Experience Design Framework for securing Large Scale Information and Communication Systems

Azadeh Nematzadeh, School of Informatics and Computing, Indiana University.
Omar Sosa-Tzec, School of Informatics and Computing, Indiana University.

Abstract

Securing Information and Communication Systems (ICSs) is a highly complex process due in large part to the feedback relationship that holds between the users and the system and its 'ecosystem' of usage. Such a relationship is critical for experience designers. The design of secure systems can thereby be enhanced by using principles from disciplines where similar relations hold, such as security engineering and adaptive systems. In this work, we propose a user experience design framework based on six principles and use a social networking system as an example of its application. The proposed design principles are grounded in complex systems theory. We address several potential security and privacy challenges inherent in the design of a large-scale adaptive system. By means of this framework we reflect upon the participation of an experience designer regarding the conceptualization, selection, review, and update of security and privacy matters. In this sense, we observe the role of the designer as a translator across disciplines. By introducing our framework, we also attempt to start a conversation about the challenges a designer faces in the appropriation of this role, either for the case of securing large-scale systems or in those situations where the boundaries of design and knowledge from other disciplines already overlap.

Keywords

Experience Design, Security and Privacy, User-System Coevolution, User Heterogeneity, Complex Systems, Adaptive Systems, Design Translation.

Considering the user experience has been important for recent approaches of designing interactive systems (Bødker, 2006; Garrett, 2010; Harrison, Tatar, & Sengers, 2007; Wright & McCarthy, 2010). The general goal of experience design is that users have a pleasant experience while interacting with the system and not only providing users a tool for accomplishing certain tasks (Forlizzi & Battarbee, 2004; Law, 2011; Law et al., 2009; Oppelaar, 2008). To achieve this goal, designers consider several elements such as functionality, usability (Krug, 2009; Rosenbaum et al., 2002; Tullis & Albert, 2010), emotion (Agarwal & Meyer, 2009; Norman, 2007), aesthetics (Bardzell, 2009; Sonderegger & Sauer,2010; Lavie & Vogel, 2013; Wright, Wallace,& McCarthy 2008), and information architecture (Bolchini et al., 2006; Ding & Ling, 2009; Garrett, 2010; Morville & Rosenfeld, 2008).

Pervasiveness of Information and Communication Technologies (ICTs) introduces Information and Communication Systems (ICSs) to people across the globe. ICSs facilitate the users' interaction by creating an environment that can connect people from all around the world by means of the Internet. Users of ICSs interact with each other from different geographical locations, and possibly using different technological devices. They may come from different levels of information and computer literacy. Moreover, they often come from different cultural values and perspectives. Also, users may change over the time. For example, cultural values, users' perspectives, and computer literacy are not fixed factors. As a result, use scenarios may change over time. The sheer richness, interconnectivity, and diversity of the Internet, whether measured in terms of social networks, infrastructure, or content, make it also difficult to consider a single archetype of user for these systems. As a result, use scenarios are often varied among various groups of users. A social network is an example of large-scale ICSs. Users of a social network constantly upload data to 'the cloud'. They generate information in different contexts of use. This information will be exchanged among the users of the social network in various contexts of use. Social, economic, and political factors can affect how users interact with these systems. Eminent advances in technological devices such as Google Glass facilitate and increase the use of ICSs. Google Glass has been recently released, and yet the ways it will be utilized will depend on its users and the contexts of use. For example, a tech-savvy person may use Google Glass to explore a new technology, whereas an anthropologist may use this device to perform ethnography.

Widespread use of ICTs and accessibility of several ICSs to perform a similar task create an extremely competitive environment. Current ICSs attract more users if they gain users' trust (Camp, 2003). Achieving users' trust comes with the cost of providing security and privacy. We argue that security and privacy at different scales and levels are of the users' interest. Thus, security and privacy consideration should be a part of experience design along with other aspects, such as usability, aesthetics, emotion, and information architecture. Designing secure large-scale ICSs entails unprecedented levels of complexity. The latter expresses itself through the number and variety of components such as users, connections, access rights, as well as difficult-to-predict security and privacy phenomena. We should take into account that modern security and privacy mechanisms involve decisions regarding specific policies, roles, and restrictions, as well as adaptive algorithms that can generate and revise such content. This process is not usual in experience design frameworks (Forlizzi & Battarbee, 2004; Garrett, 2010; Law et al., 2009). Notwithstanding, we argue that security and privacy matter in experience design, since it focuses on people and the different factors that affect their activities within a context of use (Wright & McCarthy, 2010). Therefore, we issue the following challenge to design practitioners:

Security and Privacy Challenges for Experience Designers:

- ***Heterogeneity of users:*** As we mentioned earlier, ICSs have different types of users who may have different security and privacy concerns. For example, the privacy concerns of college student Facebook users may not the same as those of their parents. The current experience design frameworks seem not to consider this matter.
- ***Diversity of the context of use:*** In designing ICTs the context of use is truly ubiquitous (Brusilovsky, 2001). Different contexts of use can cause different privacy and security concerns. For example, social norms may affect the usage of Facebook. Certain types of content in Facebook profiles, such as profile pictures, may require different privacy decisions, though the archetype of a user is the same. A simple aspect such as geographical location can add different features to the archetype of users.
- ***Multiple use scenarios:*** Use scenarios of an ICS are diverse and unlimited. For example, Egyptians used Facebook pages to inform each other about an upcoming protest during the Arab spring (Khondker, 2011). Meanwhile, an Egyptian musician might have been using Facebook to create a fan page. Diversity of the contexts of use can result in creating more use scenarios. Security

and privacy use scenarios are no different. For example, a Facebook user may divide his/her Facebook friends into different groups such as family, classmates, close friends, and set different privacy settings for each of these groups. On the other hand, another Facebook user may set the same privacy setting for all of his/her friends. Most of the experience design practice is to create a tool with a certain functionality that considers a certain type of user with certain use scenarios. Thus, diversity of security and privacy use scenarios is a challenge that experience designers may face.

- ***Evolvable use scenarios:*** In designing large-scale ICSs, the system to be designed is a black box—the system can be a black box with very little information known about it. *In particular, security and privacy use scenarios are not clearly and completely defined. They are often unpredictable and prone to future changes* (Hebig, 2010; Friedman, 2002). Due to unsettled specification of the system requirements, the ways of using a particular artifact can change during its life span. For example, an earlier release of Facebook was only aimed to connect college students. The current usage of Facebook is far different; for example, it has been used as a platform for micro-blogging, creating fan pages, advertising said pages, as a news channel, and for organizing events. Not only has Facebook been changing over time, but Facebook users have changed too. A particular Facebook user may not use Facebook the same way as when he joined. Security and privacy awareness of users usually grows over time. This matter sometimes becomes more important in security and privacy scenarios, since many of the security and privacy threats are recognized through the usage of the system.
- ***Evolution of ICTs infrastructure:*** In addition to the aforementioned issues, the infrastructure that supports ICSs may change with time. For example, new devices, new software, and faster internet access can all change. Current experience design frameworks may fail to consider this.

The ongoing interactions of the aforementioned challenges, including the heterogeneity of user profiles, the dynamics of how information is deployed and managed by those users, unpredictable use scenarios, the interrelationship between security and privacy, and the unfolding dynamics inherent to users' behaviors, describe **a Complex System** (Weaver, 1948; Rosen, 1987)**.** Thus, we consider security and privacy aspects of ICSs as belonging to the category of Complex Systems. To address the aforementioned challenges in designing security and privacy aspects of ICSs, we apply the concepts and tools that characterize a complex system. A **user-system coevolution approach** in terms of changes on users, outcomes of the system, and ICTs infrastructure would allow us to manage security and privacy issues in complex systems. By considering the perspective that security and privacy systems are embedded in an *evolving security ecosystem*, these systems should be designed for not only addressing existing threats but also for shaping the nature, incentives, and prevalence of future threats.

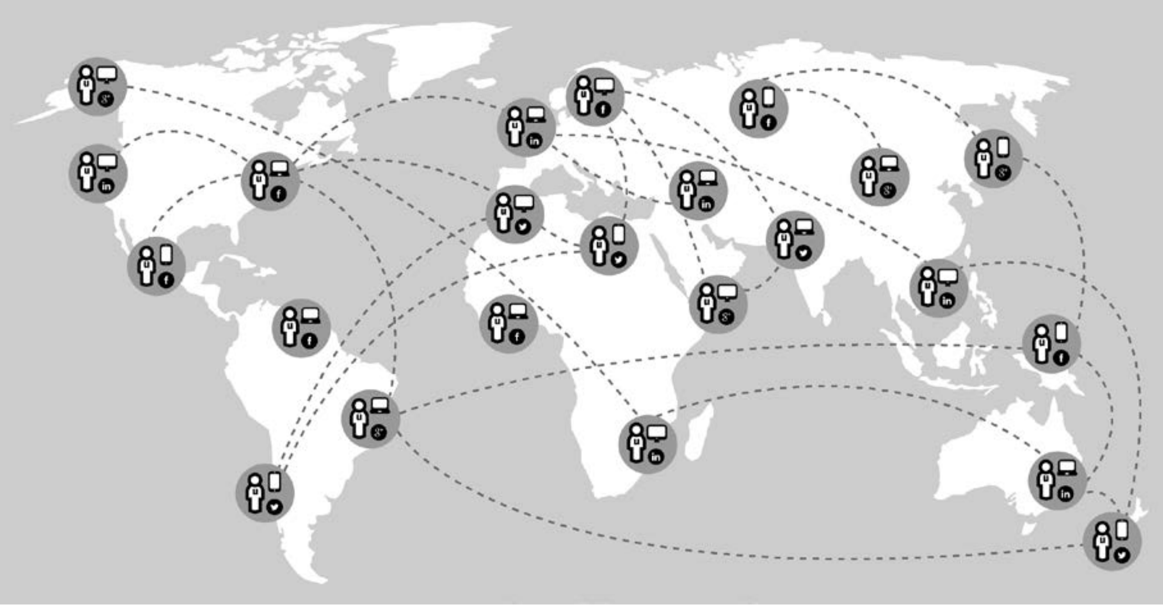


Figure 1: A social network is a complex system. Users of a social network build and publish their pages. They post and share information. They link and connect to other existing pages. All of these user's activities have been done individually and independent of others. Social Networks such as Facebook, which users have created over time has several general structural and topological properties that describe how it grows, how information propagates and some becomes trendy and popular, and how information dies off. Image by the authors.

In this paper, we propose an experience design framework to support design practitioners to inform and reflect on their designs regarding privacy and security matters. The principles that constitute our framework entail a synthesis of work developed both in the disciplines of Complex Systems and Security and Privacy. By bringing such synthesis to the realm of design, we introduce the approach that ICSs, as complex systems, will co-evolve accordingly to the changes regarding the users. Hence, this work focuses on introducing the aforementioned framework. To examine the proposed framework, we use social networks such as Facebook as a case study. Facebook is one of the most recent and influential ICSs[1]. Through the case study, we explain the use of the proposed principles in experience design. We chose Facebook mainly due to its fast growth during last 10 years, its diversity of users, its dynamic use scenarios, and the wide range of privacy and security threats introduced by it.

This paper is structured as follows. In the first section, we introduce the key concepts that characterize Complex Systems. Also, we set the general panorama to understand large-scale ICSs. Later, we present the principles that constitute our experience design framework, which derive from critical aspects pointed out in security and privacy literature. To clarify the concepts regarding the framework, we present the case study of a social network. We then discuss the implications for experience design in terms of practice and pedagogy and close with our conclusions and ideas for future work.

[1] In March 2014, "Facebook passes 1.19 billion monthly active users, 874 million mobile users, and 728 million daily users", a large number considering the population of the world is only a little more than seven billion.

Complex Systems, ICSs, and Security

The notion of Complex Systems

Principles of modern computer science, artificial intelligence, and computation theory were introduced in meetings and discussions held from 1946 to 1953 among eminent scholars of different fields at the Macy conference (Wiener, 1948). Collaboration between these scholars to answer interdisciplinary wartime challenges required the creation of a new conception and approach to scientific problem solving. The new scientific discipline was originally known as the **cybernetics movement** (Heims, 1991). *Complex systems research* can be considered as the next generation of cybernetics. It is a more recent interdisciplinary scientific field that merges principles and properties of computer science, physics, biology, sociology, and mathematics in order to study the dynamic and adaptive behavior of a variety of systems (Prigogine, 1985).

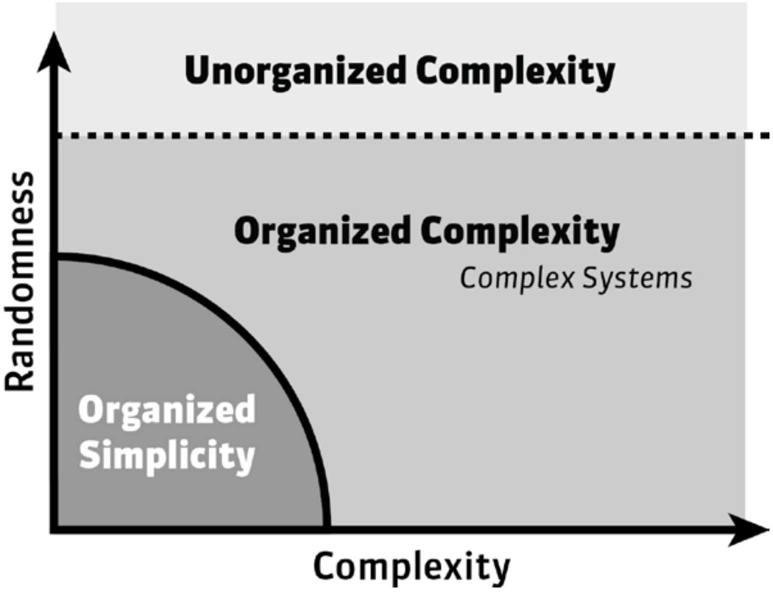


Figure 2: Complex Systems belong to the category of “Organized Complexity”, those are the problems too complex to solve analytically, but that have a certain structure by which it is possible to observe behaviors and properties. Figure based on (Weinberg, 1975). .

A complex system is a system that has a large number of parts that interact together in an indeterminate manner without central control (Simon, 1962; Weaver 1948). In such a system the holistic properties of the system cannot be easily inferred from its parts (Klir, 2001). Studying complexity thus involves studying the structure or organization of systems (Ashby, 1962). Complicated, hard to predict, and global behavior can emerge from simple interactions among components of a complex system.

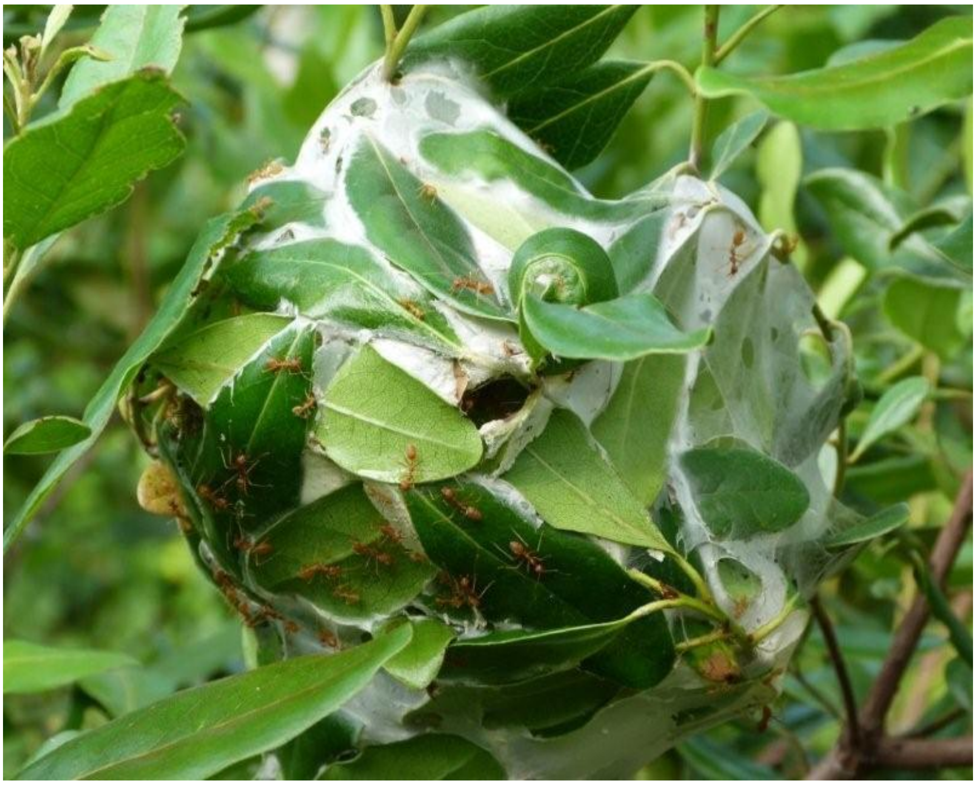


Figure 3: Millions of ants create a complex structure known as an ant colony. A single ant is not smart but the colony of ants is. Ants interact through chemical signals. Survival of each ant is dependent on the survival of an ant colony. Ants use this structure to search for food, fight an intruder, or build a nest. Photograph retrieved from http://tinyurl.com/k76l85y.

Properties of the Complex Systems

Weather forecasting, traffic control, urbanization, brain networks, swarm intelligence, immune systems, riot formation, the Internet, and social networks are a few of the widely known examples of complex systems. All of these systems share common features and characteristics that qualifies them as complex systems. We list below some of the important properties of complex systems that inspired us to create an experience design framework. These properties are embedded in modern large-scale ICSs, such as social networks and other web-based applications.

Dynamics

Complex systems change over time. The future states of a system will depend on its current state and inputs (Devaney, 2003). For example, the stock market and global climate are two of the examples of dynamic systems.

Self-organization

Feedback constitutes the means by which a complex system self-organizes. A system organizes itself without any pre-defined planning or control. Consequently, organized behaviors emerge to help a system best fit its environment. These organized behaviors are hard to predict. For example, synchronous flashing of fireflies is a self-organizing system (Camazine, 2003). In these systems order emerges from disorder (Ashby, 1962).

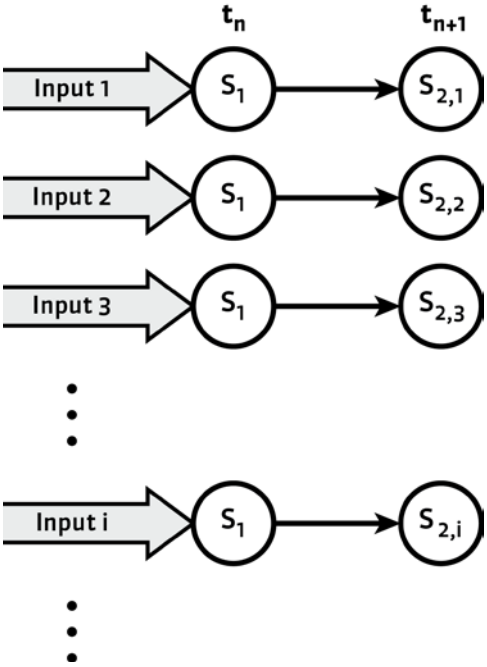


Figure 4: Dynamics of a Complex System. Different inputs will lead to different states of the system. Figure by the authors.

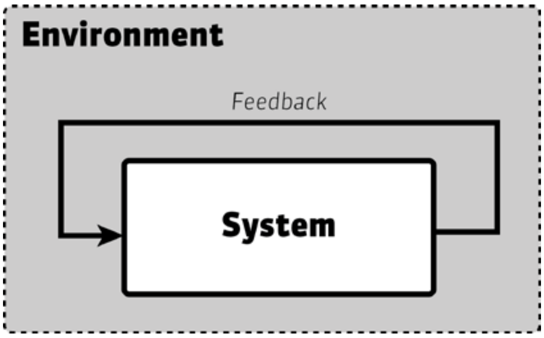


Figure 5: Environmental inputs affect the states of the system. However, the feedback that the system provides itself also influence in the changes of those states. Figure by the authors.

Emergence

In the context of complex systems research, a universal property of the system that has emerged from the collective behaviors of the system components is called "emergence" (Funtowicz, 1994). This means that random interaction of system components can emerge the pattern that shows the system behavior.

Chaos

In studying the Chaos in complex system, chaotic systems can be considered as deterministic dynamic systems (Crutchfield, 1981; Eckmann, 1985). Although chaotic systems are deterministic, behaviors of the system at narrow scale can be unpredictable. That is, small perturbations in the system cause large changes in future behaviors of the system.

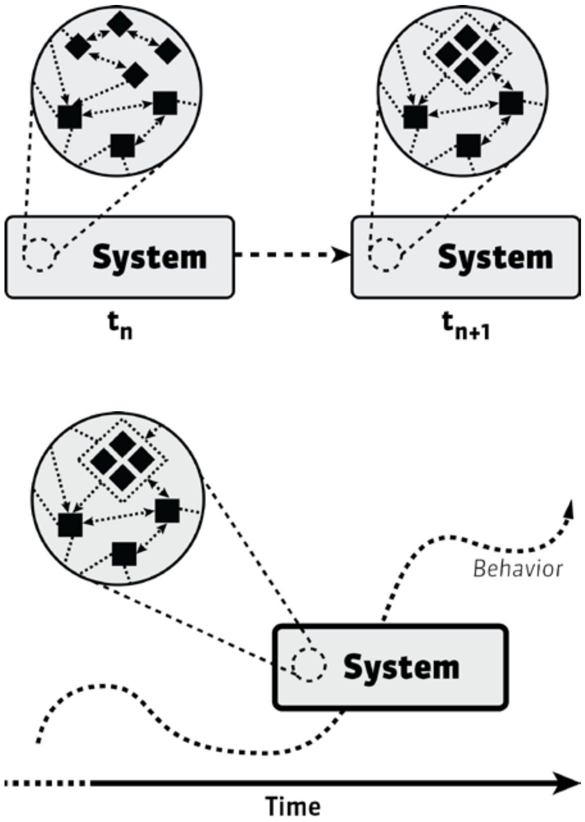


Figure 6: Collective behaviors among the components of a system can emerge to a pattern. Moreover, changes or perturbations in the system can affect its behaviors. Figure by the authors.

Evolution

The evolutionary properties of complex systems are defined by their adaptive behaviors. Adaptive behaviors include those that change over time to increase survival chances. Complex system behaviors evolve through learning and the evolutionary process, only the strongest traits – the ones that increase the chance of success or survival – should be 'selected'. In this sense, complex systems are also adaptive systems, where learning and evolution are a result of the collective and dynamic behaviors in the system (Holland, 1992).

Coevolution

Systems are part of and environment. Systems and the environment interact and affect each other throughout their lifetimes. For example, environmental changes cause changes in a system's behavior. Systems should adapt to environmental changes to fit best the environment and survive (Ehrlich, 1964). Likewise, the environment can go through changes due to system fluctuation.

Figure 7: The Stick bug or walking stick is one of the many organisms that have several adaptations. For example, their coloration is as their environment. Not only is their shape similar to a stick, they also can stay still to deceive the predator, and they can also imitate the tree branches movement with the breeze or wind. Photograph by the authors.

ICSs as Complex Systems

We argue that securing a large-scale ICS, in conjunction with the overall ICT's infrastructure that supports it, create a complex system. In this case, complexity rises as a consequence of the large number of users, intertwined content, and technological devices. Although users are an essential part of the system, influencing the structure and organization of the system, the proliferation of internet-connected databases allows attackers to infer more personal information about a target than any other source permits (Clifton, 1996). Thus, both the safety of users and the system share the same level of relevance. The way users behave and how the system is used affect both aspects.

Large-scale ICSs are perceived as complex systems, and hence as adaptive systems, and are coupled to a changing and complex external world. Security and privacy concerns about these systems can affect and be affected by a dynamically changing legal climate, as these issues come into ever-increasing public awareness (Kagal, 2006). In addition, technological possibilities are also evolving. For example, spammers learn to avoid filters, and passwords become easier to crack as computing power increases.

Security and privacy aspects of ICSs satisfy the complex systems characteristics, and system safety is an emergent property when system components operate together (Leveson, 1995). System safety aims to decrease hazards and system failure by emphasizing safety-critical functionality, and thereby increase system safety and reliability. For ICSs, security and privacy requirements sometimes are indefinite, or there are no specified user requests. Furthermore, variation in users' security and privacy requirements of the same system lead to a vague and incomplete system specification (Friedman, 2002).

Security and Privacy Principles for Experience Design

In this section we introduce our proposal for an Experience Design framework. The framework is constituted by six principles: 1) Security and Privacy matters, 2) Personalization, 3) Adaptability, 4) Expandability, 5) Usability, and 6) Avoid unintentional disclosure. For each principle, we describe key aspects that experience designers should take into account in the design of large scale ICSs.

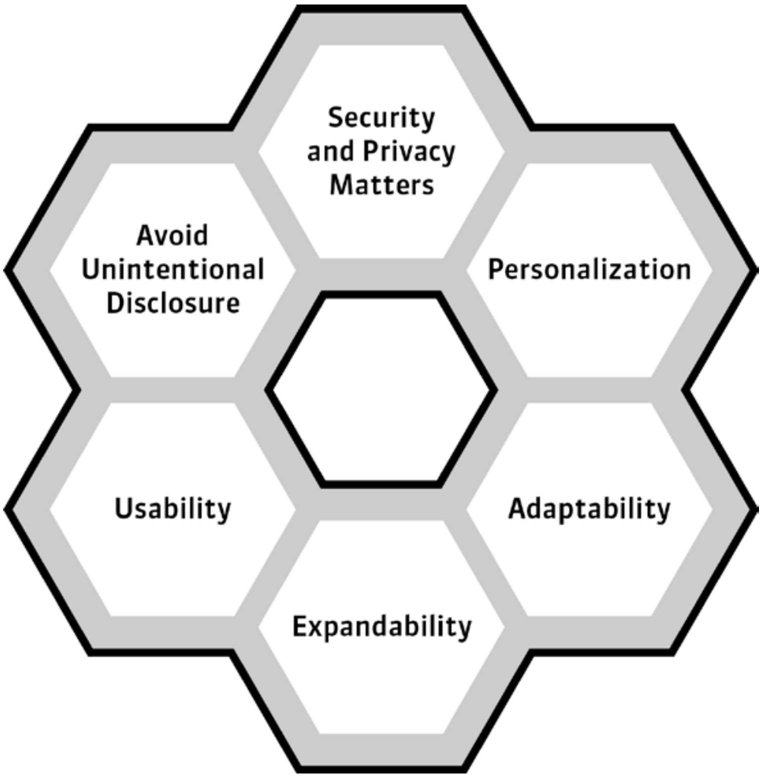


Figure 8: Principles that constitute the Experience Design Framework presented in this figure. Figure by the authors.

Security and privacy matters

Security, privacy, and system safety (Bishop, 2002) should be considered as critical features of systems. We argue that the experience designer should be informed by specialists, discuss, and reflect about how to mitigate future attacks. Security and privacy failures are some of the most costly processes of an organization (Camp and Wolfram, 2000). Decreases in the cost of future patching justify the early cost of designing highly secure systems (Mouratidis, 2003).

We suggest that the designer should analyze potential generalities on users, context of use, and technological aspects in order to determine how basic interaction flows are related to possible adaptive security and privacy mechanisms. We argue that the designer should keep in mind that any potential mechanism has the aim of predicting future system failures and responding to them. In this sense, the designer should be aware of basic notions of safety engineering (Leveson, 1995). Safety is not a separate component to be added once the design is complete, but rather considered throughout the whole process. We suggest the experience designer should take into account that users of the system will have dynamic behavior. Consequently, any adaptive or security mechanism proposed for developing should seek for the users safety in future interaction flows.

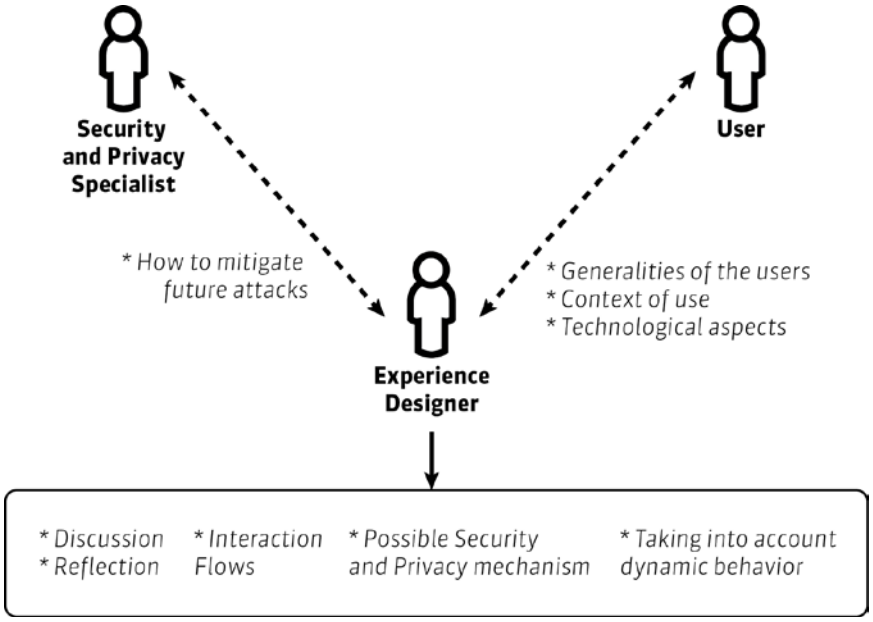

Security and Privacy Specialist
User
* How to mitigate future attacks
* Generalities of the users
* Context of use
* Technological aspects
Experience Designer
* Discussion
* Reflection
* Interaction Flows
* Possible Security and Privacy mechanism
* Taking into account dynamic behavior

Figure 9: Diagram that represents the Security and Privacy principle. Figure by the authors.

Personalization

Users from ICSs usually have different goals, and hence assess the experience differently. For example, a photographer may use Facebook as a professional photography website. He may prefer to keep his photo albums public. In this way, all Facebook members can see his work. On the other hand, other Facebook users may prefer to apply a personal, but systemic, access policy to each of their photo albums. Thus, users should be able to adjust security and privacy according to their preferences.

Personalization is the ability of the system to learn about its users (Mobasher, 2000). It provides the mechanisms of the system to know the characteristics of its users, such as gender, job, preferences, and security and privacy concerns. By considering the heterogeneity of users, the experience designer should be aware their different needs and concerns regarding security (Sheehan, 2000). In fact, among users there is a different understanding of security and privacy (Sheehan, 2002). Some users may see an economical value on security and privacy, whereas others may not.

Personalization enables users to control their security and privacy choices. We propose that the experience designer should consider how personalization will be implemented in the system. Due to personalization, systems should be designed in such a way that users or groups of users can adjust their own ‘sensitivity parameters’ for security and privacy. Intelligent personalization enables these choices to be learned by the system (Anand, 2003). For example, spam filtering should be personalized according to specified user needs.

One possible personalization mechanism is to let users set their privacy settings by giving them a constrained set of technologically appropriate choices. This approach runs the risk of leading to the paradox of choice (Cross, 2004) in which users become confused by too many choices. Another possible mechanism could be achieved by automating personalization via the application of different profiling techniques (Kobsa, 2003). The role of the experience designer is to find a balance between personalization and other elements of the user experience.

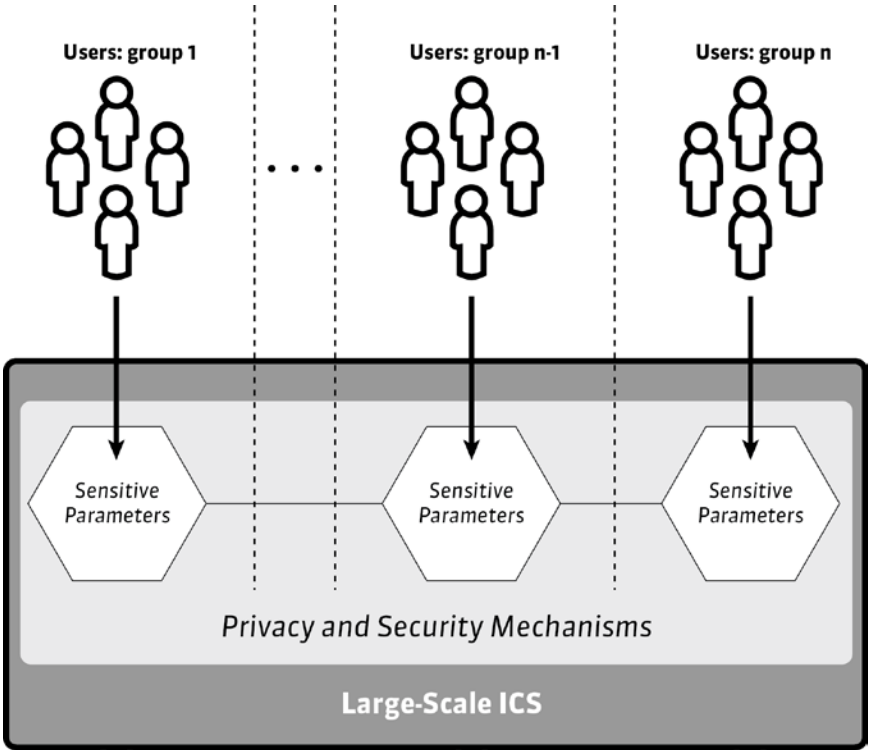


Figure 10: Diagram that represents the Personalization principle. Figure by the authors.

Adaptability

An adaptive system (De Castro, 2006) changes due to several factors, such as the changes in characteristics of its users (Anton, 2010). These changes affect the context of use, since different users have different sensitivities regarding private information, ICSs should adapt to the different users and their attributes. We suggest that the experience designer take into account what security and privacy control mechanisms can be offered to the users in relation to their attributes. We remark that attributes change with the time. The system should recognize any changes in the attributes from the users and adapt to them accordingly. We argue that embedding adaptable algorithms in security and privacy mechanisms enables the ICSs to evolve with changes in the context of use. Adaptability enables the system to respond to these changes efficiently.

Furthermore, adaptability enables system/user coevolution. System/user coevolution (Arondi, 2002) deals with hidden security and privacy requirements beyond user preference. We argue that coevolution (Thompson, 1994) assures that mandatory security and privacy mechanisms are in place and remain in place as individual and system changes occur. For example, an increase in attacks against ICSs may be invisible to a user. However, it requires adaptation from the system. An adaptive algorithm can analyze previous breaches in order to find common patterns (Abi-Haidar & Rocha, 2008), which can be automatically inserted into security and privacy mechanisms.

Adaptability has the potential to predict changes and emerging threats before they happen. Adaptive mechanisms and machine learning techniques can mitigate several security and privacy threats. Intrusion and anomaly detection systems can analyze log files (that describe the system’s past behaviors) by applying machine learning and pattern recognition techniques to predict trends. For example, classification algorithms have been used to differentiate the spam from the ham in email servers (Abi-Haidar, 2008). Adaptability often requires iterative design approaches, as the system changes over time (Ellis, 1998). Mechanism design is one approach to implement adaptive components in a secure system (Nisan, 1992).

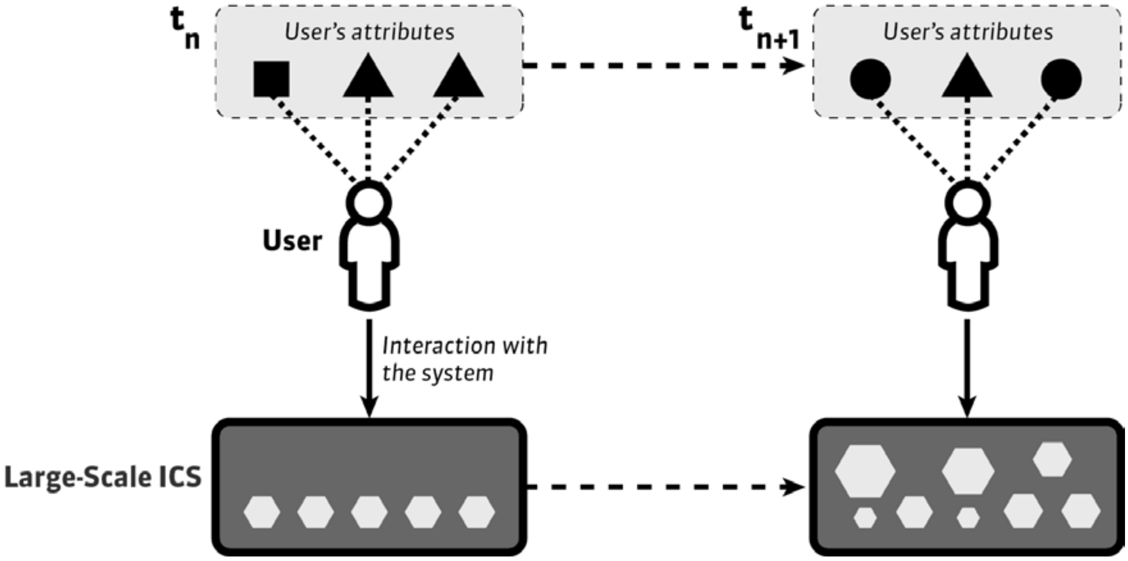


Figure 11: Diagram that represents the Adaptability and Expandability principles. As time passes user's attributes change. Consequently, the system will change in features as well. The system should be prepared to include new Privacy and Security mechanisms for those changes. Figure by the authors.

Expandability

Expandability (Pressman & Jawadekar, 1987) is a capability of the system to have new features, while avoiding the redesign of the whole system, but also applying future customizations. Adaptive systems continuously respond and update themselves when changes occur in the context of use (Holland, 1992). Without expandability a system cannot be adaptable in practice. We argue that the system and its components need to be expandable in the sense that these can be modified to adapt according to environmental changes and any possible new systems requirements. Expandability and customization provide adaptability; thus, drastic redesigns should be avoided, as the system will embrace their 'natural' evolution.

Expandability provides a dynamic nature of the security and privacy in adaptive systems. Thus, we suggest that experience designers should allow for the possibility of future customizations of a system. Further, they should take into account how customization can be automated by adaptable algorithms. Expandability resonates deeply with design theory of sustainable systems (Birkeland, 2002) since expandable systems were built for long-term use. We remark also that expandability is one of the basic requirements of system maintenance. In case of failure, the system should be designed to patch or add a new component to fix the system while affecting as little as possible of the user experience.

Usability

Many security and privacy mechanism have been disregarded by users due to usability problems (Lampson, 2009). For example, encrypted email (PGP) never reached wide utilization due to the complexity of use (Whitten. 1999). We argue that the experience designer should take into account the usability of security and privacy mechanisms by users with different levels of knowledge and technological literacy. For example, the secure communication protocol *https* was once available in Gmail. However, this feature was disabled by default. Many users were never aware of the existence of this feature.

Experience designers should account usability for enhancing the ways the system informs its users about the security and privacy mechanisms available. The system should provide a guideline and encourage users to apply security and privacy mechanisms. It is important that users get information about the security and privacy risks in order to know whether and when they want to use these mechanisms. For example, the explicit risks of security and privacy breaches should be clear to the user. This creates personal incentives for security and privacy awareness.

Creating clear and unambiguous privacy and security policy is essential (Nielsen, 1994). Currently, security and privacy policies are often vague, unreadable, and do not gain the attention of the users (Anton, 2004). Clarity in policies becomes more crucial as security and privacy policies get more complex, personal data gets more sensitive, and usage scenarios differ between different stakeholders. System operators are seeking to profit from sharing private data, but users are seeking to limit access. Another important thing that should be cleared in the policy is how government regulations impact the security and privacy of the users. Policy should be written with no hint of evasiveness. If ICSs did not have to digress so much in their policy descriptions, then users would have been more thoughtful about what information they put in these media. ICSs have been used for data collection purposes as well. Since collected data can include sensitive information about users, the ICCs should be clear about their data collection policies.

However, the usability of the system should not be compromised by the ability of the users for managing or applying the security and privacy mechanisms available. Adaptive design for security and privacy can increase the usability of the system for at least two reasons. First, by considering personalization, adaptability, and user coevolution, the system will be aware of how users can manage their security and privacy. Second and more importantly is that with the adaptive design we proposed, the development of a system that can preserve its own safety with little involvement from its users.

In the domain of security, it is particularly difficult to define usability approaches at the initial stages of the design process, since it is unlikely to understand the users, their tasks, the contexts of use, or even their individual approaches (Kensing, 1998). We suggest that the experience designer should foresee how and on which measure the future adaptations of the system will be able to control any of the security and privacy mechanisms in the background. Thinking about adaptive design implies thinking about mechanisms that learn. In turn, the latter implies that a policy can be defined according to what is acceptable in a particular context of use.

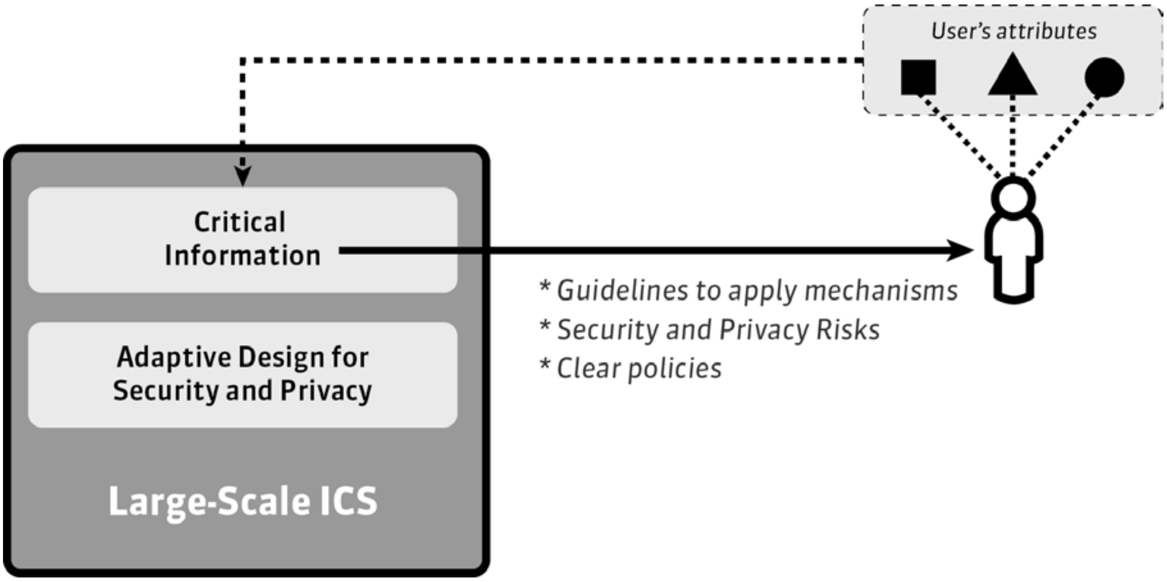

User's attributes
Critical Information
Adaptive Design for Security and Privacy
Large-Scale ICS
* Guidelines to apply mechanisms
* Security and Privacy Risks
* Clear policies

Figure 12: Diagram that represents the Usability and Avoid Unintentional Disclosure principles. Figure by the authors.

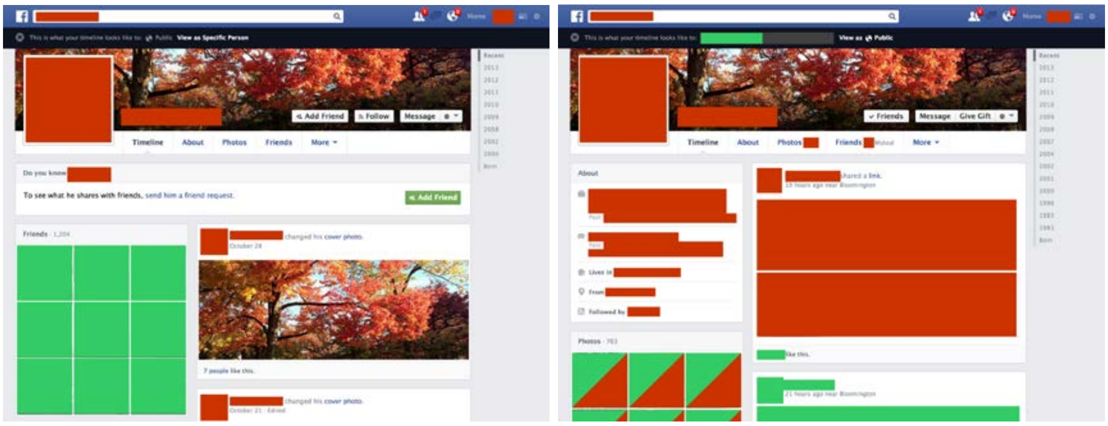
Avoid unintentional disclosure

Accidental disclosure of private information has come to be known as “Misclosure” (Caine, 2009). Misclosures may happen in various ways. People can disclose certain information about themselves unintentionally. We find an unintentional disclosure of private data as a possible hidden privacy threat. Users remain concerned about losing control over their personal data even after it has been already disclosed (Smith, 1996). In particular, social networks practically reveal private data from their users in an automatic fashion. The latter occurs because of the lack of complex inference mechanisms or statistical analysis within the system in order to properly address the users’ performance. The experience designer should be aware of the possibilities of unintentional disclosure of data by means of inference. These issues and their consequences for the user experience should be discussed.

One of the main security and privacy concerns in ICSs is that controlling the privacy of users does not depend on the users themselves. The experience designers should be aware of possible relations among users, how disclosure can occur as consequence of those relations, and how that disclosure can affect the users. By considering an adaptive design for an ICS, experience designers can glimpse scenarios where the system prevents disclosures of private data from any user. In general, the principles that we have proposed so far will result in considering a design rationale for decreasing unintentional disclosures of data by showing the design concerns at the interaction time. For example, policies to be shown during the interaction can clarify to users how their data will be collected and distributed.

Case study

In this section we study Facebook as a large-scale information system. We explain how we can enhance this technology by considering our design principles. Personally identifiable data is visible and accessible on users’ profiles. It consists of a user’s name, status updates, wall comments, profile photo, photo albums, date of birth, phone number, email address, college name, residence, address, dating preferences, relationship status, political views, and interests related to music, books, movies, along with their list of friends. If a Facebook user fills in her profile page, it will contain approximately 40 pieces of personally identifiable information (Grimmelmann, 2009). We perform a threat analysis to find the security and privacy threats of Facebook. Then we show how proposed principles can be applied in design process to mitigate the risks of these threats.



This is what your timeline looks like to: Public View as Specific Person

Do you know

To see what he shares with friends, send him a friend request.

changed his cover photo.

October 24

7 people like this.

changed his cover photo.

October 21 · Edited

This is what your timeline looks like to: View as Public

shared a link.

like this.

Figure 13: A feature on Facebook that shows the amount of information disclosed depending on the type of user. In red is covered the potential user’s information whereas friends’ information is covered by color green. Left: the appearance of the “public” timeline. Right: the appearance of the same user’s timeline for a friend of her. Image by the authors

Security and privacy matters

Spam, *scam*, *phishing*, and *malware* applications are some of the common security and privacy threats to social networks (Fong, 2009). These common threats result in a hidden threat of expediting the spread of malicious applications. Social networks facilitate the spread of these malicious applications through users' contacts, friends, and followers. Facebook does not have an effective mechanism to manage malicious third party applications or scam advertisements. However, embedding scam/spam detection applications in Facebook's logic layer can alleviate these threats.

Personalization

Facebook is quite successful at providing personalization by implementing role-based access. Users can create groups of friends and control their access to wall posts, photos, and profile information. Users can control the posts in their wall; however, they are not able to control posts about them on other users' walls. Thus, if a user is reckless about his privacy setting, he can threaten other people's privacy in his network. What is missing in Facebook's personalized security and privacy is the lack of an automatic mechanism to detect potential changes in users' preferences. Additionally, systems can learn about the users' preferences and apply them in the future interactions.

Adaptability

Facebook has already implemented filters to detect bogus profiles and spam accounts. These filters work based on users' reports of a fake profile. In addition to relying on users' reports, Facebook can implement a mechanism to detect trustworthy accounts from bogus accounts. This mechanism can study user behavior and identify benevolent behavioral patterns from unacceptable or suspicious behaviors. Similar treatment can be used to avoid malware, scams, and malicious advertisements.

Adaptive mechanisms can recognize possible intrusion signals or sources of malware spread within the networks. For example, a user with lots of connections can be the source of spread. Facebook can co-evolve through time by interacting with users and learning about their privacy concerns and needs. For example, users should be able to report misbehavior of other users if they are publishing their information.

Expandability

Facebook has been changed drastically from its earlier release. These changes are mostly due to enhancing its usability or patching security and privacy breaches. These changes are not dynamic and they have not constructed automatically. The goal of adaptive design is providing the autonomy for the system. Thus, it helps the system to build new structures or to detect the necessity of adding a new application.

Usability

In spite of the importance of usability, sometimes experience designers do not consider the need to design usable security and privacy mechanisms; this can be due to limited time to release the product. For example, several security and privacy control mechanisms are not enabled by default in Facebook. If users were not aware of these mechanisms they would not activate them. Earlier releases of Facebook had very few security and privacy treatments. They were also not visible to users. For example, in order to make a user's profile only accessible to her friend list, users were required to adjust about 50 items in their privacy settings. However, Facebook has recently provided a menu indicating five different levels of privacy such as 'Public', 'Friends', 'Only me', and 'Custom'.

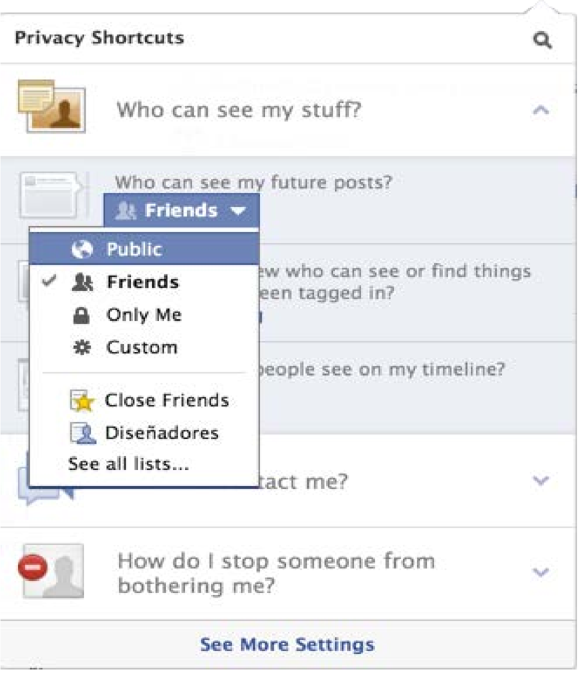
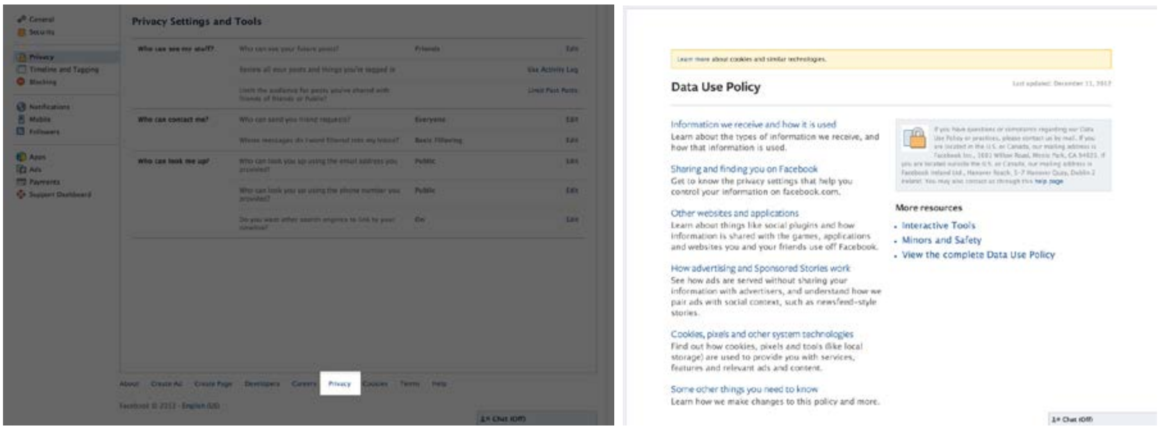


Figure 14: Menu of privacy shortcuts currently available in Facebook. Image by the authors.

Facebook should provide a user-friendly tutorial that overviews its policies. This tutorial may also include strategies or mechanisms to mitigate privacy risks. Moreover, they can teach users about security and privacy threats and new settings or mechanisms related to security and privacy protection. This could be accomplished by showing them dialog boxes each time they sign in to their profile.

We carefully read and analyzed Facebook's privacy policy. Although Facebook publishes its policies in the Facebook's Privacy Policy section, more user-friendly guidelines that use descriptive language are needed, so that every user could understand the meaning of each policy. Some policies have been vaguely written in order to hide their main meaning from users. Due to the sensitivity of the information that people may post on their personal profiles, Facebook should avoid posting such a vague policy. Over the past few years Facebook has changed its default privacy settings. However, users have not received any notice from Facebook about these policy changes. Facebook could easily announce any policy changes to its users beforehand.



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
	Whose messages do I want filtered into my Inbox?	Basic Filtering	Edit
Who can look me up?	Who can look you up using the email address you provided?	Public	Edit
	Who can look you up using the phone number you provided?	Public	Edit
	Do you want other search engines to link to your timeline?	On	Edit

Learn more about cookies and similar technologies.

Data Use Policy

Last updated: December 11, 2012

Information we receive and how it is used
Learn about the types of information we receive, and how that information is used.

Sharing and finding you on Facebook
Get to know the privacy settings that help you control your information on facebook.com.

Other websites and applications
Learn about things like social plugins and how information is shared with the games, applications and websites you and your friends use off Facebook.

How advertising and Sponsored Stories work
See how ads are served without sharing your information with advertisers, and understand how we pair ads with social context, such as newsfeed-style stories.

Cookies, pixels and other system technologies
Find out how cookies, pixels and tools (like local storage) are used to provide you with services, features and relevant ads and content.

Some other things you need to know
Learn how we make changes to this policy and more.

If you have questions or complaints regarding our Data Use Policy or practices, please contact us by mail. If you are located in the U.S. or Canada, our mailing address is Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025. If you are located outside the U.S. or Canada, our mailing address is Facebook Ireland Ltd., Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland. You may also contact us through this help page.

More resources

- Interactive Tools
- Minors and Safety
- View the complete Data Use Policy

Figure 15: By clicking on "See more settings" of the menu shown in Fig. 14, the user can click on "Privacy" (left) at the bottom of the screen for accessing to the privacy policy (right). Image by the authors.

Avoid unintentional disclosure

Facebook users sometimes reveal critical security information in their profile such as their mother's maiden name or date of birth. This information then can be used to infer sensitive information such as the secret code of their credit cards. To take another example, Facebook users' posts or status updates may not contain privacy critical data at time the users posted them, but these statuses can be retrieved and analyzed in the future. If a potential employer looks at an applicant's Facebook wall posts, he may find potential applicants are unprofessional and refuse to offer the job on that basis.

We find that on Facebook, even if a user makes all the information in his profile private and only provides read access to others, his privacy can still be threatened by other users. A Facebook user cannot control posted information about him in other users' profiles. For example, Facebook users cannot define a setting to prevent other users from posting or tagging their photos. A possible mechanism that could mitigate unintentional disclosures of data could be sent out by email to a user to get her confirmation before publishing a post, photo, or comments about her.

Implications for Design

We argue that secure large-scale ICSs introduce a series of challenges to experience design. Pursuing the traditional approach in experience design is not sufficient to design all the complex aspects of ICSs. Experience designers acknowledge the importance of people's needs in the different contexts of use (Bødker, 2006; Forlizzi & Battarbee, 2004). However, the nature of ICSs and the complexity of security and privacy requirements entail a further dimension in terms of experiences and contexts.

For example, users are distinguishable due to their different privacy and security. Variation in users' security and privacy concerns can be due to several aspects such as their informational and technological literacy, socio-cultural values, and emotional triggers. Although these aspects might be hard to measure, they are relevant to experience designers to understand the relation between the users, the system, and its context of use. As we explained in the introduction section, secure ICSs are complex systems that impose several challenges to experience designers. The Complex Systems properties inherent in ICSs adds a major complexity for both the design problem and solution, comprehended as a whole (Schön, 1990), since thinking of a given context is not enough. Experience designers have as one of their goals to support situated actions (Harrison, Tatar, & Sengers, 2007). However, ICSs introduce challenges that make such approaches difficult to follow.

By participating in the design of ICSs, experience designers also deal with ICTs a relevant factor to consider during the process. Designing technological products either in the form of software or hardware face more complexity since the underlying technological infrastructure is rapidly growing and changing even in a short period of time. Technological factors such as the proliferation of mobile devices, advances in hardware, and the increasing of Internet bandwidth can influence experience designers in how to frame the design situation and how to come up with a design solution. For example, accessing ICSs through mobile phones create further security and privacy concerns, which are new to using ICSs through the computers.

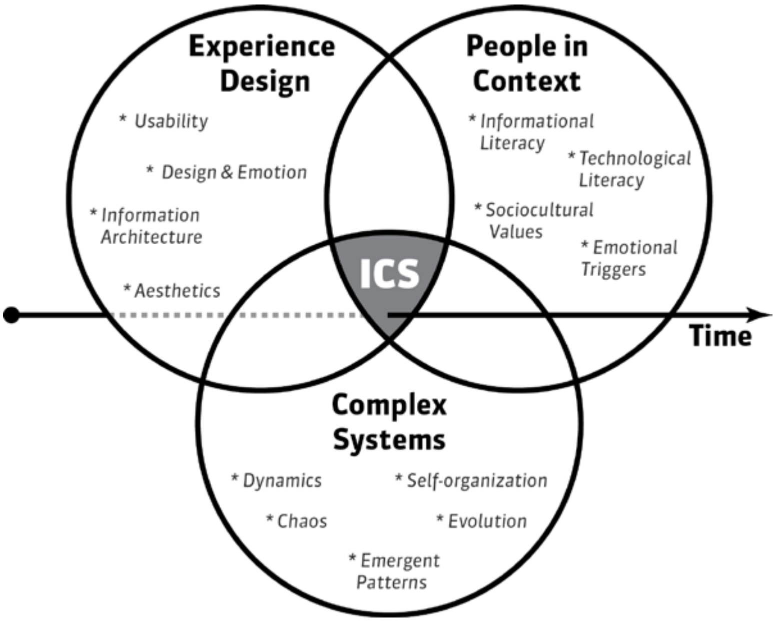


Figure 16: Design space in which ICSs belong. Figure by the authors.

ICSs create the ecosystem in which users and systems coevolve. Users learn about the system and potential system usage through the time. Systems can change users' behaviors and awareness; in particular, privacy concerns of users grow with time. Future users' needs can results in future system changes. User-system coevolution is a significant feature of ICSs. In designing such a system, experience design practitioners and scholars face new properties of a system that are e.g. dynamic, self-organized, emergent, unpredictable, and evolvable. We remark that current approaches for experience design, such as the hierarchical modeling of user archetypes and their goals (Pruitt & Adlin, 2006) is not sufficient to design a co-evolutionary properties of ICSs. We believe that experience design for ICSs can open the door to explore new design-oriented approaches to consider system-user coevolution and heterogeneity of users.

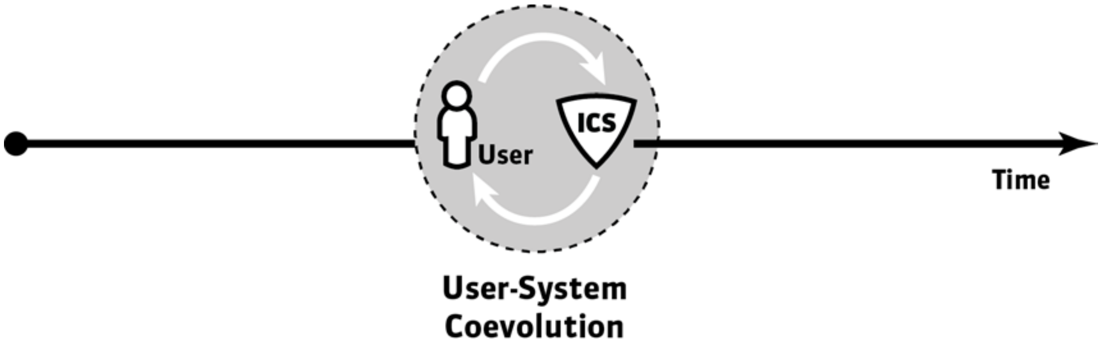


Figure 17: Experience design for ICSs takes into account the relation of security and privacy aspects and user-system coevolution. Figure by the authors.

Security and privacy of ICSs has both user-centered and system-center aspects. Security of the system is important since system should not break and should not be misused for malicious purpose. Security and privacy of users are important to preserve the confidentiality and authenticity of the information. Security and privacy have been widely studied in Computer Science. Several security and privacy threats of ICSs have been recognized and their mitigation mechanisms have been introduced. But security and privacy issues that result from system dynamics and user-system coevolution have not been fully recognized. However, it is worth to mention that security specialists often are not familiar with the type of competences that designers have (Nelson & Stolterman, 2012), which are relevant in terms of user experience

We argue that experience designers are capable of embracing the complexity of secure large-scale ICSs and also create a bridge with the discipline of Security and Privacy, due to three main reasons. First, experience design practitioners have been trained to consider the problem and solution as a whole (Schön, 1990). Second, experience designers have been trained to manage the relationship among the client, stakeholders, and users, in such way that foregrounds users. Third, experience designers understand the critical role of communication as part of the design process, and hence they are accustomed to play role of facilitators or mediators (Nelson & Stolterman, 2012; Yee et al., 2009; Aakhus, 2007; Pericot, 2006).

We remark the need for a ***translation*** of the technical knowledge generated by security and privacy specialists. Experience designers can contribute to the designing of secure large-scale ICSs not only by establishing a dialog with the specialists in security and privacy, but also by finding the appropriate means to communicate the aforementioned complexity in order to inform the design process. We refer to communication as a means for transferring knowledge from the security and privacy field into the design field. Consequently, the design competences of the practitioners would be extended. Therefore, *being a translator* might be a valuable component for the conformation of the *repertoire* (Schön, 1987) of an experience designer.

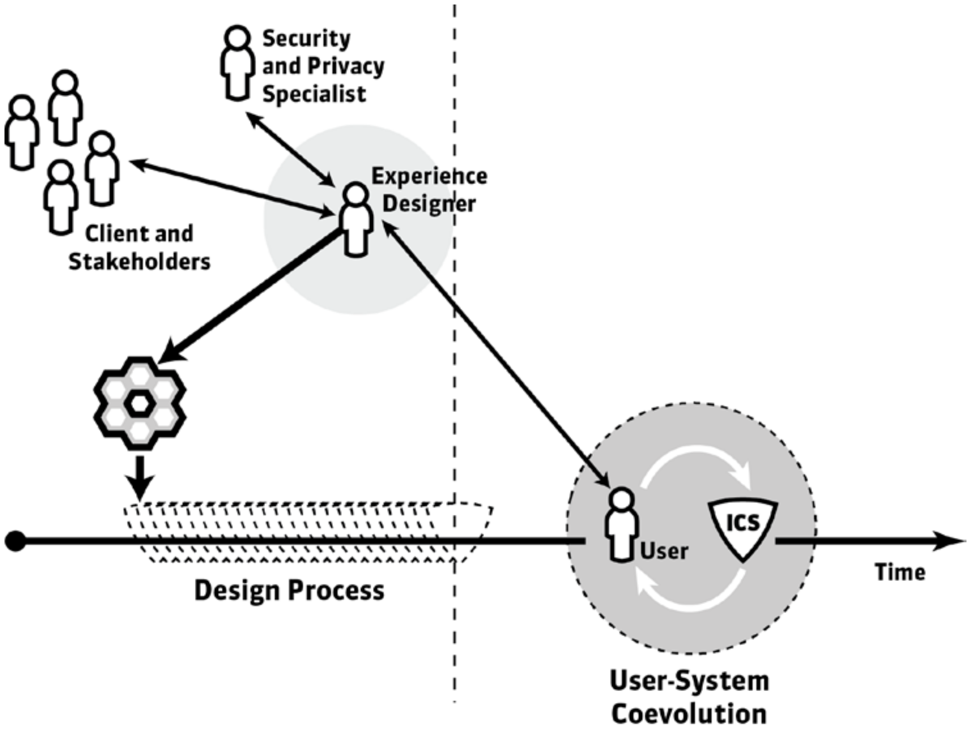


Figure 18: The role of the experience designer in the design of Large-Scale ICSs. Figure by the authors.

The proposed framework is an attempt for advocating the mentioned translation. We conceptualize each principle of the framework as a hub, in which an ‘initial translation’ is presented. Taking the explanation for each principle as a basis, the experience designer has the responsibility of creating links between issues of security and privacy, complex systems, and experience design. The resulting *network* is in turn a *mental schema* (Arbi, 1992; McVee, Dunsmore, & Gavelek, 2005) which encapsulates the framing of the current problem in terms of secure ICSs and complex systems. Knowing how to externalize this schema is critical for the translation. The designer can explore the proposed principles one by one and communicate the mental schema to the audience. Design schemas (Nelson & Stolterman, 2012) or schematic sketches might be an adequate medium for such task, either to be employed before team members, client, or stakeholders of the actual ICSs design project.

Conclusions and Future Work

In this paper we introduced an experience design framework for securing large-scale information and communication systems (ICSs). We remarked that as a consequence of having heterogeneity of users, diverse contexts of use, changes in the technological infrastructure, and evolvable use scenarios, large-scale ICSs (e.g. social networks) can be described as Complex Systems. Although designers are familiar with dealing with the "design as a wicked problems" (Rittel, 1973), the notions of complex systems and large scale ICSs, including their issues on security and privacy, might not be a part of design-oriented disciplines.

We presented basic properties found in complex systems, namely: dynamics, self-organization, emergence, and evolution. From our analysis about complex systems and experience design we elaborated a framework constituted by six security and privacy principles, in which we settle the basis for a translation of the knowledge already developed by specialists of security and privacy to be embedded in the field of experience design. Our framework allowed us to see the relevance of this type of translation as part of the *repertoire* (Schön, 1987) of an experience designer. Furthermore, we glimpse the relation of experience design with other design fields (e.g. sustainable design) for the case of ICSs. We find our framework as a contribution to start a conversation among design practitioners and scholars about how the current approaches for experience design require accounting the complexity and its implications inherent in the ICSs.

As an exploratory work for bringing the notion of complex systems, heterogeneity of users, user-system coevolution, security and privacy, and experience design, we recognize the limitations of this work. Our framework hasn't been assessed within a design process. An expert in both of the fields of Security and Privacy and Complex Systems carried out the analysis for the case study presented in this work. We have divided our future work in two main agendas. The first one is the assessment of the framework itself. For instance, the case of Google Glass requires an expansion or rethinking of the current framework since the issues of privacy and security affect not only its users, but also to the actual people within the context of use—the people that can be captured by the glasses. One approach we are considering is to set a dialog with experience designers in order to discuss issues of ICSs and our framework. Our second point in the agenda is related with Design Pedagogy. We are interested in observing the potential and limitation of the current framework in a studio oriented experience design course (Blevis et al., 2007; Hundhausen et al., 2012, 2011, 2010; Sosa-Tzec et al., 2013). In this regard, our aim is to find pedagogical issues, and hence to elaborate possible guidelines to teach all the ideas mentioned in this work. In other words, it is our intention to contribute to the development of a *design-oriented thinking* (Siegel & Stoterman, 2009) and design competences, to foster reflection (Schön, 1983), and the relevance of communication during the conformation of the design repertoire (Schön, 1983). Other aspects of either complex systems or ICSs can be discussed in relation with experience design. Conversely, setting a profound background on the phenomenology of experience design –or any other aspects considered as a part of experience design– in relation with complex systems, heterogeneity of users, or user-system coevolution, might bring interesting insights for design theory.

References

Abi-Haidar, A., & Rocha, L. M. (2008). Adaptive Spam Detection Inspired by the Immune System. In *ALIFE* (pp. 1-8).

Agarwal, A., & Meyer, A. (2009, April). Beyond usability: evaluating emotional response as an integral part of the user experience. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems* (pp. 2919-2930). ACM.

Anand, S. S., & Mobasher, B. (2003, August). Intelligent techniques for web personalization. In *Proceedings of the 2003 international conference on Intelligent Techniques for Web Personalization* (pp. 1-36). Springer-Verlag.

Anton, A. I., Earp, J. B., He, Q., Stufflebeam, W., Bolchini, D., & Jensen, C. (2004). Financial privacy policies and the need for standardization. *Security & Privacy, IEEE*, *2*(2), 36-45.

Anton, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *Security & Privacy, IEEE*, *8*(1), 21-27.

Arbib, M. A. (1992). Schema Theory, in the *Encyclopedia of Artificial Intelligence*, Editor Stuart Shapiro, 2: 1427-1443. Wiley.

Arondi, S., Baroni, P., Fogli, D., & Mussio, P. (2002, May). Supporting co-evolution of users and systems by the recognition of Interaction Patterns. In*Proceedings of the Working Conference on Advanced Visual Interfaces* (pp. 177-186). ACM.

Aakhus, M. (2007). Communication as design. *Communication Monographs*, 74(1), 112-117.

Ashby, W. R. (1962). Principles of the self-organizing system. *Principles of Self-organization*, 255-278.

Bardzell, J. (2009, April). Interaction criticism and aesthetics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2357-2366). ACM.

Birkeland, J. (2002). *Design for Sustainability: A Sourcebook of Integrated Ecological Solutions*. Earthscan.

Bishop, M. A. (2002). *The art and science of computer security*.

Blevis, E., Lim, Y. K., Stolterman, E., Wolf, T. V., & Sato, K. (2007, April). Supporting design studio culture in HCI. *In CHI'07 Extended Abstracts on Human Factors in Computing Systems* (pp. 2821-2824). ACM.

Bolchini, D., Colazzo, S., Paolini, P., & Vitali, D. (2006, October). Designing aural information architectures. In *Proceedings of the 24th annual ACM international conference on Design of communication* (pp. 51-58). ACM.

Bødker, S. (2006, October). When second wave HCI meets third wave challenges. In *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles* (pp. 1-8). ACM.

Brusilovsky, P. (2001). Adaptive hypermedia. *User modeling and user-adapted interaction*, *11*(1-2), 87-110.

Caine, K. E. (2009, April). Supporting privacy by preventing misclosure. In*CHI'09 Extended Abstracts on Human Factors in Computing Systems* (pp. 3145-3148). ACM.

Camazine, S. (Ed.). (2003). *Self-organization in biological systems*. Princeton University Press.

Camp, L. J. (2003). Designing for trust. In *Trust, Reputation, and Security: Theories and Practice* (pp. 15-29). Springer Berlin Heidelberg.

Camp, L. J., & Wolfram, C. (2000, October). Pricing security. In *Proceedings of the CERT Information Survivability Workshop* (pp. 31-39).

Clifton, C., & Marks, D. (1996, May). Security and privacy implications of data mining. In *ACM SIGMOD Workshop on Research Issues on Data Mining and Knowledge Discovery* (pp. 15-19).

Cross, N. (2004). Expertise in design: an overview. *Design studies*, *25*(5), 427-441.

Crutchfield, J., Nauenberg, M., & Rudnick, J. (1981). Scaling for external noise at the onset of chaos. *Physical Review Letters*, *46*(14), 933.

De Castro, L. N. (2006). *Fundamentals of natural computing: basic concepts, algorithms, and applications*. CRC Press.

Devaney, R. L. (2003). An introduction to chaotic dynamical systems.

Ding, W., & Lin, X. (2009). Information Architecture: The Design and Integration of Information Spaces. *Synthesis Lectures on Information Concepts, Retrieval, and Services.* 1(1). Morgan & Claypool.

Eckmann, J. P., & Ruelle, D. (1985). Ergodic theory of chaos and strange attractors. *Reviews of modern physics*, *57*(3), 617.

Ellis, R. D., Jankowski, T. B., & Jasper, J. E. (1998). Participatory design of an Internet-based information system for aging services professionals. *The Gerontologist*, *38*(6), 743-748.

Ehrlich, P. R., & Raven, P. H. (1964). Butterflies and plants: a study in coevolution. *Evolution*, 586-608.

Fong, P. W., Anwar, M., & Zhao, Z. (2009). A privacy preservation model for facebook-style social network systems. In *Computer Security–ESORICS 2009*(pp. 303-320). Springer Berlin Heidelberg.

Forlizzi, J., & Battarbee, K. (2004, August). Understanding experience in interactive systems. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques* (pp. 261-268). ACM.

Friedman, B., Hurley, D., Howe, D. C., Nissenbaum, H., & Felten, E. (2002, April). Users' conceptions of risks and harms on the web: a comparative study. In *CHI'02 extended abstracts on Human factors in computing systems* (pp. 614-615). ACM.

Funtowicz, S., & Ravetz, J. R. (1994). Emergent complex systems. *Futures*,*26*(6), 568-582.

Garrett, J. J. (2010). *Elements of User Experience, The: User-Centered Design for the Web and Beyond.* Pearson Education.

Grimmelmann, J. (2009). Saving facebook. *Iowa Law Review*, *94*, 1137-1206.

Harrison, S., Tatar, D., & Sengers, P. (2007, April). The three paradigms of HCI. In *Alt. Chi. Session at the SIGCHI Conference on Human Factors in Computing Systems* San Jose, California, USA (pp. 1-18). ACM. Retrieved from http://people.cs.vt.edu/~srh/Downloads/HCIJournalTheThreeParadigmsofHCI.pdf

Hebig, R., Giese, H., & Becker, B. (2010, June). Making control loops explicit when architecting self-adaptive systems. In *Proceedings of the second international workshop on Self-organizing architectures* (pp. 21-28). ACM.

Heims, S. J. (1991). *The cybernetics group*. MIT Press (MA).

Hundhausen, C. D., Fairbrother, D., & Petre, M. (2012). An empirical study of the “prototype walkthrough”: a studio-based activity for HCI education. *ACM Transactions on Computer-Human Interaction (TOCHI),* 19(4), 26.

Hundhausen, C., Fairbrother, D., & Petre, M. (2011). The prototype walkthrough: a studio-based learning activity for human-computer interaction courses. *In Proceedings of the seventh international workshop on Computing education research* (pp. 117-124). ACM.

Hundhausen, C., Agrawal, A., Fairbrother, D., & Trevisan, M. (2010). Does studio-based instruction work in CS 1?: an empirical comparison with a traditional approach*. In Proceedings of the 41st ACM technical symposium on Computer science education (pp. 500-504)*. ACM.

Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, *121*(1), 17-30.

Kagal, L., Finin, T., Joshi, A., & Greenspan, S. (2006). Security and privacy challenges in open and dynamic environments. *Computer*, *39*(6), 89-91.

Kensing, F., & Blomberg, J. (1998). Participatory design: Issues and concerns.*Computer Supported Cooperative Work (CSCW)*, *7*(3-4), 167-185.

Klir, G. J. (2001). *Facets of systems science* (Vol. 15). Springer.

Khondker, H. H. (2011). Role of the new media in the Arab Spring.*Globalizations*, *8*(5), 675-679.

Kobsa, A., & Schreck, J. (2003). Privacy through pseudonymity in user-adaptive systems. *ACM Transactions on Internet Technology (TOIT)*, *3*(2), 149-183.

Krug, S. (2010). *Rocket surgery made easy. The do-it yourself guide to finding and fixing usability problems*. New Riders.

Lampson, B. (2009). Privacy and security Usable security: how to get it.*Communications of the ACM*, *52*(11), 25-27.

Law, E. L. C., Roto, V., Hassenzahl, M., Vermeeren, A. P., & Kort, J. (2009, April). Understanding, scoping and defining user experience: a survey approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 719-728). ACM.

Law, E. L. C. (2011, June). The measurability and predictability of user experience. In *Proceedings of the 3rd ACM SIGCHI symposium on Engineering interactive computing systems* (pp. 1-10). ACM.

Leveson, N. G. (1995). *Safeware: system safety and computers*. ACM.

McCarthy, J., & Wright, P. (2004). *Technology as experience*. MIT Press.

McVee, M. B., Dunsmore, K., & Gavelek, J. R. (2005). Schema theory revisited. *Review of Educational Research*, 75(4), 531-566.

Mobasher, B., Cooley, R., & Srivastava, J. (2000). Automatic personalization based on Web usage mining. *Communications of the ACM*, *43*(8), 142-151.

Morville, P., & Rosenfeld, L. (2008). *Information architecture for the World Wide Web: Designing large-scale web sites.* O'Reilly Media, Inc..

Mouratidis, H., Giorgini, P., & Manson, G. (2003, January). Integrating security and systems engineering: Towards the modelling of secure information systems. In *Advanced Information Systems Engineering* (pp. 63-78). Springer Berlin Heidelberg.

Nelson, H. G., & Stolterman, E. (2012). *The Design Way: Intentional Change in an Unpredictable World.* MIT Press.

Nielsen, J. (1994). Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods, John Wiley & Sons, New York, NY.

Nisan, N., & Ronen, A. (1999, May). Algorithmic mechanism design. In*Proceedings of the thirty-first annual ACM symposium on Theory of computing*(pp. 129-140). ACM.

Norman, D. A. (2007). *Emotional design: Why we love (or hate) everyday things.* Basic books.

Ozcelik Buskermolen, D., & Terken, J. (2012, August). Co-constructing stories: a participatory design technique to elicit in-depth user feedback and suggestions about design concepts. In *Proceedings of the 12th Participatory Design Conference: Exploratory Papers, Workshop Descriptions, Industry Cases -Volume 2* (pp. 33-36). ACM.

Oppelaar, E. J. R., Hennipman, E. J., & van der Veer, G. C. (2008, January). Experience design for dummies. In *Proceedings of the 15th European conference on Cognitive ergonomics: the ergonomics of cool interaction* (p. 27). ACM.

Pericot, J. (2006) The designer as formalizer and communicator of values. *Temes de disseny*, (23), 96-109.

Pressman, R. S., & Jawadekar, W. S. (1987). Software engineering. *New York 1992*.

Prigogine, I. (1985). New perspectives on complexity. *The Science and Praxis of Complexity*, 483-492

Pruitt, J., & Adlin, T. (2006). *The persona lifecycle: keeping people in mind throughout product design.* Morgan Kaufmann.

Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy sciences*, 4(2), 155-169.

Rosen, R. (1987). On complex systems. *European Journal of Operational Research*, *30*(2), 129-134.

Rosenbaum, S., Wilson, C. E., Jokela, T., Rohn, J. A., Smith, T. B., & Vredenburg, K. (2002, April). Usability in Practice: user experience lifecycle-evolution and revolution. *In CHI'02 extended abstracts on Human factors in computing systems* (pp. 898-903). ACM.

Schön, D. A. (1987). *Educating the reflective practitioner*. San Francisco: Jossey-Bass.

Schön, D. A. (1990). The design process. *Varieties of thinking*, 110-141.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of*

Public Policy & Marketing, *19*(1), 62-73.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21-32.

Siegel, M. & Stolterman, E. (2008). “Metamorphosis: Transforming Non-designers into Designers”, *DRS Conference*, July, Sheffield, 2008.

Simon, H. A. (1962). The architecture of complexity. *Proceedings of the American philosophical society*, *106*(6), 467-482.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Sonderegger, A., & Sauer, J. (2010). The influence of design aesthetics in usability testing: Effects on user performance and perceived usability. *Applied Ergonomics*, 41(3), 403-410.

Sosa-Tzec, O., Beck, J. E., Siegel, M. A. (2013). Building the Narrative Cloud: Reflection and Distributed Cognition in a Design Studio. *DRS // Cumulus 2013. 2nd International Conference for Design Education Researchers.*

Thompson, J. N. (1994). *The coevolutionary process*. University of Chicago Press.

Tunick, M. (2013). Privacy and Punishment. *Social Theory and Practice*, *39*(4), 643-668.

Tullis, T., & Albert, W. (2010). *Measuring the user experience: collecting, analyzing, and presenting usability metrics*. Morgan Kaufmann.

Vogel, M. (2013). Temporal Evaluation of Aesthetics of User Interfaces as one Component of User Experience. In *Proceedings of the Fourteenth Australasian User Interface Conference (AUIC2013)* (pp. 131-132). ACM.

Weaver, W. (1948). Science and complexity. *American scientist*, *36*(4), 536-544.

Wiener, N. (1948). Cybernetics; or control and communication in the animal and the machine.

Whitten, A., & Tygar, J. D. (1999, August). Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium* (Vol. 99). McGraw-Hill.

Wright, P., Wallace, J., & McCarthy, J. (2008). Aesthetics and experience-centered design. *ACM Transactions on Computer-Human Interaction (TOCHI)*,15(4), 18.

Wright, P., & McCarthy, J. (2010). Experience-centered design: designers, users, and communities in dialogue. *Synthesis Lectures on Human-Centered Informatics*, 3(1), 1-123.

Yee, J., Tan, L., and Philip, M. (2009) The emergent roles of a designer in the development of an e learning service. *In: First Nordic Service Design Conference*, 24-26 November 2009, School of Architecture and Design, Oslo