Back to the Future: Evaluation Model for Wearables Based On the Past Experience

Marta Piekarska and Shinjo Park and Altaf Shaik
Security in Telecommunications
Technische Universität Berlin
Berlin, Germany
Email: marta OR shinjo OR altaf@sec.t-labs.tu-berlin.de

***Abstract*—Today every user has a plethora of devices to choose from, depending on the task. In addition to omnipresent laptops, smartphones and tablets, we have recently seen an expansion of a new type: the wearables. Wearable devices vary from fitness trackers, through watches and glasses, all the way to medical-grade equipment. This Systematization of Knowledge paper investigates the historical shift in the security and privacy considerations when smartphones started replacing laptops, and tries to predict how the change will look like this time. We examine the categories of attacks on laptops and mobile devices and analyze how those will work on wearables. We also recognize the additional threat layers when these elements are combined into Internet of Things. Finally, we propose mitigations and potential defenses to some of the biggest challenges. In summary this paper contributes to the field by a thorough systematization of knowledge of the attack vectors on various devices and proposes a method of predicting the security threats to new device types.**

***Index Terms*—privacy, internet of things, wearables, systematization of knowledge**

I. Introduction

Personally Identifiable Information is a concept describing linking of attributes (has cancer or is in a certain location) to a particular person. It ranges from strictly private data like phone number or address, through common locations all the way to browser fingerprinting [1].

The market of wearable technology is predicted to rise to over $37B by the end of 2020 [2]. It is not yet well understood what will be the consequences of such expansion on privacy and security. One is sure: nowadays computer security impacts everyone, even if they don't use what they think of as a "computer" [3]. In fact, any modern computer is a system far too complex for any individual to grasp it as a whole. The problem of securing every element of the stack gets additionally complicated when we grow it by connecting several devices into Internet of Things. The number of attack vectors does not simply become a sum of attacks on each device included.

With our work we contribute by:

1) **Systematization of Knowledge**
2) **Possible Attack Vectors for Wearables**
3) **Security of Internet of Things**
4) **Countermeasures and defenses** to the identified problems

The rest of the paper is organized as follows. The next section talks about the history: what were the threats that were common to laptops and smartphones, and what were the problems previously unknown that emerged with the popularization of the smartphones. Section II describes the model that we built to evaluate any new device. We then apply this model to present the evaluation of wearables in Section III. Next, in Section IV we spent some time to point out the elements very specific to the nature of Internet of Things. Finally, in Section V we present some of the suggested defenses and mitigations, and conclude in Section VI.

II. Building a Model

We have found very few approaches that try to systematize the evaluation of the devices. Among them there is [4] where the authors tried to predict the future of mobile phones by analyzing the models, algorithms, applications and middleware. In their followup work from 2014 [5], they note however, that the approach did not prove to be useful, and they failed to predict certain developments. Another notable paper was written by Delac et al [6], in which authors summarize the mobile security threats. It is a good but post-factum analysis, and their model does not scale to other device types.

We assume that the technology moves in an upward spiral manner and every new device is build on top of the previous ones, which makes the assessment simpler. Moreover, we believe we can build a universal security stack where each layer is protected by the previous ones. Lastly we think a complete analysis can be performed by naming the assets, identifying the threats, looking at historical vulnerabilities and attacks, and defining the risks.

Security assessment can be seen as a cycle of 6 steps. Initially, we define the assets a device can hold, next we try to find the threats, identify the vulnerabilities, and ways to exploit them, finally predicting the risks connected to those we can focus on designing countermeasures and implementing defenses. However, looking just at the big picture might not be enough for a complex system. That is why we define layers of security stack that need to be inspected. On the bottom there is the Network Infrastructure - everything that allows a device to stay connected. Next comes the hardware - physical elements that comprise a device, like sensors, memory etc. Together with it we need to consider the drivers that allow

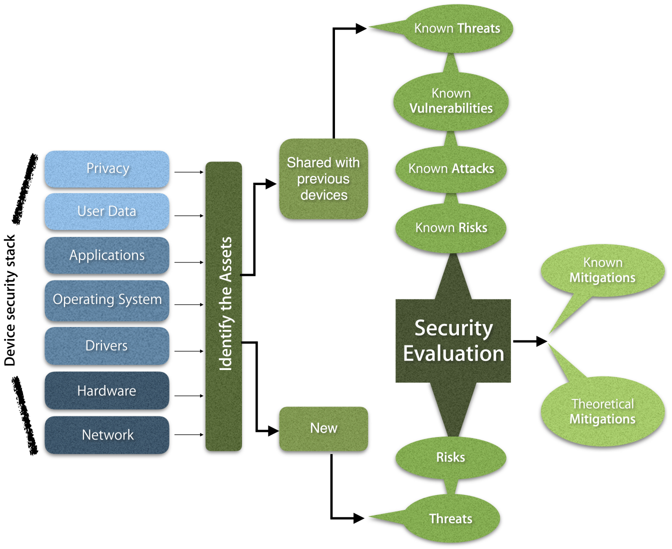

Fig. 1. Model for security evaluation of a new device.

for access and manipulation of the device. The layer above that is the Operating System(OS) that governs the behavior of the device, and manages access control to the file systems. On top of the OS, in most cases, sit the applications - some devices, like the fitness trackers will not allow for third party applications, but still there is a software installed in addition to the OS. Finally we come to the user data which is all the information that an owner of the device generates, everything that can be considered PII. We put privacy on top of the stack, as protecting it mostly means protecting from leakage of user data. The model we build based on the above assumptions is presented in Figure 1.

III. Security Evaluation of Wearables

Having a model and some hints on what are the differences and commonalities between security challenges on laptops and mobile devices, we now move to evaluation of the wearables.

A. Assets

We consider four types of wearable devices: fitness trackers, smartwatches, headmounted devices and medical devices(IMDs).

Each layer of the security stack has many assets connected to it. In case of mobile devices and smartwatches we first have the network: the contents of communication that goes over the channels and the infrastructure. Next, there is the hardware: sensors the device has. The more sensors there are, the more possibilities of attacks.

On the software side, we start with the drivers: ensuring the integrity of the binary files so that the attacker cannot manipulate the hardware. In the Operating System we have its integrity, access to the memory, availability. Next, come the applications. What is protected is again thier integrity and availability of the services.

We then come to the third big part - the user data and privacy. In case of fitness trackers data includes fitness level that comes from monitoring the heart rate – the pulse, estimation of calories burned etc, location over time, sleep patterns and user-input data like their age, weight, height and so on. In terms of smartwatches in addition to the above we have much more elaborate health data that can be tracked either with the watch itself or by connecting other monitors to it. These include e.g. nutrition facts, reproductive health, blood pressure, temperature and so on. Additional data contain things we normally think of in terms of mobile devices: recordings and photos, contacts, passwords, list of applications, emails and messages and so on. Lastly, protecting the integrity and confidentiality of the data stored.

B. Threats

Wearables have the same set of sensors, are connected, quite powerful, very personal. Depending on the category, the threat models will be slightly different: fitness trackers and medical devices are less powerful, thus will not be used for heavy computations, while smartwatches and glasses are almost identical in construction to mobile devices and will be exposed to threats.

On the network level the threats are similar, as the assets are also fairly identical: the Golden Graal is to be able to intercept and possibly modify data that come from and to the wearable. The impact and incentive, however, is higher as the data is more valuable. Most of the wearables use the same connectivity methods as mobile devices: Bluetooth, ANT radio, cellular data and Wi-Fi. Some devices, use proprietary protocols or advance of software-defined radio (SDR) enabled decoding of proprietary wireless communication standards. [7]. The threats include: stealing the contents of communication, gaining access to the elements of a network (eg., Wi-Fi hotspots, Base transceiver station (BTS) etc.), modifying the contents of communication and altering the message path (forwarding the message to unauthorized person).

Most of the wearables, are still dependent on a ”bigger brother” - be it a smartphone, a laptop, or a dedicated terminal - to process data and perform heavier computations. Thus another threat is intercepting or modifying that communication. That requires compromising the OS or gaining access to the hardware. As wearable devices almost always have a full OS installed, in these terms, again the threats popular in mobile devices will also apply to them. Thus, poor user authentication due to the form factor and lack of secure key storage can be seen as big challanges.

Finally, threats to privacy on wearables are more significant. Data is collected unconciously and becones very valuble. Its improper protection of the data may also lead to leakages that can be dangerous (revealing information about location), embarrassing (search history), or cause financial losses (access to payment information). Moreover the stealth capturing of scenes can be abused by either the attacker or the owner spying on the surrounding. Until today many companies have ot yet included Wearables into their Mobile Device Management policies.

Final threat to privacy is based on the correlating data. What happens if the increased heart rate is combined with information that the user is in a hotel during work hours? What is in addition to it we can also find the sounds in the room? Can we then accuse them of adultery?

Due to the form factor of the screens the way we inteact with wearables has changed compared to other devices. Voice recognition became more popular way of navigating these devices which means more data transmitted and stored over potentaily insecure channel. Lack of proper displays also impairs the way we can inform users about the privacy policies and warnings, which means poor transparency. Wearable devices are powerful, have access to a lot of information about their owners, yet present no transparency of what tasks are being executed.

Laptops gather information about our activity, mostly things we download, history of usage. Smartphones have the ability to record elements like our position, movement, things that happen around us - through camera applications. Wearables go further. More than any others, these devices are able to collect more precise data over time - gathering a detailed description of the owner's life. They can also be better instrumented to understand the context in which user is. Without good diversification it is easy to gain access to information about user's whole life just by attacking this singe element.

Wearables as a new category of devices are not yet subject to any standardization procedures. We still lack policies that would describe how to deal with the authentication problems - what are good ways to implement secure storage on devices, how to manage the Personally Identifiable Information(PII), and most importantly - what to do with very sensitive data, like health results. The threat is that without such standards every manufacturer will implement their own, possibly faulty, mechanisms.

C. *Vulnerabilities and Attacks*

One of the earliest attack on fitness tracker is done by Rahman et. al [8] using Fitbit. It presents attack on spoofing device sensor, eavesdropping and injecting data between base and web services.

1) Smart Watches: A good overview is provided by HP Fortify and the Internet of Things report [9]. They have evaluated top 10 smartwatches and found that 70% of the firmwares is sent through unencrytpted channels, 30% of the devices were vulnerable to Account Harvesting, allowing attackers to guess login credentials and gain access to user account, and as much as 90% of communication(!) could be easily intercepted.

One of the earliest attacks on MDs is presented by Halperin et. al [7] in 2008. This work covers security of externally controllable implanted pacemaker. Kune et. al [10] presented EMI injection attack on medical sensors inside pacemaker, which could trigger unintended operation of medical devices.

In October 2011 Barnaby Jack managed to override the insulin pump's radio control and its vibrating alert safety feature, enabling to dose a an unaware patient with a lethal amount of insulin [11]. Li et. al [12] also presented an attack on insulin pump with similar result.

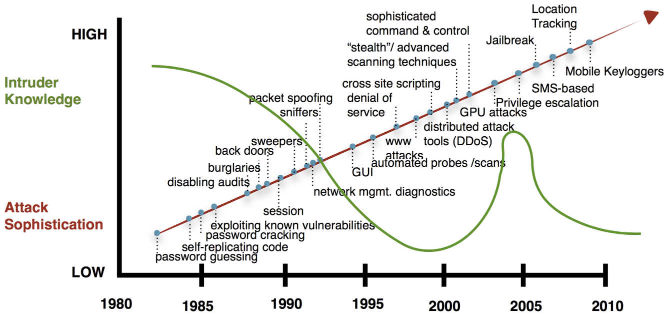

Fig. 2. Attack Sophistication vs. Intruder Technical Knowledge.

The conclusion can be drawn that a significant problem with medical wearables comes from the fact that we are still in the phase of patching together existing devices with embedded computers rather than designing them from the scratch. We have little to no "Security by Design" approach, which is crucial as we are speaking of things that when exploited, more than any others, can threaten human lives.

Wearables mostly inherit Operating Systems from smartphones. That means that whatever could be exploited on one can also be done on the other. Thankfully manufacturers tend to improve their systems and patch the bugs which means that old problems cannot be revisited. However we have already seen report that Google Glass runs Android 4.0.4, which is subject to the adb restore race condition [13].

D. *Risks*

In his report from 2002, Lipson, presented how the sophistication of attacks developed while the intruders technical knowledge dropped over time [14]. Figure 2 is an extension of the original one with attacks that have become biggest risks to smartphones, like rootkits or location tracking. As can be seen, we believe that there was a brief spike in the requirement in the knowledge of an intruder when a new device type was introduced - it was no longer as obvious as before how to attack it. But we quickly got back to repackaging everything into simple tools and today, it is enough to go on a website that will give you those information, or download a simple package to jailbreak your iPhone.

The risks are directly proportional to what the attacker can gain. In the era of laptops the goal was gaining access to computing power. Distributed attacks were created so that viruses could spread in millions of copies and allow intruders to create a network of computers working to their advantage. Today even the attacker model changed: one is Malfoy, who owns a device and wants to root it. He becomes a hostile actor towards his own device. Second is Mark, who tries to steal data off other devices. And Mark in the world of smartphones will not seek computing power. It is too cheap to buy otherwise. He will want to gain access to PII, most probably to later sell it to advertising companies or governments. Today it is the information that brings money and is most valuable.

IV. When it all comes together: IoT

Internet of Things(IoT) is not just a combination of various devices connected with each other. The attack surface is not calculated by a simple addition of all attacks known to each of the elements of IoT but a multiplication.

A. Assets

For the purpose of this paper we will focus on a ”single user IoT”: what happens when we connect wearables with smartphones and laptops. On top of what each of those ”things” brings to the table additional assets include:

- communication between devices,
- ability to control one through the others,
- ability access data over another device,
- pervasiveness - even if one device is not there, another will be,
- permissions given to each device.

On the last point: there is no clear way how to negotiate and see sharing data between the devices. It is not necessarily the case that user will agree to tracking on every element of IoT - if so, how should that communicate to the other ”things”?

B. Threats

The problem with IoT is that each of its elements is different, yet a security solution must cover it all. The design is influenced by the threat model, device architecture, protocols and interfaces required and power and performance targets. In addition to protecting each element separately, a mechanism of ensuring trust between them has to be deployed. Now, the CIA – Confidentiality, Integrity and Availability has a second level. Each ”thing” has to have an identity that can be proven to other devices, it has to act in a predictable way that cannot be altered by an attacker to change the behaviour of the whole system. What follows is that the communication channels between the elements have to be protected from unauthorized access, as well as the data on the devices. Most importantly, it is crucial to ensure a certain separation – so that failure of one ”thing” does not compromise the whole system. The devices that comprise IoT are often produced by various vendors and need to communicate, which may create various problems with the protocols: they need to be well examined and understood.

C. Vulnerabilities and Attacks

Security of IoT is a big problem. 80 percent of Amazon’s top 25 best-selling SOHO wireless router models have security vulnerabilities [15]. What is more scary, the same report states that almost one third of IT professionals and 46% of employees do not change the default administrator password on their wireless routers. A big part of IoT threat is that whatever happens the impact will be bigger. There are more devices, more computing power, more data, thus more incentives and more vulnerabilities.

IoT devices are operating in non-traditional area of network, like personal area network (PAN), body area network (BAN) or controller area network (CAN). Like Ubertooth for Bluetooth, KillerBee can decode ZigBee and IEEE 802.15.4 packets. [16] ZigBee and/or IEEE 802.15.4 is used in home appliances, thermostats, manufacturing systems, medical devices, retail, transportation, etc. KillerBee provides tools to capture and decode 802.15.4 signals, with custom firmware on AVR RZ Raven USB stick as radio device. Choi et. al [17] presented reverse engineering IEEE 802.15.4 based home and transportation appliance using KillerBee.

IoT devices communicating with BLE or other insecure channel share the communication privacy and identity problems [3], [18]. Unlike wearables, IoT devices are designed with infrequent human interaction and longer continuous operation in mind. As a result, security incident reported by IoT devices might not be handled in timely manner, and software patching for security problem could not be possible in some cases where parts are discontinued or a manufacturer has been closed.

V. Defenses and Mitigations

We will now discuss technical countermeasuers and design considerations of wearable devices which allow the users to monitor and control the exposure of their private data from the wearable device.

A. Authentication and encryption techniques

Although the main focus of existing literature is on securing MDs [19], we believe that the same defence measures can be applied to other types of wearable devices. One of the first concepts proposed was symmetric-key based authentication methods for distributed access control in wearables [20]. By pre-distributing the keys, the device and any authorized body can easily generate pairwise keys to perform authentication. However, Symmetric Key Cryptography (SKC) based methods suffer from numerous disadvantages [21].

There are SKC-based techniques that do not depend on pre-distributed keys and require additional hardware devices [22]. This out of band secure channels inlude USB connections [23], infrared [24], visual [25], audio but mean adding extra hardware. This requirement is unrealistic and is against the global trend of device miniaturization.

In Identity Based Encryption (IBE) technique where no prior key distribution is necessary between the users and devicescite [26]. On the other hand, traditional IBE techniques demand heavy computation and are not appropriate for body area networks. To solve this problem authors of [27] provide a lightweight IBE-based access control mechanism built using elliptical curve cryptography (ECC). Its main limitation is that once a certain number of secret keys are leaked, the master key can be compromised. Besides IBE, Attribute Based Encryption (ABE) is also studied in the literature. For example, ciphertext policy ABE was introduced in [28] to allow role-based access control on encrypted data in WBAN’s.

Authentication with non-cryptographic methods such as proximity based, biometric based and channel based methods are also studied in the literature. By extending the Diffie-Hellman (DH) key exchange protocol the authors in [29] could develop authentication mechanism for co-located devices. Ensemble technique [29] and co-location based pairing scheme [30] also propose proximity based authentication scheme. Ramussen et al. [31] use ultrasonic sound signals to compute the distance between the programmer and IMD. Capkun et al. [32] proposed integrity code which protects the integrity of the messages sent over insecure wireless channel. Gollkota et al. [33] proposed tamper-evident pairing. It assumes infeasibility of signal cancellation, and exploits unidirectional error detection codes to provide message tamper-evidence.

The use of physiological signals (biometric data) for securing wireless medical devices was first introduced in 2003 [34], and later adopted for electro-cardiogram(ECG) and photoplethysmogram (PPG) signals by Poon et al. in 2006 [35]. Further, in [36], inter-pulse intervals (IPIs) and heartbeats are potential source for generating secret keys. Besides that, a more robust usage of IPIs with measurement noise for authentication is presented in [37]. However, encryption based on ECG signals is more prominent in the literature [38], [39], because of its higher randomness as compared to other physiological signals (PVs)such as heart rate, glucose level in blood, blood pressure and temperature along with the preceding ones.

In general, due to their unique, random and time-sensitive nature, physiological information can serve as a reliable source for authentication and secret key derivation among the wearable devices. Nevertheless the major drawback is that physiological information is usually accompanied with high amounts of noise and variability. Hence it is difficult to guarantee consistent physiological measurements with same accuracy for sensors located on different positions on human body. Moreover, all physiological parameters do not have the same level of entropy for key generation.

B. Design Considerations

Hitachi's Business Microscope identity badge, which contains embedded infrared sensors, an accelerometer and a microphone sensor, purports to capture the interaction patterns in the workplace but also the quality of employee collaboration [40]. Monitoring of our emotions, health status and the quality of our human interactions strikes at the very core of our most intimate selves. The interaction medium with the wearable device also has an impact on the user's privacy. The users capability to modify, perhaps switching the input mode from audio to text would be a possible design modification to enhance privacy.

User privacy is one aspect but the privacy of others around the user is another. With wearable devices, that are seamlessly embodied into undistinguished objects, such as shirt buttons, eyeglass frames, watches it is quite effortless to gather information about others without their awareness [41]. Similarly, users have privacy concerns about location information, primarily because wrist-mounted devices are able to track their position and immediately publish it online in social media applications to a network of contacts. To combat this issue users must be able to choose their desired level of privacy.

Roesner et al. identified potential security issues with wearable devices and explored the problems these devices create in terms of law and policy [42]. Further, researchers have studied several methods to protect privacy in an IoT scenario. Examples of such works include frameworks to design for protocols for communication, privacy focused designs, protocols for anonymous communication, evaluation metrics for privacy and its models. At the same time, the legal frameworks need to adapt to the use of wearables, as they put new requirements on the protection of personal integrity and privacy as well as information security.

It is essential to abide by certain design principles enumerated below, for protecting privacy in the wearable computing environment, as the characteristics of today's wearables evolve in tandem with the Internet of Things.

- transparent authentication and security mechanisms and device functionalities
- dynamically calibrated privacy rules that provide tight control of what the device does
- user controlled network connection and disconnection
- privilege escalation on the device

Finally, practical implementation of security measures in wearable devices depends on several factors. There is no single method that suits all situations. One needs to collectively consider the application security requirements, system security requirements, hardware/software/physical/power restrictions and the possible tradeoffs among them.

VI. CONCLUSIONS

In this paper, we built a general model to evaluate any new device on the market based on the past experiences rather than from the scratch. We observed how did the attacks change when smartphones took over the market. We applied the model to predict the future problems that we will see in the wearables. We also presented what we see as the biggest challenges that Internet of Things will face - the multiplication rather than addition of attack vectors. Finally, we discussed what could be the possible defense mechanisms that we should build prior to the attacks.

Among various security measures, authentication and encryption are the crucial steps in building secure communications with the wearables. Additionally we need to develop dynamically calibrated privacy rules to meet individual's privacy needs and expectations, integrate simple design features so that the wearable device can reflect personal privacy preferences, and call on organizations to enhance their privacy policies with dynamic and interactive data maps and infographics to show relationships in the wearable computing device ecosystem. Finally, it is important to touch on the question of transparency. While security is a problem that can be boiled to meeting a certain standard, sometimes the best we can do in terms of privacy is being clear about what and when happens on the device. We are lacking mechanisms that inform users that their data is being collected and uploaded in the real time. We see that as the next challenge to the academia.

REFERENCES

[1] E. McCallister, T. Grance, and K. A. Scarfone, "Sp 800-122. guide to protecting the confidentiality of personally identifiable information (pii)," Tech. Rep., 2010.

[2] Research and Markets, "Global smart wearables market forecast and opportunities, 2020," Tech. Rep., 2015. [Online]. Available: http://www.researchandmarkets.com/research/j7fhxw/global_smart

[3] F. Stajano, *Security for Ubiquitous Computing*, 2002. [Online]. Available: http://www.cl.cam.ac.uk/~fms27/secubicomp/

[4] G.-C. Roman, G. P. Picco, and A. L. Murphy, "Software engineering for mobility: A roadmap," ser. ICSE '00. [Online]. Available: http://doi.acm.org/10.1145/336512.336567

[5] G. P. Picco, C. Julien, A. L. Murphy, M. Musolesi, and G.-C. Roman, "Software engineering for mobility: Reflecting on the past, peering into the future," ser. FOSE 2014. [Online]. Available: http://doi.acm.org/10.1145/2593882.2593884

[6] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in *MIPRO, 2011 Proceedings of the 34th International Convention*.

[7] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," *Proceedings of IEEE Symposium on Security and Privacy*, 2008.

[8] M. Rahman, B. Carbunar, and M. Banik, "Fit and vulnerable: Attacks and defenses for a health monitoring device," *Privacy Enhancing Technologies Symposium*, 2013. [Online]. Available: http://arxiv.org/abs/1304.5672

[9] C. Smith and D. Miessler, "Internet of things security study: Smartwatches," Tech. Rep., 2015. [Online]. Available: http://go.saas.hp.com/fod/internet-of-things

[10] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," *Proceedings of IEEE Symposium on Security and Privacy*, 2013.

[11] D. Goodin, "Insulin pump hack delivers fatal dosage over the air," *The Register*, 27 Oct 2011. [Online]. Available: http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

[12] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011*, 2011.

[13] [Online]. Available: https://twitter.com/saurik/status/327857009754001408

[14] H. F. Lipson, H. F. Lipson, P. D, and P. D, "Tracking and tracing cyber-attacks: Technical challenges and global policy," 2002.

[15] T. Vulnerability and E. R. Team, "Soho wireless router (in)security," 2014. [Online]. Available: http://www.tripwire.com/register/soho-wireless-router-insecurity/showMeta/2/

[16] J. Wright, "KillerBee: Practical ZigBee Exploitation Framework," 2009.

[17] K. Choi, Y. Son, J. Lee, S. Kim, and Y. Kim, "Frying PAN : Dissecting Customized Protocol for Personal Area Network?" *Proceedings of the 16th International Workshop on Information Security Applications*, 2015.

[18] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and Privacy Threats in IoT Architectures," *International Conference on Body Area Networks*, 2012.

[19] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," *Proceedings of IEEE Symposium on Security and Privacy*, 2014.

[20] M. Mana, M. Feham, and B. A. Bensaber, "A light weight protocol to provide location privacy in wireless body area networks." [Online]. Available: http://arxiv.org/abs/1103.3308

[21] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *Wireless Commun.*, 2010. [Online]. Available: http://dx.doi.org/10.1109/MWC.2010.5416350

[22] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," ser. INFOCOM'10. [Online]. Available: http://dl.acm.org/citation.cfm?id=1833515.1833857

[23] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks."

[24] D. B. Smetters, D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," 2002.

[25] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu, "Gangs: Gather, authenticate 'n group securely," ser. MobiCom '08. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409957

[26] C. Rong and H. Cheng, "Authenticated health monitoring scheme for wireless body sensor networks," ser. BodyNets '12. [Online]. Available: http://dl.acm.org/citation.cfm?id=2442691.2442700

[27] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Ibe-lite: A lightweight identity-based cryptography for body sensor networks," *Trans. Info. Tech. Biomed.*, 2009. [Online]. Available: http://dx.doi.org/10.1109/TITB.2009.2033055

[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," ser. SP '07. [Online]. Available: http://dx.doi.org/10.1109/SP.2007.11

[29] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara, "Amigo: Proximity-based authentication of mobile devices," ser. UbiComp '07. [Online]. Available: http://dl.acm.org/citation.cfm?id=1771592.1771607

[30] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," ser. MobiSys '11. [Online]. Available: http://doi.acm.org/10.1145/1999995.2000016

[31] K. B. Rasmussen and S. Čapkun, "Realization of rf distance bounding," ser. USENIX Security'10. [Online]. Available: http://dl.acm.org/citation.cfm?id=1929820.1929854

[32] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *Dependable and Secure Computing, IEEE Transactions on*, 2008.

[33] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure in-band wireless pairing," in *In USENIXSecurity Sym.,2011.*

[34] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Parallel Processing Workshops, 2003*, 2003.

[35] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *Comm. Mag.*, 2006. [Online]. Available: http://dx.doi.org/10.1109/MCOM.2006.1632652

[36] S.-D. Bao, C. C. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *Trans. Info. Tech. Biomed.*, 2008. [Online]. Available: http://dx.doi.org/10.1109/TITB.2008.926434

[37] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," ser. CCS '13. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516658

[38] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *Information Technology in Biomedicine, IEEE Transactions on*, 2010.

[39] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *INFOCOM, 2011 Proceedings IEEE.*

[40] R. G. of the Office of the Privacy Commissioner of Canada, "Wearable computing: Challenges and opportunities for privacy protection," 2014.

[41] K. Krombholz, A. Dabrowski, M. Smith, and E. Weippl, "Ok glass, leave me alone: Towards a systematization of privacy enhancing technologies for wearable computing," in *1st Workshop on Wearable Security and Privacy*, 2015.

[42] F. Roesner, T. Denning, B. C. Newell, T. Kohno, and R. Calo, "Augmented reality: Hard problems of law and policy," ser. UbiComp '14 Adjunct. [Online]. Available: http://doi.acm.org/10.1145/2638728.2641709