Security and User Guidelines for the Design of the Future Networked Systems

Seppo Heikkinen, Sari Kinnari
Department of Communications Engineering
Tampere University of Technology
Tampere, Finland
firstname.lastname@tut.fi

Kari Heikkinen
Communications Software Laboratory
Lappeenranta University of Technology
Lappeenranta, Finland
firstname.lastname@lut.fi

Abstract—Emergence of new networking technologies and paradigms provides users multitude of ways to communicate with each others and exchange information irrespective of time and place. Diversity of the available environments, however, sets requirements for the design processes so that the new architectures can offer a concise and secure usage experience. This cannot be answered in an off-hand fashion or as an add-on feature, but security and usability need to be taken into account right from the start. Seamless design cooperation of both is vital in achieving secure user experience. In this paper we discuss how security and user design guidelines within the ubiquitous future environment can be used to enhance both the security and user experience of the communication services. The paper brings forth network, service and user level aspects that need to be kept in mind when considering the technology oriented design processes of such networks.

Keywords—Ambient Networks, design, security, user experience

I. INTRODUCTION

Future holds much promise for the ordinary user of the communication systems. Connectivity is available everywhere and the ambient intelligence around the user takes automatically care of the complexities of the technology and concentrates on bringing services to the user at the right moment and at the right place. Thus, the end user should not need to ask how, why, what, when, and where as we take a plunge towards ubiquitous media society.

While this vision certainly sounds attractive, the diversity of the environment sets challenging requirements for providing a concise user experience and enabling secure and flexible interworking between the available heterogeneous networks and composed services. Security is imperative to make the users trust and use the systems, but the design has to take into account the user experience factors as the complex configuration of security measures too often leads to a situation, where these measures are not used.

In this paper we discuss the ambient vision for the future networked systems and base many of the technical concepts on the findings of Ambient Networks (AN), a partly EU funded project [1]. The motivation is not to list all the possible results of the project, but to concentrate on the relevant security topics discussed within the project and show how they can be used to enhance the security of the ubiquitous environment [2]. As AN mostly concentrated on the network level, we also bring the user and usability factors into the picture in order to show that it can be challenging for the technical solutions to respond to the decisions made by the user. Thus, we are trying to determine, whether there is in this setting any common ground of mutual benefits between these different viewpoints, which often have contradictory goals.

The paper is organised as follows. In the next section we discuss the evolving ubiquitous environment. In the third section we present various technical guidelines and principles that the future network design should take into account in order to ensure the security of the systems. The fourth section discusses similar guidelines from the user perspective. The fifth section considers both security and usability factors and the benefits of their combination in the design process. The final section concludes the paper.

II. EVOLUTION TOWARD AMBIENT ENVIRONMENT

A. Network level aspects

Forward looking projects, such as Ambient Networks, envisage the drastic change in the future landscape of networking as the user is put in the focus [3]. The availability and internetworking of heterogeneous networks provides the possibility of getting seamless connectivity and services in a ubiquitous manner. This ubiquity sets requirements for the terminal devices in terms of adaptability and usability as people also have the possibility to use different devices within a session, i.e. the users are less device dependent. Also, one should not forget that in this kind of versatile environment the security will play even more important part as the mobile users no longer clearly separate the time they are on- or off-line and possibilities to interact with various previously unknown parties are vastly different.

The user context affects the available services as the surrounding networking environment adapts to the needs of the user, which could be related, for instance, to the offered prices and quality. Various pieces of information are made available to the networks in order to provide a concise user experience, thus leading to privacy issues. This also brings user and network levels closer to each other as service specific network overlays are introduced and cross layer principles are applied for enhanced performance.

In traditional use scenarios the users have placed their trust on the operators, either consciously or subconsciously. It has been rather clear that the big telecom operators provide the communication services and the people have static relationship with them, be it in the form of post or prepaid. In the future this will change as there will be more players.
entering the market. In essence everybody could be an operator providing access through their own networks as the technical development enables even a single node, i.e. a networked device, to provide access services in automated fashion. Even though some may have idealistic views about offering services to anybody for free, to most there still will be clear motivation to get compensation for the provision of their resources. This calls for solutions to ensure that the every party gets what they have agreed to. New business models and roles will emerge, and the value chains transform into more complex value nets. User identity will be a valuable commodity.

Single nodes will exhibit more intelligence and can provide access services to other, perhaps slightly more limited devices. Thus, everything will be considered to be a network. Hence, they interwork with other networks and compose into even bigger entities with common control plane, which hides the differences resulting from the specific technological domains and allows controlled sharing of resources [4].

B. User and service level

From the user perspective one of the major issues in the ambient environment is the user privacy. There will be plenty of information available about the user as information is mediated and recorded, and the lifespan of information availability is vastly different. Hence, it is easier to target attacks against a particular user. Information availability is already evident in the emergence of social networking and the way people freely give out information about themselves and the people they know, providing avenues for identity theft. Think, for example, the amount of information people publish about themselves in services such as Facebook with no real guarantee about the privacy of the data [5]. The emergence of virtual worlds and online games and their accompanying side economies provide yet additional ways of cheating the user [6].

In a sense these social networking sites provide an application framework, which forms a limited overlay network with its own semantic properties. While they currently work on application level, the work done on developing service specific overlays for network level will shorten the gap [7]. Thus, it becomes increasingly more important who is controlling the overlay and how the collected information is used. When the borders become blurred, it can be challenging for the user to know, which action has what sort of privacy sensitive consequences. Especially dangerous can be if the user is presented with opt-out policy as default action, i.e. in order to restrict the information disclosure the user has to actively know how to configure the system right from the start.

Information about the users can leak in various other ways, as well. Existence of caches and archival services ensure that the data is still available, even though the person may think that it has been removed [8]. Availability of context information, for networks and users, provide new interesting possibilities to spy on people and launch personalised attacks, e.g., in the form of phishing involving social engineering techniques. The availability of accurate personal information can also be used to falsely build a context of trust and then this trust can be abused. However, one should note, that the strictest privacy would mean zero personal information transfer; i.e. all personal data would lie in personal trusted device(s) (PTD), and no data would be collected, e.g. by the operator. Such devices naturally would make even more attractive targets of trickery.

Additional disclosure threat is that when people are no longer so location dependant in their service usage and use the services casually in public places, it provides more opportunities for simple shoulder surfing and eavesdropping.

Also, using multitude of social networking services means that the users are at the mercy of the security of these services. Lately there has been news about incidents, where the user database of the services has been acquired through vulnerabilities in their software. Thus, even though the users might have conducted proper password policies, their credentials can still leak. This is even more disastrous in cases, where people use the same password on multiple sites as often seems to be the case. In a way this is quite understandable, because the burden of remembering numerous passwords is getting higher as people use more and more of these services. In similar sense, the systems offering federated authentication and single sign-on have the risk of cascading. This sets more strict requirements for privilege granularity.

The possibility to use ubiquitous service environments may also mean that in the name of better usability, various places provide external display or input devices for mobile devices, which themselves are limited in this respect. This can pose a threat to the user, if it is not certain under which administration these external devices are. They can be compromised and steal sensitive user information or even execute unintended action on behalf of the user. For instance, there could be a scenario, where one inserts a smart card into a compromised public reader. While the user credentials may stay safe, the card can be made to create signatures on unintended data.

The future concepts also talk much about the flexibility and adaptability of the system. This can, for instance, happen through reconfigurable devices. That, however, can present additional threats to the user as already has been seen with programmable environments in mobile handsets. Even though it can be claimed that the security model of such environment controls tightly the privileges of each component, the user can still be tricked into giving additional rights by promising free SMSs, for instance [9]. Thus, it cannot be certain that the user is always capable of making the right decisions in terms of privilege granting. In fact, allowing the user to make any decisions in the system without knowledge of his mental models for security and privacy is a pitfall. Some vendors are already providing more controlled environments with requirements for vendor signed components, but they tend to result in public outcry for openness.
III. TECHNICAL PRINCIPLES AND MECHANISMS

A. Technical design guidelines

In building future secure networks, several general technical design guidelines need to be followed. The list is not focused on any given technology, but rather on the context(s) of the future ambient networks. The designers should keep in mind the classical general principles, as well [10]. The list includes:

- Security in design right from the start
- Ease of configuration
- Security by default
- Secure naming
- Privileges and delegation
- Decoupling authentication and authorisation
- Liability brokers

The first and foremost point to consider is the design process itself and how security is brought into it. Quite often security is added as an afterthought and this has a tendency to lead to patched approach, which will cause additional vulnerabilities and degrade usability [11]. Hence, the design process needs cooperation of all the parties right from the start (including both security and usability experts). It is also important that they understand each other, i.e. speak the same "language". Otherwise, the parts of the solution might not support each other and instead end up confusing the user even more.

All the more confusing to the user is the complex configuration of security measures [12]. The users have tendency to think in service centric terms, i.e. they are interested in the added value that the service will bring to them, and not in the details of configuration. For instance, a person might buy a WLAN access point, plug it in, notice it works, and then happily starts using it. However, the user easily forgets that there is no security configured as the user would have to get involved with the complexities of the configuration settings. Thus, there is need for making the configuration as easy as possible in terms the user understands, for instance, by using templates to abstract away the details and mechanisms to support autoconfiguration. Currently, dominant dynamic address configuration method, Dynamic Host Configuration Protocol (DHCP), is a good example of a mechanism that requires little user involvement. Additional specifications were needed to add security features, but due additional manual configuration requirements these features are hardly ever deployed.

While design effort should go for making the security configuration as easy as possible, it is even more important that there is always some security present. In other words, the design of future ambient networks should follow the security by default principle. It means that there always is some level of security available and it is not something you are able to turn off at the time of the deployment with an excuse of increasing performance or usability. While this approach does not protect against all the possible threats, it is better to have at least some security than nothing at all.

If you want to provide security between the different communicating parties, you also want to be able to name all these parties in a secure fashion. This way you can refer to these entities without having to worry about the possibility of spoofing. Currently, for example, in a typical cellular setting the user and the home network know each others, but the user has no real knowledge about the identity of the access network. Therefore, it should be required that the protocol design can explicitly identify every party involved in the transaction.

When you are able to name the parties, you can also assign privileges to them. One should not just adopt the approach, where you authenticate an entity and then give implicitly all the possible rights. Instead, one should honour the least privilege principle, which dictates that you only give the rights needed in the current context. This way you minimise the actions that might lead to exploits. In addition, one need to make sure that authentic data cannot be used in unauthorised context. Privileges also enable one to use delegation mechanisms to outsource the execution of specific tasks to others in order to gain performance benefits. One can, e.g., delegate certain signalling tasks to core network rather than expecting always the end device to do them.

When an entity has a privilege, it is authorised to execute a specific action. However, it is important to remember it should be possible to decouple authorisation from authentication. In other words, it is not always necessary to actually know who the entity using the service is, as long as it has legitimate authorisation for its actions. This helps to alleviate the privacy concerns and the service providers still can be sure that the users are legitimate ones and there is a party, which can be held liable for the actions.

Such liability needs to be established with the help of trusted third parties (TTP). They are needed to broker between the previously unknown parties, because the transactions having real world effects, such as those related to money, need the level of assurance and scalability, which can only be offered by well established institutions that provide financial liability to the interaction. While the old incumbent operators could assume this role, it is also a new business opportunity for the potential new identity providers.

B. Security design building blocks

In building future secure networks, several building blocks need to be implemented to adhere to the above mentioned principles. The list is by no means exhaustive, but rather provides examples of the essentials needed to realise the ambient visions. The list includes:

- Cryptographic identifiers
- Opportunistic trust
- Secure network attachment
- Authorisation tokens
- Non-repudiative service usage

For implementing secure naming one can use cryptographic identifiers. In other words, every entity is assigned an identifier, for which it can provide proof of ownership. That is, it is not probable (in mathematical terms) that anybody else could use the same identifier. Basically,
this is a representation of a public key pair. Authentication of the identifiers does not necessarily require existence of any global infrastructure, such as Public Key Infrastructure (PKI), but can take the benefit of local decisions. Thus, there is no need for the user to worry about the complexities involved with PKI [13]. Also, the identifiers can be either short or long lived. When the identifier is only used for a short period of time or it is discarded after use, the privacy of the user can be better preserved. Note that the employment of identifiers on several different levels also demands user centric identity management solutions.

By relying on the "self-certifying" nature of these identifiers, it is possible to provide a default level of security. This relies on the concept of opportunistic trust, which is based on the sameness property of the identifiers. In other words, there might not be assurance about the real identity, but the invariability of the identity can be guaranteed. Usually this approach works in environments, where the attacks are more likely to be passive in nature, such as snooping of information. Thus, attacks like man in the middle can still be a concern.

As the ambient vision states that there will be a multitude of different kind of access networks, there will also be a need for secure way of attaching to them. This can lead to configuration nightmare. Instead of having many different mechanisms, one should consider providing a common approach, which can be adapted to various interworking layers. This is done with the help of network attachment protocol [14], which in its origin resembles Host Identity Protocol (HIP) [15]. This procedure provides the means for the parties to exchange their identity information and establish keying material, which can be used to secure any subsequent communication. Additionally, a conceptual identity layer is created, which can be used for directing traffic between the entities, thus allowing decoupling the locator and identity information for the benefit of better and secure mobility. An important point is also the consideration for Denial of Service (DoS) mitigation through the use of adaptive puzzle scheme as DoS is currently one of the major threats to the modern data networks. The protocol is run with the help of a four way handshake and it is possible to include additional information into the signalling messages. This could be, for instance, dynamic configuration information to replace DHCP [16]. Subsequently, additional information elements can be exchanged in a secure fashion. Thus, just using basic opportunistic mode the procedure can provide zero-configuration capability.

While the above mentioned procedure can provide the identifiers of the involved parties, it should be further enhanced with the possibility of including authorisation statements, which dictate the rights of the entities and are securely bound to their identifiers. Such statements could be made with the help of X.509 certificates or Security Assertion Markup Language (SAML), but a more flexible (and concise) approach for this environment can be achieved through Simple Public Key Infrastructure (SPKI) certificates [17]. The use of such assertions naturally requires that the parties have a common understanding about the trust levels associated with the entities, who have issued the statements. They could be individual delegations or statements issued by the liability brokers. Thus, TTP can, e.g., assign an authorisation to an ephemeral identifier of the user, underlining the fact that the authenticity of the user is not as important as the accompanying token, which ensures the right to perform the action.

While the involved parties, such as operators, can establish agreements concerning their interaction and the actions of their roaming users, there is still need to make sure that the agreements are honoured. Nowadays, in a typical setting the accounting of a visited network is based on the declaration of the visited party. While overly large figures can be spotted, the dynamic environment requires more stringent measures to ensure that the agreed services are received at the agreed terms. Thus, there is need for protocols that ensure non-repudiation, so that the user can be sure that he gets the service he is paying for and the service provider can be sure that it can get the compensation for the provided resources. This can be realised with the help of signed hash chains, which can be used as micropayments, i.e. they present piecemeal commitment to the service usage [18]. I.e., if no service is received, no new hash chain values are provided. Similarly, if no hash chain values are received, no service is given. At later stage the user cannot repudiate the use of the chain values, because they are signed with his identity or that of his operator.

In the Table 1 we have listed some of the presented guidelines and the suggested mechanisms for implementing them. As can be seen the cryptographic identities play an important part in many of them and should be considered to be one of the key building blocks for ensuring the security of the future networks. Naturally, important principles such as security in design right from the start need to be considered more broadly than just in terms of certain mechanisms.

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security by default</td>
<td>Opportunistic trust, secure network attachment</td>
</tr>
<tr>
<td>Ease of configuration</td>
<td>Secure network attachment</td>
</tr>
<tr>
<td>Secure naming</td>
<td>Crypto ids</td>
</tr>
<tr>
<td>Privileges and delegation</td>
<td>Crypto ids, authorisation tokens (e.g. SPKI)</td>
</tr>
<tr>
<td>Decoupling authentication and authorisation</td>
<td></td>
</tr>
<tr>
<td>Liability brokers (TTP)</td>
<td>Authorisation tokens, non-repudiative service usage</td>
</tr>
</tbody>
</table>

IV. USER DESIGN GUIDELINES

The future networked landscape will have several emerging trends that will especially affect on how users will interact with the ambient networks. Let us consider the fact the fundamentals of an ambient network are built on the promises of i) intelligence (algorithms, learning capability), ii) natural interaction (e.g. multi-modal interfaces) and iii) ubiquity (provided by the communication technology). This part focuses on the intelligence and natural interaction, which affect the level of obtrusiveness the user can experience.
Riva has introduced several psychological principles for designing ambient spaces [18]. These principles can be applied to any ambient “front-end”, i.e. the environment in which the user interacts.

- The environment has to identify what the user is aiming to do. Literally this means that a lot of data has to be collected in order to identify the user objective. If a situated and context-aware profile were available, the environment could respond either proactively or be triggered based on some not (necessarily) known event.
- The environment has to be able to identify the equipments (e.g. mobile phone) the user needs to carry out the objectives. These equipments include both physical and social tools.
- The environment has to be able to understand the current path of user thinking (and future behavioural patterns). This piece of information helps to make decisions, e.g., when a particular task will end. Different sensors will become valuable information collectors.
- The environment should interrupt the user as little as possible. Most of the actions should be carried out automatically. The intervention should occur only as last resort (i.e. the user has to be helped out). However, the environment should also be transparent to the user. That means that the user is aware of its actions and does not need to “worry” whether things have been appropriately done.
- The environment should be able to utilise situated contextual benefits and restrictions of it in a transparent manner.
- The environment should also support social behaviour of the user; identifying the roles and social networks in a manner supporting normal activity of a given user.

As the principle list above indicates, it is important to understand the behaviour of a human being and the reasons behind that. Thus, in order to achieve the principles mentioned above we should look deeper into human cognitive activity and social psychology. However, within the confines of this paper, more detailed discussion is out of scope. Even though the environment mostly carries out the tasks based on profiles of the user without explicit orders from the user, the user sometimes has to interact with the environment explicitly. The key elements here are natural interaction and multimodality. These multimodal interaction models include things like speech recognition and spoken interaction, physical interaction, adaptive graphical interfaces, gesture and gaze interaction, haptic interaction, and space and virtual reality-oriented interaction. Jameson has emphasized the following goals for enabling enhanced user experience [20]. As such they act as guidelines and design restrictions. These elements include

- Predictability
- Visibility
- Manageability,
- Non-disturbance
- Privacy and feeling of being secure
- Depth and severity of the experience

User design and the success of any given design need to be validated by criteria developed for ambient environments. These criteria include heuristics that are relevant for natural and seamless interaction while utilising positive user experience. This heuristic list would consist of tens of rules of thumb.

A. User experience in security

As the discussion above has indicated, the security should be built-in, not an add-on feature. Security as a theme focuses on the risks and uncertainty. These are extremely difficult concepts for the people to evaluate, argues West in [21]. Furthermore, he argues that it is more important to understand the basic principles of human behaviour (as also the previous section indicates). He also lists a comprehensive list (see Table 2) of predictable and exploitable characteristics of our decision-making.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Comment and effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users do not think that they are at risk</td>
<td>The users most often think that they are better than others, and thus either do not use security features or proceed with more risky behaviour.</td>
</tr>
<tr>
<td>Users aren’t stupid, they are unmotivated</td>
<td>Human beings (as a species) tend to favour quick decisions based on learned rules and heuristics. Security can be seen as overly exhaustive action.</td>
</tr>
<tr>
<td>Safety is an abstract concept</td>
<td>The less concrete the threat is, the less willingness there is to carry out security instructions.</td>
</tr>
<tr>
<td>Feedback and learning from security-related decisions</td>
<td>Behaviour is shaped by positive or negative reinforcements. In security domain, most often the reinforcements are negative.</td>
</tr>
<tr>
<td>Evaluating the security vs. cost trade-off</td>
<td>Gains are often abstract and the negative consequences stochastic, the cost is real and immediate.</td>
</tr>
<tr>
<td>Making trade-offs between risk, losses, and gains</td>
<td>If security gains are intangible, with well-known costs, and while negative consequences involve probabilities, it is possible to try to make security more “profitable” for the user.</td>
</tr>
<tr>
<td>Users are more likely to gamble for a loss than accept a guaranteed loss</td>
<td>People react differently on whether they think they are gaining or losing something (in concrete value).</td>
</tr>
<tr>
<td>Security is a secondary task</td>
<td>People tend to focus on the immediate task. As such, security decisions need to be carried out most often in the middle of some other (more relevant) task.</td>
</tr>
<tr>
<td>Losses perceived disproportionately to gains</td>
<td>People do not perceive gains and losses equally. So the user has to perceive gain visibly better than a loss.</td>
</tr>
</tbody>
</table>

West also lists several approaches that could help the security designer to improve human compliance (to security) and decision making. These approaches include i) rewarding pro-security behaviour (feedback), b) improving the user awareness of risk, c) catching security policy violators (non-repudiation/deterrence), and d) reducing the cost (for the user) of implementing the security.
With respect to the interaction with the user, it is important to also consider the amount of information provided to the user, i.e. how obtrusive the systems can be. If the user is overloaded with information it might lead to cases (e.g. SSL warning messages), where the user no longer evaluates the information but just concentrates on absorbing or merely ignoring. Similar things can be faced if poorly functioning heuristic systems are used to evaluate potential threats to the user and too many false positives "condition" the user to ignore the warning messages, just like crying "wolf" too many times [22].

V. DISCUSSION

As we have shown, the users are facing risks and uncertainties in the evolved networked service landscape due the user mindset, information leakage, and shortcomings of the platforms. The users are not generally interested about security and even less about configuring security; they only want to get their own tasks done. This can become evident in a case, where the user has the option of choosing either secure or insecure service and for some reason the secure version does not work. Thus, if, e.g., DoS is launched against the secured service, the user is tempted to use the available insecure version instead [23]. Nevertheless, the end users are increasingly facing the fact that they are expected to become their own systems administrators, at least within their home networks.

Thus, we underline the importance of keeping the security in the design process right from the start, i.e. user should enjoy default security with zero configurability and mental/cognitive etc. concerns. Additionally, secure identification along with proper privileges need to be applied to control the information disclosure. As we have shown, many other mechanisms can be based on the existence of secure naming as a building block and proper identity management can also be used to alleviate the previously mentioned shortcomings of purely password based systems.

It should be noted, however, that the user mindset (security vs. usability) is a challenging topic for solely technically oriented design, thus, the lessons learnt from the user experience design can pave the way for a more holistic approach. Many security techniques originate from military world where those who need to use a system, are educated to use it and the rest are kept in dark. In the modern world we need to recognise both the heterogeneity of networks and the heterogeneity of users. Trying to add usability on top of an already designed and implemented service or a product can lead to serious problems. Another fact is that security mechanisms are designed, implemented, applied, and breached by people. Thus, the user-centered design is essential for all security related systems. Interestingly, hackers seem to pay more attention to the human link in the security chain than security designers do [24].

Designing secure architectures that should both be visible to users and hide security implementation, e.g. protocols used, is challenging. Reducing the user’s burden of complex configurations is possible, but it requires rethinking of design methods and phases. Usability studies reveal critical errors and give feedback for iteration. This can be simple as writing lists of “anti-requirements” (things that design should not allow user to do) and doing "default-action“ tests as in [22] to reveal the security level of the system. Although the product development of networking devices has strived for both satisfying user experience and security, as in [25], generally the architecture design takes purely a technical approach and lacks the support for usability aspects. There have, however, been success stories of designing usable security; in [26] WLAN user has to go through only 4 steps instead of 38. Thus, innovative design and disruptive thinking is required for building a holistic approach. Changes might still be needed within usability testing itself, too [27].

It is unavoidable to consider the tradeoffs between invisible and transparent security when designing secure systems, but letting the user decide about the critical security features is simply bad design. There are numerous examples of situations where the problems of complex networking security have been shifted to user interface level. Many applications even offer users possibilities to bypass security elements. Relying solely on user’s skills to make decisions or education as a solution to security problems is doomed to fail. Gutmann [22] has pointed out the need of considering theoretical vs. effective security: if security measures are misused, turned off, or bypassed, the system offers very little effective security. Thus, models with "always on" security should be applied, e.g. with technologies presented earlier. Also, as mentioned previously, predictability is an important property in user experience, therefore consistent solutions are needed, such as those providing secure attachment procedures across different networks.

In Table 3 we have summarised the relations between the presented security and user guidelines in order to show that even though the concepts can be claimed to be residing on different levels, correct security design decisions taken already at lower levels can benefit the user experience and increase the overall effective security. It should be noted, though, that most of the security guidelines base on the existence of secure naming, thus underlining its importance.

VI. CONCLUSION

In this paper we have elaborated some of the results found within the Ambient Networks project and related work. While they cannot be said to be conclusive, they still provide guidelines and solution concepts, such as secure naming, which can be used to ensure the security of the future ubiquitous systems.

Although networks can be seen as technical concepts, the holistic design processes have to also remember the existence of the user. The user experience factors can dictate whether the system will ever be deployed or used. Security and user experience design have to go hand in hand and be in the design process right from the start.

Thus, we need to learn more about the users and how they process security related issues. The guidelines presented in this paper provide a feasible plan going forward but the real measure can only be taken when we can proudly say that we are able to provide secure user experience in the same contextual cue.
<table>
<thead>
<tr>
<th>Security guideline</th>
<th>User guideline</th>
<th>Usability goal</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security by default</td>
<td>Reduce cost of implementing security</td>
<td>Unobtrusiveness</td>
<td>No extra mental burden is put to the user as an expected level of security is always present.</td>
</tr>
<tr>
<td>Ease of configuration</td>
<td>Reduce cost of implementing security</td>
<td>Unobtrusiveness</td>
<td>User is not needlessly interrupted with secondary tasks, but still has a sense of being in control for additional security.</td>
</tr>
<tr>
<td></td>
<td>Improving user awareness</td>
<td>Visibility</td>
<td></td>
</tr>
<tr>
<td>Secure naming</td>
<td>Improving user awareness</td>
<td>Privacy</td>
<td>Assurance about the communicating parties and invariability of them either with short or long term identities.</td>
</tr>
<tr>
<td>Decoupling authentication and authorisation</td>
<td>Improving user awareness</td>
<td>Controllability</td>
<td>Only authorisation is explicitly linked to the execution of certain actions.</td>
</tr>
<tr>
<td>Privileges &amp; delegation</td>
<td>Reward pro-security behaviour</td>
<td>Controllability</td>
<td>Efficient execution of tasks and assigning privileges as needed for controlling the disclosure of information with timely feedback.</td>
</tr>
<tr>
<td>Liability brokers</td>
<td>Catch policy violators</td>
<td>Unobtrusiveness</td>
<td>Outsourcing the trust evaluation and reliance on external mechanisms (such as litigation)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy</td>
<td></td>
</tr>
</tbody>
</table>

**REFERENCES**