Security and User Aspects in the Design of the Future Trusted Ambient Networked Systems

Seppo Heikkinen[1], Kari Heikkinen[2], Sari Kinnari[1]

[1]Department of Communications Engineering
Tampere University of Technology
Tampere, Finland
firstname.lastname@tut.fi

[2]Communications Software Laboratory
Lappeenranta University of Technology
Lappeenranta, Finland
firstname.lastname@lut.fi

***Abstract*—Research visions of ambient computing promise seamless co-existence of technology and user in such a way that the environment adapts to user context. This adaptivity also means more extensive information disclosure, hence the security concerns become paramount. While new architectures should be able to provide security as a basic feature, they also need to take into account the way users behave and experience the system, as users are not likely to be interested in technical details and configurations, but instead in the added value they can get. Thus, if the users find the system too complex to use, they might find it hard to trust and not adopt it. Therefore, usability and user experience issues have to be considered tightly along with security and they need to be in the design process right from the start. In this article we discuss how security and user design aspects within the ubiquitous future environment can be used to enhance both the security and user experience in the creation of the trusted communication services.**

Keywords-Ambient Networks, design, security, trust, user experience

I. INTRODUCTION

The 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 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 article we extend the work presented in [1] by further elaborating the user perception of security and user experience for the successful design of future networked systems. We discuss the presented ambient visions and base many of the technical concepts on the findings of Ambient Networks (AN), a partly EU funded project [2], in which one of the authors participated. 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 [3]. As AN mostly concentrated on the network level with an objective of creating a scalable and affordable mobile communication system for heterogeneous environments, we also bring the user and user experience 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 article is organised as follows. In the next section we discuss the evolving ubiquitous environment. In the third section we provide a short introduction to user-centric design methodology. The fourth section presents different aspects of trust within the context of our work. The fifth section considers various technical guidelines and principles that the future network design should take into account in order to ensure the security of the systems. The sixth section considers both security and usability factors and the benefits of their combination from the user experience point of view. Additional discussion is provided in section seven. The final section concludes the paper.

II. EVOLUTION TOWARD AMBIENT ENVIRONMENT

Different kinds of terms, such as ambient intelligence, ambient networking and ubiquitous computing, have been introduced to portray the visions of enhanced interaction between the users and the surrounding technology. One vision lists the following as key requirements [4]:

- Unobtrusive hardware
- Seamless communication
- Dynamic and distributed device networks
- Natural feeling human interfaces
- Dependability and security

We do not claim this to be a conclusive list nor does the transition to this kind of system take place overnight. We would like to, however, emphasise the dynamic interaction aspects (both with technology and other users) and

concentrate on networking and users with security viewpoint. It could be further noted that it can be claimed that ubiquitous computing already is here, even though not in a very seamless nor unobtrusive fashion, whereas the "clean" ambient vision is something that is always "just around the corner" [5]. This can be actually seen in the various Future Internet research activities, which basically try to address similar issues. However, on less physical scale, this mixing of technology and social world is, in fact, already quite prominent in the proliferation of social online communities, where, e.g., certain user threats have already become an issue.

A. *Network level aspects*

Forward looking projects, such as Ambient Networks, envisage a drastic change in the future landscape of networking as the user is put in the focus [6]. The availability and internetworking of heterogeneous networks provide 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 dependant. 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 relationships with them, be it in the form of post- or pre-payment. 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 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 can be considered to be a network. Hence, they interwork with other networks and compose into even larger entities with common control plane, which hides the differences resulting from the specific technological domains and allows the controlled sharing of resources [7].

B. *User and service level threats*

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 [8]. The emergence of virtual worlds and online games and their accompanying side economies provide yet additional ways of cheating the user [9]. One can argue, though, 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 attractive targets of trickery, thus they require strong security solutions.

In a sense these social networking sites provide an application framework, which form a limited overlay network with their own semantic properties. While they currently work on application level, the work done on developing service specific overlays for network level will reduce the gap [10]. 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 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.

The information about the users can leak in various other ways, as well. The existence of caches and archival services ensure that the data is still available, even though the person may think that it has been removed [11]. The 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 or various other kinds of identity thefts can be done.

An 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 a 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 out. 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 [12]. Thus, one 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. DESIGN PROCESS AND METHODOLOGY

So, how does one approach the problem of designing a system that should take into account the user aspects and the aforementioned threats that emerge in the introduction of completely new way of service interaction? ISO 13407 [13](*Human-centered design processes for interactive systems)*, is a widely acknowledged international standard, established in 1999, that provides general guidance for user-centered design (UCD). ISO 13407 focuses on the descriptions of principles and activities to be used in a user-centric design. In the standard there are four particular characteristics that have to be fulfilled in the design activities in order to claim them user-centric. These four characteristics are a) *user involvement*, b) *function*, e.g., carrying out some security related task, c) *iterative manner of design* and d) *multidisciplinarity*. The standard emphasises the role of planning, and one should spend adequate amount of time in planning the study; i.e., identification of users, user demand (for particular task) and task or/and goal setting.

In the first phase context of use has to be found based on collected user, task and environment details, i.e., try to learn to understand the users. Most often in technical oriented studies these are written in a form of narrative scenarios. Naturally, the textual description utilises figures, story-like narration, sketches etc. to support the flow of scenario. The scenario is described from the user point of view and may include different varying constraints and relevant background information. By using such a description it is possible to capture more information about the user's goals and the context the user is operating in. One has to understand that different stakeholders handle the scenarios differently. As an example, an interaction designer looks different aspects while reading the scenario, as he/she looks all the transactions that take place between the human and the computer/device/UI. At the same time he/she follows the description of flow of the activity the user is supposed to be doing. In the second phase all possible requirements are collected, i.e., user, system, organisational, software requirements etc. In the third phase one has to produce appropriate concepts. In the fourth phase the evaluation is carried out to find out if the requirements are met.

Scenario analysis is also a common technique for finding and analysing the security requirements of the system to be designed. Common Criteria (CC) is another alternative for security requirement evaluation, but is has a steeper learning curve [14]. Thus, in a research project the scenario approach is often favoured as it is easier to get involvement from a larger party, even though it is not so readily quantitative. This was also the approached adopted in AN project [15]. Naturally, one also has to have an understanding of the threat model in the envisaged environment. This can further lead to risk management decisions, e.g., a certain risk is deemed so improbable that the mitigation effort to be invested is not seen feasible.

Figure 1 illustrates how security and user aspects can be processed in an iterative manner. The figure is a modified view of the UCD design process. The starting point of the spiral is in the center and curves firstly towards understanding the users. In the first iteration the current knowledge and state-of-the-art understanding are collected so that the awareness of user behaviour, user perception, user motivation, and user attitudes can be obtained. After obtaining that information the conceptualization begins, in which user requirements, software requirements (front-end for the user and back-end for the system) and security requirements are taken into account. In first iteration, low level fidelities of created concepts are available in user studies, which could involve, e.g., simple paper prototypes. These user studies also are used for evaluating whether requirements are met. These first user studies would be followed with some constructive research, e.g., creation of algorithm or mechanism so that a concept can be further prototyped in the second iteration.

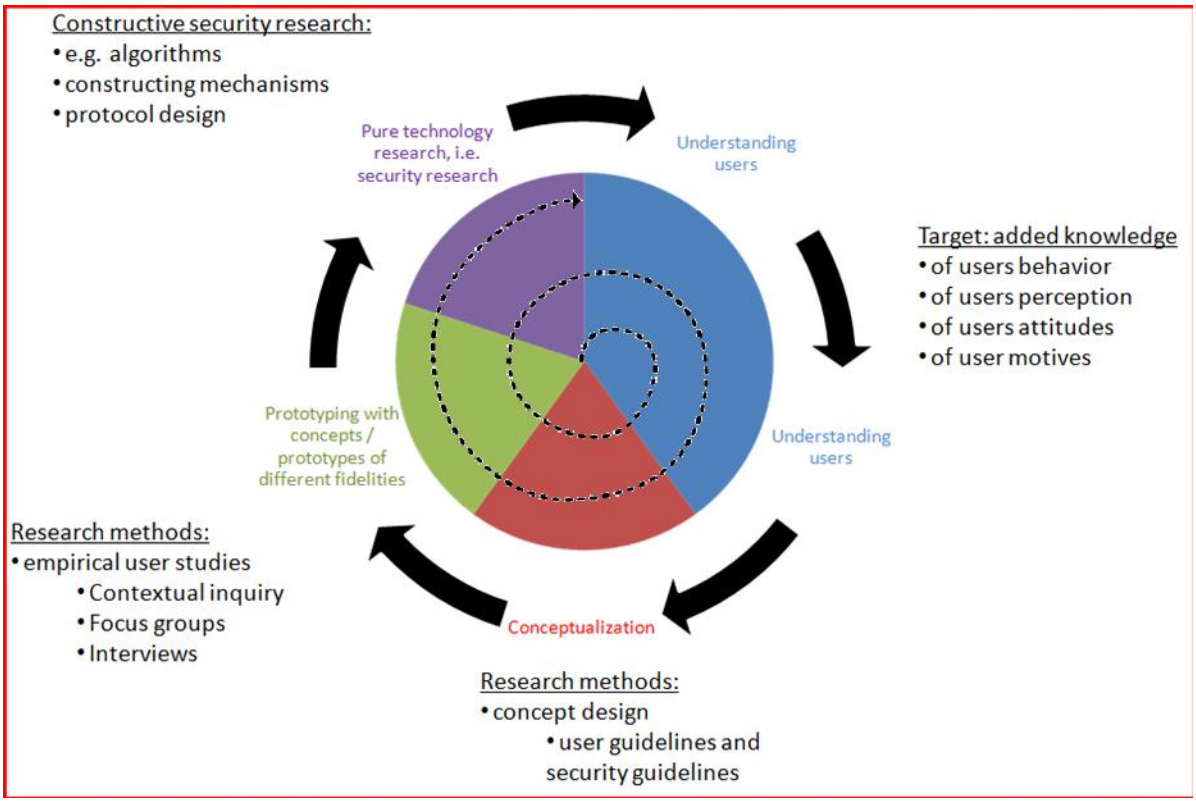

Figure 1. Process for guideline integration

In the second iteration we have a concept design of one or several context(s) of use. We are able to collect user experience within selected contexts by, e.g., observing users. User studies carried out in the first iteration provide us better understanding of user behaviour, user perception, user motivation and user attitudes towards security. In the second round, user studies would have prototypes of higher fidelity in use. Again in constructive security research, a more complex and detailed security-related research is carried out. In theory, the spiral is never-ending, and all the time the accuracy of understanding of users will increase.

The following sections V and VI are linked to the Figure 1. Section V along with sections I and II provide the basis for conceptualization with respect to the security guidelines and security mechanisms. Section VI is focused on user guidelines that are present in conceptualization, user studies and in understanding users.

IV. ASPECTS OF TRUST

As ambient computing is about interaction, there generally has to be some sort of trust relationship between the communicating parties. Thus, when doing the initial environment analysis, one needs to understand in what ways trust enters the picture. In technical sense, one can say that trust relationship entails establishing the identity and certain characteristics (such as expected behaviour) of an entity. Here we briefly list different categories of security relations from technical viewpoint. However, one should also note that the trust can be very subjective matter from a user point of view. Therefore, one also needs to analyse the user perception of trust within the evolved landscape.

A. *Technical trust*

There are several ways of establishing trust relationships, depending on the use scenario and the requirements set by the policies. The simplest case, of course, is to have no protection at all and just blindly trust that nothing goes wrong, i.e., relying on that fame and other external factors, like fear of legal actions, will provide enough protection against misuse. While this is quite common approach nowadays in Internet, this clearly is not recommended in the future setting of potentially unknown operators.

Direct trust on the other hand is based on some common knowledge that has been agreed beforehand. It can be, for instance, a shared secret as is done in the current Subscriber Identity Module (SIM) based solutions. While this can be used to secure mutual connections, it requires some form of pre-configuration. Thus, it is not suitable for most dynamic environments. However, direct trust can be delegated leading to a brokered trust setting, where the trustworthiness of an entity is vouched by an entity one is willing to trust. Through this kind of transitivity the trust relationships can be extended more easily, although in this kind of setting one should talk about liability instead of trust, which often has rather unambiguous meaning. Especially in cases involving compensation and monetary exchange, there is incentive to accept a potential risk only to a certain amount. For instance,

a visited operator provides service under the assumption that the home operator accepts liability for the roaming user, hence ensuring the compensation for the visited operator even though the real identity of the roaming user may remain unknown.

The last trust category is based on the opportunistic approach. While it is close to the blind trust case as it takes a leap of faith in the beginning of the communication, it provides an assurance that the party of the initial communication does not change. In other words, you may not know who the communication partner is, but you know that it has remained the same all through the session or that it is the same one with whom you conversed previously. While not suited to every case, it can be a flexible and simple way of providing security in the absence of security infrastructures.

One can also approach trust from the reputation perspective. In other words, the historical behaviour of the entity affects how it is viewed. This can be evaluated with various kinds of mathematical trust metrics. Naturally, it is easy to argue that the past behaviour is not a guarantee of expected behaviour (much like the commonly used phrase in the stock market) and having multiple faked identities allows you increasing your reputation in a certain community (i.e., Sybil kind of attack). Basically, however, the trust based on reputation reduces to the categories discussed above.

B. User perception of trust

The previous technical discussion about trust is somewhat straightforward with quantitative properties suitable for engineers and the like. However, when one talks about trust between persons, there is always a certain amount of uncertainty and it is very subjective experience dependant on the context. Thus, it can be said to be an attitude, based on beliefs and feelings, and implying expectations and dispositions [16]. One can also see it as a process that takes time to develop and shapes the interactions people have [17]. With new things, the reputation and recommendations can form the basis of the initial attitude, but it also depends on the risk-taking attitude of the individual, given the potential benefits. Thus, in the advent of ambient computing environment, user has to trust the system in order to agree to disclose information about themselves, i.e., adjust their privacy settings accordingly. However, the trust evaluation made by a person can be affected and it is not always a rational thing. For instance, the mere look and feel of the system can heavily impact how trustworthy the user sees it [18]. While challenging topic, the design process should also take into account the user perception of trust. Additionally, it is worthwhile to remember that the user can be actively influenced and the user trust abused, e.g., by social engineering means [19].

V. TECHNICAL PRINCIPLES AND MECHANISMS

When one starts conceptualizing the initial scenario ideas, one also needs to start considering the security guidelines you wish to follow within the design. This should then lead to some ideas of the actual building blocks used to ensure that the guidelines are followed. Naturally, this entails the actual research to come up with the suitable solutions.

Thus, next we discuss some of the technical aspects of the ambient design in order to ensure that trust relationships can be created. Examples of mechanisms are given, but it is more important to pay attention to the design principles, which should guide the design decisions made early on.

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. Many of them (naming, default security, authorisation) already appear in the AN security architecture principles [3]. The designers should keep in mind the classical general principles, as well [20]. For instance, one should honour the defence in depth thinking and not rely solely on one defence mechanism. 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 [21]. Hence, the design process needs cooperation of all the parties right from the start (including both security and usability people). 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 [22]. The users have a 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 start 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 a 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 auto-configuration. 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 into 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 that can be turned off at the time of 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. In other words, one should consider opportunistic approach to trust, as discussed earlier.

If security provision is desired between the different communicating parties, naming these parties in a secure fashion would also be desired. This way it is possible to refer to these entities without having to worry about the possibility of spoofing, which can become evident, for instance, in the case of three party protocols. Currently, for example, in a typical cellular setting the user and the home network know each other, 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 needs 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 or proxy elements 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 for 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 building blocks suggested for implementing the AN security architecture [3]. They were chosen here for the sake of their fundamental nature as essentials for realising the ambient visions. The list includes:

- Cryptographic identifiers
- Secure network attachment
- Authorisation tokens
- Dynamic roaming agreements
- 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, e.g., key continuity. Thus, there is no need for the user to worry about the complexities involved with PKI [23]. Also, the identifiers can be either short or long lived. When the identifier is only used for a short period of time and 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 aforementioned 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. However, this allows adhering to the “better than nothing” security principle and one notable example of this is the success of Secure Shell (SSH). Introduction of TTP can be used to further enhance the level of security (see below), if the use case has more stringent requirements.

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 a 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 [24], which in its origin resembles Host Identity Protocol (HIP) [25]. This procedure takes advantage of the well studied security properties of HIP and provides the means for the parties to exchange their identity information and establish keying material, which can be used to secure any subsequent communication as is done, e.g., in the typical use case of HIP (see [26]). 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 an 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 [27]. Subsequently, additional information elements can be exchanged in secure fashion. Thus, by using just 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 [28]. After all, on network level one also needs to consider packet fragmentation issues. 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. In other words, there is decoupling between the authorisation and the authentication of the real identity.

It was already mentioned that the operator landscape can change. Hence, it no longer can be expected that the static roaming agreements can cover all the internetworking between the future operator entities as the relationships are more dynamic in nature and perhaps only contain one transaction. This requires measures for establishing dynamic roaming agreements, which also subsequently affect the trust evaluations of the individual subscribers. The operator entities engage in a similar association creation procedure as is done in the network attachment phase. However, this also includes offer and counter-offer steps, which could additionally include an external entity for brokering the agreement or it could be handled by a federation of brokers. The framework for dynamic roaming agreements is depicted in Fig. 2 [29] . In a sense, such setting is currently employed between current incumbent operators, which exchange traffic through closed networks, such as GPRS Roaming Exchange (GRX) networks, although in this setting no direct authorisations for actions are provided by the GRX operators, but instead carrier services with certain security and quality parameters are offered.

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 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 service. This can be realised with the help of signed hash chains, which can be used as micropayments to represent a piecemeal commitment to the service usage [30]. In other words, 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 a later stage the user cannot repudiate the use of the chain values, because they are signed with his identity or that of his operator during the initial service negotiation phase. In practise this requires involvement of TTP, which will ensure the liability of the user, i.e., the service provider knows the brokering party. Thus, the service does not need to learn the “real” identity of the user as long as the presented identity (possibly very short lived one) is asserted by TTP.

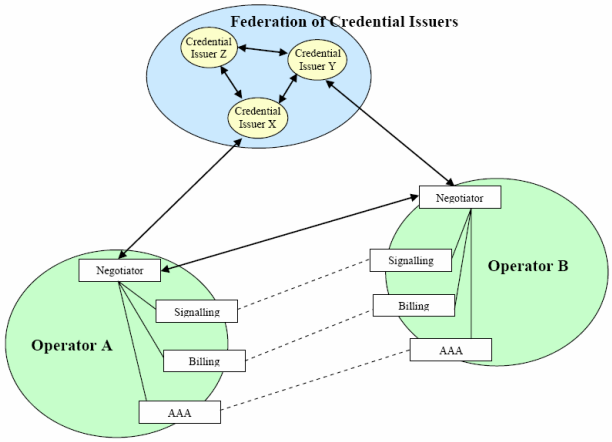

Figure 2. Framework for dynamic roaming agreement [29]

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 1. CORRESPONDENCE OF GUIDELINES AND MECHANISMS

Guideline	Mechanism
Security by default	Secure network attachment
Ease of configuration	
Secure naming	Crypto ids
Privileges and delegation	Crypto ids, authorisation tokens (e.g. SPKI)
Decoupling of authentication and authorisation	
Liability brokers (TTP)	Authorisation tokens, dynamic roaming agreements, non-repudiative service usage

VI. USER EXPERIENCE FOR AMBIENT SYSTEMS

As indicated above, the design is not just about solving technical obstacles. The future networked landscape will have several emerging trends that will affect how users will interact with the ambient networks. Let us consider the fact that 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 section focuses on intelligence and natural interaction, which affect the level of obtrusiveness the user can experience.

Riva has introduced several psychological principles for designing ambient spaces [31]. 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 assistants as 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.

Even though the environment mostly carries out the tasks based on, e.g., situated and context-aware profile 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 (or sounds/voices in general)
- Physical interaction (e.g., touch-based)
- Adaptive graphical interfaces (e.g., appropriate for public spaces)
- Gesture and gaze interaction
- Haptical interaction
- Space and virtual reality -oriented interaction.

In a sense ambient systems are challenging for user-centric design as you cannot summon experiences from other researchers. Thus, for pioneers it might be partially guesswork. If the technology goes into background and you have to rely its black-box way of operation in which you have to start trusting to the system so that it operates as it was designed and as you were told. Thus, the environmental characteristics in the context of use for understanding the users are different.

A. Introducing user experience

According to [32], experience can be put into four realms based on the level of participation of a user and his/her connection to experience itself. The first realm is pure entertainment, in which users are passive viewers (e.g., opera). In the second realm, the user is actively absorbing information from the environment (e.g., classroom with active learning settings). In the third realm, experience is summoned in immersed manner (e.g., flight simulator). In the fourth realm, the immersion is obtained in a passive environment (e.g., going to a medieval castle). The user perception in all these realms is different; thus user experience should surpass the expectations. As new technology is often viewed sceptically, surpassing the expectations should not be a big hurdle.

There is no single definition of user experience (UX). COST 294 action (MAUSE, towards to Maturation of information technology Usability Evaluation) tries to build a holistic view on the UX. In their deliverables ([33],[34]), user experience is viewed from many angles; for their purposes user experience terminology is put into statements that deal with fundamental assumptions underlying UX (principles), positioning of UX relative to other domains (policy), and action plans for improving the design and evaluation of UX (plans) [33]. By their terminology, e.g. trust is seen as one attribute of structuring user experience. The structuring of UX itself is part of the principles. As said, UX is a broadly defined term, including attainment of behavioural goals, satisfaction of non-instrumental (or hedonic) needs, and acquisition of positive feeling and well-being. Neither a universal definition of UX nor a cohesive theory of experience yet exists how to practically design for and evaluate UX [34].

In [34], UX is differentiated from usability because i) UX aims to follow holistic approach, ii) UX is subjective and iii) UX aims towards positive experiences.

i. Usability strongly focuses on tasks and user accomplishment. UX holistic approach aims for a balance between pragmatic aspects (i.e., usability) and other non-task related aspects (hedonic), such as beauty or self-expression.

ii. As conceptual origins of usability are in cognitive psychology, work psychology and human factors, usability is more of an objective expert-oriented approach. In contrast, UX is subjective and is not based on task success or results of usability studies. UX is explicitly interested in how users experience and judge, e.g., technology products they use. Thus, the perception of a user plays a much bigger role.

Usability focuses on negative aspects of the studies; most often problems, errors etc. are investigated through usability studies. However, UX tries to build positive outcomes of the use or possession of technology, e.g., positive emotions such as joy, pride, and excitement.

User experience is mostly collected by observing / interacting with people. This can be done in laboratory settings which might distort the results, as some people might not behave naturally when observed. Observation can also be done in field, e.g., travelling in buses for few weeks and just observing how users use their mobile phones. One can get the general trend and maybe the frequency of using mobile device, but not necessarily the details. Of course, in a research setting, a researcher has to use multiple research methods, both qualitative (e.g. interviews) and quantitative (e.g. surveys).

B. *Designing good user experience*

Jameson has emphasised the following goals for enabling enhanced user experience especially in the context of user adaptive systems [35]. As such they act as guidelines and design restrictions in ambient intelligence environments. These elements include

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

Predictability and visibility relate to the working of a system according to the user expectations. Thus, if the observed behaviour is in contradiction to what the user expected, the user is bound to get confused. In the case of a mental model of security this can be quite dangerous, because the user may end up compromising his security without really realising it.

Manageability or controllability refers to the amount of control the user has over the system. The system could, for instance, ask the user to decide whether to accept certain connection attempts. However, this can be a challenging topic when weighted against the unobtrusiveness.

The system should not bother the user unnecessarily. Otherwise the user may find the system obtrusive and burdensome to use. It can also overload the user with too much information, thus the user no longer evaluates information carefully. The discussion in the next subsection about SSL with too many warning messages is a good example of this.

User adaptivity generally requires storing information about the user and his actions. Some of this could be even considered to be very sensitive information. Thus, the potential information disclosure to unauthorised parties can have severe consequences. Some users might even get a "big brother is watching" feeling and turn off any functionality that otherwise might enhance their user experience.

Breadth of experience can be seen as a challenge of filtering too much information and hence limiting the user decisions. In other words, the user "learns" less, when all the decisions are made for him by the system.

This last (depth of experience) is important in order to get main stream experience correctly. However, it is difficult to get those extreme set of experiences of first-timers and those who like to do it "my way". It might be reasonable to downplay the benefits of technology, so that it actually surpasses the user expectations, and thus user perception is positive, which provides better overall for, e.g., a task that is not previously seen important or cumbersome to carry out.

C. *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 [36]. 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 2. USER CHARACTERISTICS IN SECURITY THEME [36]

Characteristic	Comment and effect
Users do not think that they are at risk	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.
Users aren't stupid, they are unmotivated	Human beings (as a species) tend to favour quick decisions based on learned rules and heuristics. Security can be seen as overly exhaustive action.
Safety is an abstract concept	The less concrete the threat is, the less willingness there is to carry out security instructions.
Feedback and learning from security-related decisions	Behaviour is shaped by positive or negative reinforcements. In security domain, most often the reinforcements are negative.
Evaluating the security vs. cost trade-off	Gains are often abstract and the negative consequences stochastic, the cost is real and immediate.
Making trade-offs between risk, losses, and gains	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.
Users are more likely to gamble for a loss than accept a guaranteed loss	People react differently on whether they think they are gaining or losing something (in concrete value).
Security is a secondary task	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.

Losses perceived disproportionately to gains	People do not perceive gains and losses equally. So the user has to perceive gain visibly better than a loss.

West also lists several approaches that could help the security designer to improve human compliance (to security) and decision making. These approaches include

- Rewarding pro-security behaviour (e.g., immediate feedback given to the user)
- Improving the user awareness of risk
- Catching security policy violators (non-repudiation / deterrence)
- Reducing the cost (for the user) of implementing the security (e.g., sufficient always-on security by default)

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, where the user no longer evaluates the information but just concentrates on absorbing or merely ignoring. Nowadays, this is quite evident with the use of SSL warning messages: users simply click ok, because they have seen similar windows so many times or actually do not even have any idea what the warning means. 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 [37].

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. We have further developed a hypothetical example scenario to illustrate the applicability of security and user guidelines presented in this paper. The scenario is, as scenarios are, narrative and focuses on user experience. Beneath it the technology research has to be read partially between the lines and as such leaves lot of room for different implementation options for the actual developer. Similar scenarios are easy to create in a hypothetical manner, but for real-world case one needs to empower and engage real users to do security related tasks in order to get relevant and accurate information from the users.

Hypothetical scenario and example case:

It is August 25th, year 2012,, and a time for the annual company party at the AmbVision Ltd headquarters. Matt Ellis, one of company's security staff, who was given the task of organizing the event for this year proudly waits for employees to arrive. In his left hand he has a company wrist clock awarded for dedicated work for the company. The wrist clock also has a security functionality and capability to communicate with the company's information system in a secure manner. It also contains wireless tag reader so that visitor tags could be read while they arrive to the AmbVision lobby and at the same time for a security check. It is still an hour and half for the company CEO speech and the official kick-off for the party, and the employers start to arrive. Some of the employees have dedicated tasks to carry out in order to make the party successful. Their tasks will be transferred to their wrist computers at the security check point.

Maria Smith is a new employee and for her this will be the first company party event. She has been working for two and half months and is really waiting for this party. However, today his boyfriend Frank Sonay came to a surprise visit and wants to come with her. After all, she has attended his parties, too. She knows that the security procedures are strict but she borrows the wrist computer of a fellow employee who happens to be in a hospital due to a traffic accident. Maria is able to delegate the watch to the identity of her boyfriend, but only with a limited profile with no access to the services of AmbVision. Frank acknowledges the watch by tapping it with his own company issued phone, which ensures the pairing of identities.

Over 100 employees have already arrived and Matt feels that nothing can go wrong today. He has made all the necessary security checks and even stricter security policies for communication. He puts the security lens on top of his eyeglasses and views the security logs, i.e., hardware reports, communication logs, network traffic graphs, and user profile data. So far no major deviations and everything is under control. Maria and Frank arrive at the security check point. Their wrist computers are scanned and the system informs the guard that the current user identity associated with the watch cannot be identified as AmbVision employee nor does it have the correct authorisation.. According to the policy, the guard is supposed to send a dedicated message to the information system which will control the further activities. Incidentally, Frank happens to be using his own employee identity and his company is also doing mutual projects with AmbVision. This same information is relayed (with information exchange to registry of Frank's company, which tells who this unidentified person is) to Matt who feels the wrist computer to tremble and sees the message and appropriate information. Matt browses the event data file and changes Maria's task in her computer so that her job is to clean the mess in a meeting room in 2nd floor in the corner of the building, far away from the CEO speech room. Maria's wrist computer begins to tremble and she reads the message and acknowledges that the task could be done faster if two persons would do the cleaning and thus Frank comes with her. They arrive at the room and Matt is already "cleaning" the room with two security staff members dressed as employees. Maria and Frank arrive and see that the mess is really big as five persons are needed to clean it. Matt asks Maria, why she has come with the boyfriend to a party. Maria starts to explain and gives her sincere apology. Matt tells her that everything is fine, he just has to change Frank's wrist computer for such ones that are meant for visitors and welcomes Frank to the party. However, Maria will lose five company points on her security portfolio.

TABLE 3. CORRESPONDENCE OF SECURITY GUIDELINES AGAINST USABILITY

Security guideline	User guideline	Usability goal	Rationale	Scenario example implications
Security by default	Reduce cost of implementing security	Unobtrusiveness Predictability	No extra mental burden is put to the user as an expected default level of security is always present.	Matt is the person in charge in selecting appropriate security policy for the event. The system has pre-set policies (so that additional policies do not need new implementation) and it is enough for Matt to select and thus also see what that chosen policy actually means on the individual, group, etc. level. in relation to the standard policy. The communication between the watches and the company systems is protected by default without the user having to configure anything. Naturally, the administrative systems are aware of the legitimate end-devices.
Ease of configuration	Reduce cost of implementing security Improving user awareness	Unobtrusiveness Visibility Controllability	User is not needlessly interrupted with secondary tasks, but still has a sense of being in control for added security.	Users do not have to go through complex configuration procedures, e.g., tapping devices together might be sufficient procedure for acknowledgement ..
Secure naming	Improving user awareness Catching policy violators	Privacy Controllability Visibility	Assurance about the communicating parties and invariability of them either with short or long term identities.	The watches carry the identity of a watch and that of its current wearer. The systems they interact with can be identified as legitimate ones. Security logs can be later on audited and one can also see who has accessed the logs. The trustworthiness of the system can be measured so that users understands/sees how it safeguards, e.g., their privacy. Also, Frank was able to control, which identity he wanted to use with the watch..
Decoupling authentication and authorisation	Improving user awareness	Privacy Visibility	Only authorisation is explicitly linked to the execution of the defined actions.	While the company watch might provide authorisation to access the event, the wearer identity does not hold such assertion, which normally could be assigned to companions, as Matt later does. The user mental model is directed toward the action, which requires authorisation instead of a person (like someone appearing with a trusted person). This may also ease the job of log administration as data protection laws may have more restrictions on the handling of data containing personal, i.e., identity information.
Privileges & delegation	Reward pro-security behaviour	Controllability	Efficient execution of tasks and assigning privileges as needed for controlling the disclosure of information with timely feedback.	The policy of the watch allows delegation of it to other people, but with limited rights. Users are always also told about the decisions and why these decisions have been made. Users are aware of control as e.g. security checkpoint in the scenario implicates. Also the security guard did not interfere for stopping the visitor as the system provided enough information for evaluation the case so that more appropriate solution could be carried out. It might have been the case that another visitor could be handled differently
Liability brokers	Catch policy violators	Unobtrusiveness Privacy	Outsourcing the trust evaluation and reliance on external mechanisms (such as litigation)	Frank is considered semitrusted as the identity system of the partner company can vouch for his identity without Frank having to actively do anything. The security logs can catch/find policy violators or possibly organisations that are liable for arranging the violating privileges.

D. Towards trusted user experience

As we are heading towards future ambient networked systems, the user should not need to ask how, why, what, when and where. However, user demand and requirements vary highly depending on the context and situation. The technology might not be mature enough yet, as fulfilling user demand and user requirements in different situated contexts faces an increasing level of uncertainty. The user demand is quite often described as a higher-level demand that can be constructed in a given situated context from the identifiable attributes. The user requirements, on the other hand, are often seen as a critical issue of using technology (e.g., so is the case in requirement engineering). Furthermore, as ambient systems naturally operate in the background, trust will become major issue in accepting new systems and environments into use.

Hoffman has created a trust model with related metrics for distributed information systems [38]. Trust model has generic model parameters and subcomponents such as security, usability, privacy, reliability and availability, audit and verification mechanisms, and user expectation. In creating user experience, usability subcomponent has as general model parameters perception issues, motor accessibility, and interaction design issues. User expectation

subcomponent has product reputation, prior user experience, knowledge of technology, and use of trusted agents.

The perception issues can also be directly linked to security characteristics, e.g., perception of controllability and observability. Motor accessibility is a personal feature and thus the interaction design issues should deal with the special target groups. Product reputation can be a powerful tool as the user can feel more trustworthy towards known brands. Prior user experience could become the major element in trust provision. In general, most of users do not want to learn new things, especially if they sound too complex or look cumbersome to manage. Thus, the technology should have high enough accurate cognition of the experience and capability of the user. Observability is also a direct perception issue, and the user should have that particular capability. The interaction should provide the perception of controllability, feeling secured in private and trusted manner [39].

It is also worthwhile to note that the attitudes of the people towards the technology and its acceptance changes over time. As noted in [40], even privacy disruptive technologies such as camera phones can become socially acceptable in a relatively short timeframe. Thus, user suspicions towards the technology have faded. It is more a question of how technology is used, i.e., in an appropriate way, and whether the users are aware of the existence of such technology. As stated in [40], the designers should try to predict and influence these adoption patterns.

Trust categories, i.e., technical and human trust, introduced in section III can be seen analogous to usability and user experience (see Table 4). Technical trust definitions, attributes of trust (e.g., level of trust, origin of trust) and carrying out trust related functionalities are very much similar to usability as both have an objective and fact-based (measurable) approach. Thus, linking them together in a conceptual level is very straightforward. On the contrary, as user experience and user perception of trust are both subjective, linking them is not as straightforward. Such kind of trust cannot be modeled based on technical modeling fundamentals such as system architectures, software architectures or messages and interfaces between different nodes or/and components. However, we have tried to identify security related user aspects brought forward in this article that are important for building holistic user experience.

TABLE 4. MAPPING OF USABILITY AND USER EXPERIENCE TO TRUST

Attribute	Characteristics	Mapping to trust
Usability	*Pragmatist view:* Usability is likely the most important user requirement as it has a heavy impact on the acceptance of technology. ISO 9126 metrics can be mirrored through user experience lens. The methods are carried out in objective manner to address the required tasks and accomplishments of the user, e.g., task of changing password based on metrics such as task success.	Technical trust • Direct trust: Common shared secret, i.e., preconfiguration • Opportunistic trust: The sameness property, e.g., key continuity • Blind trust: Metrics of uncertainty
User experience	*Holistic view:* Integration of task related issues and non-task related issues such as challenges (e.g., in a fashion of games) and stimulation in order to give more joy and excitement of performing "mandatory" security functionalities, i.e., user overall experience is taken into account. The final set of functions should be based on subjective design, implementation and evaluation.	User perception of trust • Being in control: User is empowered to manage and audit the decisions taken by the system • Feeling safe: Physical security • Privacy: How and what information is disclosed • Reputation: Expectations and brand trust • Level of comfort: User is not cognitively overloaded • Assurance: System functions as expected

VII. DISCUSSION

As we have shown, users are facing risks and uncertainties in the evolved networked service landscape due to the user mindset, information leakage, and shortcomings of the platforms. Users are not generally interested in technical details such as 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 DoS is launched against the secured service, the user is tempted to use the available insecure version instead [41]. 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. The security systems provided by user's work organisation do not cover leisure time and private mobile devices.

Thus, we underline the importance of keeping the security in the design process right from the start. So, the user can always enjoy default security without having to concern him or her with configuration issues as it is evident that users prefer unobtrusive systems, which do not require them to understand the mental models behind the security mechanisms. The importance of such proactive design choices is also underlined in [42], which proposes research priorities for future mobile telecommunications.

Additionally, secure identification (be it short or long term) along with proper privileges need to be applied to control the information disclosure. Also, many other mechanisms can be based on the existence of secure naming as a building block and proper identity management can be used to alleviate the previously mentioned shortcomings of purely password based systems. It should be noted, however, that the user mindset 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.

As known already for decades there has been confrontation between security and usability. Many data 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 recognize 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 also that security mechanisms are designed, implemented, applied, and breached by people. Thus, the user-centered design is essential for all security related systems. It has been argued that hackers pay more attention to the human link in the security chain than security designers do [43].

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. Although the single product development of networking devices has strived for both a satisfying user experience and security, as in [44], generally the architecture design takes purely a technical approach and lacks the support for usability aspects.

Considering the tradeoffs between invisible and transparent security is unavoidable procedure 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 [37] 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.

There have been success stories of designing usable security; instead of forcing the user through 38 steps of WLAN configuration with decisions and actions, by designing a user interface there are only 4 steps to go [45]. Innovative design solutions and disruptive thinking, which take a holistic approach to the whole problem rather than concentrating on one specific problem field at a time, will be needed. Similar holistic approach can also be used when applying cross-layer thinking to reduce the performance effect of multiple overlapping security mechanisms on several protocol layers [46].

Although global PKI is still considered too complex and out of reach for typical end users, work for thinking locally has resulted in usable and secure wireless network [23]. The use of cryptographic identifiers on local scale can further benefit such systems. However, the design decisions do not have to be anything huge and unprecedented. They include small steps keeping the user in mind and also testing early prototypes. Writing lists of anti-requirements (things that your design should not allow the user to do) and simple "default-action"-tests given in [37] reveal the security level of the system.

Changes are required also within usability testing itself: e.g., better use of data logs of the systems, reformulating activities that we are observing in the field studies, and reconsidering the methods and topics of the interviews [47]. Designing tests for security systems that also take into account the usability and user experience factors differs from designing ordinary customer products or services. Thus, the development teams of security systems or architectures should always include also persons with expertise in usability and understanding of user experience.

VIII. CONCLUSION

In this article we have presented and 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 raise the security of the future ubiquitous systems to a level, where there is always a baseline of security present.

Even though networks can be seen to be technical concepts, the holistic design processes have to also remember the existence of the user. The user experience factors on the chosen solutions can dictate whether the system will ever be deployed or used. Security and usability have to go hand in hand and be in the design process right from the start in order to ensure secure user experience. It is not enough that the designer thinks that the user is safe; the user also has to have the feeling of being secure. If the user finds the system obtrusive or too complex to understand, it is likely that there is little trust towards the system, hence hindering the adoption of the system.

Integration of user experience into security design is on its early stages and is not very well studied so far, even

though usability and security have been the subject of many studies. In this article we have taken initial steps to introduce a more holistic view towards designing a trusted user experience, so that one can take into account the behaviour of the user and how the user perceives trust in an ambient environment.

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 a secure user experience and the user can agree to that.

[1] S. Heikkinen, K. Heikkinen, S.Kinnari, "Security and User Guidelines for the Design of the Future Networked Systems". Proceedings of the *Third International Conference on Digital Society (ICDS 2009)*, Feb 2009.

[2] M. Johnsson (Ed.), "AN System Description", Ambient Networks project deliverable D18-A.4, Feb 2008.

[3] F. Kohlmayer (Ed.), "Ambient Networks Security Architecture", *Ambient Networks project deliverable D7-2*, Dec 2005.

[4] K. Ducatel (Ed.), "Scenarios for ambient intelligence in 2010", European Commission IST Advisory Group report, Feb 2001.

[5] G. Bell, P. Dourish, "Yesterday's tomorrows: notes on ubiquitous computing's dominant vision", *Personal and Ubiquitous Computing*, Vol 11, Issue 2, Jan 2007.

[6] N. Niebert et al, "Ambient Networks: An Architecture for Communications Networks Beyond 3G", *IEEE Wireless Communications*, Vol .11, No. 2, Apr 2004.

[7] 3GPP. "Network Composition Feasibility Study", 3rd Generation Partnership Project Technical Report, TR22.980 V8.1.0, June 2007.

[8] Facebook. "Terms of Use", November 15, 2007. Available http://www.facebook.com/terms.php (accessed 01/2008)

[9] Y. Chen, J. Hwang, R. Song, G. Yee, L. Korba, "Online Gaming Cheating and Security Issue", Proceedings of *International Conference on Information Technology: Coding and Computing*, Apr 2005.

[10] M. Kampmann et. al., "Dynamic Adaptable Overlay Networks for Personalised Service Delivery", Proceedings of *The First Ambient Networks Workshop on Mobility, Multiaccess, and Network Management*. Oct 2007.

[11] J. Nolan, M. Levesque, "Hacking Human: Data-Archaeology and Surveillance in Social Networks", *ACM SIGGROUP Bulletin*, Vol. 25, Issue 2, Feb 2005.

[12] J. Niemelä, K. Tocheva, M. Tolvanen, "F-Secure Trojan Information Pages: Redbrowser.A", http://www.f-secure.com/v-descs/redbrowser_a.shtml, (online article, accessed 10/2007), Mar 2006.

[13] ISO/IEC, "ISO 13407:1999 Human-Centred Design Processes for Interactive Systems", International Organization for Standardization Standard, 1999.

[14] M.H.Diallo, J. Romero-Mariona, S. E. Sim, D.J. Richardon, " A Comparative Evaluation of Three Approaches to Specifying Security Requirements", Proceedings of 12th *Working Conference on Requirements Engineering*, Jun 2006.

[15] B. Busropan (Ed.), "Ambient Network Scenarios, Requirements and Draft Concepts", Ambient Networks project deliverable D1.2, Oct 2004.

[16] T. Govier, "Social trust and human communities", McGill-Queen's University Press, 1997.

[17] L. Perusco, K. Michael, "Control, trust, privacy and security: evaluating location based services", *IEEE Technology and Society Magazine*, Vol 26, Issue 1, 2007.

[18] F. N. Egger, "Trust me, I'm an online vendor: towards a model of trust for e-commerce system design", Proceedings of *Conference on Human Factors in Computing Systems*, Apr 2000.

[19] S. Heikkinen, "Social engineering in the world of emerging communication technologies", Proceedings of *Wireless World Research Forum Meeting #17*, Nov 2006.

[20] J.H. Saltzer, M.D. Schroeder, "The protection of information in computer systems", Proceedings of the *IEEE*, Vol. 63, Issue 9, Sep 1975.

[21] K. Yee, "Aligning Security and Usability", *IEEE Security & Privacy Magazine*, Vol. 2, Issue 5, Sep 2004.

[22] A. Whitten, J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", Proceedings of the *8th USENIX Symposium*, Aug 1999.

[23] D. Balfanz, "In search of usable security: five lessons from the field", *Security & Privacy Magazine, IEEE*, vol. 2, 2004.

[24] T. Rinta-aho et al, "Ambient Networks Attachment", *16th IST Mobile and Wireless Communications Summit*, Jul 2007.

[25] P. Jokela (Ed.), "Host Identity Protocol", *IETF RFC 5201*, Apr 2008.

[26] S. Heikkinen, M. Priestley, J. Arkko, P. Eronen, H. Tschofenig, "Securing Network Attachment and Compensation", Proceedings of *Wireless World Research Forum Meeting #15*, Nov 2005.

[27] S. Heikkinen, H. Tschofenig, "HIP Based Approach for Configuration Provisioning", Proceedings of the *17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep 2006.

[28] S. Heikkinen, "Authorising HIP enabled communication", Proceedings of the *10th International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, Jul 2007.

[29] M. Georgiades (Ed.), "Security Requirements, Concepts and Solutions for Secure Access and Mobility Procedures", Annex 2 of Ambient Networks project deliverable D7-2, Dec 2005.

[30] S. Heikkinen, "Non-repudiable service usage with host identities", Proceedings of the *Second International Conference on Internet Monitoring and Protection*, Jul 2007.

[31] G. Riva, "The Psychology of Ambient Intelligence: Activity, situation and presence", IOS Press, 2005.

[32] B. J. Pine, J. H. Gilmore, "The Experience Economy: Work is theater & every business a stage", HBS Press, 1999.

[33] E. Law, A. Vermeeren, M. Hassenzahl, M. Blythe (Eds.), "Towards a UX Manifesto", COST294-MAUSE affiliated workshop. Sep 2007.

[34] E. Law, E. T. Hvannberg, M. Hassenzahl (Eds.) "User experience: Towards a unified view", Proceedings of the *2nd International Workshop on User eXperience*. Oct 2006

[35] A. Jameson, "Adaptive Interfaces and Agents", Human-Computer Interaction Handbook, Erlbaum, 2003.

[36] J. West, "The Psychology of Security", *Communication of the ACM*, Vol 51, No. 4, Apr 2008.

[37] P. Gutmann, "Security Usability Fundamentals," Available http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf (online article, accessed 01/2008).

[38] L.J. Hoffmann, K. Lawson-Jenkins, J. Blum, "Trust Beyond Security: An Expanded Trust Model", *IEEE Communications of the ACM* Vol 49, No. 7, July 2006.

[39] K. Heikkinen,N. Prasad, "Empowerment: Enabler for Personalized Security and Privacy",Proceedings of *IEEE Globecom Workshops* Nov 2007.

[40] G. Iachello, K. N. Truong, G. D. Abowd, G. R. Hayes, M. Stevens, "Prototyping and Sampling Experience to Evaluate Ubiquitous Computing Privacy in the Real World", Proceedings of *CHI 2006*, Apr 2006.

[41] B. Schneier, "Secret and Lies", Wiley Computer Publishing, 2000.

[42] R. Savola (Ed.). "Security, Trust, Dependability and Privacy in Wireless and Mobile Telecommunications", White paper appearing in eMobility deliverable D2.1, Nov 2008.

[43] A. Adams, M. A. Sasse, "Users are not the enemy," *Communication of ACM*, Vol. 42, Issue 12, Dec 1999.

[44] S. Elmore, S. Hamilton, S. Ivaturi, "Designing software for consumers to easily set up a secure home network,", Proceedings of *25th SIGCHI Conference on Human Factors in Computing Systems 2007*,, 2007.

[45] G. Balfanz, R. E. Durfee, D. Grinter, P. Smetters, P. Stewart, "Network-in-a-box: How to set up a secure wireless network in under a minute," Proceedings of the 13th *USENIX Security Symposium*, 2004.

[46] J. Arkko, P. Eronen, H. Tschofenig, S. Heikkinen, A. Prasad, "Quick NAP - Secure and Efficient Network Access Protocol", Proceedings of the *6th International Workshop on Applications and Services in Wireless Networks*, May 2006.

[47] D. K. Smetters, R. E. Grinter, "Moving from the design of usable security technologies to the design of useful secure applications," Proceedings of *New Security Paradigms Workshop 2002*, 2002.