Modern age burglary

March 15, 2010

Kevin de Kok - Jeroen Klaver
kevin.dekok@os3.nl - jeroen.klaver@os3.nl

Supervisor: Tjerk Nan

University of Amsterdam
System and Network Engineering

Abstract

Until recently alarm systems where connected mostly through the public telephone network to their control room. This set up changed because of the wide availability of Internet and VoIP. The protocols used on the Internet are not designed with security in mind. The connection between the alarm system and the control room connected over the Internet could be abused by the known flaws. The approach to research this is done by capturing traffic from different events and by analysing the traffic. Datasets are created from the captured traffic, those sets contain traffic to trigger different events from the alarm system by replaying them to the control room. The result is that it's possible to trigger different events by replaying traffic to the control room. The conclusion is that the protocol was not designed with security in mind and can be abused for burglary without getting notified by the control room.

Contents

1 Introduction **5**
1.1 Description . . . 5
1.2 Research question . . . 5
1.3 Scope . . . 6
1.4 Related work . . . 6

2 Overview **7**
2.1 PSTN-2-IP . . . 7
2.2 Network setup . . . 7
2.3 Standards . . . 8
2.4 Approach . . . 9

3 Packet analysis **10**
3.1 General . . . 10
3.2 Registration . . . 11
3.3 Heartbeat . . . 13
3.4 Activating alarm . . . 13
3.5 Deactivating alarm . . . 14
3.6 Triggering sensor . . . 16
3.7 Different account numbers . . . 16
3.8 Decoding . . . 17
3.9 Standards . . . 18

4 Attack vectors **20**
4.1 General . . . 20
4.2 Activating and deactivating the alarm . . . 20
4.3 Activating and triggering the alarm . . . 21
4.4 Triggering alarm sensor from a disabled alarm . . . 22
4.5 Brute force attack . . . 22
4.6 DoS attacks . . . 23

5 Impact **24**
5.1 Coverage . . . 24
5.2 Improvements . . . 24

6 Conclusion **26**

7 Future work **27**

8 Acknowledgements **27**

A Overview Activating and deactivating the alarm **28**

B Overview Activating and triggering the alarm **29**

C Overview Triggering alarm sensor from a disabled alarm **30**

D bruteforce.py **31**

1 Introduction

1.1 Description

Until recently alarm systems where connected mostly through the public telephone network to their control room. This set up changed because of the wide availability of Internet and VoIP. A lot of Dutch ISPs provide Internet packages containing an Internet connection and VoIP. This combination is much cheaper then having the telephone line separated from the Internet connection. This is the main reason users decide to switch to VoIP and unsubscribe from their separate telephone connection. To communicate between the alarm system and the control room over the Internet a transceiver is needed. This device emulates the telephone signal from the alarm system over the Internet to the control room. The transceiver is plugged into the alarm system and is connected to a switch or router in the local network.

The old telephone network is not easy accessible, the reason for this is that the network is controlled by one company. To eavesdrop on this communication the line should be physical accessible. The connection between the telephone and the endpoint at the telecom company is point-to-point and this makes the telephone network private.

The Internet on the other hand is public available and is autonomous. This makes it easier to eavesdrop on the communication between hosts. The protocols that are used on the Internet where not developed with security as primary concern. The combination of the Internet and the lack of security in the protocols used creates new threats on the communication of the alarm system.

1.2 Research question

Our main research question is:

Is it possible to perform a burglary without getting noticed by influencing the communication between the alarm system and the control room?

Sub questions:

- Which attack vectors that targets communication can be used to bypass the alarm system?
- What could be the impact if alarm systems over IP-based networks are vulnerable for different attack vectors?
- Which improvements can be made if alarm systems over IP-based networks are vulnerable for different attack vectors?

1.3 Scope

The research will be focused on network traffic analysis between the transceiver and the end node at the control room. From the analysis on the traffic possible attack vector will be described.

Inside of our scope:

- Focussing on communication between the *PSTN-2-IP transceiver* and the end node at the control room.
- Theoretical research of the impact from the possible vulnerabilities.
- Research to the possible improvements if there are vulnerabilities.

Outside of our scope:

- Obtaining control over the alarm system or the control room.
- Attacking the hardware of the alarm system(hardware components).

1.4 Related work

There is no previous research done on the subject of alarm communication over IP. The systems using IP are new and the manufactures are keeping most of the information secret.

Research is done on the subject of reverse engineering network protocols. The paper Discoverer: Automatic Protocol Reverse Engineering from Network Traces [1] describes automated protocol reverse engineering. The techniques mentioned in this document describes some steps about how to do reverse engineering. Most of the other related research comes down to what is mentioned in this paper.

2 Overview

This section gives an description of the components used in the research. First some information about the transceiver that is used to connect the alarm system to the Internet. Second is the network setup that was used during the research. Last is the approach we took during the research.

2.1 PSTN-2-IP

The device that is used to connect the alarm system to the Internet is called "PSTN-2-IP" and is manufactured by Alphatronics. This device is placed in the casing of the alarm system, since there is a sabotage protection on the casing the device can not be reached. The transceiver has two connections: a PSTN connection to the alarm system and an Ethernet connection to connect the device to the Internet.

The PSTN-2-IP needs to be configured using a web interface where all the device settings can be found. The local IP address, the IP address from the control room, network port usage and the account number are configured in the web interface. The device has a hardware switch that can be used to turn off the web interface, in the situation that this research was done the web interface was enabled. Also the default username and password were not changed so it was easy to take a look at the interface.

The transceiver is communicating to the alarm system using the old PSTN protocol. This way the alarm sees no difference between the old and the new situation. The protocol used between the transceiver and the alarm is in the SIA-format [2]. This standard is created by the Security Industry Authority (SIA) and is world wide used for burglar alarm communication over PSTN. When the transceiver receives a message from the alarm system it will send an acknowledgement. The transceiver will not wait for the control room to get an acknowledgement.

2.2 Network setup

To be able to capture the network traffic between the alarm system and the control room the network setup needed to be changed. The new situation can be seen in figure 1. To be able to capture the traffic from the alarm system to the Internet a hub is placed. The alarm system, the router and the packet analyser are connected to that hub. The hub will send all traffic it receives to all the ports and thereby the packet analyser can capture the network traffic. The packet analyser is also connected to the router for remote management via a second interface. The connection between the alarm system and the control room is established over ADSL[1] line.

Ubuntu Linux is installed on the packet analyser. The reason to use Linux is that the software that is needed to perform the research is available on this

[1] http://en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line

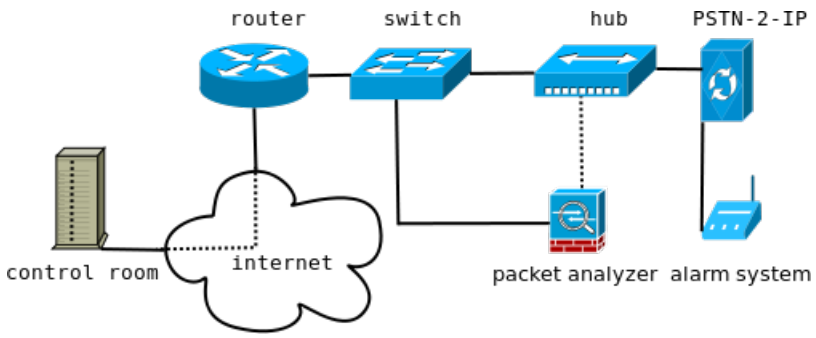

Figure 1: Network setup of experiment

platform. Packet capturing is done with the tool *tcpdump*[2]. A snaplen of 0 is chosen to capture the entire packet. Restructuring of packets is done with *scapy*[3] and *editcap*[4]. Replaying the packets is also done with scapy.

2.3 Standards

There are some standards that apply to alarm communication over IP. The European Union has a standard called NEN EN-50136 1/2 that describes which type of security levels can be applied. The standard also describes which security measurements need to be taken at the different levels. Since this standard is not publicly available this document could not be retrieved. In the Netherlands the alliance of the safety and security organizations has released a guideline for alarm over IP communication [3] based on the NEN. The guideline is inspired by the NEN and describes how the measurements should be done and what is demanded. At the level for low risk like homes and small shops is defined that nothing needs to be done for information security. At higher levels the data tampering should not be possible. At the highest level the data should be unreadable.

The communication over IP for alarm systems has not been standardized internationally. There are some standards around that are made by local organizations. In the Netherlands VEBON[5] is an organisation for safety and security solutions (fire and burglar alarms) that publicised a standard for alarm communication over IP called Vebon IP protocol [4]. This standard was first completed on 25 August 2006 and later revised and the latest version is from January 2007. In America there is a similar standard called [5] that has been developed by SIA (Security Industry Association) that has been publicised in 2007. SIA is also the creator of the protocol that was used over the PSTN lines.

[2] http://www.tcpdump.org/tcpdump_man.html
[3] http://linux.die.net/man/1/scapy
[4] http://linux.die.net/man/1/editcap
[5] http://www.vebon.org

The standard still uses the SIA-format to transfer the data to the control room.

Both standards define that data should be encrypted using 128 bit AES encryption. The key is exchanged using 1024 bit RSA. To fill out the possible empty space in the packet random padding is used. At the end a hash is used for verification, the hash functions that are used are CRC-16 and SHA1.

2.4 Approach

At first the research was approached as a blackbox, trying to look at the system with only information from the outside. This approach let to the problem that it was hard to identity parts in the found payload. Because the research was running to a dead end it was decided to try if the control room could be involved. The control room was willing to help with the research and provided test accounts. The test account made it possible to test an event with different accounts. The control room was also willing to verify the events from the alarm system.

3 Packet analysis

This section describes the analysis of the traffic that is send between the alarm system and the control room. The payload of the packets that were captured was not recognised by the tools that where used. Therefore an analysis of the payload was needed to get more information about the messages that where send across the wire. The payload showed that it consisted out of 2 parts, the first part is referred as the header and the second part is specific for events. The content of the payload is described in the following order. First the header and acknowledgement are described. Followed by the analysis of different events.

3.1 General

This section displays an overview of the header and the acknowledgement that was found in the payload.

3.1.1 Header

When analysing the packets it became clear that the payload at the begin was following a pattern, this is displayed in table 1. The table describes what can be found at which byte location of the payload. At some bytes there is a difference between packets, these differences are slit up using a "|". This is seen at byte 5 where a difference is in packets send from the control room or the alarm system. Byte 4 is the length of the payload, which was discovered when the hexadecimal value was converted to a decimal value. Since the packets have variable length this byte can change for every packet.

At other positions there are multiple differences and similarities but what the values mean is not known. For example at byte 17 to 21 there is a number of hex value 0x85 after each other. This could be padding data to fill out a field. This could also be a separation between fields or data. There is also a link between what is send by the alarm and what is send by the control room. At byte 14 the alarm system always has value 0xb4 and the control room sends back that value at byte 16 in the acknowledgement.

3.1.2 Acknowledgement

The acknowledgements that are send back from the control room to the alarm system are always the same. There are two kind of acknowledgements send from the control room that have a minimal difference. The payload of the acknowledgements is displayed in table 2.

It is not clear why there are differences in both of the packets. An analysis is done to see if recognizable patterns about which kind of acknowledgement are used. No patterns in time or message response were recognized. The differences seems to appear at random moments and we can not predict when the payload contains 0x85 or 0x00.

Byte	Hex values	Description
1-3	00 00 00	
4	52	Length
5	12 | 01 | 02	Message ID
6	01	SIA protocol
7-8	80 80	
9	d7 | c4	
10-13	c6 cc d5 f3	
14	b7 | b4	
15	ab	
16	b4 | bd	
17-21	85 85 85 85 85	
22-23	17 87	ID
24-28	85 b9 a2 95 8f | 84 a9 84 85 85	
29-34	85 85 85 85 85 85 | 00 00 00 00 00 00	

Table 1: Description of header

00	00 00 00 33 01 01 80 80 d7 c6 cc d5 f3 b7 ab b4
01	85 85 85 85 85 17 87 85 b9 a2 95 8f **85 85 85 85**
02	**85 85** c4 c6 ce cb ca d2 c9 c0 c1 c2 c0 a5 c8 c0
03	d6 d6 c4 c2 c0 **1f 7f**
00	00 00 00 33 01 01 80 80 d7 c6 cc d5 f3 b7 ab b4
01	85 85 85 85 85 17 87 85 b9 a2 95 8f **00 00 00 00**
02	**00 00** c4 c6 ce cb ca d2 c9 c0 c1 c2 c0 a5 c8 c0
03	d6 d6 c4 c2 c0 **1c 61**

Table 2: Differences in acknowledgements

3.2 Registration

The alarm system needs to register itself at the control room before the communication is started. In this communication both sides do not know each other and they need some form of authentication. This section is about how the alarm system registers itself at the control room.

3.2.1 Network traffic

The registration consists of two parts: first registration at port 2525 and second registration at an assigned port. The registration at port 2525 is done when a connection is lost, change of IP address or when the system boots. Since the alarm system does not know what port it has assigned when it boots. The system needs to get the port number to communicate after the initial registration request at port 2525. From this it is known that the assigned port number is

communicated in the acknowledgement after the initial registration. The first registration process is displayed in table 3 on line 1 and 2.

After the first registration at port 2525 there is a second registration at the assigned port 2616. After the second registration the registration process is completed. The registration packets of this process are displayed in table 3 on the third and fourth line.

No.	time	src.ip	dst.ip	proto	sport	dport
1	09:44:41.997295	10.x.x.253	80.x.x.198	UDP	2607	**2525**
2	09:44:42.243250	80.x.x.198	10.x.x.253	UDP	2525	2607
3	09:44:44.457156	10.x.x.253	80.x.x.198	UDP	2607	**2616**
4	09:44:44.571119	80.x.x.198	10.x.x.253	UDP	2616	2607

Table 3: Network traffic of authentication

3.2.2 Payload

The messages to the control room are almost the same for every account, only the last byte is changed. The first and second message contain the payload as displayed in table 4.

00	d7 c0 c2 cc d6 d1 d7 c4 d1 cc ca cb a5 d7 c0 d4
01	d0 c0 d6 d1 20 **dc**
00	d7 c0 c6 ca cb cb c0 c6 d1 a5 d7 c0 d4 d0 c0 d6
01	d1 1e **54**

Table 4: Differences in the payload of registration

The acknowledgements that are send differ from the normal acknowledgements as in 3.1.2. The messages are displayed in table 5

00	d7 c0 c2 cc d6 d1 d7 c4 d1 cc ca cb a5 d7 c0 cb
01	c0 d2 c4 c9 a5 c4 d1 a5 d5 ca d7 d1 a5 b5 **b7 b3**
02	**b4 b3** 2b 72
00	d7 c0 c6 ca cb cb c0 c6 d1 c0 c1 a5 c4 d1 a5 d5
01	ca d7 d1 a5 b5 **b7 b3 b4 b3** 21 21

Table 5: Differences in the payload of registration acknowledgements

In the acknowledgement are some differences at the end of the payload. This was expected because the packet must contain the assigned port number as explained in section 3.2.1. The last 2 bytes are not interesting but the 4 bytes before that show a pattern similar to the account codes in section 3.7.

3.3 Heartbeat

Before the capturing of network data started there was already the expectation that there was heartbeat between the alarm system and the control room. Since Internet is unreliable and the control room wants to know if the alarm system is still up and running. Therefore a trace was done when there was no action at the alarm system(e.g. sensor trigger or switching the alarm on) to see if there are polling messages.

3.3.1 Network traffic

A fragment of traffic that was captured is displayed in table 6. Every five minutes the alarm system send a heartbeat to the control room. The heartbeat is acknowledged by the control room.

No.	time	src.ip	dst.ip	proto	sport	dport
1	12:08:59.095831	10.x.x.253	80.x.x.198	UDP	2607	2612
2	12:08:59.261572	80.x.x.198	10.x.x.253	UDP	2612	2607
3	12:14:00.270911	10.x.x.253	80.x.x.198	UDP	2607	2612
4	12:14:00.437307	80.x.x.198	10.x.x.253	UDP	2612	2607
5	12:19:01.483459	10.x.x.253	80.x.x.198	UDP	2607	2612
6	12:19:01.648678	80.x.x.198	10.x.x.253	UDP	2612	2607

Table 6: Network traffic of 3 heartbeat moments

3.3.2 Payload

The heartbeat packet that is send from the alarm system to the control room is always the same. Not much can be derived from the payload since it is short and no constant differences are present. The payload from this packet is displayed in table 7:

3.4 Activating alarm

When the alarm system is activated the control room must be informed so that they can observe the events from the alarm system. In the message it is likely that there is some kind of identification so the control room can identify which alarm is activated. Although this information is already known because of the registration as described in section 3.2

00	ec 01 f3 e0 a4 1f 57

Table 7: Payload of hearthbeat message

3.4.1 Network traffic

The network traffic is displayed in table 8. The traffic consist of 4 messages that are send to the control room and the four acknowledgement that are send back. The communication is done at the assigned port from the registration.

No.	time	src.ip	dst.ip	proto	sport	dport
1	12:37:54.404264	10.x.x.253	80.x.x.198	UDP	2607	2612
2	12:37:54.540037	80.x.x.198	10.x.x.253	UDP	2612	2607
3	12:37:57.276008	10.x.x.253	80.x.x.198	UDP	2607	2612
4	12:37:57.501188	80.x.x.198	10.x.x.253	UDP	2612	2607
5	12:37:59.546871	10.x.x.253	80.x.x.198	UDP	2607	2612
6	12:37:59.737640	80.x.x.198	10.x.x.253	UDP	2612	2607
7	12:38:02.742340	10.x.x.253	80.x.x.198	UDP	2607	2612
8	12:38:02.905437	80.x.x.198	10.x.x.253	UDP	2612	2607

Table 8: Network traffic of activating the alarm

3.4.2 Payload

The messages that are send to the control room are displayed in table 9, this is from one sequence from a test account. The first and the last message are always

00	c1 a6 bc b7 b5 b7 14 1e 92
00 01 02	de cb f1 ec b4 b3 bf b6 b4 aa f7 ec b5 b4 aa ec e1 b5 b5 b4 aa f5 ec b5 b5 b5 aa c6 c2 46 31 80 1b b8
00 01	cb c4 c1 c0 c0 c9 c7 ab cc cb c2 a5 a5 c6 cf d7 0a 26 d4
00	c5 b5 0a 1b b8

Table 9: Payload of activating messages

the same for every activating sequence. The second and third message have some differences in the payload. The activating has been done multiple times with the same account number at different times and with different accounts. Although there are some differences they are not consistent enough to make assumptions about which information is placed where in the payload. In the second message it looks like the hex value 0xec is some kind of delimiter since it is repeated every now and then.

3.5 Deactivating alarm

Like activating the alarm also deactivating needs to be known by the control room. It is likely that for deactivating the alarm some form of identification is

needed. To capture this specific data the alarm was deactivated multiple times with the same account credentials to recognise differences in the payload.

3.5.1 Network traffic

The network traffic of deactivating the alarm system is displayed in table 10. The traffic from deactivating the alarm is similar to the traffic of activating the alarm. The traffic shows that the alarm system sends 4 packages to the control room. There are four types of messages that mostly appear in the same order. The are cases where an sequence is started but after the second packet it reinitializes the sequence and starts over. The second and third message sometimes switch order.

No.	time	src.ip	dst.ip	proto	sport	dport
1	07:24:07.613791	10.x.x.253	80.x.x.198	UDP	2607	2612
2	07:24:07.749433	80.x.x.198	10.x.x.253	UDP	2612	2607
3	07:24:10.484980	10.x.x.253	80.x.x.198	UDP	2607	2612
4	07:24:10.706299	80.x.x.198	10.x.x.253	UDP	2612	2607
5	07:24:12.789207	10.x.x.253	80.x.x.198	UDP	2607	2612
6	07:24:12.945528	80.x.x.198	10.x.x.253	UDP	2612	2607
7	07:24:15.995412	10.x.x.253	80.x.x.198	UDP	2607	2612
8	07:24:16.125150	80.x.x.198	10.x.x.253	UDP	2612	2607

Table 10: Network traffic of deactivating the alarm

3.5.2 Payload

The packets from deactivating the alarm are similar to the packets activating the alarm. The first and last messages are the same and the second and third message have not much differences with activating. The messages are displayed in table 11.

00	c1 a6 bc b7 b5 b7 14 1e 92
00 01	de cb f1 ec b5 b1 bf b1 b2 aa f7 ec b5 b7 aa ec e1 b5 b5 b4 aa f5 ec b5 b5 b5 aa ca c2 4b 31 16
00 01	cb c4 d0 cc d1 c2 c0 d6 c6 cd ab a5 a5 c6 cf d7 12 26 9c
00	c5 b5 0a 1b b8

Table 11: Payload from deactivating the alarm

3.6 Triggering sensor

When a sensor is triggered the control room needs to be informed. Alarm messages are send to the control room when a sensor is triggered.

3.6.1 Network traffic

The traffic flow from when a sensor is triggered is displayed in table 12. When an alarm is triggered there are three packets send to the control room. This sequence is repeated constantly until the alarm has been deactivated.

No.	time	src.ip	dst.ip	proto	sport	dport
1	11:10:44.498449	10.x.x.253	80.x.x.198	UDP	2607	2612
2	11:10:45.005670	80.x.x.198	10.x.x.253	UDP	2612	2607
3	11:10:49.622475	10.x.x.253	80.x.x.198	UDP	2607	2612
4	11:10:50.042383	80.x.x.198	10.x.x.253	UDP	2612	2607
5	11:10:52.781065	10.x.x.253	80.x.x.198	UDP	2607	2612
6	11:10:52.999076	80.x.x.198	10.x.x.253	UDP	2612	2607

Table 12: Network traffic of triggering the alarm

3.6.2 Payload

The payload of the alarm messages are similar to what is seen before in activating and deactivating the alarm. The first messages are almost the same and the second and third message have similarities at the beginning from the payload. It is hard to retrieve information from the payload because there are no bytes changed during the tests. Those messages are displayed in table 13.

00	c1 a6 bc b7 b5 b7 14 1f 00
00 01	de cb f1 ec b4 b3 bf b0 bc aa f7 ec b5 b7 aa ec e1 b5 b5 b4 aa f5 ec b5 b5 b5 aa c6 c2 4b 31 8a
00 01	cb c4 c1 c0 c0 c9 c7 ab cc cb c2 a5 a5 c6 cf d7 0a 26 d4

Table 13: Payload of triggering the alarm messages

3.7 Different account numbers

Test accounts where provided by the control room during our research. The accounts where used to identify differences in the packets within the same event.

3.7.1 Network traffic

The payload in the network traffic is changed when using different accounts. The UDP port at the control room changes. The port at the alarm system does not change. The ports from the test accounts that are used are: 2615, 2616, 2617 and 2618. The port numbers are in order and the test accounts are created after each other. So there is a link in creation of the account and the increasing port number.

3.7.2 Payload

The payload displays differences from the test accounts. The difference is four bytes and the account number is four digits, so there is likely a match. It was not hard to recognise the pattern in the numbers, every zero in the account number is translated to 0xb5 and every 1 to 0xb4. More information about decoding of the account number can be found in section 3.8.

Account	Account #	payload byte 43-46
Test 1	0010	b5 b5 b4 b5
Test 2	0011	b5 b5 b4 b4
Test 3	0012	b5 b5 b4 b7

Table 14: Differences between account codes

The bytes at position 22 and 23 and the last byte also differs. These 2 bytes provide likely some identification of the alarm system. The 2 bytes give a total of 65536 possible identification numbers for alarm systems. Like the account number this information is also decrypted, more can be found in section 3.8.

Account	Account #	ID bytes	Last byte
test 1	0010	85 95	dc
test 2	0011	85 94	db
test 3	0012	ac 97	de
test 4	2902	17 87	f5

Table 15: Last byte of payload authentication message to control room

3.8 Decoding

The decoding of the entire payload was unsuccessful because it was not known what information is send in a packet. This makes it difficult to reverse engineer the protocol in the payload. The data in the packets is not random so no strong encryption like AES is used.

The exception of data we could decode are the account numbers and the port numbers. The account code became clear after we got test accounts. Now the

ciphertext[6] could be compared to the plain data that was known to be there. Decoding using different character encoding schemes was tried, but this was unsuccessful. For decoding a website called Hackvector [6] is used. This website provides different encoding schemes.

Since decoding did not work the next possibility was simple encryption. An easy encryption is the XOR cipher[7] that can be easily broken by a known plain text attack. To try if XOR was used the ciphertext and the plaintext was used as input for the cipher. The output was the same for every combination namely 181. This is visualised in table 16 where the plaintext, the hexadecimal value from the data and the key are displayed. The encryption could not be used at the other part of the payload.

Plaintext	0	1	2	3	4	5	6	7	8	9
Hexadecimal	0xb5	0xb4	0xb7	0xb6	0xb1	0xb0	0xb3	0xb2	0xbd	0xbc
Decimal	181	180	183	182	177	176	179	178	189	188
Key	181	181	181	181	181	181	181	181	181	181

Table 16: XOR decryption of numbers used for account and port number

The decryption of the ID found in section 3.7 that is used in the header part was not encrypted like the account code. It is known that the alarm system only has a account code where it can identify itself with. But unlike the account number above now there are less bytes used in the packet so there is no easy XOR done. Since there still was a pattern in the numbers it was also clear that the encryption that was done was not strong. The three test accounts all started with the same byte and also the first two numbers in the account number are the same. In both situations the last part only differs from the payload as displayed in table 15.

The encryption was done by dividing the account number into two parts. The divided parts are treated as hexadecimal values. For example the account number 0011 results in "0x00" and "0x11". The size of the account number is now equal in size to the bytes found in the payload. The encryption is an XOR with key "0x85" as displayed in table 17.

3.9 Standards

In section 2.3 it was already explained that there is some standardization for the communication of alarm system over IP. The finding from analysing the packets show that the protocol that is defined in the standard is not used in the device we looked at. The lack of randomness in the payload and the many similarities that where found in the packets show that a modern encryption like AES or DES is not used.

[6] http://en.wikipedia.org/wiki/Ciphertext
[7] http://en.wikipedia.org/wiki/XOR_encryption

Packet value	Account hex	Key
0x85	0x00	0x85
0x95	0x01	0x85
0x94	0x11	0x85
0x87	0x02	0x85
0x97	0x12	0x85
0xac	0x29	0x85
0x17	0x92	0x85

Table 17: Decryption of ID using XOR

What could be retrieved from the standard was that most likely some attributes where in the packets like the length, type of message and protocol type. There were mentioned in the standards and for example the length was in plain text in the protocol of the PSTN-2-IP and that was also mentioned in standard. We looked at more points that were in the standards but most of that is not findable in the protocol that was going over the line.

Although the communication show some major weaknesses it is still confirm the guideline that is followed in the Netherlands. The standard describes that no security measurements are needed in a home situation. The protocol that is used for communication does more on security then the standard describes.

4 Attack vectors

After capturing all traffic different attacking vectors need to set up. The attack vectors are set up by taking the important aspects in mind for a burglar. The attack vectors are set up by the following questions.

- Is it possible to deactivate an alarm on location Y which is activated on location X with the same credentials.
- Is it possible to activate an alarm on location X and trigger the alarm from location Y with the same credentials.
- Is it possible to trigger an alarm on location X, which account is disabled from location Y.
- Is it possible to trigger alarm sensors from different alarm systems to set up a DoS attack.

4.1 General

As preparation for the replay attacks four pcap-files are created. Each pcap-file contains packets from the different events. The four pcap-files contain:

- Authentication packets, see chapter 3.2
- Activating packets, see chapter 3.4
- Alarm triggering packets, see chapter 3.6
- Deactivating packets, see chapter 3.5

Performing the attack vectors is done by replaying the pcap-files in the right order. The pcap-file that contains the authentication packets is replayed only once to the control room. The reason for this is that the alarm system needs to identify itself to the control room, otherwise the communication is discarded by the control room. Replay from the authentication packets is done in the first attack vector.
In every attack vector a timeline is added. The timeline visualizes the succeeded attacks. The network infrastructure with the attacker is visualized in figure 2. The sub section *timeline* contains references to the tables which matches the timestamps from the packets against the alarm messages that are received at the control room.

4.2 Activating and deactivating the alarm

In this attack vector the alarm is activated from location X. Deactivating the alarm system is done from location Y. The pcap-files are replayed sequentially:

- Replay authentication packets from location X

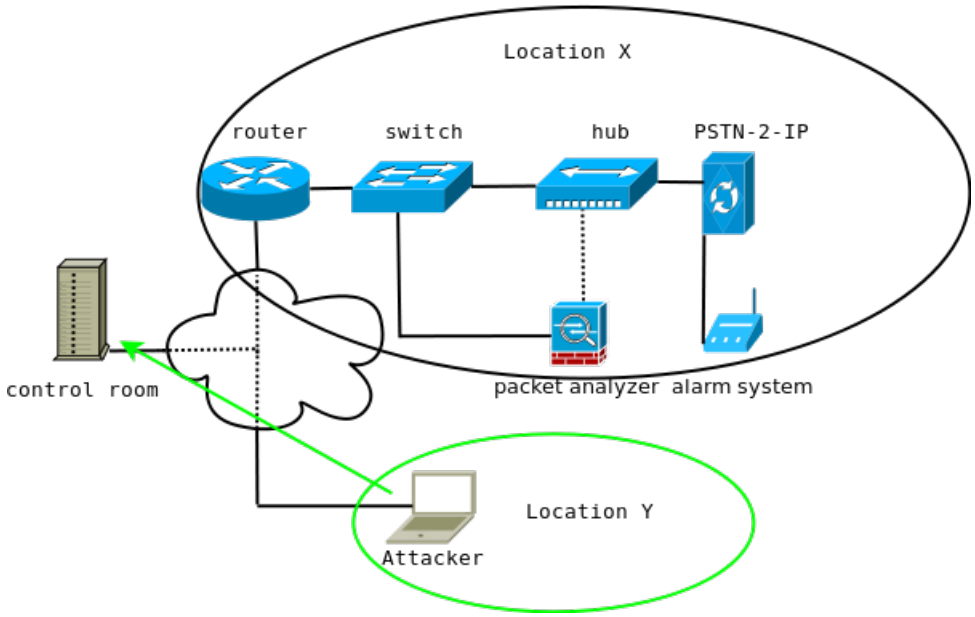

Figure 2: Network infrastructure with attacker

- Replay activating packets from location X
- Replay deactivating packets from location Y

4.2.1 Timeline

The captured traffic from authenticating and activating the alarm is displayed in table 18. The traffic from deactivating the alarm is displayed in table 19. The log entry from the control room is displayed in table 20. The tables are appended to appendix A. The conclusion is that the replay attack is successful because the messages are verified by the control room as displayed in the tables.

4.3 Activating and triggering the alarm

In this attack vector the alarm system is activated from location X, the alarm system is triggered from location Y with the same account credentials. This is done with replaying the correct pcap files from both locations to the control room. The replaying is done according to the following steps:

- Activating alarm on location X
- Trigger alarm from location Y
- Deactivating alarm on location X

4.3.1 Timeline

The captured traffic from activating the alarm is displayed in table 21. The traffic from triggering the alarm is displayed in table 22. The captured traffic from deactivating the alarm is displayed in table 23. The log entry from the control room is displayed in table 24. The tables are appended to appendix B. The conclusion is that the replay attack is successful because the messages are verified by the control room as displayed in the tables.

4.4 Triggering alarm sensor from a disabled alarm

In the previous attack vector the alarm system is deactivated. The second step is replaying the pcap-files with the packets to trigger an alarm from location Y with the same account credentials as used to deactivate the alarm. This attack vector creates a state which is unknown by the control room. When the alarm is deactivated, it is still possible to send alarm messages to the control room. The control room discards those messages. The log file from the control room can be found in appendix C.

4.5 Brute force attack

When registering at the control room a packet is send which contains the account code in byte 22-23 as described in section 3.1.1. The payload from the response packet from the control room contains the port number and account code which is needed for full operation.

After analysis on the payload from the different packets as described in section 3.2.2, it is possible to set up a brute-force attack on the account numbers. When sending the first registration packet to the control room with a working ID the control room responds with a packet which contains the registration port for that account including the account code itself. By extracting this information from the payload as described in section 3.2.2 a port number with the corresponding port is known.

To set up a perfect DoS against the control room from the alarm system a brute force attack is needed to gather information about all accounts. Setting up this brute force attack takes some amount of time.

The following information is gathered through a brute force attack:

- Communication port
- Account code
- Checksums

With this information packets containing the payload to trigger an alarm sensor from all accounts can be created. The amount of time that is consumed by the brute force attack is calculated like:

Account with 4 digits in the range $[0-9]$, this gives $10^4 = 10000$ possibilities of accounts.
The checksum is one byte, therefore $16 * 16 = 256$ possible checksums.
This brings a total of $10000 * 256 = 2560000$ possibilities.
$(2560000/2pps)/60s/60m/24h \approx 15$ days.
This is calculated with 2 pps, 2 pps is chosen to avoid getting recognised as a potential attacker.

During the project a test model from a brute force attack is done within the boundaries from the test accounts. The script that is used for this attack can be found in appendix D.

4.6 DoS attacks

After the brute force attack there are new possibilities for an attack vector. It is possible to DoS the control room on system and human resources. With this approach alarm systems from other people can be abused without even gaining network traffic from those accounts.

4.6.1 System resources

With combination of account code and corresponding registration port it is possible to set up a DoS attack on the system resources. Packets containing payload from triggering alarm sensors can be send to the control room with different account information in the header. Packets containing traffic which reports that an alarm is going off from different accounts can result into a DoS on the human resources.

4.6.2 Human resources

The impact from a DoS on the system resources can result into having not enough security guards to invest the different alarm messages from different property's. A burglar could succeed in his job when theft is done by break-in into a house which is not near by the control room.

5 Impact

Now that we have done the packet analysis and could perform some attack what is the impact of our findings? First will be about if there are similar system like the PSTN-2-IP on the market. Second what kind of improvements need to be done in order to make this communication become more secure.

5.1 Coverage

The PSTN network in the Netherlands is going to disbanded by KPN [7]. This makes it certain that all alarm systems need to switch to a new communication network. Since Internet is already available in most houses and the data traffic is free this is the most likely network to use.

There are two kind of systems that are used: converters like the PSTN-2-IP and alarm systems that already have IP built in.

5.1.1 PSTN to IP

Converters like the PSTN-2-IP from Alphatronics are not easy to find on the Internet. Some shops have a converter for sale but that were only Dutch websites. The control rooms also don't promote which devices are used. All this makes it hard to estimate how often this type of devices are actually used.

5.1.2 Newer systems

There are newer alarm systems available that can communicate over the Internet without any extra devices. The majority of those systems claims to use AES encryption and a version of SHA. Although these system were not analysed it shows that the industry is busy with making the change from PSTN to IP.

An other option that is offered by KPN. They made an agreement with several control rooms to set up a VPN connection between the alarm system and the control room [8]. This VPN [9] is controlled by KPN and uses QOS[8] to ensure delivery of the network packets. This setup is used for companies who are graded by their insurance company to be at higher risk. The VPN has a high availability to ensure that the connection is guaranteed. Also GPRS is used as backup line.

5.2 Improvements

With old alarm systems the communication between the alarm system and the control room was done over a more trustworthy communication channel. Eavesdropping on a telephone line between the alarm system and the control room is not an option for a burglar. Special equipment is needed to do this. The research has proven that the protocol that is used for communication between

[8] http://en.wikipedia.org/wiki/Quality_of_service

the alarm system and the control room is not developed with security in mind. The protocol is vulnerable for:

- Replay attacks
- Brute force attacks
- DoS attacks
- Identity theft

When taking security into account placing the results against the CIA[9] triad, the used protocol fails on all three core principals.

Confidentiality

Disclosure of account information is possible by intercepting and re-using the traffic with the account information. With the account code the personal information of the owner of an alarm system can not be retrieved. Although the account code from the alarm system can be abused to trigger falsified events.

The account code can be retrieved because of the use of weak cryptography and being vulnerable for replay attacks. See section 4.2 and 3.8 for more information.

Integrity

The payload can be decrypted without authorization. This makes it a weak protocol. By intercepting the data and analysing it the data can be changed. The data that is received by the control room is not trustworthy. The source from where the data originates can be any source on the Internet. See section 4.5 for more information.

Availability

By abusing traffic on a large scale against the control room it is possible to make the resources from the control room unavailable. Not only the computer resources can become unavailable but also the human resources at the control room. See section 4.6 for more information.

A redesign of protocol according to the CIA triad as described above would improve the security of the protocol.

[9] http://en.wikipedia.org/wiki/Information_security

6 Conclusion

Referring to the research question:

Is it possible to perform a burglary without getting noticed by influencing the communication between the alarm system and the control room?

Yes, it's possible, but to perform a burglary like this, technical knowledge about protocol analysis and knowledge about networks is mandatory. Datasets with different payloads from the functionalities from the alarm system are required for protocol analysis.

Analysis of the traffic payload concluded that:

- No advanced crypto is used
- Alarm messages are vulnerable for replay attacks
- Replay attacks can result in DoS
- It's not possible to disable the physical alarm

To set up a perfect burglary without getting noticed by the control room the burglar needs to invest a lot of time and effort. Without the usage of multiple test accounts it's a lot harder to get a understanding of the protocol. Datasets can be retrieved from alarm systems with using known techniques. Also gaining access to the web interface went without any problems. A default user name and password can be used to login and to change account information. So by using an alarm system that is connected over the Internet to the control room does NOT secure your property and a way that you want it to be.

By investigating the protocol and how the protocol operates on top of UDP the conclusion is that the protocol was not designed with security in mind. The packets that travel between the alarm system and the control room do not provide any security. By doing in-depth analysis on the payload of the protocol packets with different payloads can be extracted. The packets that are responsible for the different processes of activating an alarm and triggers alarm sensors can be replayed over the Internet from different locations.

7 Future work

Future work on this subject could be done in the following subjects:

First the calculation of the checksum that is used at the end of the packets. If that routine can be found the attacks using brute force can be shortened. This will shorten the attack 256 times and then it becomes feasible to perform the attack.

The second subject could be to look how other system that are available work. This way it can become more clear if this an problem of one system that is not secure or if the problem is wider.

Third could be to look at the impact of these kind of systems on the network infrastructure. Should ISP make special services for the alarm communication? And what threats are there from known network attacks to take out the control room and then do the burglary. Because if maybe the protocol is secure the communication can still be disturbed because the network is publicly available.

A last option could be to fully decode the packet and fully understand the protocol. This step is not needed to perform but could lead to full control what is send and thereby more effective.

8 Acknowledgements

We would like to thank the following people for their information, guidance, resources and explanation we got during the research.

- Christiaan Roselaar
- Ruud Haller
- Tjerk Nan

Appendices

A Overview Activating and deactivating the alarm

No.	time	src.ip	dst.ip	proto	sport	dport
1	16:31:54.710701	145.x.x.11	80.x.x.198	UDP	2607	2525
[...]	[...]	[...]	[...]	[...]	[...]	[...]
6	16:31:55.110575	80.x.x.198	145.x.x.11	UDP	2615	2607
1	16:34:38.676825	145.x.x.11	80.x.x.198	UDP	2607	2615
[...]	[...]	[...]	[...]	[...]	[...]	[...]
10	16:34:38.990584	80.x.x.198	145.x.x.11	UDP	2615	2607

Table 18: Authentication and activating packets from location X.

No.	time	src.ip	dst.ip	proto	sport	dport
1	16:35:14.500569	10.x.x.253	80.x.x.198	UDP	2607	2615
[...]	[...]	[...]	[...]	[...]	[...]	[...]
8	16:35:15.280553	80.x.x.198	10.x.x.253	UDP	2615	2607

Table 19: Deactivating packets from location Y.

DATUM	DAG	ONTV	KODE	MEL	OMSCHRIJVING	GEBRUIKERS INFORMATIE
25/01	Mon	16:37	CG00012	CLO	DEELB.ING	CJR
25/01	Mon	16:38	YO	MSG	INBRAAK	Woonkamer
25/01	Mon	16:39	BR10021	RST	Inbraak	algemeen
25/01	Mon	16:40	OG00012	OPN	UITGESCH.	CJR
25/01	Mon	16:40	OG00012	OPN	UITGESCH.	CJR

Table 20: Log entry from the control room(in Dutch).

B Overview Activating and triggering the alarm

No.	time	src.ip	dst.ip	proto	sport	dport
1	16:47:25.106359	145.x.x.11	80.x.x.198	UDP	2607	2615
[...]	[...]	[...]	[...]	[...]	[...]	[...]
9	16:47:25.422666	80.x.x.198	145.x.x.11	UDP	2615	2607

Table 21: Activating packets from location X.

No.	time	src.ip	dst.ip	proto	sport	dport
1	16:51:59.795623	10.x.x.253	80.x.x.198	UDP	2607	2615
[...]	[...]	[...]	[...]	[...]	[...]	[...]
9	16:52:00.226069	80.x.x.198	10.x.x.253	UDP	2615	2607

Table 22: Sensor packets from location Y.

No.	time	src.ip	dst.ip	proto	sport	dport
1	16:55:31.870277	145.x.x.11	80.x.x.198	UDP	2607	2615
[...]	[...]	[...]	[...]	[...]	[...]	[...]
8	16:55:32.263053	80.x.x.198	145.x.x.11	UDP	2607	2615

Table 23: Deactivating packets from location X.

DATUM	DAG	ONTV	KODE	MEL	OMSCHRIJVING	GEBRUIKERS INFORMATIE
25/01	Mon	16:50	CG00012	CLO	DEELB.ING	CJR
25/01	Mon	16:54	YO	MSG	INBRAAK	Woonkamer
25/01	Mon	16:58	OG00012	OPN	UITGESCH.	CJR

Table 24: Log entry from the control room(in Dutch).

C Overview Triggering alarm sensor from a disabled alarm

DATUM	DAG	ONTV	KODE	MEL	OMSCHRIJVING	GEBRUIKERS INFORMATIE
25/01	Mon	16:58	OG00012	OPN	UITGESCH.	CJR
25/01	Mon	17:02	YO	MSG	INBRAAK	Woonkamer

Table 25: Log entry from the control room(in Dutch).

D bruteforce.py

```
#!/usr/bin/env python

import os, sys, datetime, re
from scapy.all import *


fp=""
lp=""

accountlist = [ ]
payloadlist = []
#for i in range(215,225):

logfile = open('/tmp/bruteforceallports.log', 'w')

def bruteforce():
        for i in range(256):
                for j in range(256):
                        for k in range(256):
                                s=str(chr(i)) + str(chr(j))
                                newpayload=fp + s + lp + str(chr(k))
                                packet=Ether()/IP(src='145.x.x.11', dst='80.x.x.198')/
                                UDP(sport=2607, dport=2525)/newpayload
                                sendp(packet, verbose=0)
                                traffic=sniff(filter="udp and src 80.x.x.198", timeout=0.3, count=1)
                                if len(traffic) != 0:
                                        logfile.write(str(traffic[0].load))
                                        logfile.write("XXXX")
#                                       print "<payload> " + s + " <payload> " + str(chr(k))

bruteforce()
print "end of bruteforce"
logfile.close()
```

List of Tables

1 Description of header . . . 11
2 Differences in acknowledgements . . . 11
3 Network traffic of authentication . . . 12
4 Differences in the payload of registration . . . 12
5 Differences in the payload of registration acknowledgements . . . 12
6 Network traffic of 3 heartbeat moments . . . 13
7 Payload of hearthbeat message . . . 13
8 Network traffic of activating the alarm . . . 14
9 Payload of activating messages . . . 14
10 Network traffic of deactivating the alarm . . . 15
11 Payload from deactivating the alarm . . . 15
12 Network traffic of triggering the alarm . . . 16
13 Payload of triggering the alarm messages . . . 16
14 Differences between account codes . . . 17
15 Last byte of payload authentication message to control room . . . 17
16 XOR decryption of numbers used for account and port number . . . 18
17 Decryption of ID using XOR . . . 19
18 Authentication and activating packets from location X. . . . 28
19 Deactivating packets from location Y. . . . 28
20 Log entry from the control room(in Dutch). . . . 28
21 Activating packets from location X. . . . 29
22 Sensor packets from location Y. . . . 29
23 Deactivating packets from location X. . . . 29
24 Log entry from the control room(in Dutch). . . . 29
25 Log entry from the control room(in Dutch). . . . 30

List of Figures

1 Network setup of experiment . . . 8
2 Network infrastructure with attacker . . . 21

References

[1] J. Kannan "W. Cui and H. J. Wang". Discoverer: Automatic protocol reverse engineering from network traces.

[2] Sia standard: Dc-03-1990.01 (r2000.11). Payed PDF - http://webstore.ansi.org/RecordDetail.aspx?sku=SIA+DC-03-1990.01+%28R2000.11%29.

[3] Guideline alarm over ip. http://www.vvbo.nl/Documenten/072(ontwerp).pdf.

[4] Vebon alarm over ip proposal. www.vebon.org/Documenten/0215.pdf.

[5] Sia standard: Dc-09-2007. http://www.hacker-soft.net/down.php?id=9745&url=1.

[6] Hackvector. http://www.businessinfo.co.uk/labs/hackvertor/hackvertor.php.

[7] Kpn quits with analog network;dutch newsitem from 2007. http://www.emerce.nl/nieuws.jsp?id=1855701.

[8] Kpn vpn connection. http://www.beveiligingswereld.nl/Nieuws/1/770-kpn_werkt_samen_met_beveiligingsbranche.

[9] Kpn vpn connection. http://www.kpn.com/zakelijk/Meer-diensten/meer-diensten/zakelijke-diensten-1-1/zakelijke-diensten/netwerken/vpn.htm.