Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things

Aleksandr Ometov[†], Sergey Bezzateev[⋆], Joona Kannisto[†],
Jarmo Harju[†], Sergey Andreev[†], Yevgeni Koucheryavy[†]

To be cited as:
A. Ometov, et al. "Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things,"
in IEEE Internet of Things Journal , vol.PP, no.99, pp.1-12

September 21, 2016

Abstract

The Internet undergoes a fundamental transformation as billions of connected "things" surround us and embed themselves into the fabric of our everyday lives. However, this is only the beginning of true convergence between the realm of humans and that of machines, which materializes with the advent of connected machines worn by humans, or wearables. The resulting shift from the Internet of Things to the Internet of Wearable Things (IoWT) brings along a truly personalized user experience by capitalizing on the rich contextual information, which wearables produce more than any other today's technology. The abundance of personally identifiable information handled by wearables creates an unprecedented risk of its unauthorized exposure by the IoWT devices, which fuels novel privacy challenges. In this paper, after reviewing the relevant contemporary background, we propose efficient means for the delegation of use applicable to a wide variety of constrained wearable devices, so that to guarantee privacy and integrity of their data. Our efficient solutions facilitate contexts when one would like to offer their personal device for temporary use (delegate it) to another person in a secure and reliable manner. In connection to the proposed protocol suite for the delegation of use, we also review the possible attack surfaces related to advanced wearables.

Chapter 1

Introduction and outlook

The Internet as we know it today has undergone a fundamental transformation over the last several decades (see Fig. 1.1). Back in the early 1990s, it was a fixed network of computers that allowed the first million of Internet users to communicate via e-mail. The Internet access points in people's homes and public spaces were, in essence, connected *places*, which offered limited connectivity supply outnumbered by the population of potential users. This has changed as of 2000s – driven by the proliferation of mobile phones and tablets – with a possibility to connect several billion more wireless Internet users. Engaged into rich social media opportunities, these connected *people* did not suffer anymore from a lack of available connectivity. It is then when we started to also connect various machines, objects, and devices to the Internet infrastructure. This ongoing phenomenon, known as the Internet of Things [1, 2], promises to add another several tens of billion or more connected *things* by 2020 and beyond[1].

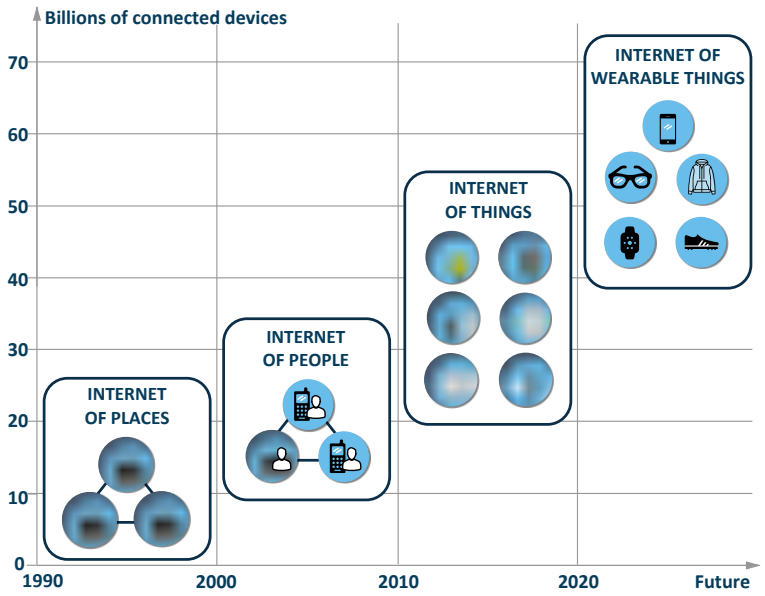


Figure 1.1: Internet evolution: from places and people to things and wearables.

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast, 2016

Employing a plethora of wireless access technologies [3], billions of connected "things" (such as sensors, actuators, smart meters, and robots) surround us and embed themselves into the fabric of our everyday lives. However, this is only the beginning of true convergence between the realm of humans and that of machines. Beyond that, an exciting innovation develops that promises to revolutionize our society thus opening a new Internet era. Connected machines worn by humans, or *wearables*, produce countless opportunities for their users, by helping them manage their personal lives, health, and safety. The rapid advent of wearables, with global sales already exceeding 20 million per quarter according to the International Data Corporation (IDC), brings along an avalanche of personal devices with new feature sets and functionalities that can be worn on a person. As worldwide wearables market soars, we are standing on the brink of another decisive Internet transformation – from the Internet of Things to the Internet of Wearable Things (IoWT).

While today's first-generation wearables are still rather limited in what they can do, the emerging IoWT devices promise to deliver a truly personalized user experience by capitalizing on the rich contextual information [4]. Complementing contemporary smart watches, fitness trackers, wristbands, on-body cameras, and eyewear, future wearable technology comprises innovative textiles, smart clothes, augmented and virtual reality gear, as well as enterprise wearable equipment. Early adopters of the next-generation wearables are envisioned to focus on self-quantification, and in fact a recent survey by Ericsson revealed that over 70% of respondents had the same level of interest in self-quantification as in wearables[2]. Obtaining the individual's health and wellness information is now increasingly simple with a wide variety of dedicated wearables, from heart rate monitoring rings, digital health networks, and posture sensors, to commuting ecometers, clean air bracelets, water quality checkers, and city microclimate monitors. All in all, modern IoWT technology already provides a range of useful functions, features, and services to its users, from simple fitness tracking to smartphone-like experience.

However, despite their promising potential, wearable devices have inherent constraints and limitations. First, owing to their slim form-factors, power efficiency is more important to wearables than to any other product. Second, the very high numbers of interconnected body-worn devices and the resultant personal user networks give rise to system scalability issues [5]. Third, it is still not common for a wearable device to interact with any nearby devices since they are operated in various platforms especially when devices are manufactured by different vendors. Indeed, wearables have the capability to connect and communicate to the IoWT infrastructure either directly through embedded cellular connectivity or via another device, primarily a smartphone, by using short-range wireless technology (see Fig 1.2). Here, the relevant contextual information may be stored and processed on the device locally or forwarded via a gateway (i.e., the user's smartphone) to a remote IoWT server. In the latter case, the gateway may not have a continuous (reliable) connection to the network due to obstacles, difficult propagation conditions (in tunnels, lifts, etc.), and unpredictable user mobility.

The above wearable-specific constraints – and primarily their limited computation power and intermittent network connectivity – accentuate the need to rethink the conventional approaches to maintaining data security, integrity, and reliability [6]. This is further aggravated by the

[2]See "Wellness and the Internet" by Ericsson ConsumerLab, 2015: `http://ericsson.com/res/docs/2015/consumerlab/wellness-and-the-internet-4x3a.pdf`

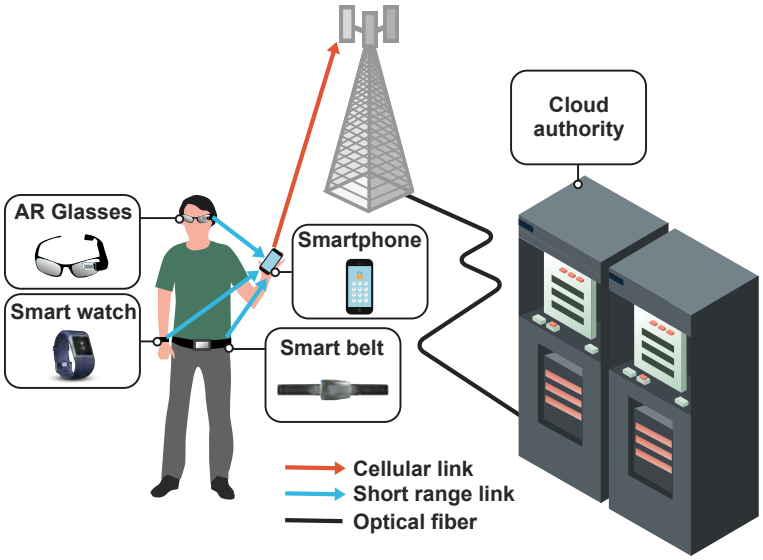


Figure 1.2: Example personal user network as part of the IoWT vision.

fact that the information that wearable devices are targeting to store and process is highly sensitive, while the devices themselves are naturally more exposed to public compared to the handheld user equipment. Indeed, with the increasing adoption of advanced wearables, we may end up "wearing" some of the most personal aspects of ourselves, including our conversations, relationships, and even health. To this end, wearables uniquely become both the most private and the most public devices, and protecting the personal user information they handle becomes a growing concern. This is particularly true for any medical data and those likely to adopt wellness services early on value the integrity of that information more than others.

Given that wearables sense, process, and transmit data about their users, they generate more *personally identifiable information* than any other today's technology. That data includes, but is not limited to wearer's location, activity, movement, and vital signs. Therefore, the biggest security risk associated with wearables becomes the *unauthorized exposure* of the personally identifiable information associated with them. According to [7], the information privacy is guaranteed if "the data can only be accessed by the people who have authorization to view and use it". Presently, a traditional enabler to achieve data privacy is secure authentication [8]. However, such approaches are complex to apply in large-scale distributed scenarios [9], especially when storing and sending the sensitive data occurs across a heterogeneous environment [10] not only via direct connections, but also remotely.

More broadly, privacy involves control over one's data, which incorporates privacy by design and contractual privacy that, in turn, implies trust. Secure authentication naturally touches upon the notion of trust [11], that is, ensures that the communications partners are actually who they claim to be. This concept of trust, together with the respective tools to manage it, have also been evolving alongside with the transformation of the Internet shown in Fig. 1.1. Initially, while the Internet mostly consisted of the terminal computers, these were able to authenticate their users with local accounts. Since then, the Internet has grown to connect

people with one another by taking advantage of centralized remote services. Most recently, the Internet of Things and thus the IoWT promise to connect our surroundings with each other and with us. The accompanying information security protocols have also traveled a long path to reach the current state of their evolution:

• In the early Internet era, access to the desired resources was granted for a particular computer/human based on the corresponding authentication procedure. In contrast, now each device has to complete such a procedure and, additionally, prove its association with its owner so that the data privacy could be guaranteed.

• Early Internet was based on the assumption that access to the target resource could only be granted based on the resource owner decision, that is, by providing a certificate or a password to the end user. Today, there is a need to provide such a certificate for each connected device explicitly by its owner, and the private data is often stored distributedly across several devices.

In light of the above transformative changes, this work targets to propose efficient means for the delegation of use [12] applicable to a variety of constrained wearable devices, so that to guarantee privacy and integrity of their data. Accordingly, since most wearables are inherently limited, our specific solutions are mindful of their restricted computation and communication budget. In particular, we target to facilitate temporary exchange of the IoWT devices belonging to different persons, groups, organizations, or companies in a secure and reliable manner to protect the contextual and personalized information they handle. The rest of this text is structured as follows. Section II surveys the related work in the target area and establishes that a comprehensive solution for the delegation of use is not yet available in the existing literature. To this end, Section III proposes a novel protocol suite to facilitate such delegation in various contexts, while Section IV details the actual protocols that comprise it. In connection to that, Section V reviews the available attack surfaces related to wearables in general and the proposed solutions in particular. Section VI concludes this work with useful numerical results and an accompanying discussion.

Chapter 2

State-of-the-art and related work overview

The existing literature is still rather scarce on the topic of the delegation of use for resource-constrained devices and services. Most of the available papers focus primarily on the challenges related to authentication between the user and the unfamiliar service/data, while having a connection to the trusted authority. Other works propose information security primitives to solve the task at hand, but do not offer effective protocols employing the out-of-the-box structures on the constrained devices. In what follows, we summarize our literature review moving all the way down the protocol stack and then towards more conceptual approaches.

A broad overview on security-centric challenges in IP-based networks for the Internet of Things (IoT) could be found in [13]. Here, the authors survey the key IoT-specific architecture and network deployment issues by focusing on a superdense IoT scenario, as well as address the technical limitations of the conventional protocols. The main conclusion is that IPv6 has the potential to solve the identification and transport challenges, thus facilitating communication between the devices, but somewhat downgrading user's privacy. The paper in question also introduces an automation control center, which acts as a trusted authority and network assistance unit by monitoring the lifecycle of the involved IoT devices. Finally, the authors speculate on the pros and cons behind distributed versus centralized architectures and the corresponding systems operation.

Another study in [14] concerns IP-based scenarios for the IoT devices with a particular emphasis on the offloading of the delegation-related traffic to the remote server in the cloud (assuming its uninterrupted availability). Here, the initial connection initialization procedure is separated from the data protection itself by utilizing DTLS protocol [15]. This is in addition to the usage of a public handshake while establishing a connection between the devices. Further, in [16], the authors reduce the protocol operation overheads by offloading the handshake procedure to a more powerful device and thus arrive at the protocol that is applicable for resource-constrained devices. Complementing this, the authors in [17] discuss a framework that enables simple authorization and access control procedures for resource-constrained equipment. The main focus of said paper is to evaluate the impact of using the Public Key Infrastructure

(PKI) cryptography on the RAM and ROM utilization. The authors claim that their approach is suitable for communication between the application server and the constrained IP-based end device.

With regards to the access controls schemes, the work in [18] surveys distributed privacy-preserving access arbitration mechanisms for sensor networks. The respective protocol implementation assumes that the users have to be provided with tokens by the the device owner (e.g., factory) in order to access the needed data from a device. The main focus of this research is on protecting the privacy of a user towards the device and hence preventing from the reuse of specific tokens. Another access rights delegation platform in [19] represents a complete framework based on the premise that the users in the IoT use cases are allowed to manage the access control system to their services and information, therefore contributing an authorization model employing the capability-based security [20]. The result in question is suitable for anonymous services using the individual's token to access any of the owned information. Similar approaches could be found in [21, 22].

The work in [23] offers a set of cryptographic primitives for the PKI-based encryption taking advantage of the time-release cryptography. The authors elaborate on a solution that allows to encrypt a message in such a way that the receiver cannot decrypt the ciphertext until a certain target time in the future. Correspondingly, privacy of the user can be maintained. Then, the paper in [7] considers privacy in the medical body area networks, from the viewpoint of the distributed data storage utilization. This research outlines an important set of requirements for distributed data storage systems as well as reviews possible attacks on the body area networks. Hence, the discussed publication reiterates on the need for fine-grained data access control that follows the concept of preset rights management, but relies on a role-based model [24].

Finally, in [25] and [26] the authors detail the Secret Key Cryptography based schemes capable of solving a distributed access control task in wireless medical sensor networks. The proposed approach utilizes a Blundo's key pre-distribution method to support the role-based access control. Owing to the pre-generated and distributed polynomial key shares, the user can easily establish a pairwise key with any authorized entity, and then encrypt a copy of sensitive data utilizing the corresponding key for the target entity. Even though patients can exert individual control over the exact access rights of the communicating entities, they would need to know the actual set of authorized users when distributing the data, and thus encrypt one copy for each user in the set, which is hardly practical.

In summary, we establish that the challenge of the delegation of use remains a sound research problem for already more than a decade. A lack of corresponding procedures for wearable devices in current academic research is profound, with only a handful of primitives and few generic solutions. At the same time, the market predictions reviewed in the previous section and the use cases discussed in what follows corroborate the prompt need for having efficient enablers to facilitate the delegation of use for wearable devices. We bridge the indicated gap in the rest of this text by outlining our own comprehensive protocol suite to support such operation.

Chapter 3

Protocol suite for the delegation of use

In this section, we begin with discussing the attractive practical scenarios for the application of our proposed protocol suite followed by its general description as well as the relevant underlying assumptions.

3.1 Use cases and market overview

Today, there are two highly contrasting opportunities in case one would like to offer their personal device for temporary use (that is, delegate it) to another person. First, there is a formal process requiring interaction with e.g., a notary officer often followed by expensive, cumbersome, and time consuming paperwork. However, in this case the owner is guaranteed that the concerned device is delegated according to the word of law and will be returned after use. Second, a more widespread case is when one is willing to lend a device to a familiar person, but without any confirmed guarantee that it will be returned except for natural human trust. In this work, we propose and advocate for a novel solution that extends the notion of "casual" delegation of use (case 2) to offer certain guaranties on the device return (similar to case 1).

In fact, a recent survey established that over a half of those who buy a wearable will stop utilizing it after only six months [27]. In connection to this, there already exist companies offering more advanced IoWT devices for a "try-before-buy" period. For example, Lumoid introduces this opportunity: for $20, anyone can try out as many as five different wearables for seven days[1]. By the end of the trial period, customers can either buy the wearables of their choosing, or return all of them to the company. While a week is not particularly long of a trial period, it could in principle be extended for as long as there is no business need for the wearables tested by their current users.

Another company, named ByeBuy, adopts a "pay-as-you-go", on-demand model for the gadgets they offer, which effectively means that the user does not actually need to purchase

[1]See "Lumoid's try before you buy wearable program helps you choose the right fitness band" by Digital Trends 2015: `http://digitaltrends.com/wearables/lumoid-wearable-rental-program/`

the latest tech products[2]. Available first to the customers in Germany and the U.K., the initial lineup of available high-end products for rental includes the Xbox One, Apple Watch, and the Parrot Bebop Drone. Interestingly, ByeBuy management maintains that there will be neither up-front payments nor minimum contract periods in their business model.

To this end, we see that the IoWT market is just in the beginning of a long journey, with a rapidly growing list of possible scenarios for (sub-)renting high-end wearable devices by the owner to the temporary user. Hence, security, privacy, and user experience aspects in this new type of context have to be carefully evaluated and Table 3.1 gives a quick overview of the candidate use cases that are both attractive and challenging for future IoWT rental business. Summarizing these, the "pay-as-you-go" model may soon take off rapidly in the wearables market. The bigger picture behind this thinking is that many Americans already prefer to *access* information and things through Netflix, Spotify, Uber, and other means rather than actually *own* them [28]. In this regard, we believe that many more objects and services may eventually adopt the flexible all-subscription model.

Table 3.1: Possible scenarios for the delegation of use

Scenario	**Description**
Golf Club	Renting smart golf equipment, such as cart, swing, glasses, etc. that are fully customizable for their temporary owner and may adjust to the personal parameters[3].
Scuba Diving	Smart wrist computers, cameras, and spear fishing gun may be rented directly on the boat[4].
Skiing	Renting smart skis, boot sensors, body armor, augmented reality glasses, etc. while being on a distant resort[5].
In-flight Entertainment	Providing a virtual reality headset for on-board customers, both naval and airborne, potentially with connectivity to the Internet[6].
Keyless Remote Access	Receive or provide access to the door merely by being in its proximity even without the Internet connection[7] for a customer, medical staff, or a police officer.

Despite bringing forth more flexible usage models, all of the device renting companies in our survey utilize conventional notary-like solutions when offering temporary access to wearables. Moreover, a user may have difficulty to receive timely digital support in situations when the

[2]See "ByeBuy Offers Alternative To Gadget Ownership With On-Demand, Pay-As-You-Go Model" by Crunch Network, 2015: `http://techcrunch.com/2015/06/24/byebuy/`

[3]See "Wearable for golf clubs helps perfect your swing" buy Mashable, 2015: `http://mashable.com/2015/01/05/epson-golf-m-tracer/#180m4nZkIiqE`

[4]See "Selected dive (and dive related) products with girls in mind" by Szilvia Gogh, 2016: `http://miss-scuba.com/gear.html`

[5]See "Hitting the slopes? This is the best new ski and snowboard tech on the market" by Digital Trends, 2016: `http://digitaltrends.com/wearables/best-smart-ski-and-snowboard-gear/`

[6]See "The Future of In-flight Entertainment? New Headsets Display HD Films Which Block Out Annoying Fellow Passengers" by The Daily Mail, 2016: `http://chinaaviationdaily.com/news/51/51056.html`

[7]See "Your Door Is About to Get Clever: 5 Smart Locks Compared" by Wired, 2013: `http://wired.com/2013/06/smart-locks/`

Internet connection to the company servers is not available. From the communications perspective, remote connectivity with the rented IoWT device could be arranged via a gateway (user's smartphone) whenever possible. In cases of guaranteed stable connection to the owner, simpler solutions including secure time and/or hash chains may become useful to control the devices [29]. However, these may be challenged to provide all of the desired functionality for advanced devices that require dynamic feedback (e.g., for policy updates as well as to extend the lease time on-demand). This problem becomes particularly involved when the rented wearables do not have a reliable Internet connection to the owner while only maintaining access to the gateway over a direct link outside of the cellular network coverage.

Our novel protocol suite detailed below offers this much needed functionality.

3.2 General description of our work

Whenever a person or a company is willing to provide the use of a device to a "trusted" or a known person, the respective solution is rather straightforward. However, there is no confirmed guarantee that the device in question will be returned on time. Our proposed solution employs a trusted authority that is involved into the process of lending the device and thus can provide guaranties on its successful return. In particular, said authority may be made responsible for controlling the duration of the temporary device delegation as well as for the corresponding interactions between the owner and a temporary user.

More specifically, we assume that the users and their personal wearable devices proceed through the initialization phase while connected to the trusted authority. Further, they may invoke the actual delegation phase at a later time, even without a reliable connection to the authority, which is especially convenient in cases of intermittent or unavailable Internet connectivity. The developed model and the corresponding set of protocols (named here the protocol suite) are specifically designed in such a way that they can accommodate most of the constrained wearable devices without imposing significant computation or transmission overheads.

Further in this work, we concentrate on the following system structure, where the overall IoWT system may comprise distributed data storage in the cloud, local wireless networks for communication with remote servers, and personal IoT networks of individual users (see Fig. 1.2). A personal user network within the IoWT consists of the following components: (i) the primary data aggregation gateway represented by e.g., the user's smartphone (or a smart gateway in home networks, etc.) The most essential required features of such a gateway are superior to wearables computation power and energy resource; (ii) the actual constrained IoWT wearables that have less resources than the gateway; and (iii) various other devices that can store, process, and transfer data, but are neither a part of the personal IoWT network nor that of the remote cloud.

In our study, we also assume that all the wireless communications channels are secure, and thus the aspects related to the corresponding well-known attacks on them are not discussed. Further, the proposed protocols could be instantiated with the specific cryptographic primitives (encryption, hashing functions, signatures, etc.) according to the effective system specifications and based on certain target requirements, as well as the particular IoWT devices in question

and their limitations. For instance, as a hashing function we may utilize any of the existing alternatives [30]: SHA-2, SHA-3, BLAKE2 [31], etc. For the certificate authority operation (in the PKI case), we may use the conventional primitives, such as (i) RSA (factorization) [32], (ii) ElGamal/Diffie-Hellman (DLP) [33] or Elliptic Curve Cryptography (ECDLP) [34].

Given our assumption on secure communications medium, it is possible to utilize the classic Diffie-Hellman [35] or Elliptic curve Diffie-Hellman [36] protocols. This is because using the PKI-based solutions for gateway-to-wearable connections is computationally-hungry and hence should be avoided. As a widely-used contemporary alternative, we may employ symmetric solutions, where additional (e.g., visual) channels are utilized to establish a secure link. In this case, the required entropy (128 or 256 bits) needs either a QR code or a shorter symmetric token matched with a password-authenticated key exchange utilizing asymmetric cryptography [37].

The issues related to the actual delegation rules, including environment, biometry, positioning, etc., are not considered in this work either. Therefore, the main focus in what follows remains on the composition and operation of the user's personal network, that is, data aggregation gateway and the associated wearable devices. The main goals of our protocol suite are to provide continuous possibility for (i) authentication between the users and their wearable devices, (ii) software and/or hardware integrity, and (iii) data security.

3.3 Protocol suite assumptions and composition

Table 3.2: Key constructs utilized by this work

Construct	**Container**	**Description**
$A, B, cloud$	–	Names of the cooperating parties: Alice, Bob, and Cloud (IoWT network).
w_i	–	i^{th} wearable device.
$\mathrm{SK}_A, \mathrm{PK}_A$	–	Secret and public keys of user Alice.
$sign_{cloud}(\mathrm{PK}_A)$	–	Here, PK_A was signed by the root cloud certificate.
t_f, t_d	–	Delegation and reset timers.
S_A	–	Secret key generated by user Alice to communicate with her wearable device.
$hash(\mathrm{SW}_i)$	–	A cryptographic hash extracted from the wearable device software by the user.
$cert_{cloud}$	$sign_{cloud}(w_i, \mathrm{PK}_A, ID_A, hash(\mathrm{SW}_i))$	Certificate generated by the cloud for data integrity reasons.
$cert_A$	$sign_A(cert_{cloud})$	User envelope to be used in the wearable certificate storage.
$m[D]_A$	$sign_A(w_i, t_d, \mathrm{ID}_A, \mathrm{ID}_B)$	An "initialize delegation" message sent to the wearable device by the owner.
$m[D]_{cloud}$	$sign_{cloud}(m[D]_A)$	Envelope verified by the certificate authority.
$m[R]_B$	$sign_B(w_i, R)$	Return request sent from temporary user to the wearable device.
$m[C(S_A)]_A$	$sign_A(w_i, C[S_A])$	A "secret removal" message sent to the wearable device by the current user.

We further assume that the IoWT network features a certificate authority employing trusted

relations in accordance with the "trusted tree" principles[8]. Every user gateway (i.e., smartphone) has a pre-generated secret key SK_A and a certificate $sign_{cloud}(\mathrm{ID}_A, PK_A)$ on its public key received from the IoWT certificate authority in the cloud. Here, $sign_{cloud}$ is obtained by using any appropriate cryptographic signature primitives with the secret key SK_{CA} of the IoWT certificate authorities. Each gateway has a certificate $cert_{cloud} = \mathrm{PK}_{CA}$ obtained from the IoWT certificate authority, while each wearable device (w_i) has a unique hardware-locked serial number (ID_i) and a factory-preset PIN (can be changed manually by using the serial number). Clearly, the PIN in question should be stored separately by the user.

Further, every "out-of-the-box" wearable device w_i already has the necessary factory software pre-installed. At a later time, the current state of this software can be reset back to the "factory default" state, that is, the trusted image provided by the manufacturer [38]. The communication between w_i and the gateway is carried out over a secure channel. As mentioned above, we assume that network connectivity is already protected against any possible malicious or "person-in-the-middle" attacks. The gateway, in turn, has a pre-generated SK_A and a certificate $sign_{cloud}(\mathrm{PK}_A)$ on its public key received from the IoWT certificate authority. Finally, each user additionally has the IoWT authority certificate $cert_{cloud}$ to verify the transmitted data as well as the validity of the devices. In case of a lost or stolen device, the user may setup a reset timer $sign_A(t_f)$, which is also assumed secure.

In summary, we provide a complete list of constructs employed for the composition of our proposed protocol suite in Table 3.2. We continue in the following section with a detailed description of the protocols comprising this suite.

[8]See "The ICSI SSL Notary: CA Certificates" by International Computer Science Institute, 2016: `https://notary.icsi.berkeley.edu/trust-tree/`

Chapter 4

Protocol descriptions within proposed suite

In this section, we offer a detailed description of the individual protocols comprising the proposed suite, which has been introduced in the previous section. To this end, Table 4.1 outlines the state machine corresponding to our solution from the viewpoint of the wearable device to be delegated. Here, a user is represented as a personal network with a data aggregation gateway (smartphone). Names *Alice* and *Bob* refer to the two users. The main phases of operation to be discussed further on are presented in Fig. 4.1.

Table 4.1: Proposed state machine (wearable device)

State	**Owner**	**User**	**Type**
1	–	–	Not associated
2	Alice	Alice	Normal use
3	Alice	Bob	Delegated use

4.1 Association (State 1 → State 2)

Here, Alice purchases a completely new wearable device from the manufacturer and is willing to add it to her personal IoWT network. In other words, we describe the procedure of adding a wearable device w_i to the personal network of the owner Alice. As the device belongs to Alice, it is associated with her by utilizing the unique ID (*alice@address.com*) with the assistance from the application center in the IoWT cloud. The key steps of the proposed association protocol are summarized in Fig. 4.2 and Algorithm 1. In practice, this construction may take advantage of already existing Transport Layer Security (TLS) primitives [39, 40].

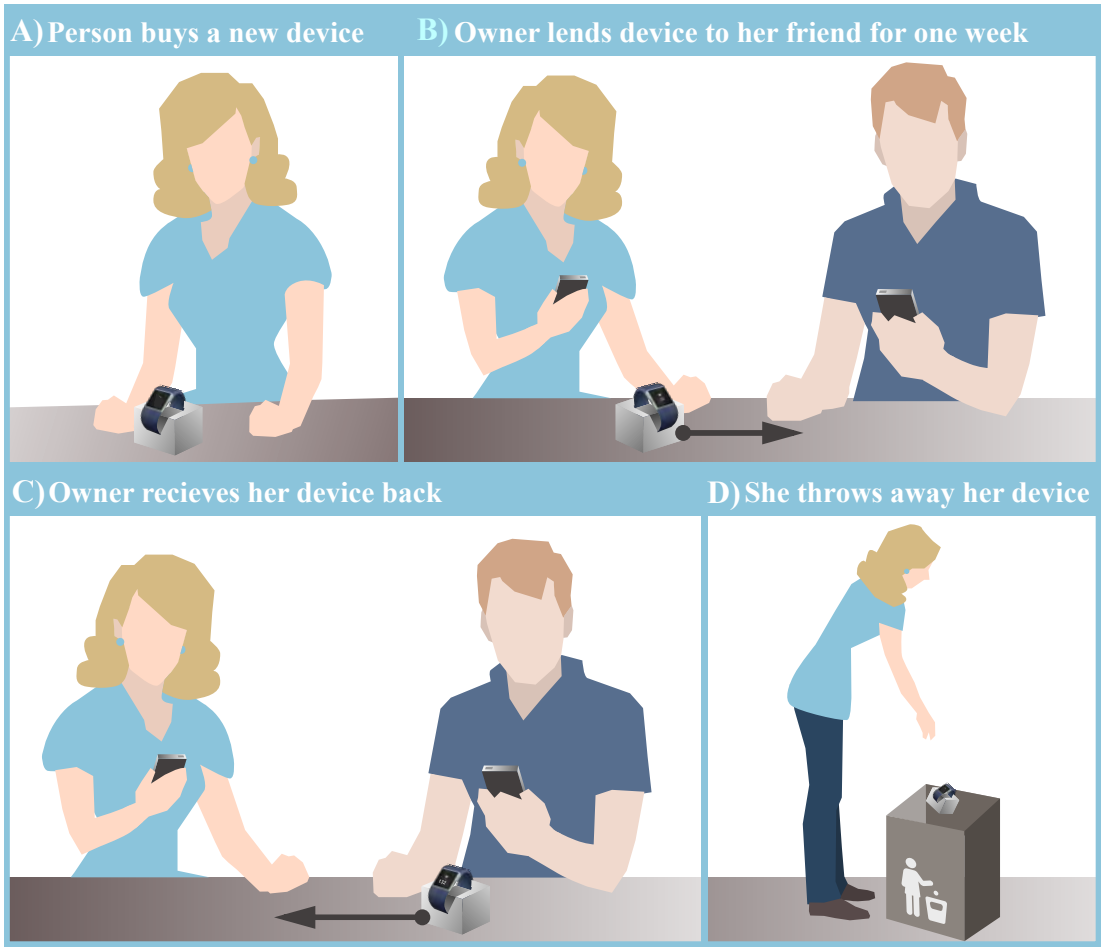


Figure 4.1: The wearable device lifecycle while delegating the use.

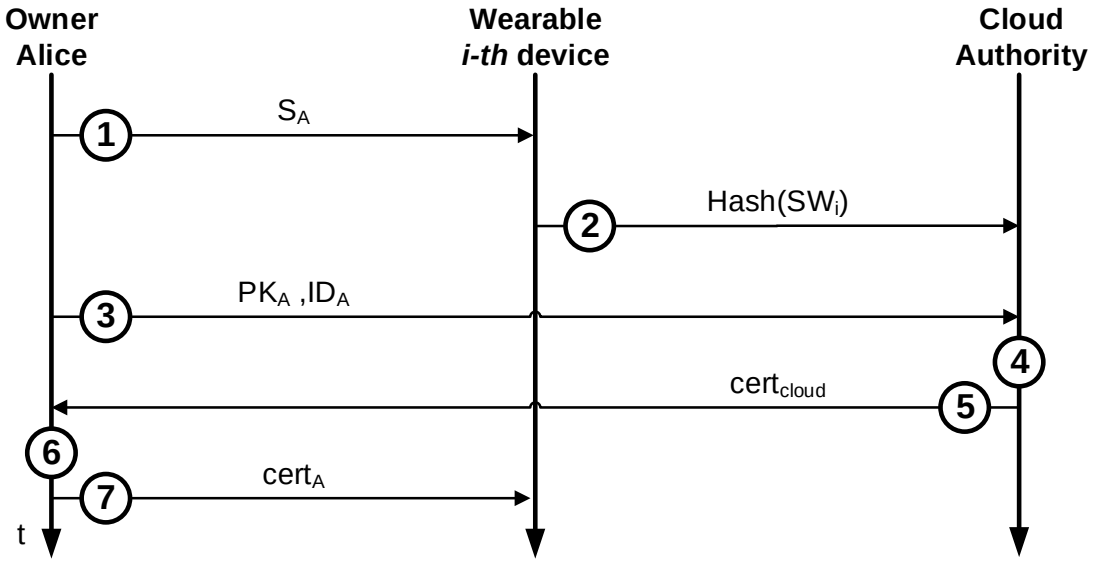


Figure 4.2: Wearable device association protocol: connection to the cloud is required.

Algorithm 1 Wearable device association protocol

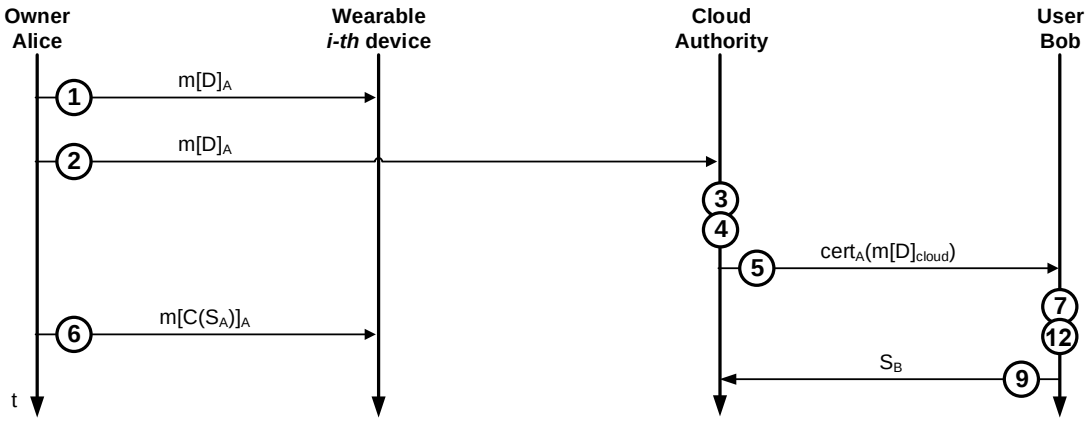
1: Alice generates S_A for the wearable w_i and sends it to w_i securely
2: w_i sends the hash of the factory software to the cloud ($hash(SW_i)$)
3: Alice also sends her PK_A and ID_A to the cloud
4: Cloud generates the certificate $cert_{cloud} = sign_{cloud}(w_i, \mathrm{PK}_A, \mathrm{ID}_A, hash(\mathrm{SW}_i))$
5: Cloud sends $cert_{cloud}$ to Alice
6: Alice signs $cert_{cloud}$ and obtains $cert_A = sign_A(cert_{cloud})$
7: Alice sends $cert_A$ to w_i

4.2 Delegation (State 2 → State 3)

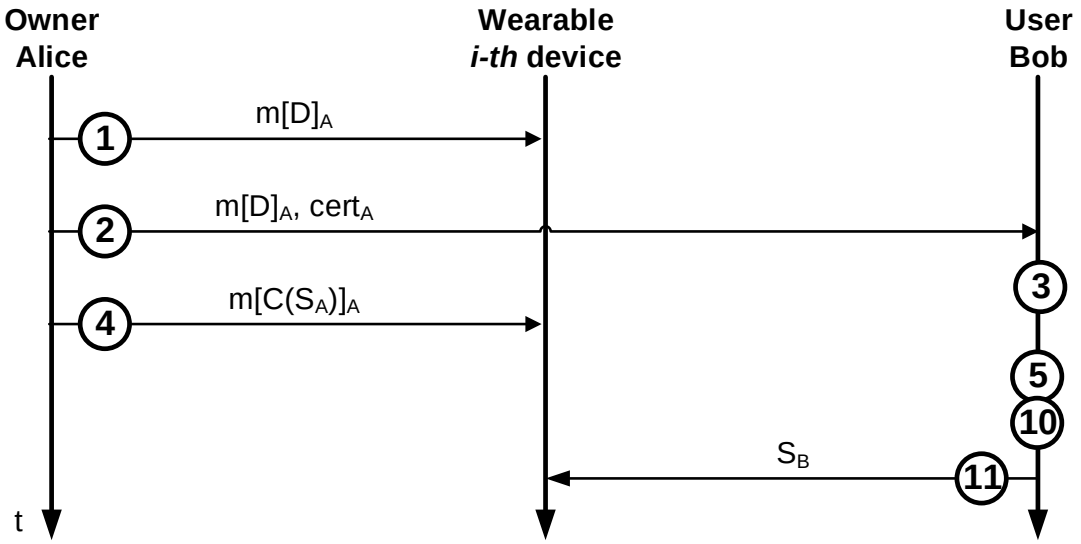
Here, Alice is willing to lend her wearable device to Bob for some time, that is, the device owner is delegating a wearable device to another temporary user. Importantly, we differentiate between two main scenarios, i.e. (i) when both Alice and Bob have a reliable wireless connection to the IoWT cloud and (ii) when at least one of them does not have it. Conveniently, our delegation procedure may in principle be executed even in situations when Alice and Bob are not geographically close to each other (in case of the door lock access delegation, for example). The key steps of the proposed delegation protocol are summarized in Fig. 4.3 and Algorithms 2 and 3.

4.2.1 Both Alice and Bob have reliable network connection

This scenario requires that the gateway has a reliable wireless connection to the certificate authority, so that it could validate all the involved operational procedures.



(a) Reliable connection to the cloud.



(b) No reliable connection to the cloud.

Figure 4.3: Wearable device delegation protocol.

Algorithm 2 Wearable device delegation protocol: reliable connection to the cloud

1: Alice sets delegation timer t_d on w_i using a message $m[D]_A = sign_A(w_i, t_d, \mathrm{ID}_A, \mathrm{ID}_B, \{delegation \quad rules\})$.
2: Alice sends $m[D]_A$ to the cloud.
3: Cloud checks the validity of $m[D]_A$ by using PK_A. If it is not valid → exit.
4: Cloud signs $m[D]_{cloud} = sign_{cloud}(m[D]_A)$.
5: Cloud sends $m[D]_{cloud}$ and $cert_A$ to Bob.
6: Alice deletes S_A on w_i using $m[C(S_A)]_A$.
7: **if** Bob does not trust Alice **then**
8: Device is reset keeping the original certificate stored and Bob checks the $hash(SW_i)$ from the $cert_A$ and hash calculated from the w_i-th software directly. If both are equal – we may proceed; otherwise, the w_i is considered malicious → exit. In this case, w_i may not be used by Bob (factory software was modified by the owner, i.e. it is not the same as the default). Importantly, reseting to factory defaults in this case keeps the certificate storage and the trusted timer unchanged.
9: **else**
10: All the applications are kept unchanged and Bob may use the software of user Alice that is free or has been previously owned by Bob.
11: **end if**
12: Bob generates new S_B for the w_i.

4.2.2 Both Alice and Bob do not have a reliable network connection

This scenario does not require that the gateway has a reliable wireless connection to the certificate authority (in/on tunnels, boats, mountains, etc.). Alternatively, the user(s) may decide to block their wireless connection intentionally.

Algorithm 3 Wearable device delegation protocol: no reliable connection to the cloud

1: Alice sets delegation timer t_d on w_i using a message $m[D]_A = sign_A(w_i, t_d, \mathrm{ID}_A, \mathrm{ID}_B, \{delegation \quad rules\})$.
2: Alice sends $cert_A, m[D]_A$ to Bob securely.
3: Bob checks if $cert_A$ and $m[D]_A$ are valid by $cert_{cloud}$.
4: Alice deletes S_A on w_i using $m[C(S_A)]_A$.
5: **if** Bob does not trust Alice **then**
6: Device is reset keeping the original certificate stored and Bob checks the $hash(SW_i)$ from the $cert_A$ and hash calculated from the w_i-th software directly. If both are equal – we may proceed; otherwise, the w_i is considered malicious → exit. In this case, w_i may not be used by Bob (factory software was modified by the owner, i.e. it is not the same as the default).
7: **else**
8: All the applications are kept unchanged and Bob may use the software of user Alice that is free or has been previously owned by Bob.
9: **end if**
10: Bob generates new S_B for the w_i.
11: Bob sends S_B to the w_i securely.
12: To ensure software integrity, Bob signs $sign_B(w_i, \mathrm{SW}_i)$.
13: **if** the delegation time is expired **then**
14: Device is reset to factory default state saving the original certificate. The timer can be reset while connected to the cloud over Bob's gateway, but it requires interaction with the original owner Alice as $m[D]_A = sign_A(w_i, t_d, \mathrm{ID}_A, \mathrm{ID}_B, \{delegation \quad rules\})$ This could also be done via a direct connection.
15: **end if**

4.3 Reclaiming (State 3 → State 2)

Here, the temporary user Bob returns the previously rented wearable device to its original owner, Alice. The key steps of the proposed reclaiming protocol are summarized in Fig. 4.4 and Algorithms 4 and 5.

4.3.1 Both Alice and Bob have reliable network connection

Algorithm 4 Wearable device reclaiming protocol: reliable connection to the cloud

1: Bob generates a message $m[R]_B = sign_B(w_i, R)$.
2: Bob sends $m[R]_B$ to the cloud.
3: Cloud checks the validity of $m[R]_B$ by using PK_B. If it is not valid → exit.
4: Cloud signs $m_{cloud} = sign_{cloud}(m[R]_B)$.
5: Cloud sends m_{cloud} to Alice.
6: Bob deletes S_B on w_i using $m[C(S_B)]_B$.
7: **if** Alice does not trust Bob **then**
8: Device is reset keeping the original certificate stored and Alice checks the $hash(SW_i)$ from the $cert_A$ and hash calculated from the w_i-th software directly. If both are equal – we may proceed; otherwise, the w_i is considered malicious → exit. The owner Alice should reset her device using the factory PIN.
9: **else**
10: All the applications are kept unchanged and Alice may use new software of the previous user Bob which is free or has been purchased by Alice while Bob was using the device.
11: **end if**
12: Alice sends to w_i generated during the association S_A.
13: To ensure software integrity, Alice signs $sign_A(w_i, SW_i)$. As a result, now w_i has only $cert_A, cert_{cloud}$.

4.3.2 Both Alice and Bob do not have a reliable network connection

Algorithm 5 Wearable device reclaiming protocol: no reliable connection to the cloud

1: Bob generates a message $m[R]_B = sign_B(w_i, R)$.
2: Bob sends $m[R]_B$ to Alice over a direct link.
3: Bob deletes S_B on w_i using $m[C(S_B)]_B$.
4: Alice checks if $m[R]_B$ is valid by $cert_{cloud}$.
5: **if** Alice does not trust Bob **then**
6: Device is reset keeping the original certificate stored and Alice checks the $hash(SW_i)$ from the $cert_A$ and hash calculated from the w_i-th software directly. If both are equal – we may proceed; otherwise, the w_i is considered malicious → exit. The owner Alice should reset her device using the factory PIN.
7: **else**
8: All the applications are kept unchanged and Alice may use new software of the previous user Bob which is free or has been purchased by Alice while Bob was using the device.
9: **end if**
10: Alice sends to w_i generated during the association S_A.
11: To ensure software integrity, Alice signs $sign_A(w_i, SW_i)$ As a result, now w_i has only $cert_A, cert_{cloud}$.

4.4 Manual de-association: disposal or sale (State 2 or 3 → State 1)

Here, the owner Alice is willing to sell or dispose of her wearable device, that is, she wants to remove all the personal data from the device including any keys and certificates. The key steps of the corresponding de-association protocol are summarized in Algorithm 6.

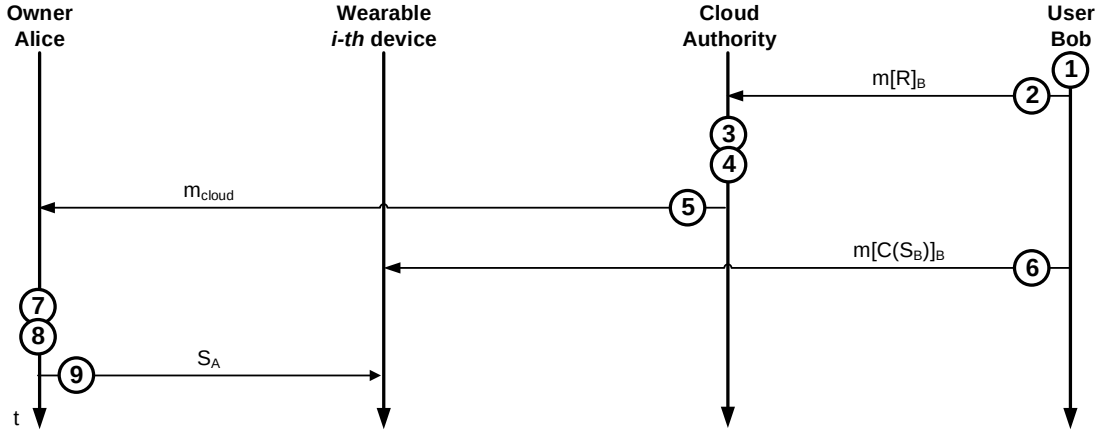
Algorithm 6 Manual wearable device de-association protocol
1: Owner Alice sends a signaling message to w_i: $m[F]_A$.
2: w_i is reset to the factory defaults thus removing all data, including the certificate storage.
3: Device can be restored by only using factory (or modified) PIN, and the connection to the cloud is required according to the association phase.

4.5 Automatic de-association: loss or damage (State 2 or 3 → State 1

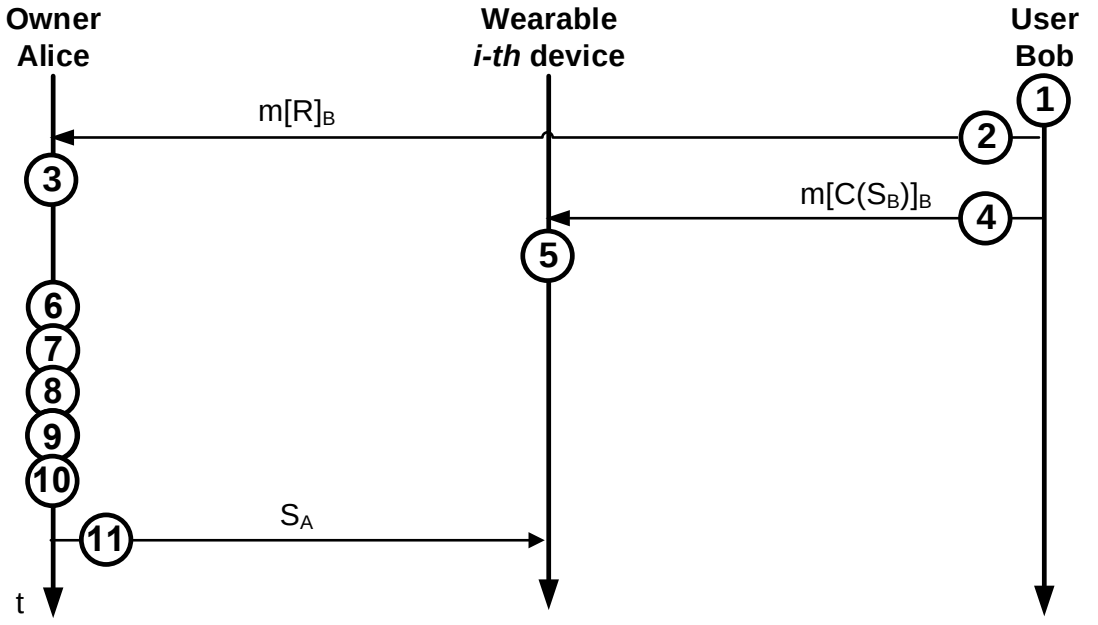
Here, we consider the situation when the wearable device in question is lost, damaged, or stolen, that is, any private data should be removed to prevent a potential third party from accessing it. The key steps of the corresponding de-association protocol are summarized in Algorithm 7. Note that this construction is similar to the case of manual de-association above, but device reset in this case is triggered based on the preset timer value.

Algorithm 7 Automatic wearable device de-association protocol
1: If w_i leaves the personal network coverage of its current user, the timer t_f is initialized.
2: If reset timer t_f expires, w_i is automatically reset to the factory defaults thus removing all data, including the certificate storage.
3: Device can be restored by only using factory (or modified) PIN, and the connection to the cloud is required according to the association phase.

Capitalizing on the proposed protocol suite accommodating the delegation of use for private wearable devices, we proceed with a thorough review of possible attacks on and threats to wearables. This aims at offering a complete and systematic perspective on utilizing this new type of user equipment in the emerging IoWT era.



(a) Reliable connection to the cloud.



(b) No reliable connection to the cloud.

Figure 4.4: Wearable device reclaiming protocol.

Chapter 5

Possible attacks on wearable devices

As a further evolution of the IoT, the IoWT and its wearable devices are susceptible to similar threats as the machine-type equipment, which served an attractive target for "hackers" for decades [41]. Contrary to the IoT devices, as we discussed in Section I, wearables are additionally vulnerable to unauthorized exposure of the personally identifiable information associated with them. Therefore, attackers could be after the physical assets of the users (i.e., the wearable devices themselves) or they could attempt to access the user's data directly on a wearable device. In addition, an attacker could be interested in the metadata about the user, which would mean, for example, any information about past device delegations.

According to the USA Federal Trade Commission[1], a comprehensive classification of the attack surfaces for wearables is illustrated in Fig. 5.1. Hence, we learn that the conventional attack areas are somewhere between the gateway and the network cloud. These are well researched upon already, whereas wearable-specific attacks call for a more detailed discussion. In the rest of this text, we review possible wearable-specific attacks and compare those against the existing alternatives. This information should help protect the actual instantiations of the proposed protocol suite with the practical primitives, when implemented.

Privacy Protocols that employ signatures, including the one proposed above, are particularly vulnerable in terms of privacy, since they typically also enable non-repudiation. This important property means that the user cannot at a later time deny the fact of the delegation or assertion. More specifically, non-interactive protocols rely on this property for their security, which causes a conflict between the security and the privacy [42].

Phishing Phishing attacks target to exploit the weak bindings between the digital and the physical identities [43]. For example, Eve masquerading as Bob initiates a delegation from Alice to Bob, but then presents her own identity. If Alice cannot verify that Bob is ID_B instead of ID_E, a phishing attack succeeds. Opportunities for phishing are aggravated

[1] See "Careful ConneCtions: Building Security in the Internet of Things" by Federal Trade Commission, 2015: `http://ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf`

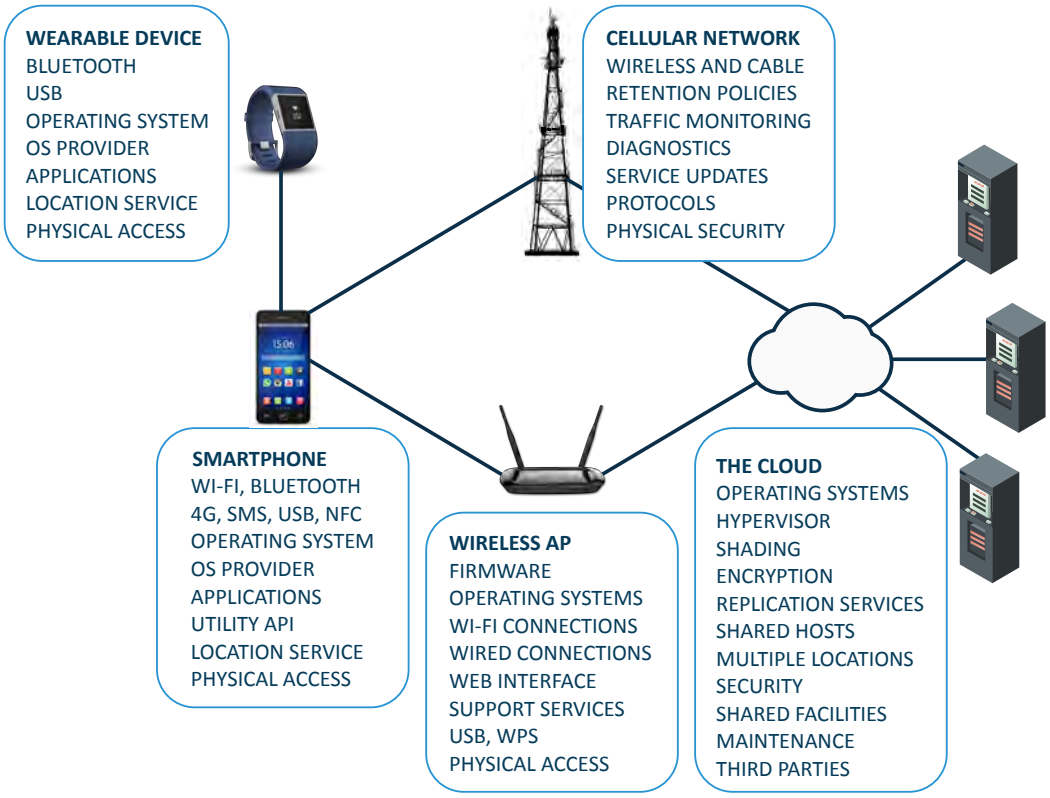


Figure 5.1: Classification of the attack surfaces for wearables.

by the intrinsic properties of wearables, including the one that they often have small or no displays. Phishing cannot usually be prevented completely (residual error and finite user effort), but it can be controlled to a desired extent (i.e., how small differences in authenticity a human user has to notice). Finally, resistance to phishing may also be in contradiction with privacy, that is, more attributes make users more recognizable, but leak information about them.

Relay attacks (also including the conventional person-in-the-middle attacks [44]) Here, Eve asks $m[D]_A$ for Bob (ID_B) from Alice, and later on introduces herself as Alice to Bob, also offering the $m[D]_A$ to Bob at that time. Alice cannot use the wearable device herself, but can observe delegations, and may convince Bob to believe that she is in fact ID_A.

Downgrade As actually employed signature primitives are not discussed as part of the proposed protocol, the general problem of "downgrade" concerns mostly the key distribution stage [45]. Accordingly, if a user has multiple public keys, they all need to withstand prolonged attacks against them. Another less severe downgrade attack happens when communication with the cloud is prevented by a malicious party, or reachability of the cloud is not verified by one of the parties in advance.

Malicious wearable After observing a valid protocol message $m[D]_A$ for the wearable device w_k from Alice to Bob, Eva crafts a malicious wearable device that reports the identity w_k and the integrity $hash(SW_k)$. Then, the wearable in question can, for example, log Bob's activity. This attack looks similar to any malicious device attack, but – due to the fact that most wearables are constrained devices – can be performed mostly on the factory side.

Wearable device compromising The devices in a personal user network are subjected to compromising [46], as they are relatively easy to be lost, stolen, or forgotten. If the entire piece of sensitive data is directly encrypted and stored inside a wearable device together with its encryption key, the compromise of this device will lead to the disclosure of data.

Network dynamics threads Naturally, a user operating the aggregation gateway (smartphone) along with the personal wearable devices is mobile throughout the day. Due to accidental failures or malicious activities, wearable devices may join or leave the network frequently [47]. This may also happen due to the battery constrains. To this end, attackers may attempt to place fake sensors in order to masquerade the authentic devices, and can then acquire legitimate devices deliberately. The important user-related data, if not well-kept in more than one device, could be lost accordingly as a result of high network dynamics.

Chapter 6

Some numerical results and discussion

As we discover in the previous section, one of the likely attacks on the proposed wearable-specific device delegation protocol is phishing, where Eve masquerades herself as Bob. If Alice does not trust Bob's certificate issued by the IoWT certificate authority (or Eve's certificate in case of attack), we may utilize the following procedure. Accordingly, Alice sends a symmetric delegation key to Bob encrypted with Bob's public key. The delegation key for Bob can be, for instance, $challenge||KDF(K_A, challenge)$, which the wearable device can verify during Bob's communication attempt. Then, the wearable device does not have to employ public key cryptography to associate the user. Here, the challenge has to have structure, which binds it to the actual delegation. Also, it is desirable to change the key $S_A : w_i$, which is the symmetric key between Alice and the device w_i.

Further, we assess the power consumption performance of our proposed protocol suite, as this should become a major limiting factor in its ultimate practical operation. This discussion is not presented in absolute numbers due to the fact that the transmission overheads depend on the practical networking scenario, the interference picture, and other unpredictable factors. Therefore, we analyze the case where network conditions remain similar for all the underlying wireless technologies. More specifically, the power consumption figures for the cellular interface are taken from [48]. For the power consumption of short-range wireless technologies, we refer to [49, 50, 51]. Based on the obtained numerical results, we estimate the transmission overheads when using our proposed protocol suite for different phases, while having equal data packet payloads.

Table 6.1: Power consumption of different radio interfaces

	WiFi	**BLE**	**ZigBee**
Consumption (mW)	720	147	71.402

In Fig. 6.1, the comparison of relative communication overheads for both in- and out-of-coverage cases is presented, whereas the calculations are based on Table 6.1. We learn that the

association and the delegation phases of the proposed protocol suite consume the most power, as they generally involve more signaling messages to travel between a wearable device and the network. At the same time, the reclaiming phase is relatively more lightweight. In addition, we observe that running the protocols over short-range WiFi radios consumes more power than executing them over less power-hungry Bluetooth Low Energy (BLE) and ZigBee technologies.

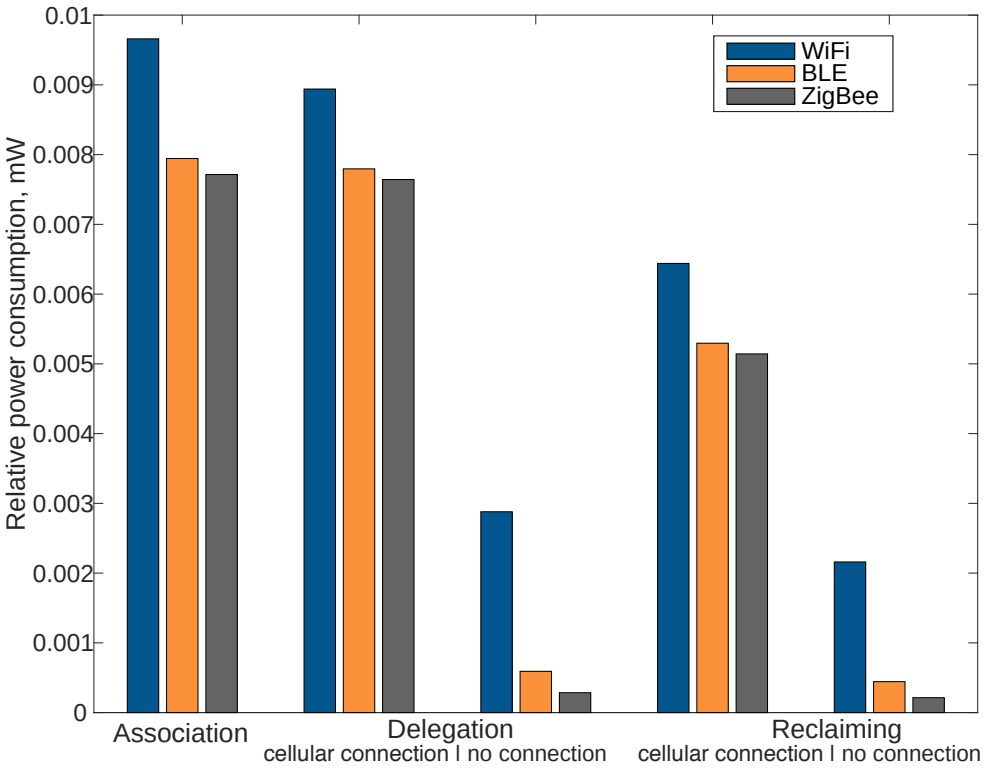


Figure 6.1: Relative transmit power consumption of the proposed protocol suite.

In summary, this work has comprehensively outlined a number of important aspects related to privacy of advanced wearables within the IoWT ecosystem that they construct. To this end, we started with a thorough review of contemporary trends behind the evolution of next-generation wearables, surveyed the corresponding security research background, reviewed the emerging device rental market, as well as offered a comprehensive overview of potential use cases. Further, we outlined a complete protocol suite enabling the delegation of use for wearable devices, whenever their owner is willing to rent a device for temporary use.

The proposed solutions are described at length, both when the personal user network has a reliable wireless connection to the IoWT infrastructure, as well as when such connection is not available. Finally, we have analyzed the associated attacks on wearable devices themselves, as well as our designed protocols, and discussed some of the important practical implications, including protection from phishing and relative power consumption. We believe that the proposed protocol suite and its accompanying discussion will become a useful consideration facilitating the delegation of wearables across multiple casual and business scenarios.

Bibliography

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, *et al.*, "Internet of Things strategic research roadmap," *O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends*, vol. 1, pp. 9–52, 2011.

[3] S. Andreev, O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler, and Y. Koucheryavy, "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 32–40, 2015.

[4] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Information Sciences*, vol. 314, pp. 255–276, 2015.

[5] H. Feng and W. Fu, "Study of recent development about privacy and security of the Internet of Things," in *Proc. of International Conference on Web Information Systems and Mining (WISM)*, vol. 2, pp. 91–95, IEEE, 2010.

[6] R. H. Weber, "Internet of Things–New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[7] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[8] F. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," in *From active data management to event-based systems and more*, pp. 242–259, Springer, 2010.

[9] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[10] S. Gürses, B. Berendt, and T. Santen, "Multilateral security requirements analysis for preserving privacy in ubiquitous environments," in *Proc. of the UKDU Workshop*, pp. 51–64, 2006.

[11] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[12] H. Kim, Y. Lee, B. Chung, H. Yoon, J. Lee, and K. Jung, "Digital rights management with right delegation for home networks," in *Information Security and Cryptology (ICISC)*, pp. 233–245, Springer, 2006.

[13] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[14] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based Authentication and Authorization for the IP-based Internet of Things," in *Proc. of Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 284–292, IEEE, 2014.

[15] E. Rescorla and N. Modadugu, "Datagram transport layer security," tech. rep., 2006.

[16] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of Things," in *Proc. of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, pp. 37–42, ACM, 2013.

[17] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in *Proc. of IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, IEEE, 2013.

[18] R. Zhang, Y. Zhang, and K. Ren, "Distributed privacy-preserving access control in sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1427–1438, 2012.

[19] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the internet of things," *Mathematical and Computer Modelling*, vol. 58, no. 5, pp. 1189–1205, 2013.

[20] T. Riechmann and F. J. Hauck, "Meta objects for access control: extending capability-based security," in *Proc. of the 1997 workshop on New security paradigms*, pp. 17–22, ACM, 1998.

[21] J. Li and A. H. Karp, "Access control for the services oriented architecture," in *Proc. of the 2007 ACM workshop on Secure web services*, pp. 9–17, ACM, 2007.

[22] A. H. Karp and J. Li, "Solving the transitive access problem for the services oriented architecture," in *Proc. of International Conference on Availability, Reliability, and Security, ARES*, pp. 46–53, IEEE, 2010.

[23] J. H. Cheon, N. Hopper, Y. Kim, and I. Osipkov, "Authenticated key-insulated public key encryption and timed-release cryptography," 2004.

[24] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, no. 2, pp. 38–47, 1996.

[25] O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in *Proc of. International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 249–254, IEEE, 2008.

[26] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proc. of the 15th ACM symposium on Access control models and technologies*, pp. 129–138, ACM, 2010.

[27] D. Ledger and D. McCaffrey, "Inside wearables: How the science of human behavior change offers the secret to long-term engagement," *Endeavour Partners*, 2014.

[28] J. Herold, M. Prabu, T. Phillips, J. Duffus, C. Steeb, P. Sutton, Z. Xu, Z. Xu, and A. Frank, "Prepaid or pay-as-you-go software, content and services delivered in a secure manner," Sept. 12 2005. US Patent App. 11/224,651.

[29] S. Heikkinen, S. Kinnari, and K. Heikkinen, "Security and User Guidelines for the Design of the Future Networked Systems," in *Third International Conference on Digital Society (ICDS)*, pp. 13–19, IEEE, 2009.

[30] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in *Fast Software Encryption*, pp. 371–388, Springer, 2004.

[31] J.-P. Aumasson, S. Neves, Z. Wilcox-O'Hearn, and C. Winnerlein, "Blake2: simpler, smaller, fast as md5," in *Applied Cryptography and Network Security*, pp. 119–135, Springer, 2013.

[32] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proc. of Third IEEE International Conference on Pervasive Computing and Communications, PerCom.*, pp. 324–328, IEEE, 2005.

[33] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in cryptology*, pp. 10–18, Springer, 1985.

[34] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[35] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[36] A. Joux, "A one round protocol for tripartite Diffie–Hellman," in *Algorithmic number theory*, pp. 385–393, Springer, 2000.

[37] F. Hao, "J-pake: Password authenticated key exchange by juggling," Internet-Draft draft-hao-jpake-02, IETF Secretariat, January 2016.

[38] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente, "On the difficulty of software-based attestation of embedded devices," in *Proc. of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (New York, NY, USA), pp. 400–409, ACM, 2009.

[39] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008.

[40] P. Morrissey, N. P. Smart, and B. Warinschi, "A modular security analysis of the TLS handshake protocol," in *Advances in Cryptology (ASIACRYPT)*, pp. 55–73, Springer, 2008.

[41] S. Cobb, "Security and Wearables: Success starts with security," in *Proc. of The Future of Wearables Conference*, December 2015.

[42] E. Bergeron, "The Difference Between Security and Privacy," *Proc. of Joint Workshop on Mobile Web Privacy WAP Forum and World Wide Web Consortium*, December 2000.

[43] L. Wu, X. Du, and J. Wu, "MobiFish: a lightweight anti-phishing scheme for mobile phones," in *Proc. of 23rd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, IEEE, 2014.

[44] M. Roland, J. Langer, and J. Scharinger, "Relay attacks on secure element-enabled mobile devices," in *Information Security and Privacy Research*, pp. 1–12, Springer, 2012.

[45] A. Ornaghi and M. Valleri, "Man in the middle attacks Demos," *Blackhat [Online Document]*, vol. 19, 2003.

[46] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems," *Technical Report CU-CS-990-05, Deptartment of Computer Science, University of Colorado at Boulder*, January 2005.

[47] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE*, vol. 20, no. 3, pp. 41–47, 2006.

[48] A. R. Jensen, M. Lauridsen, P. Mogensen, T. B. Sørensen, and P. Jensen, "LTE UE power consumption model: for system level energy and performance optimization," in *Proc. of IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, IEEE, 2012.

[49] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," in *Proc. of 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON)*, pp. 46–51, IEEE, 2007.

[50] D. Halperin, B. Greenstein, A. Sheth, and D. Wetherall, "Demystifying 802.11n power consumption," in *Proc. of International Conference on Power Aware Computing and Systems*, p. 1, USENIX Association, 2010.

[51] P. Smith, "Comparing low-power wireless technologies," *Tech Zone, Digikey Online Magazine, Digi-Key Corporation*, vol. 701, 2011.