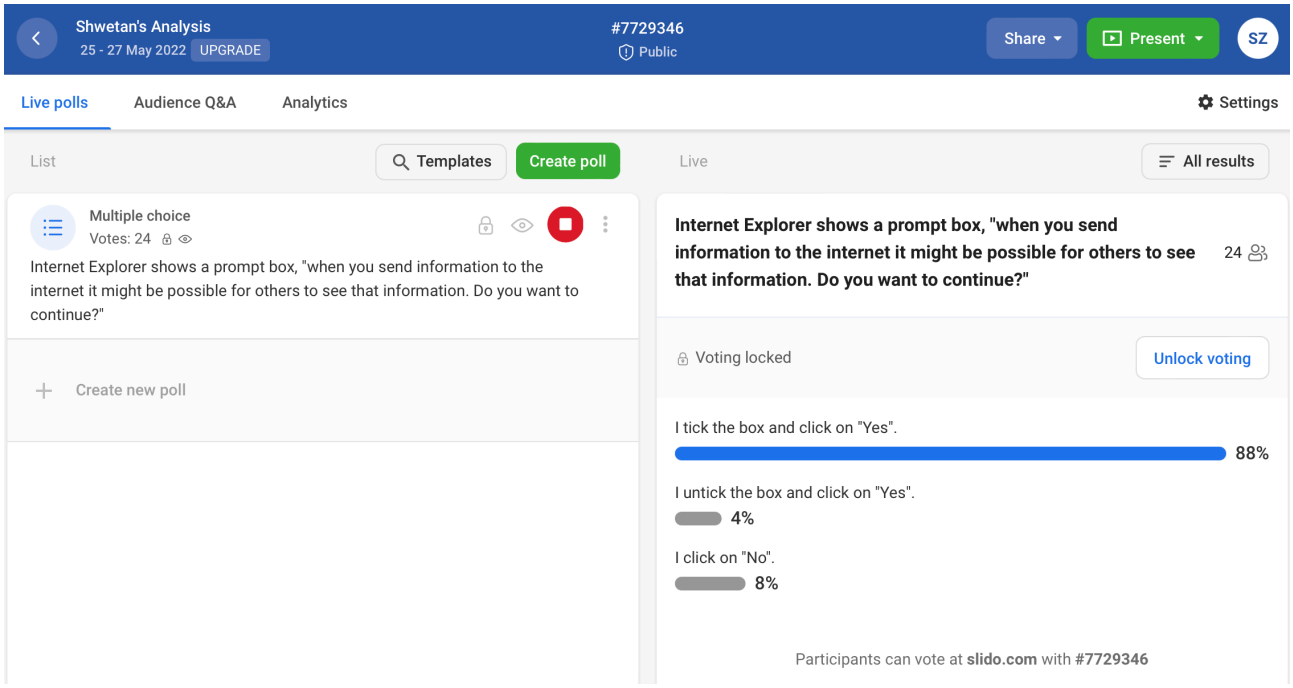
## 1. Introduction

IT systems and services need security, privacy, and usability. Users and authorities want secure, private systems. Security and privacy controls should not burden workflows and be user-friendly. This challenge requires close user engagement during development and runtime. In this essay, I provide a user-centred paradigm for usable security and privacy that aligns with UCD standards [34] and the HCD methodology [28]. I provide a way for designing practical security systems based on this paradigm. The concept and method let developers find and fix security and privacy flaws with user input. My research is motivated by an IoT/smart house situation. Usability and privacy are important due to the volume of private data and rigorous data protection laws. My idea and method aren't restricted to smart homes and can be used whenever usable security and privacy are important for a system.

IT systems have crucial and intrinsic quality attributes such as security, privacy, and usability. However, optimising all qualities at the same time is often difficult [8]. Systems must be sufficiently safe and respect users' privacy in order to be trusted from the users' perspective. At the same time, the systems must be usable, particularly the security procedures they provide. Security and privacy-enhancing technologies, on the other hand, are by their very nature complex, and they frequently complicate operations. As a result, they often have a negative influence on usability [45, 46], for example, in terms of efficiency. In other terms, if the security isn't convenient, people would either not do it or they will prompt a risk to the organisation/themselves. I did a small survey with 24 people, few were random, some were my friends and some were my security-focused classmates. And here is the result, https://app.sli.do/event/eCR2HBJzjRYpENtWoJ65fy (I have attached the screenshot below as well in case the link doesn't work)




Based on my poll results, we can see that 88% of people wanted convenience and didn't bother to understand the risk behind that simple prompt box. And I'm sure that those 8%, who were cautious about sending their information are my fellow Information Security classmates.

### *1.1 My Ideas*

We propose a methodology that focuses on user privacy as the bridging factor of security and usability. Privacy is "control over the extent, timing, and conditions of sharing oneself (physically, behaviorally, or intellectually) with others", according to HHS [40]. As customers' perceptions of privacy vary, it will be difficult for IT companies to convince them to trust privacy safeguards. The EU's "General Data Protection Regulation" [12] fines companies up to 4% of their

yearly worldwide revenue if they lack comprehensive privacy protections. Gartzke and Roebel [22] state that "getting their approach to privacy right while being consumer-friendly will be vital to their success."
Here are three goals:

1. Protecting personal data requires privacy-enhancing technologies and controls.
2. Control methods must be made transparent so the general users understand these control methods.
3. Users must have a personal understanding of the control mechanism and their privacy. This mental model determines a user's trust in systems.

Through active user interaction, our technique may detect and quantify problems with understanding, application, and acceptance of privacy measures. Our strategy covers a number of interrelated privacy elements and questions. In addition to Fischer-Hübner et al. [16] requirements (representation of legal requirements, transparency, and confidence), we focus on the user's mental model and system acceptability. Our approach follows User-Centered Design (UCD) [34] and Human-Centered Design (HCD) [28] criteria and is part of an iterative improvement process. This allows for privacy evaluation and optimization at development and runtime [15]. Our approach and method enable security developers to understand users' privacy goals and needs (e.g., security-relevant information about missing encryption [4]). Developers will be able to boost privacy-enhancing technologies' adoption.
We use an Internet of Things (IoT) example to stimulate our work and frame following conversations. The paradigm and method are not confined to this domain but can be used in any system development process that emphasises usable security and privacy.

### *1.2 Structure*

In Section 2, we continue with the example. In Section 3, we describe our model's incorporation into UCD and iterative improvement. Section 4 presents related work, and Section 5 gives us the conclusion.

## 2. Internet of Things security and privacy

IoT provides customers and service providers with several possibilities. All kinds of things—physical objects, sensors, automobiles, buildings—are connected to the Internet. In the future, there will be 40-60 billion IoT applications. Services can be offered, optimised, and customised based on things and their data. Smart Home gadgets (heating, metering, door locks), wearables (Smart Watch, intelligent clothing), and connected automobiles are famous IoT applications (e.g., autonomous vehicles). IoT is a "combination of hardware, software, data, and service" [33].

### *2.1 Privacy in IoT*

The data acquired by gadgets is a tremendous burden for users. Less than 10,000 Smart Homes create 150 million data points daily [14]. Massive amounts of data raise privacy concerns. According to [25], 71% of consumers think their personal information may be stolen and 64% fear their data may be taken and sold. Fear is also caused by the data's sensitivity. The aggregation of data from diverse sources can, in theory, create a complete user profile. The problem is that users don't control their data, or don't feel like they do. Privacy declarations and control methods are hard to read and understand. According to [11], only 15% of EU residents feel they have full control over their online data. 31% have no control. The definition of privacy varies per country. While Germans are most concerned about loss of control (just 4% say they have complete control, 45% think they have none), Greeks are the least concerned (31 percent think that they have complete control, only 22 percent think that they have no control at all). It all leads to two conclusions. Users find present control methods insufficient. This may be because credible control mechanisms are missing or because users don't know, understand, or trust them. Users' perceptions of privacy and control mechanisms vary widely. A one-size-fits-all solution may not be viable, thus privacy techniques must be adapted to distinct user groups or people. Companies are realising this challenge and looking for ways to handle data lawfully and transparently. This includes only processing data with user consent and for allowed uses. The design of processes, technologies, and user interactions is unclear. In line with our conclusions, we believe solutions must be developed iteratively and in direct interaction with users whose needs must be the focus.

*2.2 Privacy in the smart home*

For instance, consider the following scenario: Rikke's new home has various smart home services. Automatic locks and app-controlled shutters. A heating system that adjusts room temperature and saves energy for Rikke. If Rikke shuts her door, the heat turns off till she returns. Automatic lights turn on and off when Rikke enters or leaves a room. She owns smart devices that can be easily integrated: Smart TVs that are connected to the Internet and can be operated by voice commands and applications are a welcome and efficient method for Rikke to engage with her TV. Rikke can use a remote baby monitor to check on her infant. These are all important to Rikke. Rikke worries about her privacy. Baby monitors and smart TV record audio and/or video in vulnerable places. This is helpful for specialised purposes, but private discussions could be recorded. Rikke worries if vendors keep these records and how they're used. Rikke is concerned that smart locks, lights, and heating are utilised to establish a movement profile.
She must know how her privacy is safeguarded to trust the vendor. However, IoT systems are constantly updated and expanded (e.g., new remote control apps). With each modification, privacy is reevaluated. This is a barrier for IoT developers since they don't know what Rikke needs to trust/ accept their service. If Rikke needs information, she has few options.

## 3. A Usable Security and privacy model

As systems, users, and settings evolve, constant user interaction and system optimization are crucial in IoT. We separated our model into (intersecting) sub-models and aligned it with UCD [34] and HCD [28]. HCD is an iterative process that makes systems usable and improves user experience by considering user demands. Context of Use, System Awareness, System Design and Design Evaluation are the four steps in our method (see Fig. 1). Each will be explained below.

*3.1 Context of use*

This phase aims to understand and specify the context of use for viable security and privacy system. Users, tasks, and environments define the context of use [16]. Through their interaction, security goals can be refined into security needs. Building a system with security in mind increases its trustworthiness. System Context definition basically creates a description of the information system context to start establishing the context of use. Information systems include applications, services, IT assets, and other information-handling components [32]. The information system must fulfil privacy goals to safeguard user privacy. Privacy aims might be legal or user-driven. System developers must identify legally protected assets to comply with laws. Assets are resources that one stakeholder values [32]. Users' privacy and PII are assets. These assets have dangers, which can impair a system or organisation [29]. With more and more risks, these assets are at more risk. To reduce risk, the system must include privacy-enhancing technology. These techniques protect security and privacy. A security goal is a component or system property that must be met to protect a user's assets from threats. Confidentiality, Integrity, Availability, Authenticity, Non-Repudiation, and Authorisation are the core security goals of ISO 27000 [29]. The overall system aims are centred on useable security and privacy.

Rikke wants to use the "Smart Home" technology. Rikke must understand her privacy. She knows the system processes private data, such as baby monitor sounds. She realises the corporation must preserve Rikke's privacy due to legal laws. The company can't save or distribute recorded data. Rikke must know how the system adapts security safeguards to trust it. She must also be able to control smart gadgets' security features. Rikke's needs, preferences, talents, and expertise must be considered when designing the system's usability.

*3.2 System Awareness*

This step creates concepts to help the user understand the system. Transparency and user interaction are vital for security and privacy. Usable security guidelines, like those from USecureD [41], Yee [45], Whitten [42], Garfinkel [20], Furnell [19], and Herzog and Shahmehri [24], can aid with this stage. Conceptual system model; The first stage is to construct a conceptual model of the system that captures the main components of the device's functionality and is appropriate and

clear for the user [16]. The system's conceptual model must match the user's mental model. At this point, focus on the system's security goals and the user's privacy goals. This level covers basic security and privacy methods.

Considering our example, Rikke worries that smart locks, lights, and heaters can be used to track her data. The system must prevent the illegal use of data. It must prevent unwanted access while making smart home functionality comfortable. Rikke must be able to control the smart home's functioning. Rikke is adept at utilising smartphone apps, therefore the system should include a mobile app to control the smart house. Encrypting app-to-system data prevents illegal access. Rikke must not be upset by the mobile app's password requirement. In her mind, a system is a person. She wants to communicate with her smart house. The app should offer natural interaction. Speech recognition is required. Interdependencies abound. User mental model must match system behaviour. Every internal and external system component must match user abilities and knowledge. This includes security and privacy tools. Users must understand how security methods meet security and privacy goals (s).

*3.3 System Design*

This section relates to ISO 9241-210's [28] step 'Producing design solutions,' but we focus on the system's security procedures. This stage identifies and implements relevant user interface patterns, creates an interaction design, and creates prototypes, which are necessary for testing the security mechanisms' proper operation and usability in the next step. *Designing Interaction;* We must exhibit interaction principles, user interface design, and screen design based on personas, use cases, scenarios, and user interface patterns. A Usability Walkthrough evaluates the usable security and privacy of interaction ideas, user interface design, and screen design. This can be done before system evaluation. *Prototype-making;* Finally, we must construct interactive and realistic interaction design prototypes to promote discussion with stakeholders, especially end-users. At this step, check conceptual usability criteria. User tasks, user-system interactions, and the user interface must meet user needs, notably usable security and privacy. We create the basic design concept, outcomes, input/output modalities, and information media.

*3.4 Design Evaluation*

The design evaluation finishes the iterative cycle of the approach for designing a usable security and privacy solution. Through systematic feedback collection and analysis, issues are identified and rated. This helps improve the following technique iteration.

*3.5 Collection of Feedback & Analysis*

This phase collects user feedback on security and privacy issues. At this step, we mix system design users with user feedback. As user feedback is sometimes ambiguous and informal, it must be mapped to one or more security or privacy safeguards. To measure the issue's severity and impact on system acceptability, its user impact must be rated. We must mix information about the current activity, the context of use, the user's mental model, and the system state. Continuous collection and analysis of mappings permit solution iteration and customisation. This step is difficult since usability issues usually include multiple factors.

## 4. Some more related research

Since the mid-1990s, usability and security have been aligned. Unusable security mechanisms or unsecured systems still cause many security mishaps [18]. Garfinkel and Lipfort [21] describe "usable security's" history and problems.
While there are guidelines and criteria for designing and evaluating a workable security system, the scientific literature provides few basic requirements. Fischer-Hübner et al. [16] propose three prerequisites for harmonising security and usability:

1. Legal data protection regulations must be user-friendly to promote understanding, awareness, and controllability and user must comprehend security and privacy methods and ideas through a system's transparency to achieve their goals.

2. A user must trust security systems and understand the implications of missing them. The user must see the hazards. The plausibility of security mechanisms must be conveyed and understood. The user is an active part of modern security chains, according to usable security literature.
3. Usable security and privacy research are both theoretical and case-based. Theoretical work [1, 7] is abstract and difficult to apply. The user is a vital, but often a weak component in useable security HCI [3, 5, 37, 44, 46].

**Conclusion**

Privacy is gaining importance. Legal rules and users themselves want privacy. Software and service providers must implement a secure, private, yet usable system. Only involving users will address this problem. Especially in IoT, where systems change often, run-time engagement is vital. User-centered design techniques don't consider security and privacy. This study presents a user-centered security and privacy concept and technique. This focus distinguishes my method from others and is the sole way to quantify consumers' privacy needs and perceptions of privacy-enhancing technologies. Developers can optimise security and privacy using the concept and technique. The model is currently too abstract to be fully applied. Derive properties and metrics for each model element. On that basis, metrics must be researched to offer development and run-time data. Using the model requires a technological implementation, such as Eclipse Modeling Framework (EMF). Applicability and generalisability evaluations remain. This is a starting step toward integrating privacy into UCD and HCD. This won't be confined to IoT in the future. Comprehensive and clear security and privacy procedures are key to attaining compliance and high user acceptance through boosting user experience and system trustworthiness. To sum it up, we have to undertake the component of “Human Aspect” and eventually the risk of “Human Error” when we talk about People-centered security and making it usable and convenient. Making information security useful and convenient for consumers is a top priority. Usable security focuses on designing effective, user-friendly security systems. It's a relatively young field that evolved in the late 1990s and early 2000s in reaction to the awareness that consumers didn't utilise security systems as intended or at all because they were too complex or inconvenient. Security systems aren't always used properly. People typically think their systems are more secure than they are. People may not realise the risks or relevance of security. Even when people realise the threats and importance of security, they may not know how to use their system's security features or find them too complicated or cumbersome. Usable security designs effective and usable security technologies to solve these concerns. A security system must guard against its intended risks to be effective. A useful security system is easy to use and comprehend and doesn't interfere with work.
Usable security system design is difficult. Security typically conflicts with usability, performance, and functionality. People generally don't comprehend or use security systems well. Even when security mechanisms are usable, they may not be used if people aren't motivated to do so. Despite the hurdles, it's crucial to build user-friendly security systems because people are the weakest link in any security system. People can use security in different ways. Design easy-to-use, understandable security systems. Design security systems to fit people's workflows. Finally, people need incentives to use security systems properly. Making security useful and convenient for people is a difficulty, but it's vital for practice and policy. By making security user-friendly, we can increase system security and make the world safer.

## References


1. Adams, A., Sasse, A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999)

2. Al-Saleh, M.: Fine-grained reasoning about the security and usability trade-off in modern security tools. Dissertation, The University of New Mexico (2011)

3. Blythe, J., Koppel, R., Smith, S.W.: Circumvention of security: good users do bad things. IEEE Secur. Priv. **11**(5), 80–83 (2013)

4. Botha, R.A., Furnell, S.M., Clarke, N.L.: From desktop to mobile: examining the security experience. Comput. Secur. **28**, 130–137 (2009)

5. Caputo, D.D., Pfleeger, S.L., Sasse, A., Ammann, P., Offutt, J., Deng, L.: Barriers to usable security? Three organizational case studies. IEEE Secur. Priv. **14**(5), 22–32 (2016)

6. Choong, Y.-Y., Theofanos, M.: What 4,500+ people can tell you – employees' attitudes toward organizational password policy do matter. In: Human Aspects of Information Security, Privacy, and Trust, pp. 299–310 (2015)

7. Cranor, L., Garfinkel, S.: Security and Usability. O'Reilly Media, Inc., Sebastopol (2005)

8. Cranor, L., Garfinkel, S.: Secure or usable? IEEE Secur. Priv. **2**(5), 16–18 (2004)

9. Eljetlawi, A.M., Ithnin, N.: Graphical password: comprehensive study of the usability features of the recognition base graphical password methods. In: Proceedings of the 3rd International Convergence and Hybrid Information Technology ICCIT 2008, vol. 2, pp. 1137–1143 (2008)

10. Ericsson: Ericsson Mobility Report – on the pulse of the networked society (2015)

11. European Commission: Special Eurobarometer 431 - Data Protection (2015)

12. European Union: Regulation (EU) 2016/679 of the European parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)

13. Evans, D.: The internet of things - how the next evolution of the internet is changing everything (2011)

14. Federal State Commission: IoT Privacy & Security in a Connected World (2015)

15. Feth, D.: User-centric security: optimization of the security-usability trade-off. In: Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering - ESEC/FSE 2015, pp. 1034–1037 (2015)

16. Fischer-Hübner, S., Iacono, L., Möller, S.: Usable security und privacy. Datenschutz und Datensicherheit - DuD **34**, 773–782 (2010)

17. Fogg, B.: A behavior model for persuasive design. In: Proceedings of the 4th International Conference on Persuasive Technology 2009, pp. 40:1–40:7 (2009)

18. Furnell, S.: Making security usable: are things improving? Comput. Secur. **26**(6), 434–443 (2007)

19. Furnell, S., Jusoh, A., Katsabas, D.: The challenges of understanding and using security: a survey of end-users. Comput. Secur. **25**(1), 27–35 (2006)

20. Garfinkel, S.: Design principles and patterns for computer systems that are simultaneously secure and usable. Gene **31**, 234–239 (2005)

21. Garfinkel, S., Lipford, H.R.: Usable security: history, themes, and challenges. Synth. Lect. Inf. Secur. Priv. Trust **5**(2), 1–124 (2014)

22. Gartzke, U., Roebel, M.: Balancing privacy and user experience: the challenge of the digital age (2016). http://techonomy.com/2016/01/balancing-privacy-and-user-experience-the-challenge-of-the-digital-age/

23. Good, N., Krekelberg, A.: Usability and privacy: a study of KaZaA P2P file-sharing. In: Proceedings of the Conference on Human Factors in Computing Systems CHI, no. 5, p. 137 (2003)

24. Herzog, A., Shahmehri, N.: Usable set-up of runtime security policies. In: Proceedings of the International Symposium on Human Aspects of Information Security and Assurance (HAISA 2007), Plymouth, UK, 10 July 2007, pp. 99–113 (2007)

25. IControl Networks: 2015 State of the Smart Home Report (2015)

26. Inglesant, P., Sasse, M.A.: The true cost of unusable password policies: password use in the wild, pp. 383–392 (2010)

27. Ismail, U., Islam, S., Ouedraogo, M., Weippl, E.: A framework for security transparency in cloud computing. Futur. Internet **8**(1), 5 (2016)

28. ISO 9241-210: Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems (2010)

29. ISO 27000 Series: Information security management systems

30. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: Proceedings of the 8th USENIX Security Symposium, 23–36 August 1999

31. Jung, C., Eitel, A., Feth, D., Rudolph, M.: Dealing with uncertainty in context-aware mobile applications. In: Mobility 2015, p. 9 (2015)

32. Kompetenzzentrum für angewandte Sicherheitstechnologie

33. “Begriffsdefinitionen in KASTEL”. https://www.kastel.kit.edu/651.php

34. Noto, G., Diega, L., Walden, I.: Contracting for the ‘Internet of Things’: looking into the Nest. Queen Mary School of Law, Legal Studies Research Paper No. 219/2016 (2016)

35. Norman, D.: The design of everyday things. Doubled Currency (1988)

36. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit (DuD) **33**(6), 353–358 (2009)

37. Rudolph, M.: User-friendly and tailored policy administration points. In: 1st International Conference on Information Systems Security and Privacy (2015)

38. Sasse, A., Brostoff, S., Weirich, D.: Transforming the ‘Weakest Link’: a human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)

39. Tank, B., Upadhyay, H., Patel, H.: A survey on IoT privacy issues and mitigation techniques. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS 2016, pp. 1–4 (2016)

40. Quay-de la Vallee, H., Walsh, J.M., Zimrin, W., Fisler, K., Krishnamurthi, S.: Usable security as a static-analysis problem. In: Proceedings of the 2013 ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming & Software - Onward! 2013, pp. 1–16 (2013)

41. U.S. Department of Health and Human Services: “Institutional Review Board Guidebook”.

42. Whitten, A.: Making security usable. Comput. Secur. **26**, 434–443 (2004)

43. Whitten, A., Tygar, J.D.: Usability of security: a case study. Comput. Sci. 1–41 (1998)

44. Whitten, A., Tygar, J.: Why Johnny can’t encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, p. 14. USENIX Association, August 1999

45. Yee, K.-P.: Aligning security and usability. IEEE Secur. Priv. Mag. **2**(5), 48–55 (2004)

46. Zurko, M.E., Simon, R.T.: User-centered security. In: Proceedings of the 1996 Workshop on New Security Paradigms - NSPW 1996, pp. 27–33 (1996)