

# Security challenges for wearable computing a case study

John Lindström

Lulea University of Technology, Sweden  
Centre for Distance-spanning Technology  
{john.lindstrom@cdt.ltu.se}

## Abstract

This paper discusses IT- and information security challenges for wearable computing encountered during the WearIT@work project. The following novel ideas are introduced in this paper: *authorization by proximity* using dynamic context information to enable transfer of authorization from one party to another, *a wearable pairing mechanism* to use devices on other wearables, and a more *intelligent management of dynamic IT-security policies* to reduce computational overhead on wearable devices having limited capabilities. The last idea includes the importance of having a *dynamic security baseline* adapted to wearables to maintain the integrity and confidentiality of the body network as well as the privacy of the wearers' personal and biometric information.

## 1 Introduction

Looking at the future, we need to find ways to improve work productivity, quality and safety. To enable the creation of more efficient work processes in areas where process innovation has been hard without the proper (wearable) supportive tools, we need new and better supportive technology. Many lines of work will not easily allow the workers to bring a computer in the form of a laptop or PDA due to the nature of their work where free or clean hands are required. For those there is a large potential in using wearable computers and systems. As wearable computers and systems get more mature and productified for different business needs, they can be used in a lot of work areas, where today there is none or very little IT-support. Wearable computers will most likely be used more and more – not only at work but also by people during spare time as the wearables, being very small and integrated in the clothing, will be brought almost everywhere. This will require a higher level of IT- and information security to protect personal integrity and privacy, confidential information and communications.

This is a case study on “IT- and information security challenges for wearable computing” encountered during the WearIT@work project<sup>1</sup>, which currently is the largest EU-funded integrated project within wearable computing, trying to develop future wearable computing platforms and also to grow knowledge on organizational and societal aspects from the introduction of wearable computing to professionals at work. The WearIT@work project has four demonstrators comprising the following areas: healthcare/hospital, airplane maintenance, car manufacturing and rescue services/fire brigade.

### Related work and motivation

Context-based security is a quite new concept and among the interesting work already done are Mostéfaoui et al. who in [1] discuss context-based security using MAUT (Multi-Attribute Utility Theory) and Simple Heuristics in order to secure transactions in the heterogenous network to make the security level more adaptive, and Brézillon and Mostéfaoui in [2, 3] who defines “security context” and discuss context-based

---

<sup>1</sup> For more information on the WearIT@work project, please see <http://www.wearitatwork.com>

security policies and how to model such with contextual graphs to achieve adaptive and reconfigurable security solutions for pervasive applications. This paper brings up, from a wearable computing perspective of today, that it is needed to take into account the system resource consumption by security software if using a dynamic adaptive security policy so that the wearable may perform adequately.

N. Saxema et al. [4] discuss secure device pairing based on a visual channel, where pairing between devices is enabled by using the devices' cameras to read barcodes on the devices for mutual authentication. This paper introduces an idea to increase the flexibility and usability for users by having a pairing mechanism that allows a wearable computer to use devices on other wearables in a similar way as in Bluetooth [5].

When addressing authorization by proximity enabling transfer of authorization from one party to another party, no published research has been found except for research<sup>2</sup> and commercial products<sup>3</sup> mainly addressing physical or logical access in combination with authorization for one party. Allowing the transfer of authorization may improve work processes and better enable team work.

In this paper, the outcome of the WearIT@work requirement engineering efforts is synthesized to highlight security issues concerning wearables, as well as to indicate a need for new security mechanisms due to new requirements discovered when using wearables.

### **Research question**

The intersection between the areas of wearable computing and IT- and information security is an interesting field to study and the research question raised by this paper can be stated as: What aspects of security for wearable computing are of special interest considering the experience gained from the WearIT@work project.

## **2 What is wearable computing?**

The *wearable computing* paradigm has evolved around three factors: minimization of computer size and at the same increasing the computational power, increased mobility of people, and increasing personalization of devices.

Closely related to each other are *ubiquitous computing*, which is introduced by M. Weiser in [6], and *pervasive computing* which refers to the vision where computers are integrated in the environment and the usage completely transparent to the user. Wearable computing may thus fall under the category of pervasive computing.

Wearable computing is also introduced by the WearIT@work project [7] as follows: *“Wearable mobile computing can empower professionals to higher levels of productivity by providing more seamless and effective forms of access to knowledge at the point of work, collaboration and communication. The new technology of wearable mobile computing will meet the need of many individual professionals for acting more flexibly, effectively and efficiently in the increasingly complicated and challenging European work environment. It can be used to enhance jobs in industry and services to make them both more rewarding and effective and re-elevate the role of the professional at work...”*

---

<sup>2</sup> “The key knob” paper available at <http://ubicomp.lancs.ac.uk/workshops/iwsawc06/papers/9-KeyKnob.pdf>

<sup>3</sup> For instance proximity badges/cardkeys/readers from “Ensure XyLoc”, “QualityKit Ltd” or “RSA Security”. “Ensure XyLoc” proximity badges may be combined with “Passlogix” single sign-on software v-GO and “RSA Security” has a similar solution in its Sign-On Manager.

### **Wearable computing – an example**

An example where wearable computing could enable process innovation is at hospitals where still a lot of work is paper-based, which require a lot of work to be repeated, with the outcome of higher costs, less time with patients for doctors and nurses, risk for errors when later on typing new notes into patient files or typing out orders for medication from handwritten papers. There is also a need to store all the paperwork and it is also quite inefficient sending paperwork around inside a hospital or between hospitals.

At the ward round in hospitals, doctors and nurses may want to do things that might require personal login to a variety of applications due to reasons of traceability/logging, accountability (digital signing) etc. which makes it hard to use only a group laptop<sup>4</sup> or a few PDAs (used by ward round members not directly in contact with patients).

If all the doctors and nurses that do the ward rounds could be online using wearable computers, it would add another dimension of *usability and possible context awareness*.

This would require other ways than ordinary, to operate the computer and input information. Sensors on for instance arms, legs and feet as well as voice may be used to operate the computer without a keyboard as well as delegating the authority to input information to a doctor or nurse close by.

### **Wearable challenges compared to ordinary computing**

General wearable challenges compared to those in ordinary computing have already thoroughly been described in [7].

Regarding security, wearables usually have limited processing power, memory, local storage facilities and possibilities to add devices - which make it harder to set up a security baseline<sup>5</sup> for needed security services (which might be required by the users' organizational IT/information security policy).

### **The next logical step...**

The introduction of wearable computing for professionals looks like the next logical step, and will not only introduce new technology but also have impact on work processes, interaction between people as well as other societal aspects.

## **3 Methodology – requirement process and how to structure the requirements**

The requirement engineering process in the WearIT@work project has been an iterative process driven by four User Centered Design (UCD) teams, supported by the Volere requirement specification process. Both hardware [10] and software [11] platform requirements have been thoroughly engineered [12].

The security related requirements were then filtered out from the final requirement specifications, and analyzed [13] in order to prioritize them, find out what can be solved by using either commercial or open source products/concepts, and what might be needed to develop as being novel features.

The AIC-triad<sup>6</sup> has been used to analyze which requirements, on a “higher requirement level”, that are more important than others – in fact different types of organizations or operations have quite a different need for the three aspects of availability, integrity or confidentiality. For instance the *military* domain may

---

<sup>4</sup> Today, most hospitals use table tops to do the majority of the work, but introducing a laptop (which is a step on way towards wearables) during ward rounds is reality [8] at for instance the Sunderbyn Regional Hospital, Luleå, Sweden, trying to reduce paper work and speed up processes. Another wearable enabler is Siemens' recently introduced RFID-infrastructure for healthcare where PDAs and tablet PCs are supported. The WearIT@work project has one demonstrator [9] developing a wearable infrastructure for ward rounds at hospitals

<sup>5</sup> The “baseline” is described more detailed in chapter 6.

<sup>6</sup> The “Availability Integrity Confidentiality-triad” or “AIC-triad”, is a simple tool to assess what kind of security requirements are the most important for any kind of organization/operation.

emphasize the importance of confidentiality, the *healthcare* domain may require all three aspects, and the *process industry* may prioritize availability and integrity.

The following areas of security were later used for categorization of the security requirements: *authentication, authorization, non-repudiation, privacy, logging, warning messages* as well as *availability, integrity, and confidentiality*.

## 4 Security challenges for wearable computing

### Challenge – protecting sensitive information

A wearable, if integrated in the clothing, is harder to lose or forget somewhere compared to a laptop, PDA or advanced cell phone. Nevertheless if sensitive information, like files or login credentials, is stored inside a wearable<sup>7</sup> – it should be protected by hard disk or file encryption. This is due to the fact that the wearables might get lost anyway: the owner may accidentally forget the garment embedding the wearable device, or lose it somehow.

### Challenge - authentication

As the user of wearables might not be able to type in a password etc. on a keyboard, the need for stable and mature biometric authentication solutions (that are easily integrated into clothing) will most likely grow, to make the wearable easier to use and operate.

### Challenge - unsecure networks and hostile environments

Using wearables and laptops outside of controlled wireless networks, requires higher communications security regarding encryption, information integrity and maybe also non-repudiation. If using ad-hoc networks or unreliable access points, there are a number of well-known security problems [14] and attacks [15] regarding both the information sent as well as availability of the network access. Unfortunately, for instance encryption and integrity checks require some processing power, which might put limitations on the strength of encryption algorithms and encryption key lengths used for wearables.

### Challenge - body area network security...

A new challenge for wearables is the *body area network* which comprises of the wearable computer, all attached devices, and sensors etc., opens up for a number of security threats [16]: sensitive information stored on the wearable device is at risk, privacy and safety issues might arise if the wearer is identified and the electronic identity stolen.

## 5 Novel ideas

### New way to authorize by using context information - authorization by proximity

New ways of using computers will appear as wearables are introduced to substitute paper-based work or laptops and PDAs (please see chapter 2 for more possible advantages using wearables compared to tablets, laptops or PDAs). That introduces a need for novel and more advanced authorization mechanisms where also the surrounding context [17] needs to be taken into account. An example is the ward round scenario in a hospital where a doctor visiting a patient wants to order an x-ray for the patient, and the doctor asks a nurse or doctor participating in the ward round to order it on his behalf using her or his *personal* wearable computer. Another example scenario is related to airplane maintenance: a specialized worker making some maintenance inside a wing may replace some mechanical parts, and may delegate one of his or hers co-workers to digitally track the part number of the mechanical parts being replaced using the

---

<sup>7</sup> Regarding USBs – there are USBs with file encryption available on the market. Thus, these should be considered instead of using regular ones without encryption.

wearable. This is often referred to as *authorization by proximity*, which is a mechanism that allows the controlled *transfer of authorization privileges from an authorizing party to the party (normally unauthorized) performing some task that requires authorization*. For authorization by proximity to be useful, it needs to be combined with the traditional user authorization within applications; each application should also declare a list of tasks where authorization by proximity can be used, and a list of parties allowed to transfer and receive authorization by proximity. Context awareness will provide the application with the information needed to detect at run-time if and how authorization by proximity is possible: such information should comprise information on task and surrounding parties. It should be possible to maintain the traceability (and accountability) of tasks or actions where authorization by proximity is used, by logging information on both the user who transferred authorization and the user who received it (as example the application could log the *task conducted by 'username "a" + username "b"'* where "a" is the authorized person and "b" is the person authorized by proximity). If any actions or tasks need a digital signature to be completed, it must be done with the authorized person's personal encryption key (preferably<sup>8</sup> at the wearable, or perhaps in a smart card if used, where the personal key resides).

Below is an example to better illustrate *authorization by proximity* where *dynamic context information is used to connect the authorizing party with the conducting party*:

The initial lead doctor needs to set up a *ward round context* at the start of the ward round either using all participants RFID tags (or using a screen on the wall to select from lists of employees), perhaps also pre-selecting an initial person who is authorized to order x-rays or medicaments etc. It is also assumed that the patients are identified with an RFID tag and that the medical staff when logging in to their personal wearable, using for instance biometric authentication, also opens up their personal credential store (smart card or similar) where among other things their personal digital encryption keys are stored. As the ward team may need to access encrypted information, group keys for wards could be used to protect the patient file information. The group keys need to be distributed to the users. One option is to use static groups of users, typically those often involved in specific ward rounds, and securely store the needed group keys in their credential stores. Another option is to distribute the group keys when needed in a context (group keys are securely kept during the duration of the context). The first option using static groups of users is not as dynamic as the second option, where dynamic groups of users are set up by the context at run-time.

The following are possible context types to be used for linking the ward round context to the doctors/nurses and the patients, as well as the patient to the doctor:

**Ward round context** [ward name; date, start, stop; *patient RFID*, *lead doctor RFID*, list of doctors, list of nurses, '*person authorized by lead doctor*' *RFID*,...]

**Personal context** [name, *RFID*, type of profession (doctor, nurse etc), level of authentication,...]

**Patient context** [name, *patient RFID*, sign in date, name of doctor, *doctor RFID*,...]

After having created the initial ward round context, the context may change depending on which patient is in focus and the lead doctor may change to be the one identified by the *patient context*. The person authorized by the lead doctor may of course also change during the course of the ward round depending on skill set or if someone has to leave the ward round. Thus, the contexts are dynamic and may change during the course of the ward round.

The level of authentication in the *personal context* could give *single sign-on* to the hospital's applications where all orders for treatment, medicaments etc can be processed. The patient's electronic file could directly be updated during the ward round eliminating today's paper based systems where the electronic patient file needs to be processed by a nurse after the ward round ends. For traceability reasons, changes in the ward round context could be logged automatically,

---

<sup>8</sup> There are also server based digital signing solutions, which may be considered for digital signing.

as well as that all tasks conducted are logged in the applications as described earlier (for accountability reasons if authorization by proximity is used). If anything needs to be signed, like the electronic patient file, the lead doctor may do it in his or her personal wearable – and thus a hash etc. of the patient file needs to be sent to the doctor’s wearable (or smart card if used) to be signed with the personal key and then the resulting signature needs to be returned and stored in the application database. If any user interaction is needed from the lead doctor when signing, it could be displayed on the bedside screen and handled by either using gestures or by using the voice to keep the hands clean and free.

#### **An idea on a pairing mechanism for wearables...to use devices on other wearables**

Another novel idea<sup>9</sup> to increase interoperability between wearables that appeared during the WearIT@work requirement engineering work is *the ability for a wearable A to use devices attached to wearable B*, by having an authentication mechanism similar to the pairing mechanism in BlueTooth [5] where both parties need to be authenticated (mutually). This would probably require a security policy that decides to allow or deny access attempts to what devices from other wearables (or a set of wearables), as well as also decides to allow or deny access to which types of devices on other wearables (or a set of wearables). *This could also have impact on how to manage a local IT-security policy together with the organizational IT-security policy* as the user may need to be able to decide which wearables (and perhaps also types of devices) to allow or deny access from and to. Thus, the organizational IT-security policy may state if pairing with devices on other wearables is allowed at all and how (and if there are pre-defined sets of wearables and types of devices to allow/deny), and then distribute the rest of the allow/deny decisions to the user and local IT-security policy. Allowing distributed decisions by the users seems necessary for professionals to be able to solve their tasks in a quick manner using their professional judgement regarding the possible security risks invoked by pairing.

Typically, a user is tied into work-processes with other users, like a doctor with his nurse or a group of workers doing maintenance. In a wearable scenario this entails the coupling of wearable devices as well, which raises the need for a security policy that treats working groups and their devices as a kind of a pool of services where all must trust each other in order to be shared.

#### **Intelligent policy management – to handle external security challenges**

The world surrounding the user today unfortunately requires the users of wearables and common computers to protect themselves from hackers, viruses, malicious code, and spy ware etc. This is usually managed by having a baseline (the minimum requirement level) of security software. However, the baseline might differ depending on what context and where a computer is used.

Having an advanced *dynamic IT-security policy* that is context dependent [1, 2, 3] and dynamically changes the level of the baseline depending on the surrounding environment, would be suitable for almost all computers but in particular wearables due to the limited system resources. To realize such dynamics, *a more intelligent policy management is needed to only put the needed (optimized) security related load on wearables’ system resources*. However, a similar result may be achieved by using a number of predefined security zones (or static contexts) which are set either when initiating the computer, when recognizing which network is used, or manually set.

The following might be a good idea to always use as a baseline, unless decided not to due to operational reasons:

- Personal firewall
- Antivirus software
- Antispy/malware software (should also be considered due to the growing activity in that field. Using wearables, which most likely will have close access to the *wearers’ personal and biometric information*, may become an integrity/privacy problem as the spyware starts to try to collect information from wearables).

---

<sup>9</sup> Idea by Dr Wolfgang Thronicke

Hard disk or file encryption, strong authentication, secure communications, ensured integrity, digital signatures etc. might also need to be considered as part of the baseline as well as other security services required by the context.

As the above security software consumes system resources – it needs to be tested and properly configured for wearables, as otherwise the wearable might be unable to perform adequately.

However, the wearables' current performance problems are expected to vanish in a couple of years as the development of hardware- and software technology progresses.

## 6 Summary

This paper has discussed IT- and information security challenges for wearable computing encountered during the WearIT@work project. The research question raised in the introduction of this paper: “What aspects of security for wearable computing are of special interest considering the experience gained from the WearIT@work project?”, was addressed by high-lighting security challenges and presenting novel ideas.

This paper has high-lighted security challenges concerning wearables which show that wearables will raise new requirements on many security services in general (to adapt to increased mobility yielded by wearables and at the same time upholding an adequate level of security), most likely including also dynamic context information to better support new work processes and better integrate into the existing IT-infrastructures.

This paper has also presented some novel ideas such as *authorization by proximity* using dynamic context information to increase usability by enabling transfer of authorization from one party to another party, a *wearable pairing mechanism* to use devices on other wearables, and a *more intelligent management of dynamic IT-security policies* to only put the optimized security related load on wearables' system resources. The last idea includes to have a *dynamic security baseline for wearables* to maintain the integrity and confidentiality of the body network as well as the privacy of the wearers' personal and biometric information.

Organizations need to address wearables and wearable devices in their IT- and information security policies to set up an adequate level of security, since wearables add new challenges to the ordinary ones. Wearables will also be used in new ways and in novel and sometimes more hostile environments compared to ordinary computers.

## 7 Acknowledgements

The majority of the security requirements have been collected by the WearIT@work project members during the initial phase of the project. A special thanks to Prof Michael Lawo at TZI, University of Bremen, for his encouragement to write this paper and to Marco Luca Sbodio at HP Italy Innovation Centre and Dr Wolfgang Thronicke at Siemens Business Services C-LAB, CEO Anders Lundkvist at Arctic Group AB, Dr Kåre Synnes and Dr Peter Parnes at Lulea University of Technology for their valuable input.

This work was funded under grant 004216 by the European integrated project “WearIT@work – Empowering the mobile worker by wearable computing”.

## 8 Future work

To prepare organizations to introduce and adapt to the new wearable technology, they need among other things to address their business requirements on wearable security as well as the legal framework on privacy protection and data security. There are plans to investigate the impact from wearables' security challenges on future IT- and information security policies within certain industry domains.

## 9 List of references

More information on the WearIT@work project is available at: <http://www.wearitatwork.com>

- [1] Ghita Kouadri Mostéfaoui, Jongwoo Chae, Mansoo Kim, Mokdong Chung: Context-Based Security Management for Heterogenous Networks using MAUT and Simple Heuristics; PARA 2004
- [2] Patrick Brézillon, Ghita Kouadri Mostéfaoui: Context-Based Security Policies: A New Modeling Approach; PERCOMW 2004
- [3] Patrick Brézillon, Ghita Kouadri Mostéfaoui: Context-Based Security Policies with Contextual Graphs; PERCOMW 2004
- [4] Nitesh Saxena, Jan-Erik Ekberg, Kari Kostianen, N. Asokan: Secure Device Pairing based on a Visual Channel; 2006 IEEE Symposium on Security and Privacy
- [5] BlueTooth security; <http://www.bluetooth.com/Bluetooth/Learn/Security/>
- [6] Mark Weiser: The computer for the 21<sup>st</sup> century, Scientific American, 265(3):94-104; September 1991
- [7] WearIT@work, Annex I – Description of Work, pages 6, 14-22; 2004
- [8] Sunderby Hospital – a new hospital for a new century;  
[http://www.nll.se/upload/IB/lg/pers/informationsmaterial/SY\\_BROSC.PDF#search=%22sunderbyn%20%2B%20lap%20top%22](http://www.nll.se/upload/IB/lg/pers/informationsmaterial/SY_BROSC.PDF#search=%22sunderbyn%20%2B%20lap%20top%22)
- [9] Victoria Carlsson, Tobias Klug, Thomas Ziegert, Andreas Zinnen: Wearable computers in Clinical Ward Rounds; IFAWC 2006
- [10] WearIT@work deliverable D07 - Showcase platform architectural design and specification – A technical document; October 2005
- [11] WearIT@work deliverable D06N - Show case framework architectural design and specification; October 2005
- [12] WearIT@work deliverable D09N - An European industrial mobile computing platform including sector specific aspects – Requirements; October 2005
- [13] WearIT@work deliverable D29 - Design and specification of wearIT@work computing system; August 2006
- [14] Varaporn Pangboonyanon: Network-Layer Security in AODV networks; 2004
- [15] Nikos Komninos, Dimitris Vergados, Christos Dogligeris: Layered security design for mobile ad hoc networks; Elsevier Computer & Security 25, 2005
- [16] SWAMI project deliverable D2 – Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities; [http://swami.jrc.es/pages/documents/SWAMI\\_D2\\_scenarios\\_Final\\_ESvf\\_003.pdf](http://swami.jrc.es/pages/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf); January 2006
- [17] Marco Luca Sbodio, Dr Wolfgang Thronicke: Context processing within an open, component-oriented, software framework; IFAWC 2006