QubiBox Security & Usability Review

Last Revision: October 21, 2017

1. Scope

Although produced by information security professionals, this writing does not dwell on technical details that require the prior knowledge of complex security notions. When we use or refer to technically-loaded terms or concepts, we will do that mostly in the footnotes, where we also provide links to online resources for explanations. Anyone interested in discussing specific implementation choices is encouraged to contact us via email at techsupport@qubito.com. We would love to hear from you!

In this document we are mostly interested in providing the rationale for developing QubiBox in a way that can be appreciated also by the average consumer and by nontechnical professionals. The reason for this choice is simple: we believe that strong security can only be achieved if users convincingly become an informed and integral part of the process supported by a product.

The fundamental ideas underlying QubiBox are quite easy to understand, and are based on simple, practical good sense. We strongly believe that common sense arguments should remain at the root of the users' decision tree also when making choices impacting the privacy and security of their information managed using digital tools. To this end, we hope you will appreciate the approach we take in discussing security topics and the constant focus we try to keep on the practical concerns of the average individual.

One note on usability, the "stone guest" of most security products.

We made concerted efforts to embed usability and convenience in the QubiBox blueprint and to simplify the product's mental model, learnability and usage flows. Field testing confirmed that our product is very simple to use in all basic operating modes, although it requires stronger user engagement in its more advanced features. Of course, our commitment is to constantly improve usability and performance in future QubiBox releases and to carefully listen to all constructive criticism.

2. IT'S YOUR DIGITAL PERSONA!

It is a very common experience, both in real life and while operating in digital domains, to be asked to authenticate oneself before accessing resources of a sensitive nature, which must be made available only to authorized individuals. Web applications, as well as software running on smartphones and PCs, typically rely on passwords as the most common, simple and convenient form of authentication based on the use of a static (i.e. fixed in time) credential.

As you know, a password is a string of characters which you typically provide to an application each time you need to be granted access to a restricted resource. Under this simplified, but still very common scenario, the privacy and security of the resources unlocked after you provide the password hinge on the secrecy of your authentication credential. In practice, the security of the resources collapses to the security of the password: if the latter is compromised, so are the resources.

The exponential growth of digital applications and online services, and the need felt by service provides to grant the required level of privacy and security to users, has made passwords and their management a major concern for the average individual. This concern, of course, extends beyond the mere management of authentication credentials, since the real practical value lies not with passwords, but with the resources and information to which they are linked and enable access.

Besides passwords, consider data such as bank account and credit card numbers, PINs and entry codes, passport and driver's license IDs, alarm codes, software license strings, wireless router configurations, legal memos, wills and testaments, private phone numbers, medical tests and diagnoses, insurance policies, private pictures & movies, meeting memos, etc. This information altogether forms your "digital persona", the digitized information that uniquely profiles you as a private individual operating both in the physical world and across several distributed digital environments.

Taking a privacy- and user-centered approach to controlling and securing your digital persona, we suggest focusing on the following questions:

i. where is your private information stored?
ii. who and what controls access to it?
iii. how is it protected?

These questions address respectively the issues of trust, availability and protection against loss, theft, hacking, malware and spyware. We believe that answers to these questions should be carefully considered when evaluating products and solutions for managing your passwords as well as your private digital information.

3. MOTIVATION & APPROACH

Quite surprisingly, discussions about digital technology and software security seem to escape simple reasoning which would be considered obvious in the context of everyday management of material goods of some practical value. We believe this should not be the case, as we will attempt to show in this Section.

Let's consider one possible way to protect a set of physical documents very important to you. Since you need to access them frequently, you decided to keep these documents in your home inside of a safe box that can be opened only with one special key. For the sake of argument, let's assume that this safe box is practically unbreakable (i.e., it cannot be forced open).

Suppose also that you placed a copy of all your documents inside of another safe box, supplied and kept by Mr. Eklow[1], a distant acquaintance, who can deliver this second safe box to you at any time and location you may request for a low yearly fee.

You conveniently keep the keys of both safe boxes in your desk drawer at home, where you have a simple alarm system protecting only the main entrance door.

Now, let's check the answers to the questions we listed in the previous Section for the document protection method described above.

Your private documents are stored inside of two locked safe boxes, one in your possession and the other supplied and kept by Mr. Eklow. You have no practical way to verify where he keeps this second box, who has access to it and how well it is protected against loss or theft. You also don't know if Mr. Eklow made a copy of the key to open the safe box before giving it to you or if the safe box itself has any material weaknesses.

Should Mr. Eklow be robbed of the safe box, the thieves could open it by trying many different keys, exploiting any construction flaw or by forcing it. On the other hand, while you are away from home, thieves could easily bypass the alarm (e.g., deactivating its simple protections or entering through a window), find the key in your desk drawer, open your safe box and steal or copy the documents.

From this simple analysis, it is reasonable to conclude that the above method cannot be considered very effective for protecting your documents for the following reasons:

- keeping all the documents inside of your (supposedly unbreakable) safe box doesn't practically offer any strong protection: in fact, even a low-skilled burglar can break into your home, find the safe box and open it with the key he/her can readily find in your desk drawer.

[1] a purely fictitious individual, no reference intended to any real person.

- once your safe box is opened, all the documents can be stolen at once (an example of a catastrophic security failure).

- providing a copy of the documents to Mr. Eklow doesn't increase their security, which is primarily determined by the safety of your home, the weakest link in the security chain. In principle (and possibly also in practice), Mr. Eklow's involvement actually lowers the security of your documents by offering an additional attack opportunity to steal them.

- the decision to trust Mr. Eklow is groundless since it brings no additional security value and because you have no practical means to assess whether such trust is misplaced.

In other words, you failed to adequately protect the documents because you didn't quite appreciate how easily someone could break into your home, locate the safe box, find the key in your desk drawer, and steal all the documents in one single shot. Mr. Eklow could do nothing to avert this attack and you are left wondering if his involvement tipped off the thieves on the existence of your safe box at home.

Now, let's see how one can improve this protection method with just a few changes.

First, you don't want to give up the convenience of keeping your documents at home since you need to access them frequently. Also, there is no reason to invest massive efforts and money to strengthen your home's perimeter defenses: given enough resources and skills, someone will always be able to overcome them. Much better to leverage the strength of your safe box (which we assumed to be unbreakable for all practical purposes) and mitigate the risk of disclosure of all the documents at once.

To start, you could keep each document stored in your safe box inside of its own small safe box (of the same unbreakable model), so that now opening the larger safe box will not expose all the documents at once, but only a set of smaller boxes.

Next, you can provide all the keys that open the small safe boxes to Mr. Eklow, who will keep them all inside of a replica of your large safe box, so that you can open it with the same key you keep in the desk drawer. Upon receiving a call from you, Mr. Eklow can promptly[2] bring the safe box containing all the keys and hand it over to you personally. You can then open it and get the keys to open the small boxes that contain the documents you wish to access. After you are done working with the documents, you can lock the safe box containing all the keys to the small boxes and hand it over to Mr. Eklow, who can now leave your premises and wait for your next call.

[2] this is a good example of a typical tradeoff between convenience and security. Depending on how "promptly" you can receive the safe box, you may be willing to accept a slightly more elaborate procedure in exchange of substantial gains in privacy and security.

Let’s now check the answers to the questions we listed in the previous Section also for this modified document protection method.

Your documents are stored inside of only one safe box in your sole possession. Even if someone overcomes the simple perimeter defenses of your home, locates your large safe box and the key to open it in your desk drawer, he/she will be disappointed to find inside only a set of unbreakable small safe boxes.

The keys of these small safe boxes are nowhere to be found in your home and calling Mr. Eklow will not help since he responds only to calls coming from you. Should Mr. Eklow be robbed of the safe box in his possession, the thieves cannot do much with it (it’s unbreakable and, anyway, it contains only keys and none of your prized documents).

This modified protection scheme performs much better than the previous one for the following simple reasons:

- accessing the safe box kept at your home causes no critical security failure since all the documents are individually kept inside of unbreakable small safe boxes. You can relax about your home defenses being inadequate and focus your efforts on the elements that you can fully control.

- the documents are always under your possession. This eliminates the possibility of someone violating their privacy without your knowledge and, more importantly, it removes the need to entrust your documents to anyone else.

- the safe box with the keys kept by Mr. Eklow can be requested only by you and released only to you, which eliminates the risk of an attack done without your physical engagement and first-hand knowledge.

Of course, one could argue that also this improved scheme is vulnerable to serious threats, such as a combined attack whereby your safe box, the one kept by Mr. Eklow and the key required to open them are all stolen and available at the same time.

But this only proves that there is no perfect security, and shifts the discussion on the *efforts* required to carry out such complex, distributed attack. This is exactly where one wishes to take the attackers, i.e. to consider the *return on investment* on their criminal efforts. In fact, one could introduce additional components to further improve the protection method, thereby decreasing the likelihood of a successful attack while increasing its cost.

We can summarize the basic conclusions of this Section by stating that a *practically effective* security architecture should:

(i) be convenient and simple, so that users will not be induced to bypass it

(ii) protect against simple, main-stream attacks within reach of average criminals

(iii) avoid catastrophic security failures by adopting a threat-based security model

(iv) limit the need to trust third-parties

(v) distribute the resources required to break all protections, and

(vi) allow introducing new components to further reduce the criminals' return on investment and their incentives to craft and launch an attack.

4. The QubiBox Value Proposition

As mentioned above, QubiBox is much more than a password manager inasmuch it provides means to also protect and manage your digital persona[3]. In this Section, we review the features that differentiate QubiBox from standard password managers and describe the operating principles that support the value proposition of QubiBox.

A typical password manager requires to install a client application on your smartphone, tablet or PC, and promises to secure and simplify the management of all your passwords by requiring the use of only one single credential (the "Master Password"), which enables access to all the application's features and the passwords it stores. To synchronize and backup the passwords on all your client devices, you are required to sign up to a service provided in the Cloud, where all your private data will need to be uploaded[4].

We don't wish to analyze in detail the implementation choices and related security flaws of specific software password managers, but rather suggest relating their architecture and business model to the first method described in Section 3. The reason is simple: current malware and spyware can easily sniff or recover the Master Password and use it to carry out devastating attacks against the database storing all passwords. Mainstream malware can even modify the information displayed on the screen of your smartphone or PC to trick you in providing additional personal information to authenticate you to the Cloud service, if needed.

Some vendors of software password manager applications realize the level of insecurity of their products once the Master Password is compromised and discreetly suggest coupling their software with external authentication devices, such as USB tokens. However, this additional protection doesn't address the core vulnerability of password managers, namely their reliance on the integrity of the host operating system. In fact, malware can be crafted to simply wait for the user to authenticate with the external device and then gain access to the entire password database with the same privileges of the user. This is a good example of how a core vulnerability cannot be patched with methods that otherwise provide good security when used in a different and better architecture.

Having briefly discussed the inadequacy of current methods and tools available to average individuals for the protection of their digital persona, let us now describe how QubiBox was designed to help filling this gap.

[3] the data which uniquely profiles you as a private individual operating both in the physical world and across several distributed digital environments (ref. Section 2).

[4] in the context of this description, if and how the data is protected before being uploaded to the Cloud is of secondary relevance for the reasons explained in Section 3.

4.1 Operating Principles

1. QubiBox doesn’t force-feed security to its Users. We believe they can decide the tradeoff between convenience and security based on their needs, once they are given relevant and timely information. Depending on the choices made by the Users, QubiBox can support the strongest security and privacy settings to protect information, but it also allows operating with security assurances comparable to that provided by software password managers to enjoy higher convenience and accessibility to their data.

2. The use of a secure hardware device with on-board cryptography functions is part of the blueprint of the QubiBox architecture, whereby the coupling between software and hardware components allows achieving strong security and high availability. It should be stressed, however, that the free software[5] provided for use with QubiBox is fully self-contained and functional also without the hardware component.

3. Seamless synchronization and backup of the User’s data across his/her client devices can be performed using the hardware device as a data hub, thereby removing the need to upload any data to a third-party Cloud infrastructure. Communication between the app and the QubiBox device occurs only over secure (encrypted) channels and data is transferred only in encrypted format.

4. Users are required to confirm the disclosure of information they marked as most sensitive by physical action, e.g. pressing the button on the QubiBox device. This requirement implements access control via physical action feedback, which thwarts scalable catastrophic attacks[6].

5. The User is a fundamental element of the QubiBox security chain and is expected to safeguard both what he/she knows[7] and what he/she has (i.e., the hardware device).

6. Security is enforced through data segregation whereby no single QubiBox component keeps all the information required to access all the User data in clear (decrypted) format.

7. Code virtualization, obfuscation and sandboxing mitigate the ability of attackers to craft targeted malware attacks against the QubiBox software component.

8. The data stored on a lost, stolen or damaged QubiBox device can be fully recovered on a new device via a restore procedure if at least one backup archive of a recent software installation synced with the QubiBox is accessible.[8]

[5] the application is provided for free and can be used also without the QubiBox device.

[6] a malware-infected client cannot emulate a physical action on the external hardware device.

[7] the two security credentials entered during the initial product configuration (ref. Section 5).

[8] if you used the QubiBox device with the application installed on your PC, smartphone and tablet, it will be possible to recover the data on the lost QubiBox using a recent backup archive and a new, non-initialized QubiBox by launching the restore procedure on any of your three client devices.

4.2 Getting Started

Let’s look at what it takes to start using QubiBox.

First, you need to download and install the free QubiBox[9] application on at least one of your client devices (smartphone, tablet, or PC). During the first run, you will be asked to choose a Login Password, i.e. the string of characters which will allow you[10] to login and use the application on that client device.

At this stage, as a standalone software, the QubiBox application can be used pretty much as any standard software password manager, although we should stress that it offers several additional functional and features to manage more efficiently and with more security your digital persona, rather than just passwords.

The QubiBox application by itself cannot share data across your client devices even after you install it on all of them. This a limitation common to all standalone software installations, including password managers. However, synchronization and backup of all your records is possible after you *link*[11] the application with a QubiBox device, and this without requiring you to upload and share any of your data in the Cloud.

To link the application with a QubiBox, connect your new QubiBox device at the login prompt. You will now be asked to choose the *Power Password*, a second, important authentication credential that you will never need during standard usage, but only for a few critical operations enabled by the QubiBox device[12].

That’s all. You are now ready to use QubiBox and to enjoy all its features and security.

[9] www.qubibox.com/downloads

[10] or anyone else who has knowledge of it and has access to your client device

[11] to *link* the QubiBox application with the QubiBox device simply means creating a binding association that allows the secure exchange of data between the product’s software and hardware components.

[12] namely: recovering all your data from a backup archive, unblocking access to the application after too many wrong login attempts and linking your QubiBox with the application installed on a new client.

5. QUBIBOX SECURITY

In this Section, we review the security assurances provided by QubiBox (device and software component). For higher readability, this discussion will not be in the format of a technical security audit, which should and will be conducted by an impartial competent third party. Instead, here we will provide information on specific controls and features that we believe allow claiming superior security and privacy vis-à-vis current software password managers. Hopefully, the evidence provided will empower also the non-technical reader to reach his/her own practical conclusions on the credibility of our claims.

Let's start by citing a few guiding principles, well known to security practitioners:

- security is an incremental process, driven by successive threat mitigations
- given enough time and resources, everything can be hacked
- practical security is all about the economy of hacking.

Which leads us to the following product manifesto regarding the QubiBox security and privacy assurances:

QubiBox supports features and procedures which allow mitigating most of the risks associated with software password managers by raising the skills and costs required to launch a successful scalable malware[13] *attack and by maintaining the private data always under the sole control of the User*.

In QubiBox, the User Data is kept permanently encrypted and only the legitimate User has all the information required to decipher it. ***The encrypted User Data is never sent to any web site or Cloud data centers****, and thus neither Qubito nor its service providers can ever access it.*

The next sections elaborate and describe how the above principles are practically enforced in QubiBox.

[13] we intentionally leave out combination attacks which require the physical control or theft of the PC, smartphone, tablet and QubiBox device. We concentrate our analysis on the most damaging scalable malware attacks that can be launched remotely without the User's awareness of anything going wrong until it's too late.

5.1 ARCHITECTURE AND COMPONENTS

The QubiBox is a multi-component product, of which the two main elements currently[14] are the free QubiBox software application and the QubiBox hardware device.

In a nutshell, the QubiBox app is an information manager that can help you handle all the data and information required to maintain your private sphere functional and integral.

The QubiBox hardware device can be linked to any QubiBox installation to allow supporting features such as strong authentication, synchronization, backup, mass storage and cryptography functions.

The User's personal information is kept in data structures called *Records*. Each Record contains several *Attributes* (e.g. URL, login name, password, account number, PIN, etc.) depending on the *Category* to which it belongs.

In QubiBox there are four preset Categories: Web, Email, Finance and Cards. However, using the *Category Builder* one can also create custom Categories with an arbitrary number of Attributes for storing any type of personal information.

In the QubiBox application, Users can create two different types of Records:

- *Unboxed* Records, which can be fully managed without a QubiBox device, and

- *Boxed* Records, which require a linked QubiBox device to be connected and operated before one can view and modify their information.

[14] a third element, the QubiCloud, will soon be deployed to provide a convenient key storage and key escrow subscription service for QubiBox customers.

5.2 The Password Manager Delusion

The root cause of most cyber breaches is the compromise of login credentials. The same holds for software password managers, which promise to deliver better security by requiring only a Master Password.

In fact, as we briefly discussed in Section 4, the approach taken by software password managers transposes the risk associated to the disclosure of each single password to the risk of disclosing the Master Password. Unfortunately, the User is left alone to handle this critical security task and to assess the associated risks, which strongly depend on the architecture and implementation details of the password manager.

The first simple observation which casts doubts on the practical feasibility of protecting the Master Password is that it is required each time the User needs to access the password manager, possibly multiple times daily. Regardless of the Master Password's complexity, basic malware and spyware will be able to log it while it is entered and even send it to a remote entity for carrying out an exploit at any later time.

The risks associated with the disclosure of the Master Password to malware and spyware cannot be mitigated even by using authentication devices, such as USB tokens. The reason lies in the ability of malicious software to simply wait until the User authenticates using the hardware token and then steal all the sensitive information unlocked by the User or accessible using the Master Password previously sniffed.

The dire conclusion is that using a strong Master Password may help against asynchronous, brute force attacks against the password manager's database or to safeguard against simple social engineering attacks, but it can little against more sophisticated main-stream scalable attacks driven by current malware and spyware which can operate with the User's same level of privileges.

QubiBox mitigates the above risk by decoupling the authentication step from the authorization step required to gain access to the private information managed with the application. In other words, although the User is only required to enter a Login Password to operate on the Unboxed records (ref. Section 5.1), this is not sufficient to access, create, view or modify a "boxed" record. For this, the User must also connect and then operate on the QubiBox device as we will describe below.

Adding access control via physical action feedback is a fundamental security improvement inasmuch it prevents scalable catastrophic attacks by malware or spyware active on the host (PC or mobile device). In fact, even in the extreme case in which the host operating system is fully controlled by the attacker, he/she will not be able to access the user's most sensitive data unless the QubiBox is connected and the user authorizes access by pressing once the QubiBox function button *for each* boxed record.

5.3 The Login Password and The Power Password

Best practice for password management suggests the following principles to generate and maintain a strong password:

- passwords should be long and random: this will make it very hard for an attacker to guess them in a reasonable amount of time;
- passwords should be unique: reusing them will increase the chance of accidental or fraudulent disclosure and the damage caused by disclosure.

These guidelines are reasonable and should be carefully followed by Users when choosing passwords for accessing resources and services. However, as we saw in the previous Section, even strong passwords cannot safeguard against threats that are due to vulnerabilities of an architectural nature.

In QubiBox there is no strict requirement to choose a strong Login Password for the following reasons:

- the application allows only a limited number of login attempts after which access is blocked and the Login Password must be reset;
- the most sensitive information managed with the application cannot be accessed without also connecting and operating the QubiBox device;
- attacks which are not mitigated by the two above provisions will also be unmitigated by using a stronger password.

To support the additional security and privacy features enabled by the QubiBox device, the product requires a second security credential, the Power Password, with the following properties:

- it will be needed only for one-time and infrequent operations, namely: to unblock and reset the Login Password, to link the application with a QubiBox device and to restore the data from a QubiBox backup archive;
- it must be strong based on criteria associated with the efforts required to brute force its cryptographic derivatives used by various product modules[15].

[15] both the Login Password and the Power Password are never directly used for any authentication or cryptographic operation for which we employ the value of their PBKDF2-HMAC-SHA256 hashes with random salt, after 10,000 to 60,000 iterations depending on the specific operation performed.

5.4 When is a Password Strong?

A password is strong and can serve its purpose only if it is difficult for a hacker to crack. Password strength revolves around one key strategy: creating a string of characters that nobody can easily predict or guess. Randomness is the main approach to creating passwords that can't be guessed, but unfortunately it turns out that humans are poorly equipped to both recognize and apply randomness in passwords. In fact, different people end up choosing very similar words or strings when they create a password. Hackers have exploited this tendency by using word "dictionaries" containing the most common password strings along with software that automatically tries to login with each of these "dictionary passwords".

Since choosing random character strings is not well suited to humans, the approach to generating secure passwords with low predictability must rely on automated tools for selecting a wider variety of characters and for estimating the string's "practical randomness" (or, to use a technical term, its entropy). The Password Generator tool available in QubiBox allows generating and copying strings that can be used as passwords and provides a measure of their strength based on the strings' entropy as a function of the generation process and of statistical information of real-life passwords commonly used.

Besides randomness, length (i.e. the number of characters in the password) is another parameter that can be very effectively exploited to complicate the cracking by hackers. In QubiBox, we support passwords with up to 64 characters in length to enable the use of passphrases so that users can choose longer strings using any characters they like (including spaces), thus aiding memorization.

The advantage of using passphrases can be appreciated from the following example:

Password:	<{3T!Xr](:uF
Length:	12
Entropy:	59 bits
Charset Size:	94 characters

Passphrase:	My cat's name is BILLY!
Length:	23
Entropy:	115 bits
Charset Size:	85 characters

As you can see, both the password and the passphrase can be considered strong for all practical purposes and can be obtained from character sets of comparable sizes. However, the passphrase has almost twice the entropy and it's clearly much (much!) easier to remember.

In the context of QubiBox, we suggest that you choose different memorable long passphrases for the Login Password and Power Password, instead of passwords.

You can instead use the Password Generator to create strong random strings for all other password attributes of records managed with the QubiBox application.

For more general information on the topic of password strength, you may wish to check the following resources by NIST (National Institute of Standards and Technology):

- Appendix A: Estimating Entropy and Strength http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

- Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html

5.5 Where is Your Data?

With reference to Fig. 1, user data are permanently[16] kept in three main locations:

- the *Application Repository* contains the encrypted unboxed records and their encrypted keys, as well as the encrypted boxed records;
- the *QubiBox Repository* contains all encrypted records (boxed and unboxed) and their encrypted keys;
- the *Backup Archive* contains data allowing to restore all records (boxed and unboxed) in case the QubiBox device is lost or damaged.

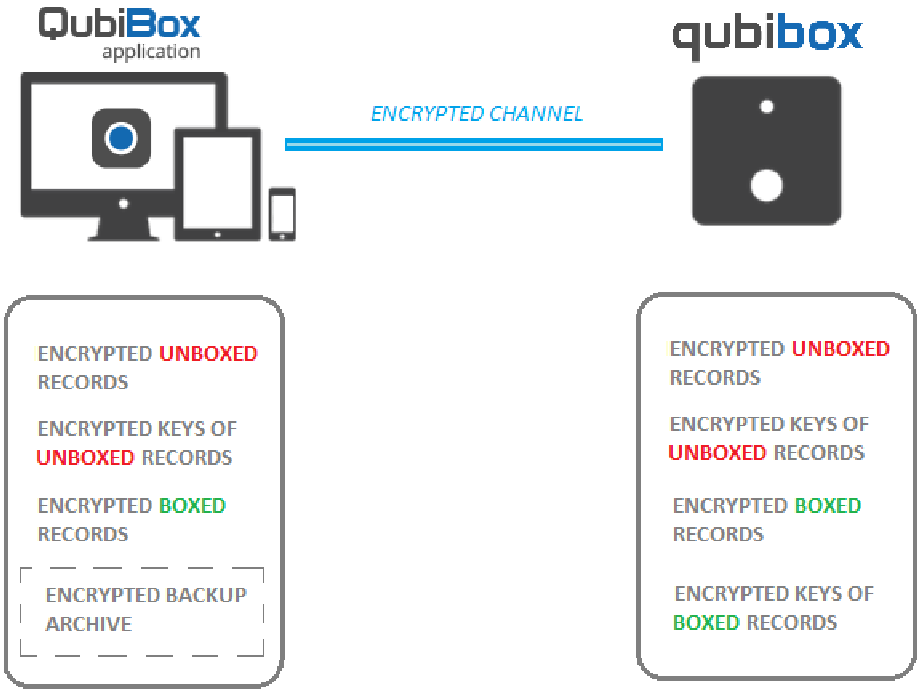

QubiBox
application
ENCRYPTED CHANNEL
qubibox
ENCRYPTED UNBOXED RECORDS
ENCRYPTED KEYS OF UNBOXED RECORDS
ENCRYPTED BOXED RECORDS
ENCRYPTED BACKUP ARCHIVE
ENCRYPTED UNBOXED RECORDS
ENCRYPTED KEYS OF UNBOXED RECORDS
ENCRYPTED BOXED RECORDS
ENCRYPTED KEYS OF BOXED RECORDS

Fig. 1 User data repositories content and location

[16] encrypted user data is also transferred between the application and the device over an encrypted channel, using RSA 1024 for key negotiation and AES 2048 for session keys.

5.6 Security of User Data

Attacks on the QubiBox user data must overcome several protection layers before they can succeed[17]. In particular, an attacker might first need to:

1. access one of the user data repositories of Fig. 1
2. reverse-engineer the target user data repository structure[18]
3. obtain the Login Password and/or the Power Password

Note that all user data is stored in permanently encrypted format and that we work under the assumption that brute force attacks against any user data repository are practically unfeasible[19]. This implies that the third item in the above list is a prerequisite for an attack to succeed within acceptable time and efforts even when the first two requirements are satisfied.

In the spirit of this document, and to empower also non-technical readers to understand the merits of QubiBox vis-à-vis software password managers, we introduce a high-level security metric related to the complexity of an attack. While the choice of any specific metric is arbitrary, in this context the metric's relevance lies in its ability to assign rough security scores which can be used for comparing threats under different attack scenarios:

Level 1: **TRIVIAL**, can be performed by low-skilled e-criminals with access to off-the-shelf hacking tools

Level 2: **EASY**, requires average skills and the ability to adapt standard malware and tools to various attack scenarios

Level 3: **COMPLEX**, can be performed only by highly-skilled e-criminals with access to sophisticated methods and know-how for crafting a targeted attack.

Let's now review the basic steps and tools[20] required for an attack to the user data repositories and discuss their respective security scores.

[17] we intentionally leave out combination attacks which require the physical control or theft of the PC, smartphone, tablet and QubiBox device. We concentrate our analysis on scalable malware attacks that can be launched remotely without the User's awareness of anything going wrong until it's too late.
[18] this entails complex analysis to bypass obfuscation and virtualization protections of critical sections and understand where key components are kept in the data repositories and how they are used.
[19] vulnerability against brute force attacks in this context must be considered either an implementation bug or a serious architectural flaw. We carefully checked QubiBox against both cases.
[20] more technically: the attack vectors.

The table below lists the security scores for the basic components of a successful attack against the user data repositories:

	Application Repository		**Application** Backup Archive		**QubiBox** Repository
1. Access Repository [21]	1	3	1,2,3	3	3
2. Reverse Engineer	2,3	1	2,3	1	3
3a. Obtain Login Password	1,2				
3b. Obtain Power Password	2,3				

Table 1. Security level scores for the main attack vectors

Let's now review the conclusions that can be drawn from this table.

1. Attacks against the Application Repository on PCs and laptops can be considered **TRIVIAL**, since accessing the repository and sniffing the Login Password are tasks that can be accomplished by malware readily available to even low-skill hackers. As mentioned before, the security of the *unboxed* records stored in the Application Repository is basically equivalent to that provided by software-only password managers.
   Suggested Mitigations:
   a. regularly update the anti-virus and OS on your client device
   b. use a strong Login Password and enter it using the provided virtual keypad
   c. keep the most sensitive information in *boxed* records

2. Attacks against the Application Repository on mobile devices can be considered **COMPLEX**, since accessing the user data requires breaking the OS sandbox environment[22].
   Suggested Mitigations:
   a. install and update an anti-virus on your mobile client device
   b. use a strong Login Password and enable support for fingerprint login (e.g. Touch ID on iOS devices)
   c. keep the most sensitive information in *boxed* records

[21] entries in the shaded column list scores when the application is running on PCs and laptops. The entries over white background list scores when the application is running in a sandboxed environment, typical of mobile operating systems.

[22] unless the mobile devices are jail-broken or rooted, we believe this to be a rather complex attack compared to the others considered in this analysis.

3. Attacks against the QubiBox Repository can be considered **COMPLEX**, since accessing the user data requires breaking proprietary hardware and firmware protections enforced at the micro-controller level[23].

4. Attacks against the Backup Archive on mobile devices can be considered **COMPLEX**, since accessing the archive requires breaking the OS sandbox environment[24].
   Suggested Mitigations:
   a. install and update an anti-virus on your mobile client device
   b. use a very strong Power Password

5. Attacks against the Backup Archive on PCs and laptops require closer scrutiny. Barring brute force attacks, which we consider practically unfeasible, the most likely attacks will concentrate on gaining access to the backup archive and obtaining the Power Password. This latter feat is obviously complicated by the fact that the User is never required to enter the Power Password during routine, standard usage of the product. However, targeted malware attacks of a medium complexity could be devised to induce the User to enter the Power Password even when it is not required[25]. Therefore, we believe that the most promising mitigation approach should focus on preventing or complicating access to the backup archive using several features and options in the QubiBox application that can support such efforts.
   Suggested Mitigations:
   a. keep the option to perform automated backups in the OFF setting
   b. activate the automated backup feature only under controlled security conditions (e.g. after a full system scan by an updated anti-virus engine)
   c. select a backup storage location inaccessible during typical usage of your PC and laptop (e.g. an external USB drive)
   d. permanently delete all copies of the backup archive from local storage
   e. use a very strong Power Password and enter it only when strictly required using the provided virtual keypad.

[23] the QubiBox device uses a STM32F2x ARM Cortex M3 processor. All data in the QubiBox Repository are kept permanently encrypted with non-extractable key(s) stored in the micro-controller secure area. Key values are generated using a Cryptographically Secure Pseudo Random Number Generator (CSPRNG). Salt values are at least 128-bit and always stored in encrypted format. Symmetric encryption is done using AES 256-bit. The secure boot loader installs and boots only a validly signed firmware. All cryptographic operations (AES, 3DES, SHA-256, RSA-1024, RSA-2048, PKCS#1 encryption and signing, ANSI 9.31 CSPRNG) are exported via secure middleware with PKCS #11 v2.20 interface. The firmware releases data of boxed records only after the User confirms by pushing the function button on the QubiBox device.

[24] unless the mobile devices are jail-broken or rooted, we believe this to be a rather complex attack.

[25] here we are obviously raising the bar of this analysis well above that dedicated to the security of software password managers, but this further supports the QubiBox value proposition.

5.7 Security and Privacy Features

Two-Level Security Classification

It is possible to classify records according to a two-step security scale:

- *Unboxed* records can be created, viewed and modified while operating solely on the client device running the QubiBox application;

- *Boxed* records can be created, viewed and modified only after connecting the QubiBox with the client device running the QubiBox application and confirming by pressing the QubiBox function button.

It should be stressed again that all records are kept permanently encrypted regardless of their classification, the main difference in security arising from protection from the attacks against the Application Repository discussed in Section 5.5.

Trusted Synchronization

QubiBox operates as a single point of synchronization between all linked clients running the QubiBox application. Each time the QubiBox is connected with the client over Bluetooth or USB, any changes to the user data and to the application settings are automatically and seamlessly synchronized. This process requires no user interaction and runs in the background for the entire duration of the connection.

Access Control via Physical Action Feedback

All critical security operations must be authorized by a non-repudiable, physical confirmation on the QubiBox device (usually by pressing once the function button). This feedback requirement provides also protection against application takeover by malware[26].

[26] malware cannot simulate a physical action feedback even after gaining full control of the client operating system.

Login Block

This feature provides mitigation from brute force attacks on the Login Password. The User can set the maximum number of failed login attempts after which the application will refuse any further input. A blocked login can be *unblocked* only by entering the Power Password and setting a new Login Password.

Login Seal

The User can set the maximum number of failed unblock attempts after which the application will be permanently sealed. A login and any linked QubiBox device which are sealed cannot be accessed in any way and can only be reset to the original factory configurations, whereby all user data is permanently and irrecoverably deleted.

Inactivity Timeout

This feature mitigates the risk of inadvertently releasing control of an active QubiBox session to a malicious third party. The User can set the time interval after which the application will auto-logout and require entering the Login Password before a new session can be established.

Password Reset

Changing or resetting the Login Password and the Power Password mitigates threats against their confidentiality. The User can easily choose new strings for either passwords after entering the current values and connecting the QubiBox device.

Bluetooth Range Limitation

The range over which the QubiBox device can support a stable communication over Bluetooth is limited to just a few meters. This feature adds an additional layer of protection against attacks to the Bluetooth encrypted channel by requiring physical proximity to connect with the QubiBox device.

Private Mass Storage

The QubiBox device can be used as a private storage device when connected to a PC over USB. A mass storage partition will be mounted by pressing the QubiBox function button for 5 seconds or after successful login to the QubiBox application.

Weak Password Warning

The QubiBox application detects the use of weak passwords[27] and warns the User about the associated risks. All records with a weak password are listed in the Weak Passwords category as a reminder to the User of the need to update the record choosing a stronger password.

Duplicate Password Warning

The QubiBox application detects the use of duplicate passwords[28] and warns the User about the associated risks. All records with a password reused in at least one other record are listed in the Duplicate Passwords category as a reminder to the User of the need to update the record choosing a unique password.

Password Generator Tool

Given that choosing random strings with low predictability is a very difficult task for humans, the QubiBox application provides a tool for generating secure passwords with a wide variety of characters to maximize the string's "practical randomness" and resistance under attack. The User can select the password length and choose between several different generation criteria: Memorable, Letters and Numbers, Numbers Only, Random. The strength of the generated password is communicated using an intuitive color coding scheme: red (weak), gray (reasonable), green (strong).

Clipboard Purge

Information is valuable only if it can be used. In the case of digital information, most often “using” equates to “sharing” with OS components and other applications. To mitigate the risks associated with in-memory persistence of sensitive data, the QubiBox application enforces a clipboard purge feature which clears the client’s system clipboard after a time interval set by the User.

[27] password strength is estimated using the *zxcvbn* library which considers a password with less than 36-bit entropy to be weak, a password with entropy between 36 to 60 bits to be reasonable and a password with entropy larger than 60 bits to be strong. For more details, see https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_wheeler.pdf

[28] the fingerprint of each password is generated using the *scrypt* key derivation function (https://www.tarsnap.com/scrypt.html) and compared with that of all other passwords. A password is marked as duplicate if any matching fingerprints are found.

Virtual Keypad

To mitigate in PCs and laptops the risk of keystroke logging[29], the QubiBox application provides the option to enter any string of characters by selecting them using mouse point & click on a software-rendered keyboard.

Backup Management

Changes to the user data are immediately committed also to the backup archive. However, to mitigate some of the attacks described in Section 5.5, the QubiBox application allows managing backups as follows:

- turn off/on backup activity
- choose the backup mode (manual or automatic)
- choose the default backup storage location
- export a backup archive
- import a backup archive
- delete a backup archive.

[29] it is more complex for malware to monitor events on the client's display and mouse to obtain the data entered via the virtual keypad, than it is to capture only the keystrokes from the physical keyboard. Of course, malware can bypass this protection by recording screenshots at regular intervals or upon each mouse click, but this requires somewhat more sophisticated and invasive methods capable of defeating also the protections deployed by the operating system and any installed antivirus.

6. QubiBox Usability

It is a common observation that unusable procedures spawn insecure behaviors. If you force users to remember long random passwords, they will write them down on a Post-it. The interplay between security and usability is, therefore, a critical element in the design and implementation of security applications and should be considered at the blueprint stage, well before development decisions are committed.

At the same time, it is also clear that gains in security can rarely be achieved without at least some compromises on convenience, one of the main elements of usability.

Thus, the practical challenge for developers and product managers lies in finding the "*unreducible balance*" between security and usability which best supports the product's value proposition[30]. Once Users convincingly become an informed and integral part of the processes supported by the QubiBox product, the challenge shifts to maintaining focus on the User's convenience and needs without departing from the committed security paradigm.

Device Ergonomics

The QubiBox hardware has been tested against all major ergonomics parameters. It's a small, light device that can be easily operated with only one hand. The slick design, high quality materials, smooth/rounded shapes and UI elements are very familiar to users of mainstream high-tech devices, represent no acceptance hurdle and stimulate touch and visual affection to the product. The ultra-bright LED clearly communicates the status of the device under all operating and lighting conditions. The accessory case and strong lanyard facilitate a firm portability and assure protection from accidental drops.

Usage Mental Model

The QubiBox mental model is primarily driven by the user interaction with the QubiBox application. Expecting users to access the information managed with the application on several different client devices, we made concerted efforts to enforce consistency across operation systems for the application's input controls, contextual cues, navigational controls, informational controls and messages.

[30] in this context, we assume that the additional security and privacy gains obtained with QubiBox provide sufficient motivation for Users to accept carrying an additional, dedicated hardware device. To this end, we observed that the ever-increasing reports of data breaches and malware attacks provide very strong incentives for a large segment of the privacy-aware consumer population.

Usage Learnability

Field testing confirmed that the QubiBox product is very simple to use in all basic operating modes, i.e. it enjoys a very high initial learnability across a large segment of users with different levels of experience with computers and smartphones. Furthermore, the QubiBox application doesn’t require any specific quality of domain knowledge or experience with similar software before users can attain understanding of the product’s main features. Extended learnability and access to more complex features is supported by awareness through visual exposure and task-driven command interfaces. Throughout the application, the user is provided both offline and online access to information resources, such as frequently asked questions and glossary, which further support usage learnability efforts and motivation.

Performance

The QubiBox product was extensively tested against metrics for effectiveness, efficiency and satisfaction for a large number of tasks representative of the intended context of use, i.e. managing sensitive personal information. In particular, satisfaction was measured using a subjective ratings scale at the end of each test session, giving scores for the user’s perception of overall gratification, efficiency, affect, controllability and learnability. Results showed that the large majority of QubiBox users think that the product lives up to their expectations and that they would gladly recommend it to friends. None of the users faced blocker incidents and rarely experienced issues which impacted task performance. Only when pushing the product to its operating limits (i.e. when managing close to 1,000 records) some users reported delays in completing tasks. This observation highlights a known architectural design limitation of QubiBox which we may address with new product versions depending on the demand received from customers under real-life usage scenarios[31].

[31] based on QubiBox user testing results and real-life software password managers’ usage reports, the average number of private information records per user is estimated to remain well below 1,000 for the next several years.

CONCLUSIONS

The average digital user operates online in a very insecure environment, with new threats constantly emerging that expose his/her privacy to catastrophic and potentially irrecoverable damage. Powerful strains of malware[32] and spyware[33] are discovered daily, against which vulnerable operating systems are powerless until patches are deployed. Even when timely information is provided, users cannot be expected to enforce all the provisions required to keep their client devices secure against all threats.

Simply put, security flaws are hard-coded in the digital architecture of client devices (PCs, tablets, smartphones) that we use every day and threats to the privacy of our digital persona are real and persistent. At the same time, incident reports[34] show that 93.5% of companies have suffered a loss of Cloud data from an insider threat and 79.1% have suffered an attack from a compromised Cloud service account.

These simple observations should provide enough motivation to select QubiBox in place of software-only password managers which rely on the security of client devices and on Cloud storage for synchronization and backup services.

More explicitly (with reference to Section 4.1):

- The QubiBox architecture enforces data segregation. The elements required to manage and access the user data are distributed over different domains (namely, the client device, the QubiBox application, the QubiBox device and the User), which are all required to be available at the same time before the private information can be disclosed.

- Even when the PC or smartphone are infected and controlled by malware or spyware, the private data stored in the QubiBox device cannot be accessed without the active, physical engagement of the User, who is required to press the function button for final authorization for disclosure.

- The private data are kept always under the sole, physical control of the legitimate User and never sent to any web site or Cloud data centers.

[32] http://www.trustedreviews.com/news/bashware-threatens-windows-10-pcs-3286410
http://www.zdnet.com/article/apple-macos-high-sierra-password-vulnerable-to-password-stealing-hack/

[33] http://thehackernews.com/2017/09/windows-zero-day-spyware.html

[34] https://www.hso.com/fileadmin/user_upload/WP-Cloud-Adoption-and-Risk-Report-Q4-2016.pdf

In other words, QubiBox removes the chance of catastrophic disclosure of the User's private information caused by security failures occurring on the client device or on the Cloud service and infrastructure.

The QubiBox architecture supports by design all the online practices dictated by security experts in order to safeguard User data and privacy.

Results of two surveys (see Fig.2 below) — one with 231 security experts, and another with 294 web-users who aren't security experts – presented at the Symposium on Usable Privacy and Security (SOUPS 2016) [35] concluded that:

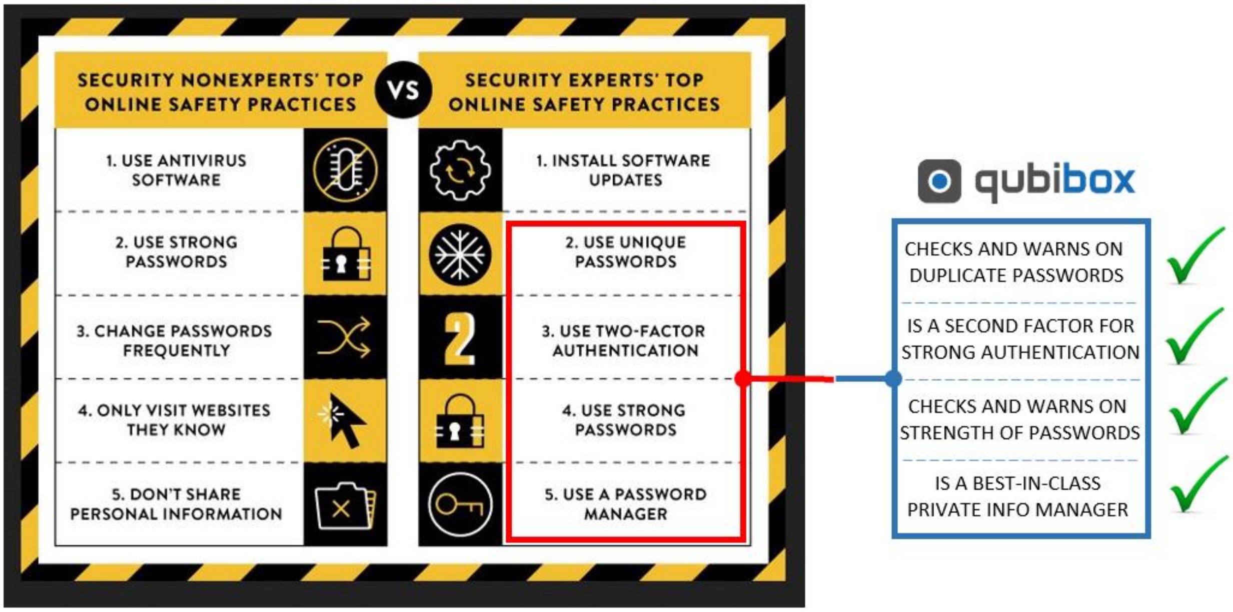
"…*the state of advice given to people today on how to stay safe online has plenty of room for improvement. Too many things are asked of them, which may be unrealistic, time consuming, or not really worth the effort. To improve the security advice, our community must find out what practices … are likely to bring the highest benefit while being realistic to ask of people*."

We hope to have convincingly shown in this document that QubiBox protects the User's digital persona by adopting a multilayered approach to security and by applying some of the strongest methods and technologies currently used in the enterprise security industry.

As a result, the usability and security features of QubiBox allows Users to finally start taking back control over their most sensitive information, understanding the unavoidable threats to which it is exposed and securing their private data as much as possible against malware attacks and spyware intrusions.

Prosit!

[35] https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf



SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

qubibox

- CHECKS AND WARNS ON DUPLICATE PASSWORDS ✓
- IS A SECOND FACTOR FOR STRONG AUTHENTICATION ✓
- CHECKS AND WARNS ON STRENGTH OF PASSWORDS ✓
- IS A BEST-IN-CLASS PRIVATE INFO MANAGER ✓

Fig. 2 Security Experts Top Online Security Practices