ATHENE
National Research Center
for Applied Cybersecurity

National Research Center for Applied Cybersecurity ATHENE

Tapplock Security Analysis Report

Christian Brandt, Matthias Cäsar

1 Summary

Vendor: Tapplock Corp.

Product: Tapplock one (TL104A), Tapplock one+ (TL203A)

Affected Version: version number unknown, newest firmware as of 2019-06-25

VCSS Score: 7.1 (High)

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

Severity: high

Remote exploitable: yes

Short description: The communication protocol between the Tapplock padlock models TL104A and TL203A and the corresponding tapplock smartphone app contains two cricital vulnerabilities. First, freshness verification of unlock messages is missing, allowing an attacker to perform a man in the middle attack. Second, the entropy of nonces is too low, allowing an attacker to probe for a previously captured challenge response data pair and subsequently performing a replay attack.

2 System under investigation

Three different padlock models from Tapplock Inc. exist. The first brought to market was the TL104A and is referred to as "Tapplock one". Later on, the TL203A appeared as its successor publicly known as "Tapplock one+". The third padlock available is the TLL05A advertised as Tapplock Lite. It is a slim alternative to the Tapplock One series and has been finally released in early 2020. Subject of this investigation are the TL104A and TL203A only. Both models can be easily distinguished by the imprint on the rear plate of the chassis. Aside from the built-in fingerprint sensor, these locks are typically used through smartphone apps available for both Android and iOS devices. Reverse engineering and exploit development have been done using Tapplocks android app version 3.2.2 which was the newest version available at the time of the analysis.

Padlocks are mainly used for theft prevention and access control. Depending on the target to be protected by the padlock, it might be necessary for the attacker to not leave any evidence of an attack. We therefore define the following three cases for differentiation.

destructive one-time: The attack shall be performed only once. The attack can be destructive and therefore detectable. One example is objects that are secured against theft, such as mountain bikes. In these cases, a mechanical approach can be used as an alternative to a cyber attack.

non-detectable one-time: The attack shall be carried out only once. However, the attack should not be detectable. This can be the case with locked rooms from which

objects are to be stolen or brought into.

non-detectable recurring: It shall be possible to perform the attack multiple times without leaving evidence of an unauthorized use of the locking system. This can be the case when sensitive documents in a locker or deposit box are to be accessed several times.

The Tapplock ecosystem provides the functionality to delegate locking rights to other users over the cloud backend. Bluetooth device pairing to obtain basic security functionality is therefore not expedient. Instead it's up to the application layer to take care of necessary security mechanisms to provide both security and convenience for such smart features. After authentication security flaws in their application layer security had been published, Tapplock Inc. implemented a new authentication method which is subject to both vulnerabilities described below.

For the described attacks we do not differentiate between various attacker capabilities. We generally assume that an attacker has the necessary hardware, such as a notebook, Raspberry PIs and Bluetooth controllers, and is in close proximity (below 100 meters) to the victim.

3 Vulnerability #1: Missing unlock message freshness verification

As soon as the Tapplock device has been powered on by pressing its central button, the corresponding smartphone app establishes an unencrypted connection when being started. An authentication using a proprietary challenge response procedure seems to be performed before any further communication takes place. This happens only once for each bluetooth connection. After that, the user presses a button to trigger the padlock to perform the physical unlock process. The unlock message is always the same for each authenticated connection. Figure 3.1 shows the messages exchanged between the smartphone and the Tapplock during challenge-response (A) and unlock procedure (B). Section (C) shows the Tapplock getting consecutively unlocked another three times.

Figure 3.1
BLE Unlock Padlock 01

Comparing the messages from section (B) and (C) shows that they're identical, which is always the case for any specific connection. To exploit this behaviour, we applied a man in the middle attack approach. The victims smartphone connects to the attacker and the attacker then connects to the tapplock. This results in two independend Bluetooth LE connections where the second connection to the tapplock is under control of the attacker. This method is undetectable by the smartphone, the Tapplock and the victim

itself. The victim can unlock and lock whatever is to be protected and subsequently leaves the area. While the first connection between smartphone and attacker is going to be disconnected, the second connection to the tapplock still persists. Now the attacker can resend the unlock message which has been obtained by eavesdropping the preceding communication.

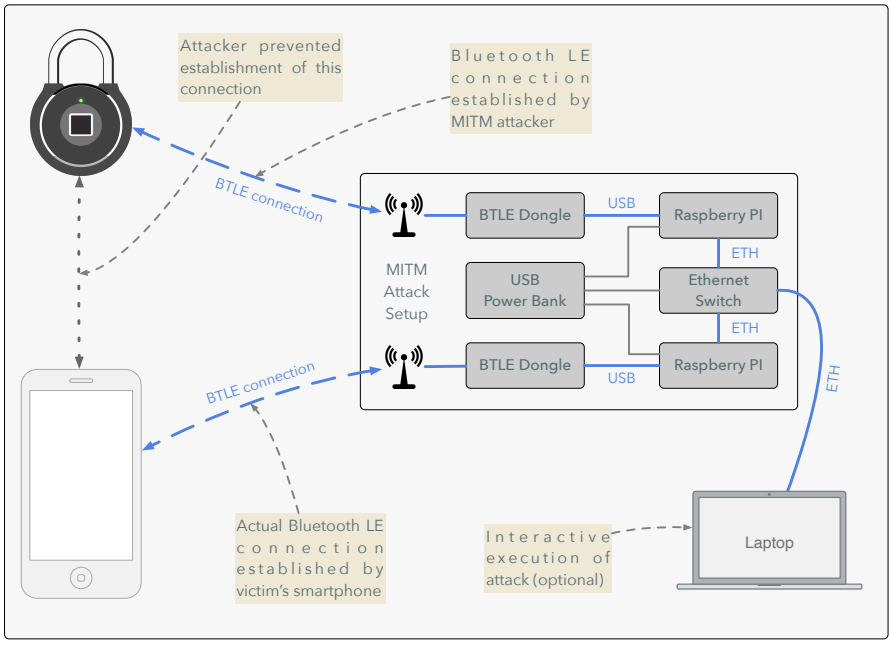

Figure 3.2
Man in the middle attack

To demonstrate MITM attacks on Bluetooth LE, we built a lightweight portable demonstrator. The basic setup consists of two raspberry PIs, two Bluetooth LE USB dongles, a USB powered ethernet switch and a power bank. For interactive analysis, a notebook is getting connected. External Bluetooth dongles are required in case of the used Raspberry PI model does not allow to change the Bluetooth device address, which is required for the attack. On the software side, our attack is fully based on GATTacker. Before performing the described attack, the targeted device has to be cloned. This can either be done with the Tapplock to be attacked or with any other identical lock. The latter case requires changing the MAC address to the Tapplock to be attacked, which can be obtained wirelessly when the victim is using his lock.

4 Vulnerability #2: Low entropy nonces and the absence of countermeasures

While the MITM procedure requires the attacker to be in close proximity to the victim every time he wants to unlock the padlock, our second attack only requires to capture the unlock procedure once. This is possible due to the fact that the security mechanisms used do not rely on proven security procotols but on weak proprietary implementation. We tested this implementation against randomness quality of the challenges provided. An attacker can request an unlimited amount of challenges without being slowed down or blocked by the Tapplock. Having a challenge response pair from a previous unlock procedure of the victim

using his Tapplock, it takes no more than sixty seconds until a challenge matching the one eavesdropped from the victim occurs. The attacker responds to that specific challenge with the matching response and has now authenticated the connection. To finally open the Tapplock, the unlock message has to be sent. This message seems to somehow be encrypted or scrambled. We discovered that if the challenges are identical, the unlock messages are too.

The attack is now straightforward and is composed of two steps. First, we capture the bluetooth communication while the victim is unlocking his Tapplock. This can easily be done using three BBC MicroBit [1] flashed with the BtleJack [2] firmware. As a result we get a triple consisting of challenge, corresponding response and unlock message. The second step is to use this information to unlock the Tapplock afterwards using a Nordic nRF52840 microcontroller. We wrote a firmware which establishes a connection to the Tapplock and requests challenges until a provided challenge matches the previously recorded challenge from the first step. Now we can send the corresponding response to obtain an authenticated connection. A button connected to our microcontroller allows us to send the corresponding unlock message as often as we want. This attack scheme can be repeated as often as desired without any boundaries, providing no less than a duplicate key which leaves no traces.

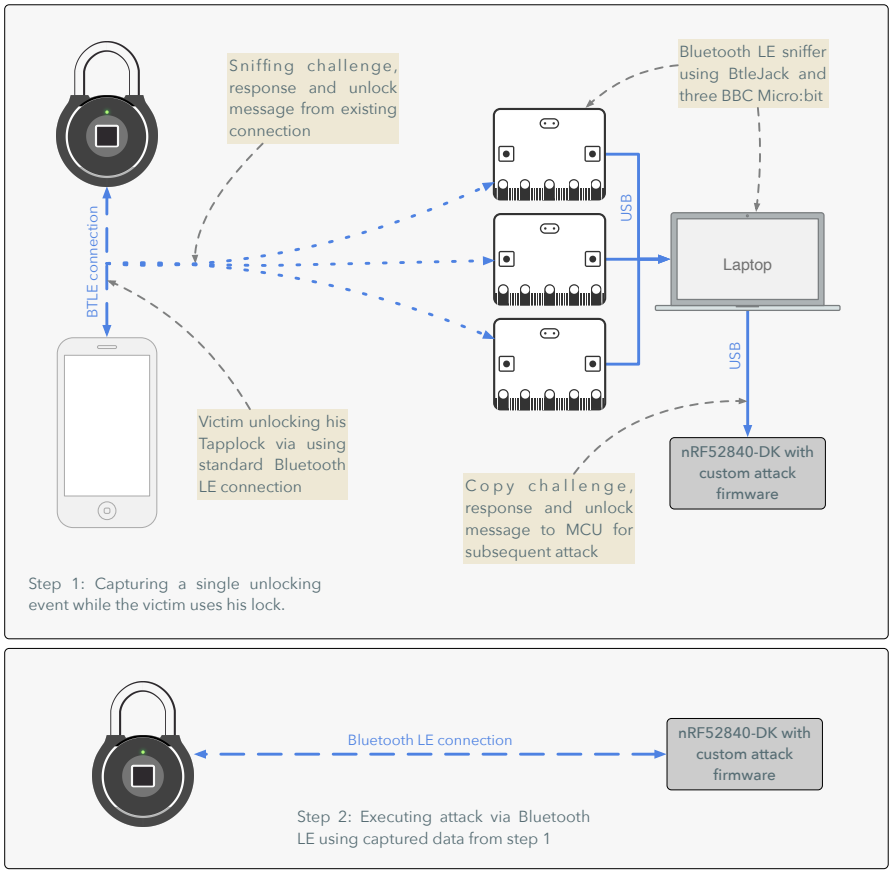

Figure 4.1
Low entropy attack

5 Conclusion

While the first vulnerability requires the attacker to be in place every time the victim uses his padlock, the second vulnerability only requires this once and gives the attacker a duplicate key for further subsequent unlocking operations and therefore has greater impact. Both attacks leave no traces and are therefore suitable for the defined attack scenarios *non-detectable one-time* and *non-detectable recurring*. When it comes to *destructive one-time* scenarios like protecting a mountain bike from being stolen, the Tapplock has little to counter against bolt cutters and therefore cybersecurity is circumstantial.

Both vulnerabilities could have been easily avoided or their impact at least minimized. A simple challenge-response based authentication scheme for every unlock procedure instead of only once per connection establishment would have prevented the first attack. The lack of a connection timeout allows the attacker to keep the connection to the Tapplock until the battery is drained and the absence of replay protection facilitates the attackers ability to replay unlock messages as long as the connection persists. Limiting the number of challenge requests for a particular connection or simply a forced delay drastically increases the time an attacker needs to find a reoccurring challenge. So even with low entropy, such an attack could take an unrealistically long time.

Fraunhofer SIT practices responsible disclosure for all security vulnerabilities found. We contacted Tapplock Inc. and sent them our findings so they are able to reproduce both attacks. Unfortunately, we haven't received any feedback afterwards. After some time, they released a firmware update for the TL203A model. Once the update was performed, our attacks stopped working. As of today, no update has been provided for the Tl104A model. We do not recommend the use of this padlock until a firmware update is provided.

Bibliography

[1] *Mirco:bit Website*. URL: `https://microbit.org/` (visited on 10/23/2020).

[2] *BtleJack: a new Bluetooth Low Energy swiss-army knife*. URL: `https://github.com/virtualabs/btlejack` (visited on 10/23/2020).