# Analyzing the Radio Interface of an ABUS Secvest Intruder Alarm System

sitsec
Schobert IT-Security Consulting

May 2012

Schobert IT-Security Consulting
Martin Schobert
Bühringstr. 12
D-13086 Berlin
Germany

E-mail: contact@sitsec.net
Web: http://www.sitsec.net

# Summary

This report documents an analysis of the wireless interface of an ABUS Secvest burglar alarm system. The analysis is based on passively received radio datagrams, which were reverse-engineered. Because the protocol offers no protection mechanism against attacks, the Secvest system cannot grant confidentiality, integrity, and authenticity of communication. This is a security weakness, especially if messages are transmitted via a shared and remotely accessible medium.

Until now there is no public review available in which the effective protection level of the Secvest system is examined. The weak link is the system's wireless interface: ABUS doesn't use encryption and message authentication and not even a simple rolling code, which is a common technique even for garage door openers. The lack of protection mechanisms allows an attacker to eavesdrop radio communication and to inject their own datagrams by spoofing addresses of components belonging to an alarm system.

ABUS offers a remote control for the Secvest system. This remote control is shipped with the "Basis set", which is a kind of starter kit containing a set of sensors and the alarm panel. Thus, the remote control might be present in many Secvest installations. Datagrams for arming or disarming the system sent by the remote control are unencrypted and basically constant. An attacker needs only to obtain the correct device address to spoof a deactivation telegram. The device address might be extracted from any intercepted message from or to the remote control.

Initially, the results are only valid for the devices from the test setup. However, adopting the results to other wireless devices like motion sensors, glass break detectors, and wireless key boxes should be straight forward.

Because there are freely available evaluation boards for the 868 MHz frequency band, developing a proof-of-concept device for practical attacks should be feasible within a few days, while a commercial product for bypassing the Secvest intruder alarm might be developed within a month.

This examination does not include an active penetration of the test setup with spoofed messages, because it cannot be guaranteed that transmitting data via radio complies with German law. In order to not transgress any official regulations, no transmission of radio signals was performed. Therefore, proof-of-concept codes were not developed and further interesting questions, for example related to datagram fuzzing, must be left unanswered.

# Contents

# 1 Introduction

Wireless intruder alarm systems have key benefits: They are easy to install. They do not require the drilling of holes or the placing of wires on or in the wall. Their setup saves time and costs, minimizes dirt, and avoids visible wires. Therefore, wireless alarm systems are the first choice for home security and small businesses, especially if an alarm system has to be retrofitted. Their major disadvantage is the shared medium burglar alarm systems use for communication. Sensors, remote controls, sirens, and the central station transmit and receive radio signals. Whereas wire-based alarm systems usually have a dedicated communication medium, wireless systems do not and expose their communication interface to the public. An attacker might intercept transmissions or send their own signals. Thus, a wireless system introduces further threats for targeted attacks. If a facility's security depends highly on the presence of a burglar alarm system and not on mechanical measures, the overall security might decrease.

Vendors of wireless intrusion alarm systems have to manage the drawbacks of over-the-air communication. Usually they monitor radio conditions to detect unintended distortions and intended jamming. This is necessary because most systems utilize radio channels within the ISM bands, which are used in general for industrial, scientific, and medical radio applications. For example, if a radio channel is heavily allocated by other applications, burglar alarm systems notify the user, switch the radio channel, or trigger a (false) alarm. Further, vendors already try to defeat simple attacks like the replaying of previously intercepted codes via radio. Many problems do not arise if a dedicated physical medium is used which is not accessible to an attacker. Where the medium is accessible to an attacker, as in wireless systems, special countermeasures have to be integrated.

Vendors usually don't disclose details of their system design, making it necessary to reveal them independently. This way it is possible to evaluate the level of protection an alarm system really offers beyond the vendor's claims.

## 1.1 Analyzed Product Family and Component Compatibility

The subject of this analysis is the Secvest product series produced by ABUS[1]. This family includes the products Secvest 2WAY and Secvest IP, which basically refers to the central alarm controller box. Both systems have a compatible radio interface. The Secvest IP has an Ethernet interface in addition and is capable of using several network protocols. Motion sensors, remote controls, smoke detectors, sirens, etc. made for the Secvest 2WAY are compatible with the Secvest IP system.

[1] Funk-Alarmanlage Secvest 2WAY, http://www.abus-secvest.com/ (last accessed on May 9, 2012)

According to ABUS the Secvest products communicate with a bi-directional protocol. This means that electronic components are not only able to send signals, but also to receive answers. For example, the remote control is able to request if the alarm system is armed or disarmed.

As far as observed, ABUS uses electronic components from the British company Cooper Security[2] (cf. section 2). Hence, this analysis might apply to Cooper Security's Scantronic product family as well, but verifying any compatibility of Scantronic and Secvest was beyond the scope of this research. It is still possible that ABUS uses customized firmware with a customized radio protocol. In this case, results are not comparable.

**Safety**

| | |
|---|---|
| EMC immunity: | Corresponds to EN50130-4, EN50131-4 |
| EMC emissions: | Corresponds to EN61000-6-3 |
| Electrical safety: | EN60950-1:2002 |
| Environmental compatibility: | EN50130-5 Class 1, 93% ambient humidity |
| Security level: | EN50131-1 Level 2 |
| Encryption: | 16.777.214 (2E24 – 2) variations |
| Wireless supervision: | Programmable |
| Access code: | 4-digit (0000-9999) |
| Each position can be a number between 0 and 9 = 10,000 code variations | |
| Code blocking: | 90 seconds |
| After four incorrect code entry attempts (consecutive) | |

**Wireless**

| | |
|---|---|
| Wireless frequency: | 868.6625 MHz, narrow band<br>EN 300.220-3, EN 300.330-2 |
| Wireless output: | 10 mW |
| Range: | ca. 30 metres (indoors)<br>ca. 100 metres (outdoors) |

Figure 1.1: Technical data from the FU8006 installation manual.

The ABUS Secvest alarm system complies with a couple of norms—most relevant is the European norm EN 50131, which is summarized in the next section. Figure 1.2 shows the technical data of the Secvest 2WAY alarm center's installation manual claiming compatibility to EN 50131 [ABU10, p. 98]. According to that the alarm center is rated with a risk grade 2. All other components of the Secvest system are rated with the same risk grade, too.

## 1.2 The European Norm EN 50131

The European Committee for Electrotechnical Standardization (CENELEC) prepares voluntary standards for electrotechnical engineering. One of these standards is the European norm EN 50131, which defines requirements and guidelines for intrusion alarm systems. EN 50131 comprises several parts, which are listed in table 1.1. This standard is accepted among CENELEC's

[2] Cooper Security, http://www.coopersecurity.co.uk/ (last accessed on May 9, 2012)

member countries. For example, the German standardization organization Deutsche Industrie Norm adopts this standard as DIN EN 50131.

| Reference | Part | Title |
|---|---|---|
| EN 50131-1 | Part 1 | System requirements |
| EN 50131-2-2 | Part 2-2 | Requirements for passive infrared detectors |
| EN 50131-2-3 | Part 2-3 | Requirements for microwave detectors |
| EN 50131-2-4 | Part 2-4 | Requirements for combined passive infrared and microwave detectors |
| EN 50131-2-5 | Part 2-5 | Requirements for combined passive infrared and ultrasonic detectors |
| EN 50131-2-6 | Part 2-6 | Requirements for opening contacts (magnetic) |
| EN 50131-2-7-1 | Part 2-7-1 | Intrusion detectors – Glass break detectors (acoustic) |
| EN 50131-2-7-2 | Part 2-7-2 | Intrusion detectors – Glass break detectors (passive) |
| EN 50131-2-7-3 | Part 2-7-3 | Intrusion detectors – Glass break detectors (active) |
| EN 50131-2-8 | Part 2-8 | Intrusion detectors – Passive infrared detectors |
| EN 50131-3 | Part 3 | Control and indicating equipment |
| EN 50131-4 | Part 4 | Warning devices |
| EN 50131-5-3 | Part 5-3 | Requirements for interconnections equipment using radio frequency techniques |
| EN 50131-6 | Part 6 | Power supplies |
| EN 50131-7 | Part 7 | Application guidelines |
| EN 50131-8 | Part 8 | Security fog devices/systems |
| EN 50131-9 | Part 9 | Alarm verification – Methods and principles |
| EN 50131-10 | Part 10 | Application specific requirements for Supervised Premises Transceiver (SPT) |

Table 1.1: Norms related to EN 50131.

EN 50131 introduces a risk grading. Requirements on components depend on this risk grade. For example, passive infrared sensors must succeed a walk-test according to EN 50131-2-2, which defines test modes, distances, and velocities depending on the risk grade. Higher risk grades require higher detection performance and higher tamper resistance. Table 1.2 lists these risk grades from EN 50131 showing for which risk classes and against which attacker types a burglar alarm of a certain grade should be sufficient.

The ABUS Secvest burglar alarm system is rated as grade 2 like many other EN 50131 compliant wireless alarm systems. Thus, the system covers up to medium risks and protects from intruders with limited knowledge. The factor knowledge is discussed later.

EN 50131 requires protection mechanisms for safeguarding the radio communication depending on the risk grade. These requirements are defined in part 5-3 of EN 50131 “Requirements for interconnections equipment using radio frequency techniques” [CEN09]. Besides some functional requirements the security requirements for the radio communication are:

| Grade | Risk | Knowledge | Tools |
|---|---|---|---|
| 1 | Low | Little | Limited range of easily available tools |
| 2 | Low to medium | Limited | General range of tools and portable instruments (e.g. a multi-meter) |
| 3 | Medium to high | Conversant | Comprehensive range of tools and portable electronic equipment |
| 4 | High | Ability/resource to plan in detail | Full range of equipment including means of substitution of components |

Table 1.2: Risk grading according to EN 50131

- **Immunity to intentional message substitution**: The norm suggests using identifier codes for each component belonging to a system. Depending on the risk grade the number of possible identification codes shall range between 100,000 and 100,000,000. Further, the probability of discovering the identification code within an hour shall be limited. Therefore, the norm defines a maximum probability depending on the grade. Even if it is not stated explicitly, this probability only makes sense for brute-forcing attacks. The corresponding compliance test calculates this probability according to a formula specified in an annex to the norm. Further, the manufacturer "shall provide information demonstrating the method of compliance." Grade 3 and 4 components shall implement some kind of message authentication.

| Requirement | Grade 1 | Grade 2 | Grade 3 | Grade 4 |
|---|---|---|---|---|
| Min. identification codes | 100,000 | 1,000,000 | 10,00,000 | 100,000,000 |
| Max. probability of discovering IDs | 5% | 1% | 0.5% | 0.1% |
| Message authentication | no | no | yes | yes |

Table 1.3: Immunity to intentional message substitution and derived requirements.

- **Immunity to unintentional and intentional components substitution**: Control and indicating equipment graded with 4 shall detect components substitution. The corresponding test checks, if it is possible to unset the alarm with a replayed unset message recorded once and transmitted continuously for one hour.

- **Requirement for the detection of a failure of periodic communication**: Receiving equipment shall recognize and report failed periodic communication of transmitters. The norm defines some time limits for this. If periodic communication is not possible for 10 seconds to 240 minutes depending on the risk grade, a failure or tamper signal shall be generated. In addition, setting the alarm shall be prevented if periodic communication fails for 10 seconds to 60 minutes.

| Requirement | Grade 1 | Grade 2 | Grade 3 | Grade 4 |
|---|---|---|---|---|
| Detect failure in periodic communication: | | | | |
| *By control and indicating equipment from detector* | 240 min | 120 min | 100 s | 10 s |
| *By control and indicating equipment from warning device* | 240 min[3] | 120 min[3] | 100 s | 10 s |
| *By control and indicating equipment from alarm transmission equipment* | 240 min[3] | 120 min[3] | 100 s | 10 s |
| *By alarm transmission equipment from control and indicating equipment* | 240 min | 120 min | 100 s | 10 s |
| Type of reaction | Fault or tamper signal | | Tamper signal | |
| Prevent setting if last received message exceeds a time limit of | 60 min | 20 min | 100 s | 10 s |

Table 1.4: Requirement for the detection of a failure of periodic communication and derived requirements.

- **Requirement for the detection of interference**: The equipment shall detect and indicate interference if interference is present for a certain period of time. EN 50131-5-3 defines this period by summing up all durations of interference within any 60 seconds for grades 1 and 2 and 20 seconds for grades 3 and 4. For periods of interference of less than five seconds in any period of 60 seconds no indication shall take place.

| Requirement | Grade 1 | Grade 2 | Grade 3 | Grade 4 |
|---|---|---|---|---|
| Device requirements for interference detection: | | | | |
| *Control and indicating equipment* | Mandatory | Mandatory | Mandatory | Mandatory |
| *Warning devices* | Optional | Optional | Mandatory | Mandatory |
| *Alarm transmission equipment* | Optional | Optional | Mandatory | Mandatory |
| Max. duration of interference | 30 s in any 60 s | | 10 s in any 20 s | |
| Ignore interference | Less than total 5 s within any 60 s | | | |
| Type of reaction | Fault or tamper signal | | Tamper signal | |

Table 1.5: Detection of interference and derived requirements.

To summarize the security requirements according to EN 50131-5-3, risk grade 2 only requires identification codes for components and that these codes cannot be discovered (by brute-forcing them) with a certain probability within one hour. It is quite remarkable that countermeasures against replay attacks are only required for grade four equipment, which means that EN 50131-5-3 doesn't require their implementation for lower risk grades.

[3]It is optional.

## 1.3 Attack Model

EN 50131-5-3 does not explicitly describe an attack model and it does not describe what happens in this one hour time frame even if attacking methods might be derived from the compliance tests. Hence, it is basically open for interpretation. Here, a slightly modified attack model is proposed.

In general, it makes sense to distinguish between the identification and exploitation of vulnerabilities. Because the Secvest system is publicly available product like many other burglar alarm systems, an attacker might acquire an intrusion alarm system to reverse-engineer the protocol between sensors and the alarm central. Once the protocol is known, an attacker investigates design and implementation weaknesses in a next step. Afterwards, an attacker might exploit vulnerabilities, which takes place on-site. This on-site exploitation of security weaknesses might be further separated into two sub-steps: An analysis of radio traffic patterns to identify used device types and their addresses and, finally, the exploitation of previously identified weaknesses.

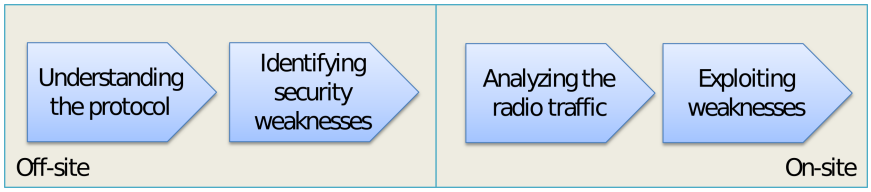


Figure 1.2: Refined attack model.

For example, in an attack scenario an attacker places a radio interception device next to an alarm protected facility and waits for special radio commands from a valid remote control. Capturing datagrams within buildings is possible for a distance up to 20 meters. It is assumed that the alarm bypassing device is a small self-operating, battery powered box, which can be hidden in the vicinity of the alarm controller. In a typical use case the last person leaving a facility would activate the intrusion alarm system, for example by using some kind of remote control. An attacker is able to intercept the activation signal and derives the corresponding deactivation signal. The time window from recording the activation signal to alarm system deactivation might not exceed one hour and therefore meets the assumption from EN 50131-5-3. Obviously, the attacker is not required to be there—at least not for the alarm system bypassing. Deactivating the alarm system does not require sophisticated knowledge. It just requires the “magic” device.

## 1.4 The Test Setup

The test setup consists of a Secvest 2WAY wireless alarm control panel of type FU8000 as the central system. A magnetic contact detector FU8320W serves as a sensor for intrusion detection.

The remote control FU8100 is used for enabling and disabling the burglar alarm. Thus, the test setup basically corresponds to the ABUS FU8001 Secvest 2WAY Basis Set, except that it lacks a motion sensor.

The alarm central's software version is 5.06.50, the radio part's software version is 05.22, and the language version is 3.12.

# 2 Dissecting Devices

Examining devices reveals useful information on the hardware design and on the system in general. Thus, the tester opened all devices from the test setup. This section documents some observations.

## 2.1 Remote Control (FU8100)

The remote control is used to toggle the alarm state and to interact with the alarm central. The remote control offers four buttons for this. One button is for activating the alarm system, another button for deactivating. A third button allows the user to query the system status, that is if the alarm system is active or not. A fourth button supports a user-defined function. Simultaneously pressing the activation and deactivation key triggers a panic function. Additionally, the remote control has a jamming detection. To give the user feedback, the remote control is equipped with four LEDs. These reflect key presses and show the activation state as well as possible errors.

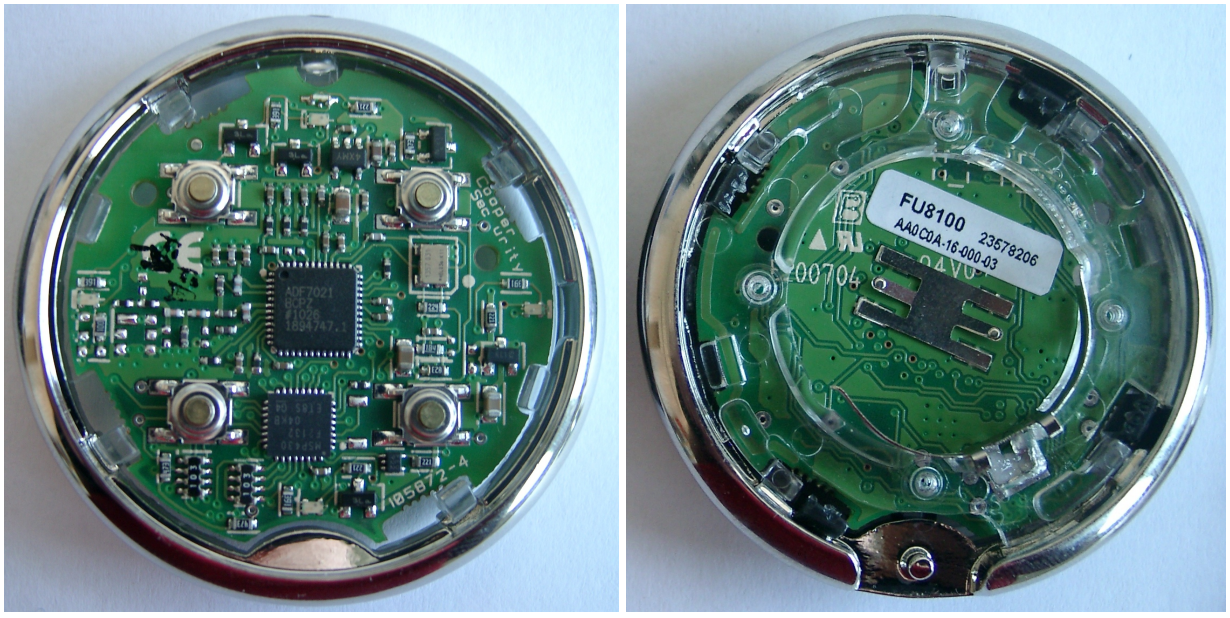


Figure 2.1: Frontside and backside.

The remote control is based on two integrated circuits: A Texas Instruments MSP430F2132 is used as a generic microcontroller and an ADF7021 produced by Analog Devices is the radio frontend. The ADF7021 is a narrowband ISM transceiver, which supports bitrates of 0.05 kbps up to 32.8 kbps and 2FSK, 3FSK, 4FSK, and MSK modulation schemes [Ana07]. The transmission is byte oriented.

Further, the device's interior shows a label with printed IDs. The number 23578206 might serve as a unique identifier for the radio communication as described in a later section. As printed on the circuit board, the company Cooper Security manufactured this device.

## 2.2 Magnetic Contact Detector (FU8320W)

A magnetic contact detector is typically installed by windows and doors to register entrance. The sensor is built up of a reed switch. If an external magnet—usually fixed on a door or window—moves close to the reed switch, an electrical circuit is either closed or opened. The ABUS magnetic contact detector is further equipped with two tampering contacts: The first contact detects if the sensor case is opened. Therefore, a long spring is mounted on a key button (cf. figure 2.2), which releases the button on frontside opening. Another key button at the backside registers if the device is pulled down from a wall (cf. figure 2.4).

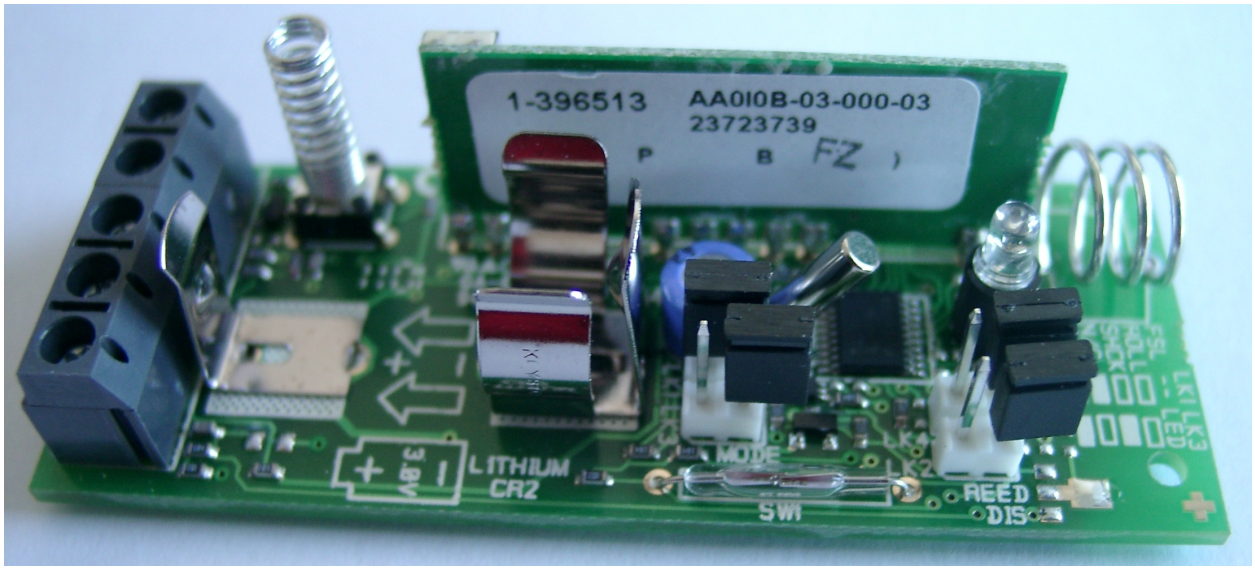


Figure 2.2: An opened magnetic contact detector.

In the test setup the magnetic contact detector is operated in wireless mode, but the device might be used in wired environments as well. Therefore, screwed contacts are mounted on the main board.

A Texas Instruments microcontroller of type 430F1111A controls the detector's operation. The radio frontend is built up of an Infineon Technologies TDK 5100 or TDA 5100 transmitter[1], which is capable of transmitting ASK and FSK datagrams in the 868 and 433 MHz frequency bands [Inf02]. The radio front-end is placed on a separate circuit board, which is plugged onto the main board as shown in figure 2.3.

[1] TDK 5100 and TDA 5100 only differ in the supported temperature range.

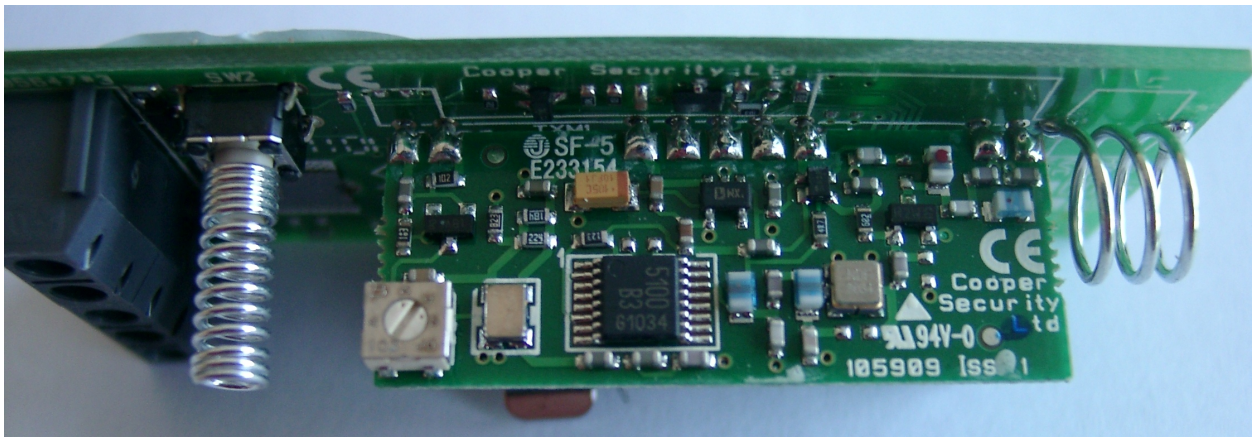


Figure 2.3: Radio module.

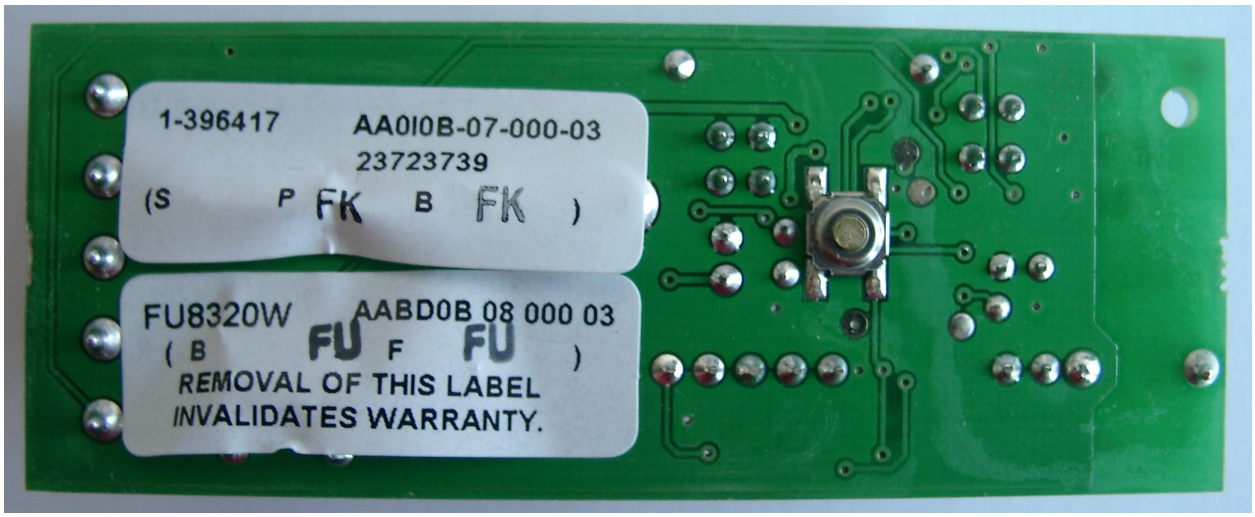


Figure 2.4: Backside.

## 2.3 Alarm Control Panel (FU8000)

The FU8000 is the heart of the Secvest 2WAY alarm system: The wireless alarm control panel receives messages from up to 48 wireless alarm zones and up to two wired alarm zones. It manages incoming messages from sensors, remote controls, and communication modules. Depending on its configuration, alarm state, and received messages, the panel triggers an alarm using the internal siren and optional external sirens. While a telephone interface is already built in, a user might add further communication modules for ISDN, GSM, or Ethernet.

Users arm and disarm the system via remote control or by entering a personal identification number (PIN) on the panel. Furthermore, ABUS ships the FU8000 with a proximity transponder, which is placed close to the panel in order to activate or deactivate the system. ABUS also offers wireless key switches and several types of mechanical locks with a wireless interface.

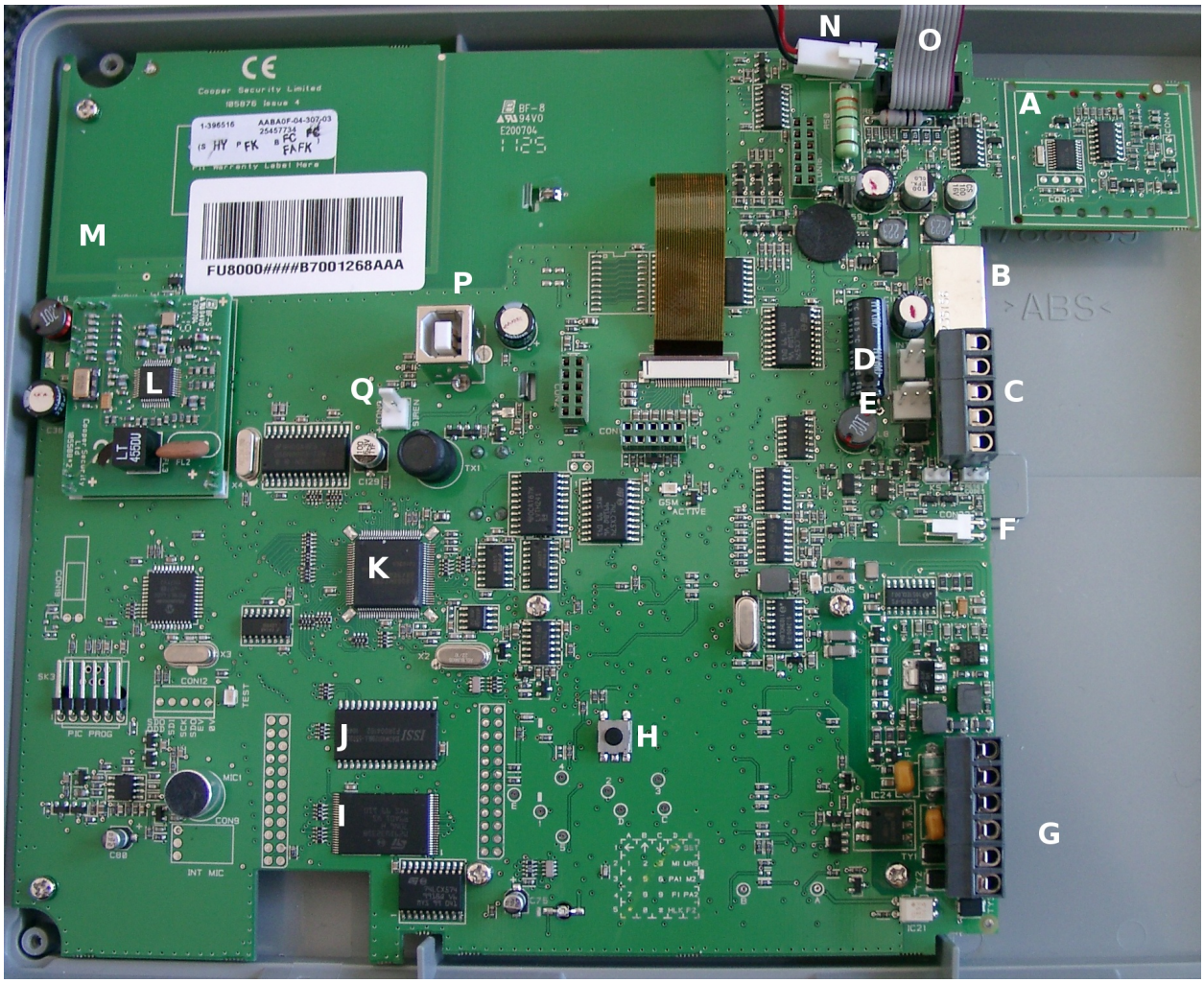


Figure 2.5: FU8000 mainboard.

Figure 2.5 depicts the panel's mainboard. According to the printings on the mainboard, it is also manufactured by Cooper Security. The letters in the image designate some identified components, which are described in table 2.1. Additionally, there are several connectors and test pads on the mainboard, which allows further investigation. However, this was not necessary for analyzing the radio protocol.

| Label | Description |
|---|---|
| A | A reader for the proximity key (cf. figure 2.8) |
| B | An extension slot for optional communication modules |
| C | Screwed contacts for an external speaker and a microphone |
| D | Internal speaker |
| E | Battery power supply |
| F | Connector for tamper detection |
| G | Screwed contacts for connecting the panel to a telephone system |
| H | Key for tamper detection |
| I | 32 Mbit Flash memory (ST M29DW323DB) |
| J | 4 Mbit static RAM (ISSI IS62WV5128BLL) |
| K | Renesas 16-bit single-chip microcomputer H8/3008 (cf. figure 2.6) |
| L | The radio module (cf. figure 2.7) |
| M | Dipole antenna for the radio module |
| N | Connector for tamper detection |
| O | Cable to the power supply circuit |
| P | USB connector for configuring the panel |
| Q | Connector for the internal siren |

Table 2.1: Labels and component descriptions for the FU8000 mainboard.

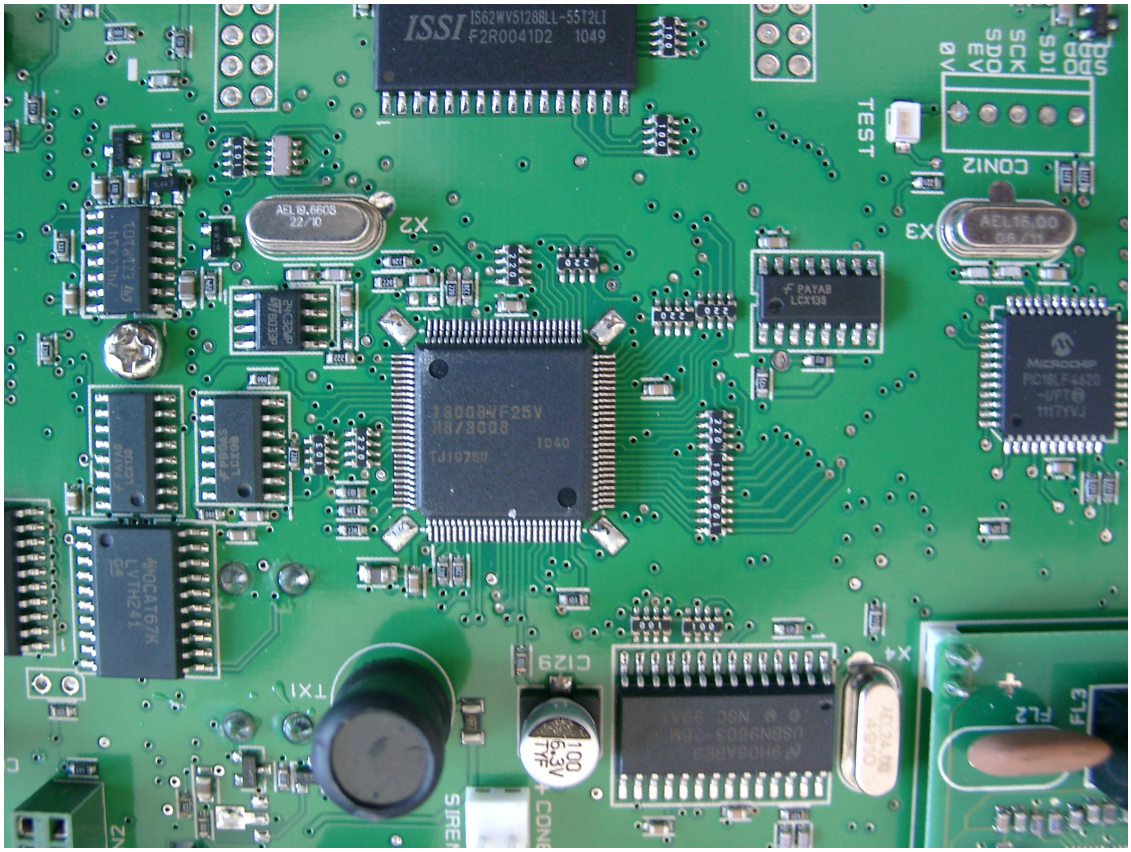


Figure 2.6: CPU.

Figure 2.7 depicts the radio module. The integrated circuit in the center is an Atmel AT86RF211SW, which is a transceiver for ISM radio applications from 400 MHz to 950 MHz [Atm02]. Next to the bottom left corner there are six test pins. These allow the chip's configuration data as well as radio messages to be intercepted.

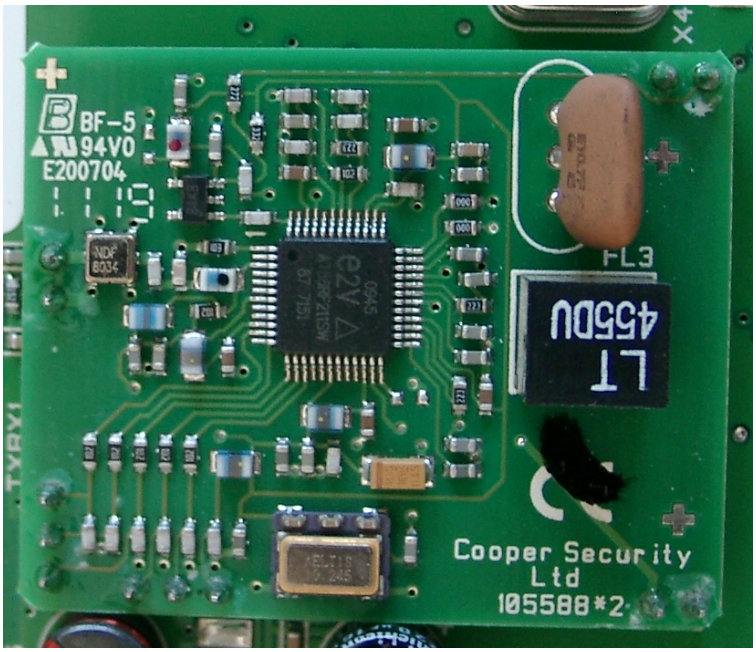


Figure 2.7: FU8000 radio module.

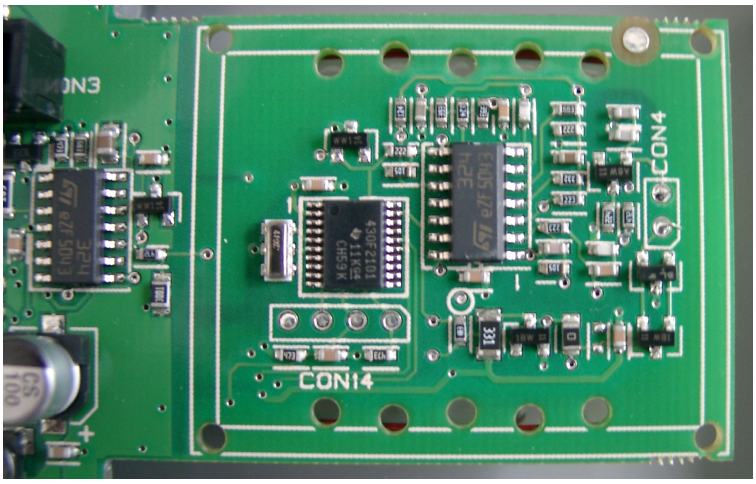


Figure 2.8: FU8000 circuit for reading the proximity key. The antenna coil is placed on the bottom side on the other side of the circuit board. The IC in the image's center is a Texas Instruments 430F2101 microcontroller. The chip labeled with "324 eZF 5043" from STMicroelectronics is most likely an operational amplifier.

# 3 Receiving and Decoding Datagrams

In order to conduct an analysis of the radio interface, receiving (and later transmitting) datagrams is essential. In a first step, the tester used a Universal Software Radio Peripheral[1] (USRP) and GNU Radio[2] to set up a simple receiver for an initial analysis. Afterwards, the tester built a hardware based receiver, which made a more robust reception of datagrams possible.

## 3.1 Analyzing Radio Datagrams

According to publicly available documentation the ABUS Secvest 2WAY and Secvest IP systems are using the single frequency 868.6625 MHz for radio communication. The Universal Software Radio Peripheral is able to receive this frequency, for example, with the RFX900 daughterboard. The radio signal was sampled with the command line program `usrp_rx_cfile.py`, which is part of the GNU Radio software suite. Afterwards, the tester analyzed the recorded traces with Baudline[3], which is shown in figure 3.1. The Secvest 2WAY system uses frequency-shift keying (FSK) for radio transmissions, which is visualized in figure 3.1 by the carrier wave's frequency-shift depending on the bits transmitted.

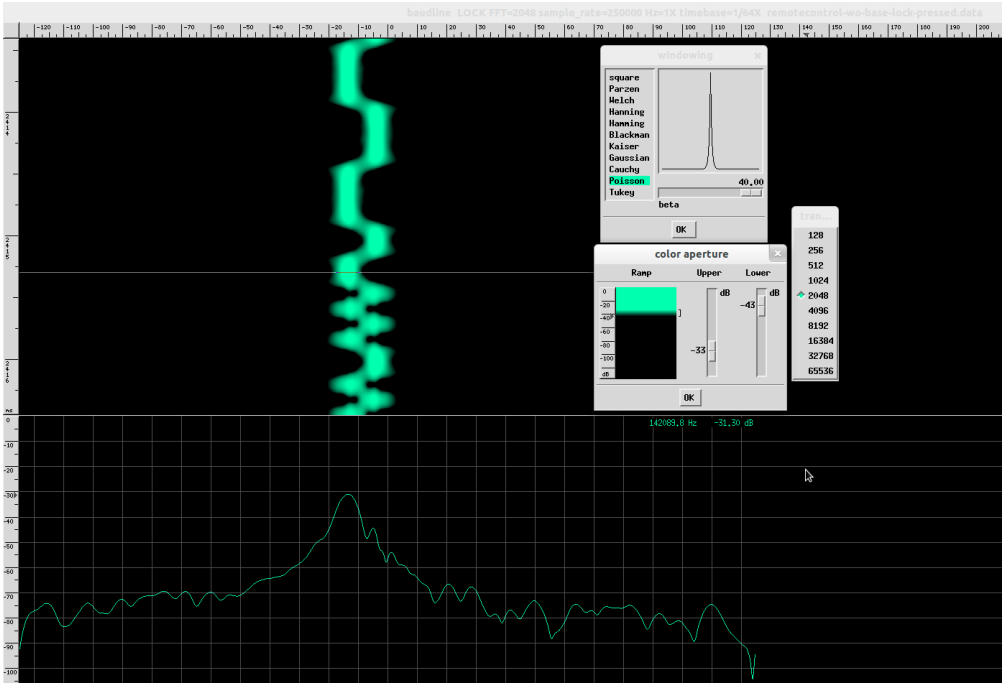


Figure 3.1: A datagram of the remote control in Baudline.

[1] Ettus Research, `http://www.ettus.com` (last accessed May 9, 2012)
[2] GNU Radio, `http://gnuradio.org` (last accessed May 9, 2012)
[3] Baudline, `http://www.baudline.com/` (last accessed May 9, 2012)

The left-right pattern (or mark and space in FSK) already represents a radio datagram. The visible part of this signal is transcribed from top to bottom as 000011110000110010101010. This bit sequence requires some further processing, which is documented later. This will transform the transmitted bits into new datagrams. To indicate that these datagrams are different, the datagram here is called "radio datagram" while the later processing results in "Secvest datagrams."

The frequency difference between mark and space was measured as 9.5 to 10 kHz and the bitrate is around 8200 bits per second.

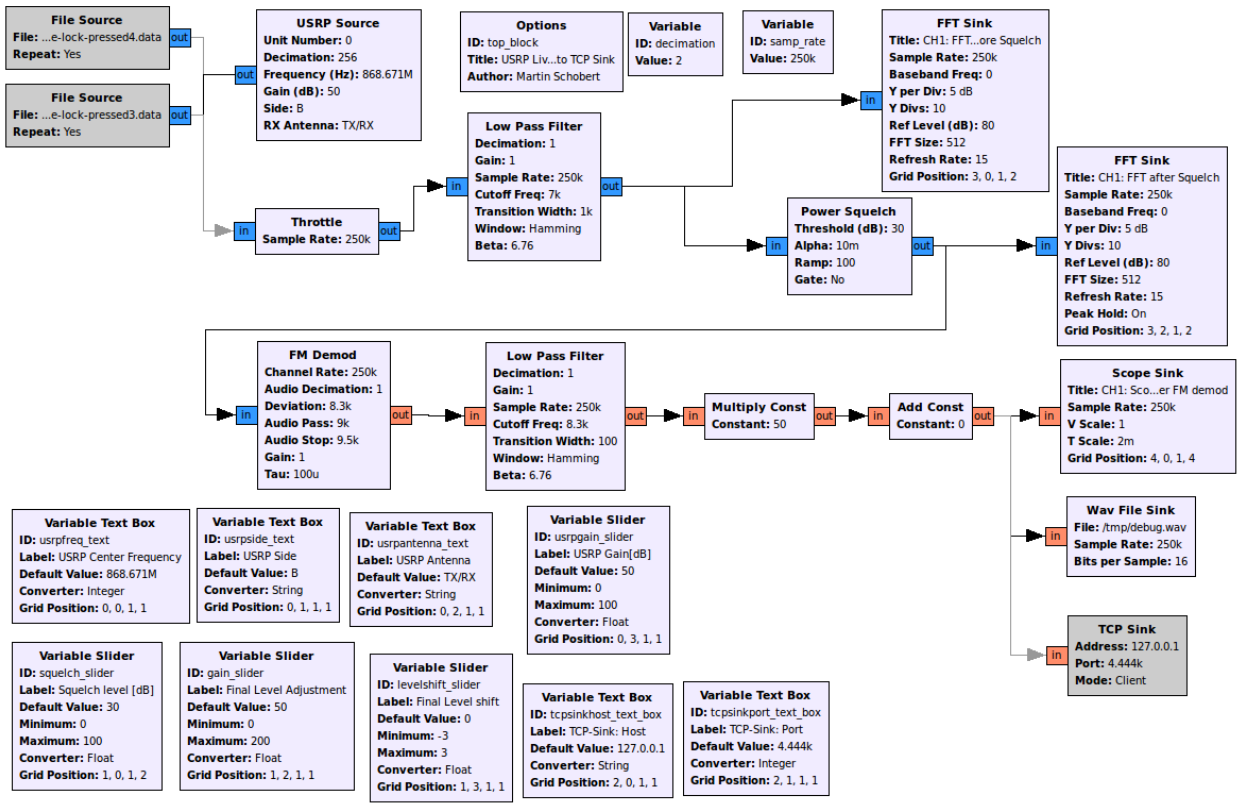


Figure 3.2: Signal flow graph to capture radio transmissions.

To capture the baseband signal the tester set up a signal flow graph using GNU Radio Companion[4]. This flow graph is illustrated in figure 3.2. The flow graph uses the USRP or files as sources, performs filter and squelch operations, and demodulates the signal. The resulting baseband signal is stored in a file or passed to a TCP socket. Running the signal flow block gives the user a graphical interface to adjust reception parameters and to inspect scopes and FFT plots (cf. figure 3.3).

The tester used this setup to record a set of radio transmissions from the remote control. Each datagram is transmitted in 72.3 ms. Seven individual radio datagrams were extracted from the recording and aligned to allow a vertical comparison, which is shown in figure 3.6. This figure

[4]GNU Radio Companion, http://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioCompanion (last accessed May 9, 2012)


Figure 3.3: GUI for adjusting capturing parameters.

illustrates the general format of a radio datagram: It starts with an (optional) preamble, followed by a short synchronization pattern and a first protocol data unit. Directly after this protocol data unit a second short synchronization pattern is observable, followed by a second protocol data unit. Finally, the remote control's radio datagram terminates with a third synchronization pattern. Both protocol data units in a radio datagram are equal.

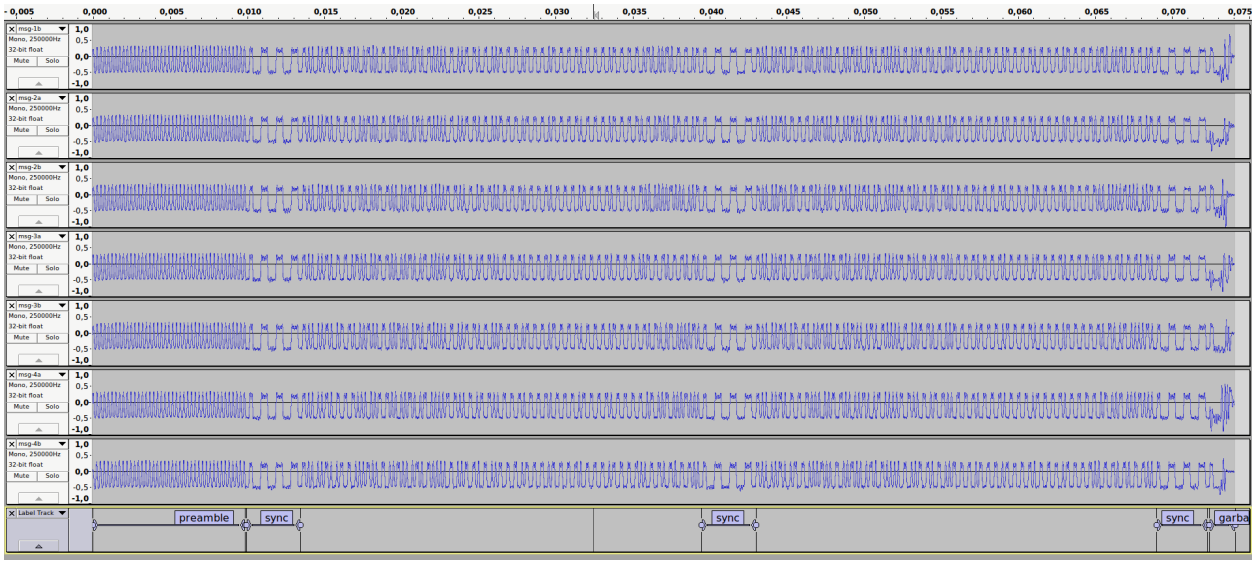


Figure 3.4: Comparison of radio transmissions.

As far as observed, Secvest datagrams from the alarm panel are repeated four times within a single radio datagram, which is shown in figure 3.5.

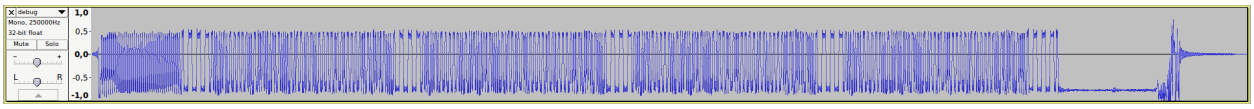

Figure 3.5: Single burst from the alarm central shows the synchronization pattern five times.

According to public sources, data is transmitted repeatedly to raise the probability of successful reception. And as observed, there is no acknowlegment of datagrams. Doubling the protocol data unit within a radio telegram seems to be a method to achieve redundancy. Further analysis of radio communication shows that data is also repeatedly transmitted in consecutive radio datagrams. This is considered in more detail later.

## 3.2 Decoding Secvest Datagrams

The protocol data unit (PDU) —that is the payload between the synchronization patterns—has to be transformed into bits. This process is documented in this section. A problem that must be solved beforehand is determining the right synchronization pattern, which reveals the correct PDU offset and gives a reasonable encoding in whole bytes.

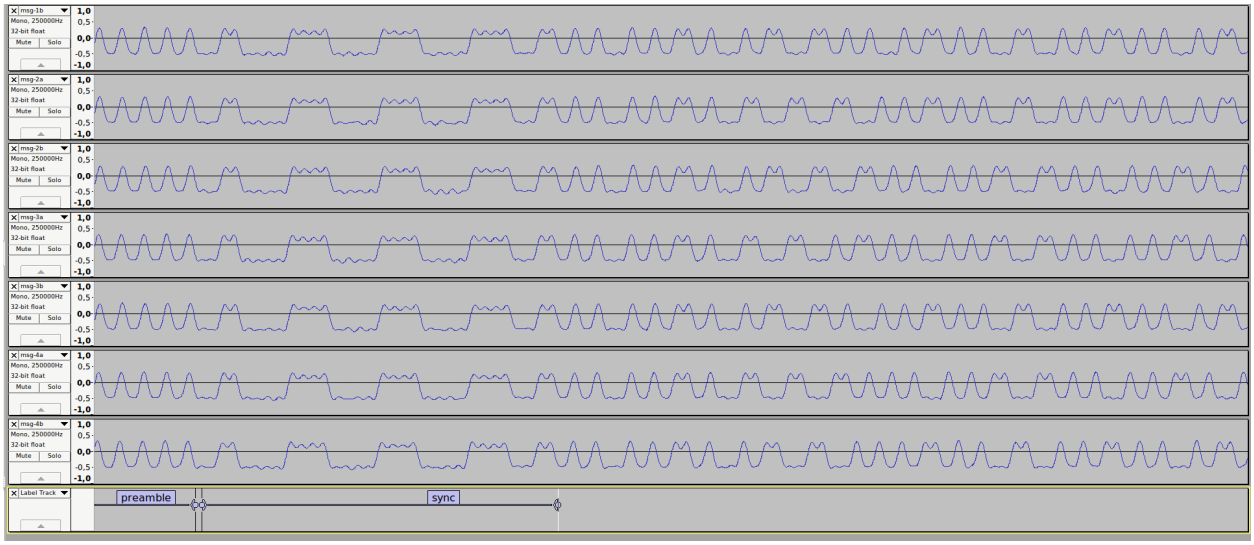


Figure 3.6: Comparison of radio transmissions: The regular pattern to the left is part of the preamble, followed by a synchronization pattern. The remainder is part of a protocol data unit.

First, it is observable that the protocol data unit has a maximum of two consecutive equal symbols like 00 or 11, while the synchronization pattern shows four consecutive equal symbols 0000 or 1111. This indicates the presence of a line encoding for the protocol data unit. Second, by

vertically comparing the messages it is observable that there are inverted patterns (cf. figure 3.6). While one sequence might be read as 001100 another message's sequence for the same offset is 110011, which indicates that bits are encoded in the transition between levels rather than the level itself, especially if only minor changes in consecutive messages are expected.

But where does the frame start and where does it end? The 000011110000111100001111 pattern (0x0F0F0F in short) is obviously part of the synchronization pattern, because it is neither part of the preamble nor part of the protocol data unit. Left and right of the 0x0F0F0F pattern are two more patterns: 0011. This "symmetry" is most likely not coincidental. Treating this additional pattern as part of the synchronization fills up the sync sequence to four bytes, without leaving some bits unassigned to a byte. Thus, the whole synchronization sequence is 0x30F0F0F3.

The derived synchronization pattern now determines the PDU's start and end. The PDU is extracted for further analysis. As mentioned above there is a line encoding present, which is a Differential Manchester encoding. By comparing two consecutive bits from the radio datagram it is possible to decide if the original data bit is either 0 or 1. If both bits are equal, the original bit is 0, otherwise 1. For example, a sequence of 01.01.00.10.11.00.10.11 decodes to 11010010. Processing the whole PDU then results in Secvest datagrams.

# 4 Analyzing Secvest Datagrams

## 4.1 Interpreting the Datagram Format

Reverse-engineering the Secvest datagrams started with analyzing transmissions from the remote control: Pressing buttons on the remote control triggers datagram transmissions. Each button-press results in four Secvest datagrams: Two Secvest datagrams are encoded in a single radio datagram as described in section 3.1 and the remote control sends out two radio datagrams. The corresponding Secvest datagrams are shown below.

Pressing the activate button on the remote control:

```
1101101000001010011000110110101001111000110001000110000001000000010000000100000001000000010101110010011001
1101101000001010011000110110101001111000110001000110000001000000010000000100000001000000010101110010011001
1101101010001010011000110110101001111000110001000110000001000000010000000100000001000000010010100111110000
1101101010001010011000110110101001111000110001000110000001000000010000000100000001000000010010100111110000
        +------+                                                +----------------------++--------------+
         counter                                                     button state            checksum
```

Pressing the deactivate button:

```
1101101000000110011000110110101001111000110001000110000001000000010000000100000001000000010100000110111101
1101101000000110011000110110101001111000110001000110000001000000010000000100000001000000010100000110111101
1101101010000110011000110110101001111000110001000110000001000000010000000100000001000000010001001110100101
1101101010000110011000110110101001111000110001000110000001000000010000000100000001000000010001001110100101
```

Pressing the user-defined button:

```
1101101000001110011000110110101001111000110001000110000001000000000100000001000000010000111000000000100100
1101101000001110011000110110101001111000110001000110000001000000000100000001000000010000111000000000100100
1101101010001110011000110110101001111000110001000110000001000000010000000100000001000000000100001001100100
1101101010001110011000110110101001111000110001000110000001000000010000000100000001000000000100001001100100
```

Pressing the query button:

```
1101101000000001011000110110101001111000110001000110000001000000010000000100000001000000010000001100000000
1101101000000001011000110110101001111000110001000110000001000000010000000100000001000000010000001100000000
1101101010000001011000110110101001111000110001000110000001000000010000000100000001000000010100100111101000
1101101010000001011000110110101001111000110001000110000001000000010000000100000001000000010100100111101000
```

Pressing the user-defined and query buttons at the same time:

```
1101101000001001011000110110101001111000110001000110000001000000011000000110000001100000101100010101010
1101101000001001011000110110101001111000110001000110000001000000011000000110000001100000101100010101010
1101101010001001011000110110101001111000110001000110000001000000011000000110000001100001011110010011110
1101101010001001011000110110101001111000110001000110000001000000011000000110000001100001011110010011110
```

Which button was pressed is directly observable in the Secvest datagrams. There are three fields encoding the button state and this field differs between transmissions. In the last example two

buttons were pressed, which is reflected by two set bits. Furthermore, comparing the datagrams reveals two more variable regions. The first region represents a counter and the last region is a checksum as described in the next two sections.

## 4.2 Identifying the Checksum Algorithm

In general, radio communication is affected by interferences. Engineers use checksums to detect errors in broadcasted datagrams. Obviously, the Secvest system requires a checksum method, too, because it is sensitive to accidentally changed bits. Thus, it is self-evident that a Secvest datagram's last 16 bits is some type of checksum: The checksum is deterministic—equal datagram bodies have the same checksum value. Furthermore, minor changes between datagram bodies result in completely different checksums.

The tester assumed that a cycling redundancy check (CRC) is used and brute-forced its parameters[1]. This reveals the truncated polynomial as `0x1021`, which is a common polynomial for CRC-16. The CRC register is initialized with zero and no final XOR operation is applied to the CRC value. The CRC-16 is calculated for the whole Secvest datagram bits in transmission order starting at offset `0`. An implementation is given below.

```
uint16_t secvest_calc_crc(uint8_t * buf, unsigned int len) {
  uint16_t crc = 0;
  unsigned int i, k;

  for(k = 0; k < len; k++ ) {
    for(i = 0; i < 8; i++ ) {
      int bit = ((buf[k] >> (7-i) & 1) == 1);
      int c15 = ((crc >> 15 & 1) == 1);
      crc <<= 1;
      if(c15 ^ bit) crc ^= 0x1021;
    }
  }
  return crc;
}
```

[1] Brute-forcing CRC parameters, http://sitsec.net/blog/2012/02/10/brute-forcing-crc-parameters/ (last accessed May 9, 2012)

## 4.3 The Counter Field

Interpreting transmitted bits from the remote control as bytes shows that the second byte is a counter. The counter value looks reasonable if the leftmost bit is treated as the lowest significant bit. The first nibble of the second byte is a four bit looping counter, while the second nibble indicates the number of the radio datagram repetition. The Secvest datagrams below are equal to the datagrams from section 4.1, though redundant Secvest datagrams are omitted.

```
5b 50 c6 56 1e 23 06 02 01 01 01 75 32  // activate
5b 51 c6 56 1e 23 06 02 01 01 01 52 1e

5b 60 c6 56 1e 23 06 02 02 02 02 05 bb  // deactivate
5b 61 c6 56 1e 23 06 02 02 02 02 22 97

5b 70 c6 56 1e 23 06 02 08 08 08 07 48  // user-defined
5b 71 c6 56 1e 23 06 02 08 08 08 20 64

5b 80 c6 56 1e 23 06 02 04 04 04 02 03  // query
5b 81 c6 56 1e 23 06 02 04 04 04 25 2f

5b 90 c6 56 1e 23 06 02 0c 0c 0c 1a 55  // user-defined and query
5b 91 c6 56 1e 23 06 02 0c 0c 0c 3d 79
```

The magnetic contact detector has a slightly different repetition pattern. It repeats radio datagrams four times (that are eight Secvest datagrams). Thus the repetition counter ranges from zero to three. An example of the traffic pattern is illustrated below. Redundant Secvest datagrams from the same radio datagram are omitted.

```
4b 90 16 40 1d  3  1  0  0  0 af 80
4b 91 16 40 1d  3  1  0  0  0 52 cd
4b 92 16 40 1d  3  1  0  0  0 55 1b
4b 93 16 40 1d  3  1  0  0  0 a8 56
```

## 4.4 The Address Field

ABUS claims that the Secvest 2WAY and Secvest IP alarm systems use encryption as documented in figure 1.2 and that there are 16,777,214 “variations”. However, this analysis shows that there is no encryption at all. Instead, these “variations” are simple addresses, which are technically required in the alarm system to identify a datagram’s source. These $2^{24} - 2$ addresses are encoded in a three byte value, which must be present somewhere in a datagram.

```
4b 11 16 40 1d  3  1  7  7  7 37 bc
5b a0 c6 56 1e 23  6  2  8  8  8 d8 69
```

The first line is an example message from the magnetic contact detector and the second line represents a remote control datagram. Obviously, the underlined sequence is the address field of three bytes.

The next Secvest datagram shows an alarm central's response to a status request from the remote control, where the address field does not contain the sender's address. Instead, this field specifies a destination address, which is the remote control.

```
5b 80 c6 56 1e 21  6 10  1 44 2e
```

The remote control's address bytes are 0xC6561E and one of the numbers printed on the label is 23578206, which is 0x167C65E in hex (cf. figures 2.1 and 2.4). Even if there are some digits in both hex numbers, this is most likely a mere coincidence. There is no obvious way to correlate the printed numbers with these addresses.

## 4.5 Hypothesis on Remaining Bytes

Because some bytes from the Secvest datagrams are constant as far as observed, it is difficult to imagine their meaning. Some questions are still left which help hypothesize how these unidentified bytes might be used. In the telegrams below the unidentified bytes are highlighted.

```
4b 11 16 40 1d  3  1  7  7  7    37 bc
5b a0 c6 56 1e 23  6  2  8  8  8 d8 69
5b 80 c6 56 1e 21  6 10  1       44 2e
```

**Datagram length:** Secvest datagrams differ in their size, depending on the device which sent it. But how is the datagram length reflected? In general, there are basically two options: Either the datagram length is explicitly encoded or it is implicitly known by the receiver. The latter requires an encoded datagram type, which helps the receiver to discriminate the datagram type. If the length is encoded explicitly, this information must be stored somewhere in the datagram. Then this information is either given for the full datagram or just for the variable part. The second nibble of the sixth byte seems to indicate the number of parameters, which is three for the sequences 7 7 7 and 8 8 8 while it is one in the last Secvest datagram, which just encodes a single 1.

**Datagram type:** If the alarm central receives a datagram it has to interpret the message. Because button-presses on the remote control are similarly encoded as the magnetic contact detector's state, the receiver has to determine the message type. This might be encoded in the seventh byte (here 1 and 6).

```
4b 11 16 40 1d  3  1  7  7  7    37 bc
5b a0 c6 56 1e 23  6  2  8  8  8 d8 69
5b 80 c6 56 1e 21  6 10  1       44 2e
```

**Device specific content:** Decoding the remaining bytes as described above leaves two, three, and four bytes for the device specific content (e.g., the button state) as shown below. This payload is further analyzed in the next two sections, but there are still some unidentified positions. The values 0x10 and 2 in the highlighted sequence might encode a message sub-type, but this is speculative.

```
4b 11 16 40 1d  3  1  7  7  7    37 bc
5b a0 c6 56 1e 23  6  2  8  8  8 d8 69
5b 80 c6 56 1e 21  6 10  1       44 2e
```

**Protocol identifier:** The first byte of a Secvest datagram might be some kind of protocol identifier. However, it might be part of the radio datagram as well. Due to lacking device samples a conclusion is not yet possible.

## 4.6 The Remote Control

As already shown in section 4.1 the remote control's button state is encoded in a Secvest datagram. Therefore, each button state is represented as a bit and the state is repeated three times within a telegram. The table below summarizes the state byte. Datagrams for combined key-presses are not always sent by the remote control, but sometimes they are. This might indicate a firmware bug.

| Value | Button(s) pressed |
|---|---|
| 1 | Activate |
| 2 | Deactivate |
| 4 | Query the alarm state |
| 8 | User-defined |
| 3 | Activate and deactivate |
| 6 | Query and deactivate |
| 9 | Activate and user-defined |
| c | Query and user-defined |

Table 4.1: Encoded button states for single and combined key-presses.

## 4.7 The Magnetic Contact Detector

The magnetic contact detector encodes its state in Secvest datagrams, too. While there is one bit for encoding the presence of a permanent magnet and one bit for indicating the sabotage state, there is also another bit which indicates if the state has changed or not. Table 4.2 gives an overview of the encoded states.

| Value | State changed | Sabotage detected | Magnet present |
|---|---|---|---|
| 0 | yes | no | yes |
| 1 | yes | no | no |
| 2 | yes | yes | yes |
| 3 | yes | yes | no |
| 4 | no | no | yes |
| 5 | no | no | no |
| 6 | no | yes | yes |
| 7 | no | yes | no |
| 7 | state independent heartbeat signal | | |

Table 4.2: Encoded states.

The example below shows a traffic pattern of the magnetic contact detector. Initially, the magnet is removed, which results in a state change. The state change is sent, where the value 1 indicates the new state. After around 180 seconds, the detector sends a heartbeat signal (with another source address), which is repeated every four minutes. Four minutes after the initial state change the current state is sent again, but flagged as unchanged using the value 5. Every four minutes the state is repeated, too.

```
4b 10 16 40 1d  3  1  1  1  1 f5 16        0.184 s
4b 11 16 40 1d  3  1  1  1  1  8 5b        0.371992 s
4b 12 16 40 1d  3  1  1  1  1  f 8d        1.493940 s
4b 13 16 40 1d  3  1  1  1  1 f2 c0        1.864996 s
4b 20 17 40 1d  3  1  7  7  7 d8 78        179.592725 s
4b 21 17 40 1d  3  1  7  7  7 25 35        180.538776 s
4b 30 16 40 1d  3  1  5  5  5 e9 a3        239.870319 s
4b 31 16 40 1d  3  1  5  5  5 14 ee        240.191142 s
4b 40 17 40 1d  3  1  7  7  7 82 69        419.446068 s
4b 41 17 40 1d  3  1  7  7  7 7f 24        419.615118 s
4b 50 16 40 1d  3  1  5  5  5 b3 b2        479.696664 s
4b 51 16 40 1d  3  1  5  5  5 4e ff        480.419579 s
4b 60 17 40 1d  3  1  7  7  7 bb 9e        659.245330 s
4b 61 17 40 1d  3  1  7  7  7 46 d3        660.190427 s
4b 70 16 40 1d  3  1  5  5  5 8a 45        719.522040 s
4b 71 16 40 1d  3  1  5  5  5 77  8        719.843148 s
```

Now the sabotage detection is triggered, while the magnet is present: The state change is im-

mediately communicated with subsequent "state unchanged" messages every four minutes. The time difference between the heartbeat signal and the state message is approx. 10 seconds, while it was 180 seconds in the previous example. This most likely means that the heartbeat signal is time-independent of the state messages.

```
4b e0 16 40 1d  3  1  2  2  2 7b cb        0.169 s
4b e1 16 40 1d  3  1  2  2  2 86 86        0.246971 s
4b e2 16 40 1d  3  1  2  2  2 81 50        0.993902 s
4b e3 16 40 1d  3  1  2  2  2 7c 1d        1.991765 s
4b f0 17 40 1d  3  1  7  7  7 f8 a5        39.970773 s
4b f1 17 40 1d  3  1  7  7  7  5 e8        40.263712 s
4b  0 16 40 1d  3  1  6  6  6 d3 5c        239.871055 s
4b  1 16 40 1d  3  1  6  6  6 2e 11        240.66344 s
4b 10 17 40 1d  3  1  7  7  7 75 70        279.769070 s
4b 11 17 40 1d  3  1  7  7  7 88 3d        280.492132 s
4b 20 16 40 1d  3  1  6  6  6 ea ab        479.696705 s
4b 21 16 40 1d  3  1  6  6  6 17 e6        481.517802 s
4b 30 17 40 1d  3  1  7  7  7 4c 87        519.595416 s
4b 31 17 40 1d  3  1  7  7  7 b1 ca        519.943402 s
4b 40 16 40 1d  3  1  6  6  6 b0 ba        719.522037 s
4b 41 16 40 1d  3  1  6  6  6 4d f7        720.593116 s
4b 50 17 40 1d  3  1  7  7  7 16 96        759.420829 s
4b 51 17 40 1d  3  1  7  7  7 eb db        759.741803 s
```

What happens if the magnet is not present and the device detects tampering? The state change is indicated by sending a 3. To encode that the state did not change a value of 7 has to be transmitted, but this is used for the heartbeat, too.

```
4b  0 16 40 1d  3  1  3  3  3 7b 4c     0.106 s
4b  1 16 40 1d  3  1  3  3  3 86  1     1.122006 s
4b  2 16 40 1d  3  1  3  3  3 81 d7     1.494001 s
4b  3 16 40 1d  3  1  3  3  3 7c 9a     2.491023 s
4b 10 17 40 1d  3  1  7  7  7 75 70     164.591497 s
4b 11 17 40 1d  3  1  7  7  7 88 3d     164.911657 s
4b 20 16 40 1d  3  1  7  7  7 67 f9     239.870352 s
4b 21 16 40 1d  3  1  7  7  7 9a b4     240.93311  s
4b 30 17 40 1d  3  1  7  7  7 4c 87     404.416228 s
4b 31 17 40 1d  3  1  7  7  7 b1 ca     405.112256 s
4b 40 16 40 1d  3  1  7  7  7 3d e8     479.696642 s
4b 41 16 40 1d  3  1  7  7  7 c0 a5     480.642800 s
4b 50 17 40 1d  3  1  7  7  7 16 96     644.242510 s
4b 51 17 40 1d  3  1  7  7  7 eb db     644.563600 s
4b 60 16 40 1d  3  1  7  7  7  4 1f     719.523034 s
4b 61 16 40 1d  3  1  7  7  7 f9 52     719.718035 s
```

It is possible that the third byte is not part of an address and has another meaning. But it is also possible that the heartbeat signal was introduced later and is not present in earlier devices.

There are enough bits left to store another state, but they are not used. Maybe using another address is a workaround for preserving protocol compatibility. If the alarm central implements this “extension”, too, the central might interpret this telegram. Else the telegram is most likely ignored, because the datagram sender is not known.

## 4.8 Alarm Central

In the test setup there was only one type of message format to observe. This is described in this section. Obviously, there must be other message types as well, because ABUS offers wireless sirens and wireless electrical sockets and these devices must be controlled via radio communication, too. However, these devices are not part of the test setup and are therefore not examined.

In the first test the alarm system is disarmed. The remote control requests the alarm system’s status. The request is sent by pressing the corresponding button on the remote control. This results in a status message, where the parameter value 1 indicates that the state is disarmed. This test is repeated. The panel always responds with value 1:

```
5b 80 c6 56 1e 21  6 10  1 44 2e
5b 90 c6 56 1e 21  6 10  1 3c 75
5b a0 c6 56 1e 21  6 10  1 b4 98
```

Now the deactivate button is pressed on the remote control while the system is disarmed. Again, the panel sends parameter value 1 back. This test is repeated three times. The message counter increments and the payload is constant, except for the trailing CRC, which differs due to a changed message counter.

```
5b b0 c6 56 1e 21  6 10  1 cc c3
5b c0 c6 56 1e 21  6 10  1 b5 4b
5b d0 c6 56 1e 21  6 10  1 cd 10
```

After pressing the activate button, the panel responds with a value 2. This indicates that the alarm system is armed:

```
5b e0 c6 56 1e 21  6 10  2 de cf
```

Requesting the status shows that the alarm system is still armed:

```
5b f0 c6 56 1e 21  6 10  2 a6 94
```

Now, the alarm system is disarmed by pressing the deactivate key on the remote control. The panel sends a value 1 back to the remote control:

```
5b  0 c6 56 1e 21  6 10  1 a6 e5
```

In the next test the alarm system should be activated, but the magnetic door contact is open. Thus, arming the alarm system is not possible, which is acoustically indicated by the panel. A corresponding Secvest datagram is transmitted, too. Here the parameter is set to 4:

```
5b 60 c6 56 1e 21  6 10  4  a 61
```

Pressing the user defined button on the remote control does not result in a response from the panel. In any other case the panel sends a status message to the remote control and uses the remote control's ID as the destination address. The payload always indicates the current status, which is summarized in table 4.3.

| Value | Description |
|---|---|
| 1 | The alarm system is disarmed |
| 2 | The alarm system is armed |
| 4 | The alarm system cannot be armed |

Table 4.3: Encoded status in Secvest datagrams sent by the panel.

# 5 Security Considerations

The threat of bypassing an intruder alarm is present. And the likelihood of exploiting vulnerabilities increases if intruders are able to use well-developed bypassing devices. For example, specialized devices for circumventing car immobilizer are already common. It is possible to develop such a device for the Secvest system and maybe many other wireless intruder alarm systems, too.

## 5.1 General Observations

The Secvest wireless protocol is a straight forward design as written in the textbooks and it is just as easy to reverse-engineer the communication protocol. The system doesn't even implement a simple form of protocol obfuscation in order to increase the reverse-engineering effort. Because the wireless protocol shows no protection mechanism against attacks, the Secvest system cannot grant confidentiality, integrity, and authenticity of communication. This is a security weakness, especially if messages are transmitted via a shared and remotely accessible medium.

**Datagrams are unencrypted:** The Secvest system uses a plaintext protocol. Hence, an attacker might eavesdrop datagrams to acquire a list of devices belonging to an alarm system. Knowing valid device addresses allows an attacker to inject datagrams into a burglar alarm system. Furthermore, an attacker might observe the state of the alarm central, which is communicated in plaintext as well.

**Datagrams are unauthenticated:** Once a valid device address is known, an attacker might inject spoofed datagrams. Datagrams are not protected by any message authentication or even any kind of rolling code.

**Datagrams are predictable:** As far as observed, Secvest datagrams are predictable. Even if there are some bytes in Secvest datagrams of a still unknown meaning, these bytes are constant. Therefore, it is not necessary to understand their meaning if an attacker just wants to disarm an alarm system.

It is not necessary to implement state-of-the-art cryptographic algorithms for an intruder alarm system, but implementing no countermeasures against attacks is insufficient.

## 5.2 Distribution of Addresses

For the test setup it was possible to eavesdrop some device addresses—two addresses of the

magnetic contact detector and one address of the remote control. These are shown below. It is possible that the third octet is the most significant byte and the first octet the least significant one. At least the 1-difference between the magnetic contact detector's addresses and the 1-difference in the last octet support this assumption. Under this assumption it is further possible that addresses are not randomly distributed over the entire address space, because the address difference is just 71344. It might be a coincidental observation. However, with more measured values, this impression can be corroborated or refuted.

```
c6 56 1e => 1e 56 c6 (?)
16 40 1d => 1d 40 16 (?)
17 40 1d => 1d 40 17 (?)
```

If this assumption of a not randomly distributed key space is true, the system would be susceptible to practical brute-force attacks. Nevertheless, identifying a valid remote control address by brute-forcing a portion of the address space would likely take several hours. In addition, for a practical attack the radio channel should not be completely saturated—regardless of the fact that this is against the law. If the alarm center fails to supervise a wireless detector for two hours, it will signal a fault (default setting in the test setup), tamper, or alarm, depending on the system configuration. Faults are reported via telephone and tamper and alarm signals will trigger an alarm. Furthermore, the alarm central detects jamming. This feature might be disabled (default setting in the test setup), but it is also possible to activate a siren. The Secvest system reports jamming if the radio channel is unusable for at least 30 seconds within one minute.

## 5.3 Recommendations

An intruder alarm system itself does not prevent intrusion. It only helps to detect intrusion in time. To protect a facility, mechanical measures should always be preferred. However, in reality things are different. Mechanical measures are often expensive, for example, if a facility is at ground level and has many windows, and an intrusion alarm with visible sirens at least serves as deterrence.

If a facility uses an ABUS Secvest 2WAY or Secvest IP intrusion alarm system and is beyond that inadequately protected by mechanical measures, using the remote control for arming and disarming should be avoided. Instead, using the proximity key or the PIN method on the alarm panel should be preferred. If an intruder enters a protected facility, the intruder has to locate the alarm panel and disarm it within a certain time. Even if the proximity transponder might be cloned, this type of attack requires much more preparation. In general, wired components should be preferred over wireless ones, but there are methods of bypassing them, too [Yea90].

# References


[ABU10] ABUS Security-Center GmbH & Co. KG. *Secvest 2WAY Installation Instructions (FU8006)*. Jan. 2010. URL: http://www.abus-sc.co.uk/content/download/161038/1971757 (visited on 05/10/2012).

[Ana07] Analog Devices. *ADF7021. High Performance Narrow-Band Transceiver IC*. 2007. URL: http://www.analog.com/static/imported-files/data_sheets/ADF7021.pdf (visited on 05/10/2012).

[Atm02] Atmel Corporation. *Datasheet: FSK Transceiver for ISM Radio Applications, AT86RF211 (aka: TRX01)*. 2002.

[CEN09] CENELEC. *Alarm systems – Intrusion and hold-up systems. Part 5-3: Requirements for interconnections equipment using radio frequency techniques*. Version EN 50131-5-3:2005 + A1:2008. 2009.

[Inf02] Infineon Technologies AG. *Datasheet: Wireless Components - ASK/FSK Transmitter 868/433 MHz, TDK 5100*. Version 1.0. Oct. 2002. URL: http://www.infineon.com/dgdl/TDK5100_DS_V1.0.pdf?folderId=db3a3043191a246301192dd42ef02ae5&fileId=db3a3043191a246301192e05e62c2b3a (visited on 05/10/2012).

[Yea90] Wayne B. Yeager. *Techniques of Burglar Alarm Bypassing*. Loompanics Unlimited, Port Townsend, Washington, 1990. ISBN: 1-55950-032-8.