A Long-term Security Concept for IoT Products

Dr. Hans Herrmann
Head of Embedded Systems at cogitron GmbH
Pliening near Munich, Germany
Hans.Herrmann@cogitron.de

Michael Huber
cogitron GmbH
Pliening near Munich, Germany
Michael.Huber@cogitron.de

***Abstract*—A growing number of IoT devices is utilized to process sensitive data and provide critical services. They play an integral part for an increasing number of personal services (storing personal data) or safety relevant functions, which need to be protected by IT security concepts. This includes the use of cryptographic methods, to avoid unintended disclosure of information or unintended access to functionalities. - Nowadays, many IoT devices do have a lifetime of several decades. Thus, cryptographic measures in today's security concepts need to be designed for the future, including future technologies that support the attack of current state-of-the-art cryptographic approaches. Since the announcement and availability of quantum computers many widespread cryptographic algorithms are rendered obsolete. The development of new approaches and algorithms is necessary to ensure their effectiveness for the future. - In this paper we present a concept which utilizes post quantum cryptography to achieve long-term security. We elaborate on critical vulnerabilities of communication paths and provide three measures to counter them. Finally, we evaluate the concept with respect to the resources and the given targets.**

Keywords—IoT-device, post quantum cryptography (PQC), vulnerabilities, passwords, long-term security concept

I. Introduction

Quantum computers will exhibit significantly higher computing power, capable of implementing and executing cryptanalytic algorithms which render currently established encryption techniques ineffective [1]. Insufficient cryptographic techniques in current IoT devices lead to many security issues every day. The described approach result in the design of IoT-devices which are cryptographically secure for an elongated time span of an estimated 30 years.

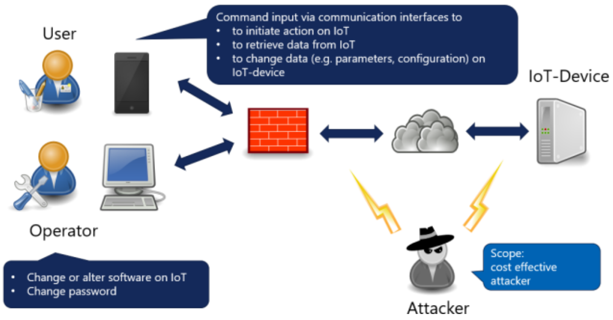
User
Command input via communication interfaces to
• to initiate action on IoT
• to retrieve data from IoT
• to change data (e.g. parameters, configuration) on IoT-device
IoT-Device
Operator
• Change or alter software on IoT
• Change password
Scope: cost effective attacker
Attacker

Fig. 1. Basic Setup, Use Cases

As depicted in Fig. 1. the article is scoped to the typical communication pathways of IoT-devices over classical network infrastructures. Furthermore, it is assumed that these devices implement the state-of-the-art concerning hardware security, thus, the depiction of the approach will be described above the hardware layer. As we talk about long-term, we expect the Y2K38-problem[1] to be solved. Furthermore, we assume the attacker will not physically compromise the IoT device due to the high costs of such action. Within this article, we highlight a threat actor, which aims at targeting large numbers of devices, which share common vulnerabilities.

Exemplary devices, which could especially benefit from this approach are utilized for continuous measurements like depicted in WELMEC 7.2 [2], smart home applications or roadside infrastructure for the realization of smart motorways.

II. Highwayman

A typical approach to obtaining passwords, is to capture them in transit, known as sniffing, and to subsequently attempting to decipher them with various cryptographic attacks (if encrypted) or exploiting weaknesses exhibited by communication protocols. In this scenario, an attacker, passing by like a highwayman, might catch the password to your IoT-device. It is assumed that there is no hard coded backdoor implemented, which seems to be a widespread fault. Consequently, the use of a single authentication token poses a

[1] Implementation storing the time as signed 32 Bit integer. See https://en.wikipedia.org/wiki/Year_2038_problem

high risk to IoT devices, implementing these simplistic mechanisms (see Fig. 2).

This issue is addressed by the first security measure that we would like to propose. As an improvement we suggest the usage of a bundle of passwords, which are indexed by an ID. The protocol would include the request of a specific password as identified by its ID by the IoT device.

As a consequence, a single compromised password does not pose an immediate threat and does not grant an attacker immediate access to the device. Since the acquired password is one out of a large set and the depicted protocol empowers the device itself (not the attacker) to demand a specific password, a potentially infeasible large number of passwords needs to be collected and compromised while at the same time the pool of all selectable passwords needs to be depleted, which, dependent on available storage capacities, can be infeasibly large.

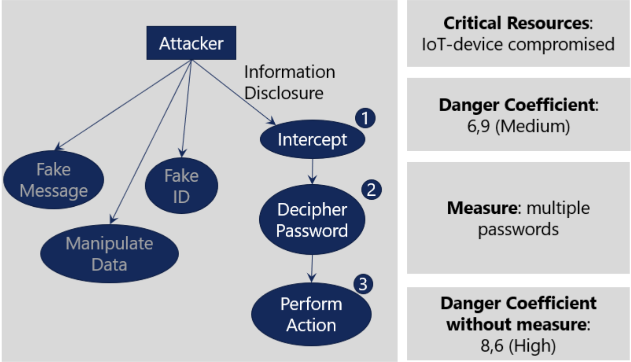
Attacker
Information Disclosure
Fake Message
Fake ID
Manipulate Data
Intercept
1
Decipher Password
2
Perform Action
3
Critical Resources: IoT-device compromised
Danger Coefficient: 6,9 (Medium)
Measure: multiple passwords
Danger Coefficient without measure: 8,6 (High)

Fig. 2. Vulnerability 1 - Password

Furthermore, it is possible to allow the use of the IoT-device by different roles or users. It is up to the IoT-device to define the ID of the next password needed to execute a command or to change the configuration. The size of the bundle of passwords should start with thousands for rarely used IoT-devices. The number increases with respective use cases. Mechanisms to counter the malicious depletion of available passwords need to be in place.

III. Quantum Computers

The next measure addresses the weakness of current cryptographic algorithms. Contemporary methods like RSA, DH, ECDH, and ECDSH will be rendered obsolete by presumably 2024[2]. DES, as used in many IoT-Devices for its simplicity, has lost the race against cryptanalytics. Its attack is depicted in Fig. 3.

Our proposal is, to use the AES, as well as FrodoKEM. AES makes use of the avalanche effect for encryption. The underlying well known basic idea of Feistel optimized by Rijndael leads to a cryptographic method, which is expected to withstand the upcoming threat of quantum computing [8].

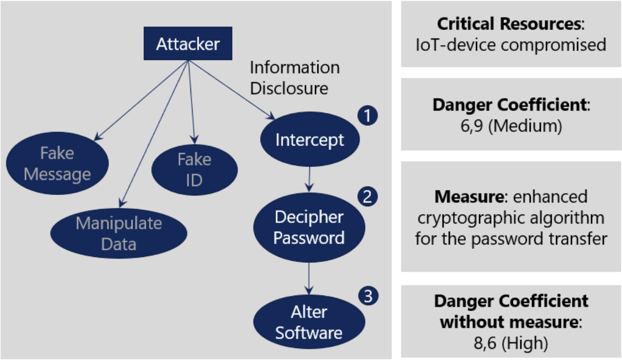
Attacker
Information Disclosure
Fake Message
Fake ID
Manipulate Data
Intercept
1
Decipher Password
2
Alter Software
3
Critical Resources: IoT-device compromised
Danger Coefficient: 6,9 (Medium)
Measure: enhanced cryptographic algorithm for the password transfer
Danger Coefficient without measure: 8,6 (High)

Fig. 3. Vulnerability 2 - Cryptography

FrodoKEM as a PQC method realizes the idea of a hard to solve problem (Learning with errors - LWE) coupled with a powerful pseudo-random function [4]. Our suggestion is, to use the variant denoted as "paranoid". It leads to a higher effort, but it fulfils our goal for long-term security.

Current investigations lead to the estimation that AES-256 as well as FrodoKEM will withstand attacks even with quantum computers.

IV. An Uncertain Future

Cryptoanalysis has developed into an ongoing business and ever improving attacks are expected to develop in the future. Since the proposed cryptographic methods could be compromised in the future, capabilities to switch the utilized method need to be implemented. This addresses implemented cryptographic algorithms for data in transfer, as well as data at rest for IoT-device.

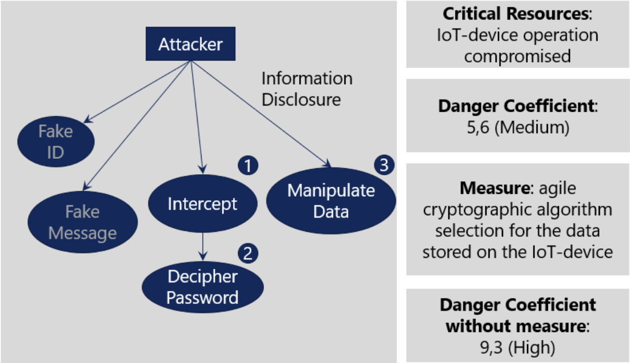
Attacker
Information Disclosure
Fake ID
Fake Message
Intercept
1
Decipher Password
2
Manipulate Data
3
Critical Resources: IoT-device operation compromised
Danger Coefficient: 5,6 (Medium)
Measure: agile cryptographic algorithm selection for the data stored on the IoT-device
Danger Coefficient without measure: 9,3 (High)

Fig. 4. Vulnerability 3 – Cryptography

The replacement of a cryptographic method should involve minimal maintenance, ideally during runtime by the operator of the system. A timely response to upcoming attacks for compromised cryptographic methods is thus possible (see Fig. 4).

[2] Announcement of IBM to build 1000 Qbit Quantum Computer in 2023. https://www.ibm.com/blogs/think/de-de/2020/12/quantentechnologie-gemeinsam-vorantreiben/

V. Mass Production

As of today, there are numerous publications describing the creation of pseudo random data. The interesting steps are the management of the passwords created, and the checks performed to qualify them [5].

Since the outlined approach relies on the usage of bundles of passwords the identification (ensuring uniqueness of the bundle) and handling of these bundles is crucial. This includes their secure persistence on the target IoT device.

VI. Resources

Concerning FrodoKEM, the memory consumption can reach up to 260 kB during operation [6]. It is thus only applicable for larger, more performant microcontrollers. The static size is measured with 65 kB [6]. Passwords will need at least 65 kB.

The performance of FrodoKEM is calculated based on [6] and [7] taking an ARM Cortex M4 and an Intel i7 as a reference.

TABLE I. Performance

Performance FrodoKEM		
Operation	***ARM C M4***	***Intel i7***
KeyGen	28,5 ms	1,4 ms
Encapsulation	36,1 ms	1,8 ms
Decapsulation	34,5 ms	1,7 ms

VII. Measuring Improvements

To evaluate each measure mentioned above, we applied the CVSS metric [3] to each vulnerability, before and after our proposed measures had been implemented. As a conservative approach, all other aspects are judged as described in the introduction.

TABLE II. Results

Evaluation Danger Coefficient (CVSS)		
Vulnerabilities	***Initial CVSS***	***CVSS with measure***
Vulnerability 1 - Password	8,6	6,9
Vulnerability 2 – Cryptography	8,6	6,9
Vulnerability 3 - Cryptography	9,3	5,6

To illustrate the improvment from another perspective the security level is calculated as the attack cost given as the base-2 logarithm. This is compared to the expected computing performance available for cryptanalytics in 2030.

TABLE III. Comparison

Device	***Level of Security***
Current IoT-device	64
Future IoT-device [4]	200

The level of security of current IoT-devices is calculated based on the assumption, that DES (64Bit) is still widespread, but used in an optimal way. The level for the future IoT-device is given by [4]. To illustrate this we estimate, that a type super computer making use of quantum capabilities will execute 2^{80} instructions per second.

TABLE IV. Estimated Time to Compromise IoT-device in 2030

Device	***Time span***
Current IoT-device	1 second
Future IoT-device	$4,2x10^{28}$ years

The three measures depicted in this article make IoT devices resilient against upcoming attacks and estimated computing power of quantum computers. It is unlikely that the typical communication pathway of an IoT-device equipped in this way will be compromised in the near future by means of cryptanalytics. It is more likely, that its original purpose might get obsolete in this time span.

Conclusion and Future Work

As shown, it is possible to fulfil the requirements defined by BSI [1]. The achieved security level assures the long-term operation of an IoT-device.

PQC algorithms are still in development. This is just a first approach to face long term problems. We expect hardware manufacturers to integrate first PQC modules in their hardware soon. This will reduce the price for this technique.

Side channel attacks are out of scope of this work. But future work should take these approaches into account.

References

[1] Migration zu Post-Quanten-Kryptografie - Handlungsempfehlungen des BSI; Stand: August 2020

[2] WELMEC 7.2 - www.welmec.org

[3] CVSS – https://www.first.org/cvss/

[4] FrodoKEM - https://frodokem.org/

[5] NIST Special Publication 800-22, 2010

[6] E. Alkim, J.W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikter, A. Raghunathan; FrodoKEM - Learning With Errors Key Encapsulation; March 25, 2020

[7] J. Howe, T. Oder, M. Krausz, T. Güneysu; Standard Lattice-Based Key Encapsulation on Embedded Devices, 2018

[8] Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Kürzel BSI TR-02102-1 Version:2020-01 Stand:24. März 2020