controller, was the focus of this investigation. The potential exploits of the software that is used to program Siemens PLCs, Totally Integrated Automation, or TIA portal, and the protocol used between them, S7CommPlus, have been addressed. A particular focus of the presented experiments is the S7-ACK packet, an acknowledgement packet in the application layer, on which multiple exploits are demonstrated to effect to the integrity and availability of the PLCs and TIA portal. The following section will document the background of PLCs, Siemens' PLC ecosystems and other related research in the area.

2. BACKGROUND AND MOTIVATION

A PLC is a small industrial computer component used in ICSs to monitor and control physical processes. Generally, a PLC consists of several digital and analogue inputs and outputs, a processing unit, a memory module, and an interface to communicate with other devices in the network. Recent PLCs contain an Ethernet interface for communication. Custom logic is created by ICS operators via software, usually

proprietary to the hardware vendors, and can be uploaded to the PLCs through the Ethernet interface. A PLC program usually contains at least one organisation block and can include other function or data blocks. Each organisation block will be executed sequentially in a cycle. IEC 61131-3 (International Electrotechnical Commission, 2013) specifies the basic programming element and languages that vendors usually expand on. Communication protocols like Modbus TCP and Profinet are used to enable transmission of data via Ethernet between devices. However, when the vendors' proprietary software is used to configure or program a PLC, a proprietary protocol is generally used on top of the usual protocols.

2.1. Siemens PLC Ecosystem

Siemens PLCs can be programmed by TIA portal, which is the proprietary software developed by Siemens. The software can control, program or diagnose devices like PLCs, SCADA systems and Human-machine interfaces (HMI). Most communications that are initialised by TIA portal uses Siemens' proprietary protocol, commonly known as the S7CommPlus protocol.

There is a range of PLCs available from Siemens: S7-200, S7-300, S7-400, S7-1200 and S7-1500. The S7-200,300 and 400 PLCs are older PLCs that use the S7Comm protocol for communication without authentications. The S7-1200 PLC with firmware version 3 uses an older version of the S7CommPlus protocol, which adopts an anti-replay mechanism comprising only one anti-replay byte and a repeat of certain bytes for authentication. This work focuses on how TIA portal interacts with the S7-1211C PLCs with firmware version 4.1, which uses a newer version of the S7CommPlus protocol, the same as the S7-1500 PLCs. The S7CommPlus protocol runs on ISO on TCP (TPKT), and Connection Oriented Transport Protocol (COTP). There now follows a brief description of how an operator initialises a conversation with a PLC using TIA portal, and the way the S7CommPlus protocol works:

(i) The operator searches the network interface for connected devices.
(ii) TIA portal broadcasts a Profinet Discovery and Basic Configuration Protocol (PN-DCP) "Identify All" packet to the network.
(iii) All Siemens PLCs or devices will reply to TIA portal with a "Identify OK" packet.
(iv) TIA portal initialises TCP handshake with the PLC, and the PLC reply.
(v) TIA portal and PLC exchange COTP packet.
(vi) TIA portal sends the first S7 packet.
(vii) PLC replies with a packet containing a one byte and a 20-byte anti-replay challenge (S7 Challenge).
(viii) TIA portal replies with a packet containing an anti-replay byte and a 132-byte array, which is the anti-replay response (S7 response).
(ix) TIA portal sends packets with the action requested to the PLC, along with a 20-byte integrity check in every packet.

Figure 1: *The option in TIA portal to go online to a PLC*

If any S7CommPlus packets do not have correct anti-replay bytes or integrity check values, the other end of the connection will send a TCP reset packet and the session will be ended. By using TIA portal, the ICS operators can "go Online" to a PLC, as shown in Figure 1, which is the function in the TIA portal that allows the operator to connect to a PLC. An S7 session will be initiated and the operator can diagnose any problem related to the PLC, upload custom program, viewing real-time data from the PLC data blocks and configure communication between PLCs and other devices, etc. During the online period of the S7-1211C PLC, three packets are sent to the TIA portal during idle time specifying details and live status of the PLC, e.g. cycle time, memory usage etc. More information on the anti-replay mechanism is detailed in Section 3.

2.2. Related work

There are a number of publications that are related to the vulnerabilities of PLCs. However, most of them are related to an older controller, older PLC firmware version, or make claims with few supporting details provided. A discussion of the most relevant modern publications is now presented.

Lim et al. (2017) has documented an investigation on the Schneider Tricon PLC (Lim *et al.*, 2017). Using reverse engineering techniques, the general structure of the Tricon communication protocol has been identified and an attack that involved recalculating packet length, CRC and checksum are demonstrated. This attack will lead to device failure that requires a reset of the Tricon PLC, which could cause significant problems in a real ICS environment.

An SNMP scanner and a SOCKS proxy (Klick *et al.*, 2015) on a Siemens S7-300 PLC was proven possible by inserting code in the beginning of a scan cycle of the PLCs, just like Stuxnet. This vulnerability introduces a network backdoor on which attackers could send packets into the network through an outward facing PLC.

Password protection is usually provided by the vendors' proprietary software to secure PLCs. However, it has been shown that password

stealing, password reset and memory control attacks (Wardak, Zhioua and Almulhem, 2016) are possible in a Siemens S7-400 PLCs by replay attacks. An older publication (Sandaruwan, Ranaweera and Oleshchuk, 2013) also demonstrated the possibility of replay attack, man-in-the-middle (MITM) attack and authentication bypass attack.

A recent publication (Lv *et al.*, 2017) has proposed a way to decompile and map byte codes into PLC program instructions. This would allow an attacker to understand the details and processes that are running in an ICS. However, the PLC involved in the work is S7-200, which Siemens already listed as a phase-out product in 2013 (Industry Support Siemens, 2013).

Regarding publications dedicated to newer PLCs, a PLC worm (Spenneberg, 2016) has been developed and demonstrated, whereby malicious code can potentially be inserted into PLCs, without human interaction. This attack exploits the vulnerabilities of Siemens' proprietary protocol, S7CommPlus, used for the communication between TIA portal and the S7-1200 PLCs with firmware version 3. The information of the protocol architecture and processes for setting up PLC connections were also documented.

Cheng et al. (2017) has provided information on the anti-replay mechanism that is used in the newest version of the S7CommPlus protocol, as used in the firmware version 4 of the S7-1200 PLC and the most advanced PLC, S7-1500 (Cheng, Donghong and Liang, 2017). By using reverse engineering techniques, the authors identified three encryption processes occurring during the authentication process of the S7 protocol. However, only sparse details were provided on these three encryptions.

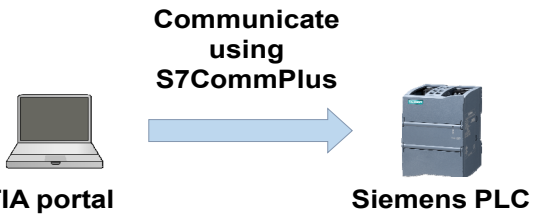

Figure 2: *The three targeted element in the Siemens Ecosystem*

2.3. Motivation

To the best knowledge of the authors, the information available in the research community related to the vulnerabilities and exploits of the PLCs are outdated or limited, although it is worth highlighting that this information is still relevant to current ICSs due to the long life-cycle of PLCs. As part of a broader program of research, the authors have been investigating in detail the anti-replay mechanism and surrounding processes used in the newest S7CommPlus protocol. During the initial phases of this investigation, a number of interesting security issues have emerged that will now be presented. There are some intrusion detection mechanisms proposed that have the ability to monitor S7-1200 traffics (Jardine *et al.*, 2016; Fauri *et al.*, 2017; Kreimel, Eigner and Tavolato, 2017), however, these works are also based on the older Siemens controller firmware and communication protocol. This paper therefore provides the information on the discovered vulnerabilities in the latest Siemens PLC ecosystems and how these may be exploited. The security issues for modern, state-of-the-art PLCs, beyond those identified in Section 2.2 are being addressed.

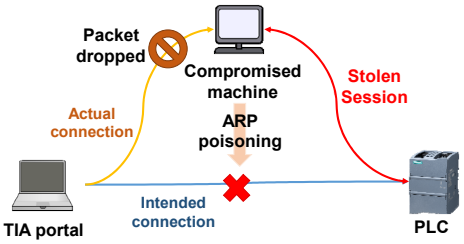

Figure 3: *Online session stealing attack*

3. VULNERABILITY AND EXPLOIT

This work only utilises well-known tools, like Scapy and Windbg, and information that is openly available via the internet. Competent attackers could easily obtain such information, especially if equipped with sufficient domain knowledge. The experiment was done in a testbed containing a switch, which connects two S7-1211C PLCs with firmware version v4.1, an engineering station and a "compromised" machine. TIA portal v14 is running in the engineering station.

Different vendors have different proprietary software and protocols which are responsible to perform or enable important controls of PLCs. Therefore the interaction between the three elements, as shown in Figure 2, are the prime target of this work. The flaw in the PN-DCP exchange, and the anti-replay mechanism enable most of the following exploits. It is important to mentioned that each vulnerabilities or potential exploits alone might not cause damage or disruption to the services of the connected ICS, however it may be the case that an enterprising attacker could combine any of the discovered issues as part of a broader series of impactful exploits.

3.1. Online session stealing

Operators can "go Online" to a PLC using TIA portal to control, diagnose, or upload custom logic to the PLCs. In order to send an S7 packet to perform a legitimate function in TIA portal, a 20-

byte integrity check must be calculated for every packet. However, it was discovered once a connection has been established, in order to stay connected to a PLC, a simple reply, with the byte "03 00 00 07 02 f0 00" (namely "S7-ACK" for the rest of this paper), to any packet sent by the PLC will allow the session to stay alive. Given that The S7-ACK packet is only a 7-byte packet, which lacks the 20-byte integrity check, and given the S7-1211C PLC only allow one S7 session in any given moment, one of the possible ways to exploit the S7-ACK is to steal the session between a TIA portal and a PLC. There are other ways on hijacking a session but for this work it is achieved by using MITM attack, by ARP poisoning for example, as illustrated by Figure 3. A Scapy script was developed to demonstrate it is possible to perform this attack both actively or passively. For active session stealing, the attacker can simply drop all the packets from the TIA portal and reply to any packet sent by the PLC with the S7-ACK packet. As the PLC only sent three packets during an idle session with no request to TIA portal, the S7-ACK packet would be enough to keep the session alive. On the other hand, passive session stealing looks for five, or sometimes four, packets that the TIA portal sent when the ICS operators "go Offline" to the PLC. The script would drop all these packets and send the S7-ACK instead – during which time the operator thinks TIA portal has gone offline. For both attacks, if the operators attempt to connect again, the PLC will reject the legitimate traffic from TIA portal and the operator would not be able to control the PLC as normal. Figure 4 shows the information from the PLC obtained by TIA portal after the attack was executed.

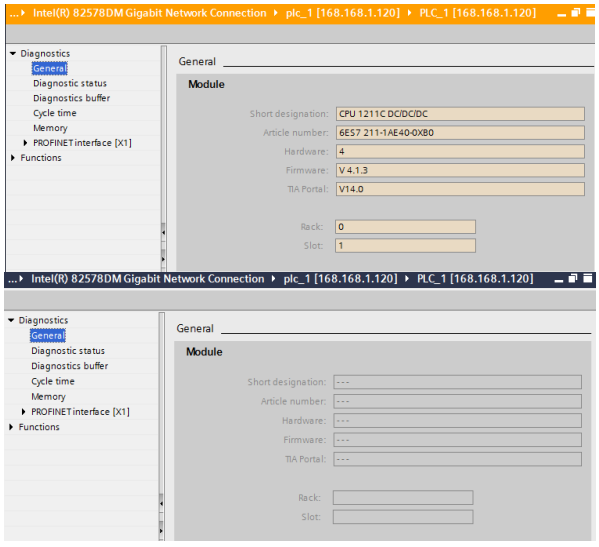

Figure 4: *TIA portal before and after session being stolen.*

3.2. Phantom PLC

It is possible to show the ICS operator a PLC that does not exist. Figure 5 shows "phantom_1" appear in the list of accessible devices in TIA portal.

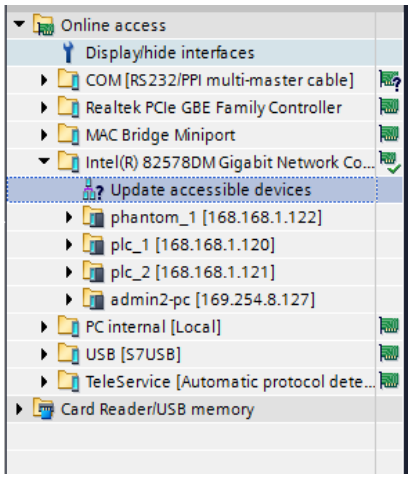

Figure 5: *The Phantom PLC appears in the list of the accessible devices.*

It is achieved by exploiting the PN-DCP protocol in the data link layer. PN-DCP is part of Profinet that is used for device discovery and identification, or to configure the device name and IP addresses. When the operator requests the list of accessible devices, the TIA portal will broadcast an "Identify All" packet to the mac address "01:0e:cf:00:00:00" and all Siemens PLCs will reply with an "Identify OK" packet. The payload of the PN-DCP "Identify OK" packet usually contains the name, IP address, subnet and gateway of a PLC. A special packet is crafted, and attacker could listen to the network and inject this packet to the network once the "Identify ALL" packet is broadcasted in the network. The impact of this exploit is limited, but it is possible to combine with other exploits, like cross connecting PLCs, to increase the chances of human error and causes misconfiguration of PLCs.

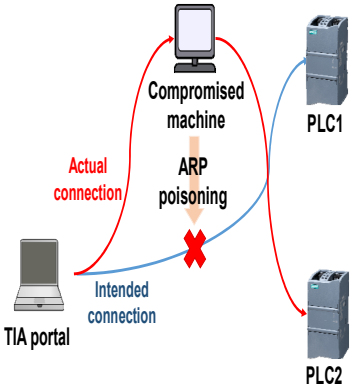

Figure 6: *Cross connecting PLC attack*

3.3. Cross connecting PLC

After the “Identify All” packet, a list of PLCs connected to the network are shown in the TIA portal. The operator can now access the information from the specific PLC in the network, for example “plc_1” with the IP address “168.168.1.120” in Figure 5. As mentioned in Session 2.1, the TIA portal will initiate a TCP session with the PLC. If an attacker performs a MITM attack between the TIA portal and PLCs, it is possible to redirect the TCP connection from “plc_1” to “plc_2”, while the ICS operator would still think the TIA portal is connected to “plc_1”. The operator may continue to configure and upload logic to “plc_1” but in fact the logic in “plc_2” would be changed instead, as shown in Figure 6. This could cause obvious significant failures in the relevant ICS. However, the operator could potentially spot abnormal information shown in TIA portal. As shown in Figure 7, there are differences in the IP address of the PLC that are shown in different pane of the UI in the TIA portal. In normal operations, it may be difficult to spot these differences as the IP address of “plc_2” is only shown if the operators explicitly check the detail of the Profinet interface, which is not required during normal operations. The different IP addresses are caused by different panes reading the same information from different sources; one IP address is read from the PN-DCP packet, while the other is from the S7CommPlus packet. It is possible to amend the S7CommPlus packet and the corresponding integrity check bytes to further disguise the attack.

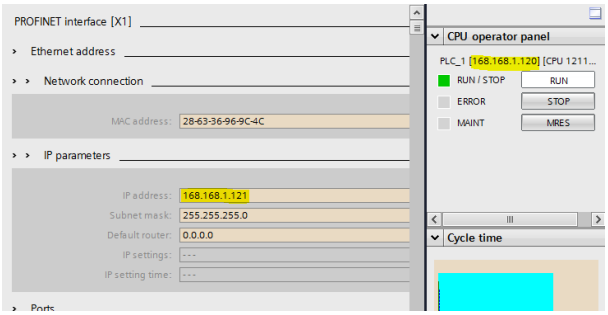

Figure 7: *Different IP addresses are shown in TIA portal.*

3.4. DoS on S7 Communication

From the result of the authors’ parallel research, it is possible to generate a S7CommPlus response packet with the correct anti-replay byte. The highlighted bytes in Figure 8 are the 132-byte array that changes every time a session is created. The two 16-byte values that are in the rectangles are the two anti-replay responses generated by two different encryption of the anti-replay mechanism first mentioned by Cheng et al. (Cheng, Donghong and Liang, 2017). A python script has been developed and the script can initialise an S7 session with the correct S7CommPlus response value to a PLC. However, instead of continuing the session by sending packets including control information, a S7-ACK packet is sent each time the PLC send a packet to the “TIA portal”. As mentioned in Session 3.1, if there is an active S7 session ongoing in the PLC, any legitimate TIA portal connection will be rejected. Although the affected PLC will continue its pre-programmed logic, there is no way to stop, re-configure or re-program that PLC, which could be critical on its own, or contribute to causing problems as part of a wider attack scenario. The S7 session can be stopped if the operator manually restarts the PLC, however the compromised machine in the network can simply initiate another connection before a legitimate request could be made after the restart. Figure 9 shows the error message displayed in the TIA portal if the operators attempt to connect to a PLC from a project that the operator created. This attack does not require the use of ARP poisoning and only uses a legitimate S7CommPlus connection.

```
0000010F  03 00 01 8c 02 f0 80 72  02 01 7d 31 00 00 05 42   .......r ..}1...B
0000011F  00 00 00 02 00 00 03 88  34 00 00 03 88 02 02 8e   ........ 4.......
0000012F  26 82 32 01 00 17 00 00  07 08 8e 09 00 04 00 8e   &.2..... ........
0000013F  0a 00 02 00 8e 0b 00 17  00 00 07 21 8e 22 00 05   ........ ...!."..
0000014F  de d0 cd b0 c8 fc 90 f3  1a 8e 23 00 04 82 10 8e   ........ ..#.....
0000015F  24 00 04 00 00 8e 0c 00  17 00 00 07 21 8e 22 00   $....... ....!.".
0000016F  05 da c0 d0 94 a0 e2 9b  c9 b6 8e 23 00 04 84 82   ........ ...#....
0000017F  01 8e 24 00 04 00 00 8e  0d 00 14 00 81 34 ad de   ..$..... .....4..
0000018F  e1 fe b4 00 00 00 01 00  00 00 01 00 00 00 b6 c9   ........ ........
0000019F  8d 18 44 81 02 b5 01 01  00 00 00 00 00 00 1a 73   ..D..... .......s
000001AF  08 1f 09 6b 42 bd 10 01  00 00 00 00 00 00 eb 76   ...kB... .......v
000001BF  21 45 d9 ac cd cb de f7  a4 cc 7d b6 3b f1 0a c4   !E...... ..}.;...
000001CF  bd 4b 51 42 96 f6 a1 cd  c5 77 d7 1f d2 4b 11 21   .KQB.... .w...K.!
000001DF  0e 87 81 d5 b2 17 e9 51  cb c6 b0 b4 d4 5f 98 b7   .......Q ....._..
000001EF  a9 ee 58 26 ca 8b d6 74  70 5d 53 d8 e5 01 80 90   ..X&...t p]S.....
000001FF  27 7e d9 f2 39 c3 c3 2e  31 e4 85 6a 5c 7e d3 68   '~..9... 1..j\~.h
0000020F  9e 2f 70 45 40 1f cd 35  77 51 4e 9a 0d 02 80 d6   ./pE@..5 wQN.....
0000021F  45 e5 73 2d aa fd 63 9f  e0 5c 43 83 82 0c 3c fe   E.s-..c. .\C...<.
0000022F  d8 a9 40 b5 0a 02 e2 29  02 60 f3 cd 29 5d 34 32   ..@....) .`..)]42
0000023F  36 6a 00 02 00 17 00 00  01 3a 82 3b 00 04 83 40   6j...... .:.;...@
0000024F  82 3c 00 04 83 00 82 3d  00 04 84 80 c1 40 82 3e   .<.....= .....@.>
0000025F  00 04 84 80 c1 40 82 3f  00 15 00 82 40 00 15 05   .....@.? ....@...
0000026F  32 3b 33 31 30 82 41 00  03 00 03 00 00 00 00 04   2;310.A. ........
0000027F  e8 89 69 00 12 00 00 00  00 89 6a 00 13 00 89 6b   ..i..... ..j....k
0000028F  00 04 00 00 00 00 00 00  72 02 00 00              ........ r...
```

Figure 8: *132-byte anti-replay array with two encryptions*

3.5. A COMBINED ATTACK

As mentioned above, an attacker could potentially combine any of these discoveries to cause a threat that is more difficult to be mitigated. For example, an attacker may start by initiating a session stealing attack as documented in section 3.1. However, TIA portal or the PLC will occasionally send a new ARP request. As the exploit is based on the MITM attack with ARP poisoning, an excessive use of ARP packet is required throughout the session to overwhelm the legitimate ARP request, which might draw attentions from the operators. Instead, when the attacker successfully steals the session and rejects the communication from the legitimate TIA portal, to achieve the same goal on keeping the session alive, the exploit documented in section 3.4 can be utilized. The stolen session can be terminated immediately, and a new S7CommPlus connection can be initiated, as demonstrated in Figure 10. This combined attack generates a much

smaller "footprint" in the network while the same goal is achieved to deny operators to go online to a PLC. Meanwhile it will be harder to detect or mitigate the threat when compared to the bare session stealing attack. This is just one of the possible attacks that involved the above exploits. In addition, if an attacker can obtain the information about the anti-replay mechanism and the 20-byte integrity check, which appears possible through reverse engineering, the possibility of the attacker to successfully execute an impactful attack after gaining access to the ICS network cannot be overlooked.

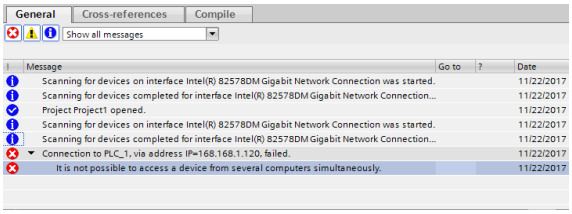

Figure 9: *PLC rejecting legitimate TIA portal connection*

4. DISCUSSION AND FUTURE WORK

All of the presented attacks require access to the ICS process control network. However, as demonstrated by Stuxnet and the Ukraine electric grid attacks, sophisticated attackers can eventually get access to such networks. Therefore, the traditionally "air-gapped" process control network will only provide a false sense of security to the operators. It is demonstrated that, by using various means, system operators may be misdirected towards configuring the incorrect PLC, or may be prohibited to connect to the PLCs using the TIA portal. The impact of such attacks would depend on the specific ICS, but a disruption of physical processes is a possible consequence. Network security measures, like firewalls and intrusion detection systems, could prevent some of the exploits mentioned in this paper, for example, detecting excessive or unknown ARP packets. However, exploits that utilise legitimate functionality, like the one mentioned in section

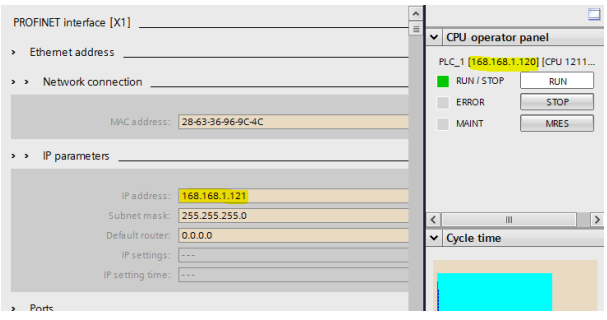

Figure 7: *Different IP addresses are shown in TIA portal.*

3.4 on an infected engineering station in the network, would still be successful since these communications cannot be blocked due to the genuine controls that TIA portal requires. An operator will not be able to connect to the affected devices and the compromised machine could initiate another session even if the PLC has been manually reset. Moreover, it was found that the S7-ACK packet, which does not require integrity or authentication details in the packet, has the potential to be exploited. A potential mitigation would be a firmware update of the PLCs, on which PLCs will disconnect any idle S7 session after certain period of time. However, if the attacker has the ability to replay packets with the correct anti-replay and integrity bytes, legitimate S7 connection could still be rejected if a new connection is initiated after the time-out.

Future work will include gathering more information on the features and vulnerabilities of the S7CommPlus protocol and similar protocols from different vendors. An investigation on how these vulnerabilities can be exploited will also be performed, especially those obtained from analysis of the TIA portal. Besides, the authors believe there are other ways to exploits the PN-DCP protocol, similar to a CVE that was recently published that affected most Siemens PLCs (Information Technology Laboratory, 2018).

A study will also be done on identifying ways to improve the security of the control systems. One potential way is to develop a realistic honeypot. The honeypot can, either actively (sniffing the network) or passively (waiting for a connection) identify whether a connection is from a legitimate TIA portal or an attacker's attempt to exploit legitimate functionalities. Ironically, most of the exploits mentioned in this paper, e.g. the phantom PLC, and the information obtained by reverse engineering the TIA portal is essential for creating a honeypot that behaves like a legitimate PLC. Furthermore, it would be beneficial for the industry to have an improved standard on the communication protocol that is responsible for the connection between engineering software and PLCs.

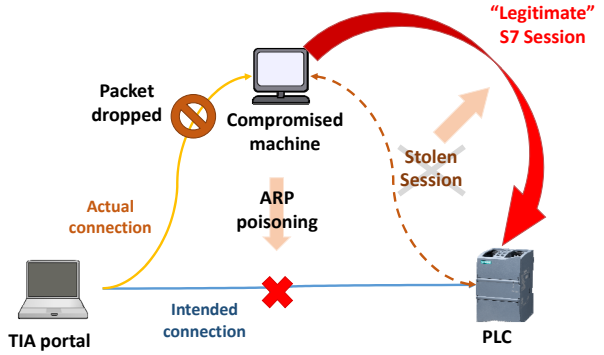

Figure 10: *Session stealing with "legitimate" S7 session*

5. CONCLUSION

This work presented several ways of exploiting the Siemens S7-1211C PLC, the proprietary protocol, and software, by using simple tools like Windbg and Scapy. Session stealing, phantom PLC, cross connecting PLCs and DoS of S7 communication has been demonstrated. Experiments have been carried out using the most current suite of PLC devices and software available, thus going beyond many published works that investigate now outdated technologies, e.g. the worm that can spread among PLCs (Spenneberg, 2016) and byte code de-compilation (Lv *et al.*, 2017). The exploits in this paper are not complicated in their own right but provide an overview on what can be done using only legitimate functionalities of the engineering software. In particular, the potential exploit of the S7-ACK packet has been uncovered in this work. Furthermore, it has been pointed out that general network security measures would be beneficial but not sufficient, especially if the attack involves the exploitation of legitimate functionalities. Potential mitigation like disconnecting idle S7 session will only have limited effect. Therefore, research has to be done on proposing a better way on securing the PLCs, including to improve the anti-replay mechanism and integrity check, and the ability to differentiate between malicious and legitimate session.

6. REFERENCES

Cheng, L., Donghong, L. and Liang, M. (2017) 'The spear to break the security wall of S7CommPlus', in *Defcon 25*. Available at: https://media.defcon.org/DEF CON 25/DEF CON 25 presentations/Cheng Lei/DEFCON-25-Cheng-Lei-The-Spear-to-Break-the-Security-Wall-of-S7CommPlus-WP.pdf.

Fauri, D. *et al.* (2017) 'From System Specification to Anomaly Detection (and back)', in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy - CPS '17*. New York, New York, USA: ACM Press, pp. 13–24. doi: 10.1145/3140241.3140250.

Industry Support Siemens (2013) *Announcement: Product Phase-Out for SIMATIC S7-200 - ID: 67598674*. Available at: https://support.industry.siemens.com/cs/document/67598674/announcement%3A-product-phase-out-for-simatic-s7-200?dti=0&lc=en-WW (Accessed: 19 March 2018).

Information Technology Laboratory (2018) *CVE-2017-12741*, *National Vulnerability Database*. Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-12741.

International Electrotechnical Commission (2013) *IEC 61131-3:2013 Programmable controllers - Part 3: Programming languages*, *International Standard*. Available at: https://webstore.iec.ch/publication/4552 (Accessed: 5 February 2018).

Jardine, W. *et al.* (2016) 'SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection', in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy - CPS-SPC '16*. New York, New York, USA: ACM Press, pp. 23–34. doi: 10.1145/2994487.2994496.

Klick, J. *et al.* (2015) 'Internet-facing PLCs as a network backdoor', in *2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015*, pp. 524–532. doi: 10.1109/CNS.2015.7346865.

Kreimel, P., Eigner, O. and Tavolato, P. (2017) 'Anomaly-Based Detection and Classification of Attacks in Cyber-Physical Systems', in *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*. New York, New York, USA: ACM Press, pp. 1–6. doi: 10.1145/3098954.3103155.

Lim, B. *et al.* (2017) 'Attack Induced Common-Mode Failures on PLC-Based Safety System in a Nuclear Power Plant: Practical Experience Report', in *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, pp. 205–210. doi: 10.1109/PRDC.2017.34.

Lv, X. *et al.* (2017) 'A technique for bytecode decompilation of PLC program', in *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. IEEE, pp. 252–257. doi: 10.1109/IAEAC.2017.8054016.

Sandaruwan, G. P. H., Ranaweera, P. S. and Oleshchuk, V. A. (2013) 'PLC security and critical infrastructure protection', in *2013 IEEE 8th International Conference on Industrial and Information Systems*. IEEE, pp. 81–85. doi: 10.1109/ICIInfS.2013.6731959.

Spenneberg, R. (2016) 'PLC-Blaster: A Worm Living Solely in the PLC', in *Black Hat USA 2016*. Available at: https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf.

Wardak, H., Zhioua, S. and Almulhem, A. (2016) 'PLC access control: a security analysis', in *2016 World Congress on Industrial Control Systems Security (WCICSS)*. IEEE, pp. 1–6. doi: 10.1109/WCICSS.2016.7882935.