SECURITY AND PRIVACY ISSUES

of Handheld and Wearable Wireless Devices

By Roberto Di Pietro and Luigi V. Mancini

THE DISTINGUISHED CAPABILITIES OF THESE DEVICES ARE ALSO THE VERY REASONS THEY REQUIRE SECURITY AND PRIVACY PROTECTIONS OF AN UNPRECEDENTED SCALE.

We are surrounded by a variety of appliances important for our daily lives and that require our constant attention, such as a wearable heart rate monitor, a car outfitted with multiple sensors, a PDA, or a cell phone possibly equipped with a GPS device. A few of these appliances can currently communicate with each other; their clever, simple, and ultimate integration is the dream of every user.

Many consumers would buy new devices to fulfill such a dream. Consider this scenario: One of the processors embedded in your car could signal your PDA that it's time for an oil change. The request for an appointment is simultaneously received by your cell phone, which interacts transparently with the PDA to schedule both the appointment and the oil change. This example indicates how handheld/wearable wireless (HWW) devices are particularly useful if they could directly interact with other appliances. To achieve such a goal, frequent communication must occur in a manner transparent to the user. This continuous activity constitutes a serious breach in the user's privacy and security, and could increase the possibility of the user being physically located, regardless of his/her actions. Here, we illustrate how the user's privacy and security appears at risk under any HWW interoperability model.

Due to their small size and mobility requirements, the design and implementation of HWW devices must consider the following con-

ILLUSTRATION BY TERRY MIURA

straints [2]: battery depletion—while a PC is usually plugged, an HWW device may not be, thus energy-saving requirement must be addressed; hardware constraints—small amount of RAM, slow processors, and usually no mass storage; limited communication range—the extent of the area covered by the wireless transmissions is usually limited both for technological reasons and for the energy-saving considerations; and transient communication—because of the mobility of the devices, the network can experience a high rate of communication failures.

The advertising of services, and the cooperation among HWW devices, requires a careful analysis of both technological and nontechnological issues. The technological issues to be addressed include the protocols, the algorithms, and the communication infrastructure to be employed. The main nontechnological issues include the design of new regulations for this virtually global environment, since the user's personal privacy and security may be more exposed than they are today [1].

Here, we discuss two models for the HWW paradigm along with the prevalent security issues and user privacy concerns.

WIRELESS COMMUNICATIONS make physical eavesdropping almost undetectable.

HWW Network Models

The concept of Web presence [10] can be defined by transposing the services on the Web that a physical object offers, and by adding transparent communications to other similar abstractions present in the Web.

Flat Web presence. Web presence requires the solution of major research problems. Consider, for example, the implementation of the anywhere-anytime paradigm for the HWW devices, which requires protocols and algorithms to provide widespread access to an open set of services supplied by almost every useful HWW device [10]. A HWW device must resort to some sort of intelligent, context-aware agent [8] that should prune the services deemed worthless to a particular user. The pruning process should also decrease the overall traffic load, thus resulting in savings in both communications and battery consumption.

The feasibility of this scenario requires a network infrastructure pervasive and distributed to an extent not experienced by the Internet to date.

Hierarchical Web presence. Restricting the scope of the Web presence of a service can reduce the complexity and the traffic load of the previously described network infrastructure. The hierarchical Web presence is based solely on local interoperability among HWW devices. Multihop communications are allowed on demand by relaying on some sort of back-

bone. Such an approach simplifies the design of the network infrastructure preserving the push paradigm among directly connected HWW devices. The access to nonlocal services is on demand only, and follows the pull paradigm. The backbone supports the look-up function for remote services.

Direct interoperability. Both models presented here must support direct interoperability, which is how the HWW devices interact when in direct communication range. The direct interoperability requires the provision of several functionalities that include service discovery—the HWW devices look for possible services providers in their direct communication range; service advertising—the HWW devices offer their services to other HWW devices (a push paradigm seems more suitable to implement such a service [3]); and service providing—the HWW devices deliver the offered service.

The possible implementation choices may depend on the resources the devices can dispose of. Note that the availability of an Object Request Broker (ORB) paradigm can simplify the design of all three functionalities.

Security Challenges

The successful deployment of HWW devices requires a satisfactory level of security. To certain extent, it seems reasonable to export the solutions identified for the wired environment in the wireless field. However, this approach is not always feasible because of the differences between the two models. For example, because of the hardware limitations of the HWW devices, no large routing tables can be maintained on these devices, thus increasing the risk of a denial-of-service attack. Moreover, the attacks that require access to the physical media are simpler. Indeed, wireless communications make physical eavesdropping almost undetectable.

Despite their differences, the two models share three basic security requirements: confidentiality—information is disclosed only to legitimate entities or processes; integrity—unauthorized modification of information is prevented; and availability—authorized entities can access a service provided they have appropriate privileges.

These issues have been enforced through different architectural choices. The wired paradigm can deliver confidentiality through the use of access control techniques [12] and the use of cryptography; integrity through the combined use of a Message Authentication Code (MAC) and cryptography; and availability through the implementation of service replication.

Here, we present the mechanisms suitable to the HWW paradigm while pointing out the potential limitations in their use.

Cryptography. The two types of cryptography currently available are symmetric and public-key cryptography (PKC). In symmetric cryptography, two devices must share their secret key in order to communicate securely. Thus two points arise: How to exchange the secret key securely; and if n devices must communicate with each other, a total number of $O(n^2)$ secret keys must be exchanged. The management of such a number of secret keys should consider the scalability issues.

In PKC, both the aforementioned problems are solved, since the partners in the communication do not require exchanging any secret keys.

According to these considerations, PKC seems the ideal candidate to enforce confidentiality. Indeed, many security mechanisms in the wired paradigm are based on such technology [6]. However, such a solution does not fit the HWW paradigm, since the computation needed to encrypt and decrypt messages using PKC is overwhelming with respect to the computation required by symmetric cryptography. This fact renders PKC infeasible for the HWW paradigm due to the poor processing power of the HWW device. Indeed, the amount of time required to encrypt/decrypt could be the bottleneck of the system. Moreover, the required computation contradicts the need to save battery power.

Thus, symmetric cryptography should be used in the HWW paradigm even with the drawback that symmetric cryptography implies, such as the key exchange and the key-refresh issues [3. 5].

Message Authentication Code (MAC). The idea underlying MAC is the sender obtains a digital fingerprinting f of a message m by applying a one-way hash function to m. If the fingerprint received with the message matches the one recalculated by the receiver, then the received message has not been modified during the transmission and is kept, otherwise the message is discarded.

As for digital fingerprint implementations, two standards—MD5 and SHA-1—are leading the pack. Note that custom solutions to digital fingerprinting, if not carefully devised, could result in a weak MAC, easy to forge, as the experiences in the wireless network field demonstrate [1].

Access control. We can identify two main subtasks related to such an issue: authentication among devices, and grant and revoke of privileges; how to assign permissions and how this set of permissions can evolve.

For the wired paradigm, these issues are covered in [6, 12]. Due to their hardware constraints, access con-

trol for the HWW environment is still an open issue. In particular, a single point of access control in the HWW paradigm cannot be identified due to the dynamic nature of the HWW architecture. In addition, the access control data structures cannot be stored on a single HWW device, unless for a very limited number of subjects. Moreover, once a certain HWW device has been scrutinized to be no more trusting, the revocation of grants must be addressed.

Therefore, the access control for the HWW network requires distributed solutions that increase the exposure to attacks. Perhaps, algorithms for sharing responsibilities, and based on cooperation [4] could help in addressing security in an HWW network.

System security. Each of the basic security requirements previously exposed focuses on a particular aspect of the security for HWW devices. Some further threats are related mainly to the system security and include routing, where communications among HWW devices not in direct communication range occur via multihop. Each of the participating elements can be a threat to communication security. Moreover, the length of the communication path increases the probability of an attack, such as the man-in-the-middle attack. Finally, consider application flaws, where programs running on an HWW device can be hacked as in the wired paradigm. Hacking can be performed exploiting a flaw in the design of the application or in the implementation. Since the applications for the HWW environment are designed with tight hardware constraints, these applications can be inherently weaker than those developed for the wired paradigm. For example, runtime bound checking may be eliminated to save computational power and memory space, thus exposing the applications to buffer overflow attacks.

It is worth noting that such a structural weakness cannot be easily overcome by resorting to additional tools. For instance, an intrusion detection system (IDS) could be employed to monitor the correct behavior of the applications. However, to deploy a IDS on an HWW device requires extra storage and extra computing power, which are the most constrained resources.

Privacy Issues

Privacy is often translated as confidentiality. Here, we stress privacy in its dictionary-based meaning: the freedom of not having someone or something to interfere in our life without our permission.

HWW devices are particularly useful if connected to other appliances [10]. In a probable future scenario, there could be a continuous exchange of information among the HWW devices around us. Such a continuous flow of information among devices takes place in a transparent way, and could constitute a serious breach in our privacy, at least concerning the possibility of being located. Here, we show how privacy is at risk in both the hierarchical and the flat Web presence models.

In the flat Web presence, we have global connectivity of HWW devices. The aim of this model is to make each object in the real world Web present. Flat Web presence could threaten privacy by automatically creating virtual paths between HWW devices logically unrelated. As an example, imagine the interaction between a user PDA and the embedded main control of a car—not the user's car. These HWW devices will exchange information, and the PDA could receive the license plate number of the car, thus resulting in a privacy violation at least as far as the location of the car is concerned. Moreover, collecting such information for a certain period of time on a specific car could allow the tracking of the user's driving path. Hence, the issue arises about the communication range of the HWW devices.

In the hierarchical Web presence, we have local connectivity of the devices. Each device creates a local vision of other devices it is in direct communication with. This local vision is communicated to other HWW devices to provide flexible and efficient support for mobility. Indeed, when a HWW enters a zone, it could have already loaded the information about the local vision for that zone. In this case, a threat to the privacy similar to the previous example can arise. However, with local connectivity, the extension to which privacy-sensitive information is exported may be limited.

Possible Solutions

Two possible scenarios can be identified to preserve the user's personal privacy in the HWW paradigm: the first is based on the logical borders mechanism; the second is based on anonymous user identity (UID) concept and may require the redesign of the current network infrastructure.

A logical border is intended to limit the propagation of a Web presence. In a simple implementation of the logical borders, Web-presence advertising should be allowed only up to the limit specified by the user, leaving the definition of the logical borders to the user. Placing such a burden on the user contrasts with basic requirements for the HWW devices—simple configuration and high usability.

A better implementation of the logical borders should support a user system profile. Such a profile

has embedded meaningful logical borders that can be refined by autonomous context-aware agents. This approach presents some open issues including the management of a mobile personal profile, and the security and the trustability of the autonomous agents. However, note that some threats to user privacy still persist, for instance, even turning off the HWW device could provide information useful to undermine the user privacy to some extent. Indeed, the most obvious piece of information is that the user probably does not want to be traced. With the logical border approach a major threat to privacy can therefore be identified in traffic analysis [7].

As for anonymous UIDs, they could be the default operating mode of any HWW devices, that is, anonymity should be a basic building block of the network infrastructure. In other words, the main functionalities of the HWW paradigm—service discovery, advertising, and providing—should be based on an anonymous UID not related to the real user. Note that the use of anonymous UIDs does not imply that users would never be identified, since for example, a user could always prove his/her own identity, at least at the application layer, if so desired. The implementation of anonymous IDs may require redesigning the algorithms and protocols of the current network infrastructure. Moreover, the redesign process should consider the trade-off between privacy and security in the network infrastructure. Indeed, anonymous IDs could expose any HWW device to anonymous attacks that could be very difficult to trace. On the other hand, a finer control over all the HWW communications could guarantee a higher level of security but might represent a threat to the user privacy.

Conclusion

This article discussed the emergence of networks of HWW devices, and the models that could enable their pervasive and integrated deployment. Furthermore, a few issues of the HWW environment related to the security of the system, and of the network infrastructure, as well as to the user personal privacy are addressed.

It appears security concerns can partially benefit from the model and solutions already deployed in the wired paradigm. In addition, the issues regarding user privacy are more complex and pervasive and require new solutions and further investigation. To our knowledge, research efforts in this direction are not even planned.

Finally, we emphasize the need for an easy to configure and manageable personal profile to control the interactions among the many HWW devices that could surround a user. The enforcement of such a profile could be a means to preserve the user's personal privacy.

An alternative solution to preserve privacy could base the main functionalities of the HWW paradigm on anonymous IDs. This solution may require redesigning a part of the current network infrastructure, and finding convenient trade-offs between privacy and security issues. C

References

1. Borisov, N. et al. Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of ACM/IEEE MOBICOM 2001*; 180–189.
2. Carman, D.W. et al. Constraints and approaches for distributed sensor network security. NAI Labs Technical Report. (Sept. 2000); www.nai.com/research/nailabs/cryptographic/a-communications-security.asp
3. Chan, H. et al. Random key predistribution schemes for sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy* (May 2003, Oakland, CA).
4. Coulouris, G. et al. *Distributed Systems: Concepts and Design.* Addison Wesley, Reading, PA., 2001.
5. Di Pietro, R. et al. Providing secrecy in key management protocols for large wireless sensor networks. *J. Adhoc Networks.* To appear.
6. Fox, A. and Gribble, S. Security on the move: Indirect authentication using Kerberos. In *Proceedings of ACM/IEEE MOBICOM 1996;* 155–164.
7. Guan, Y. et al. Preventing traffic analysis for real-time communication networks. In *Proceedings of IEEE Milcom* (Nov. 1999), 744–750.
8. Harter, A. et al. The anatomy of a context-aware application. In *Proceedings of ACM/IEEE MOBICOM 1999;* 59–68.
9. Hermann, R. et al. DEAPspace—Transient ad hoc networking of pervasive devices. *Computer Networks 35* (2001), 411–428.
10. Kindberg, T. et al. People, places, things: Web presence for the real world. *MONET 7,* 5 (Oct. 2002), Kluwer A.P., 365–376.
11. Myers, B.A. Using handhelds and PCs together. *Commun. ACM 44,* 11 (Nov. 2001), 34–41.
12. Sandhu, R. et al. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Trans. Info. and System Security 3*, 2 (May 2000) 85–106.

Roberto Di Pietro (dipietro@dsi.uniroma1.it) is a Ph.D. student in the Department of Computer Science at the University of Rome "La Sapienza," Italy.
Luigi V. Mancini (mancini@dsi.uniroma1.it) is a professor in the Department of Computer Science at the University of Rome "La Sapienza," Italy.

This work was partially funded by the WEB-MINDS project supported by the Italian MIUR under the FIRB program and by the EU IST-2001-34734 EYES project. This work was written during the authors' visit to George Mason University's Center for Secure Information Systems, Fairfax, VA.