Adaptive User-Centered Security

Sven Wohlgemuth

Adaptive User-Centered Security

Sven Wohlgemuth

Center for Advanced Security Research Darmstadt (CASED)
Mornewegstr. 32, 64293 Darmstadt, Germany
sven.wohlgemuth@trust.cased.de
http://www.cased.de

Abstract. One future challenge in informatics is the integration of humans in an infrastructure of data-centric IT services. A critical activity this infrastructure is trustworthy information exchange to reduce threats due to misuse of (personal) information. *Privacy by Design* as the present methodology for developing privacy-preserving and secure IT systems aims to reduce security vulnerabilities in the early requirement analysis phase of software development. Incident reports show, however, that not only an implementation of a model bears vulnerabilities but also the gap between rigorous view of threat and security model on the world and real view of a run-time environment with its dependencies. Dependencies threaten reliability of information, and in case of personal information, privacy as well. With the aim of improving security and privacy during run-time, this work proposes to extend *Privacy by Design* by adapting an IT system not only to inevitable security vulnerabilities but in particular to their users' view with different, eventually opposite security interests.

Keywords. Security, privacy, usability, resilience, identity management

1 Data-Centric Society and Security

One future challenge in computer science is the integration of humans in an infrastructure supported by Big Data Analytics and Cyber-Physical Systems (CPS) for promising innovative IT services aiming at sustainable and improving welfare of a society [1,45]. Their IT services should automatically predict, prepare for, response to, and recover from incidents in real-time. This flexibility requires availability of a sufficient amount of authentic personal data from different origins for the analyzing services implying disclosure of personal data and derived information to third parties, their aggregation, and secondary usage. Such IT services are data-centric as seen for business applications relying on information exchange as basic activity [42].

Data-centric services raise severe privacy concerns not only in well aware applications domains as eHealthcare [31], but also on areas where one would not expect these challenges, e.g., as in Archaeology [25]. While collection of personal data is of no real concern to most, their cross-domain usage is. Current studies shows that the majority of a population refrains from participating in data-centric services due to this

concern [14]. The key issue to be resolved is usage of (personal) data in compliant to agreed-upon social and business rules. This is necessary to achieve acceptable quantity and quality of required information [36], which reduces error rate of data-centric services and so a vulnerability by misuse of (personal) information.

1.1 Privacy by Design and User-Centered Security

Beside citizens as participants in an information exchange service providers of data-centric services become attractive for cyber-attacks [20]. Incidents arise mainly via third parties [12], i.e. dependencies between IT systems participating in an information exchange. *Privacy by Design* postulates to consider IT security requirements in all phases of software development to reduce vulnerabilities [5,16]. Software engineering process models are enriched by threat and risk modeling, which combine functional requirements as *liveness* properties with IT security requirements as *safety* properties [4]. An equilibrium of the participant's individual security interests [40] specifies a privacy policy, which formalizes 'balanced' *safety* and *liveness* requirements as security properties [10]. Isolation separates then trustworthy from non-trustworthy participants as well as reliable IT systems from failed ones. Irrespective of a software development process, the scope of implementing *Privacy by Design* ends at present after the release of an IT system. Its enforcement of a privacy policy holds as long as events and executions of the IT system during run-time correspond to its security model. Data-centric services, however, constantly changes their dependencies due to information exchanges with other users.

User-Centered Security extends *Privacy by Design* by integrating users' requirements and view on the IT system of an information exchange into the threat model and IT security architecture [54]. Even though an iterative software development process model with short cycles might reduce the consequences of a security incident, it reacts on a vulnerability instead of preventing their exploitation. In addition, enforceability of a privacy policy, and in general of a security policy, is at present decided by rigorous enforceability of *safety* properties. Security mechanisms are statistical program analysis, signaling with equivalent security policies as detectors, monitoring control traces with enforcement monitors, and re-writing control traces. The result is that enforcement of *safety* properties can violate required *liveness* properties and it is not decidable in case of vulnerabilities by non-observable traces [27], e.g. covert channels. This is as well the challenge for enforcing the 'right to be forgotten' as granted to European citizens as a countermeasure against misuse of personal information [11].

1.2 Contribution

The contribution of this work is *Adaptive User-Centered Security* in adapting the threat model, IT security model, and its enforcement to users as participants in an information exchange, dependencies, and incidents of an IT system during run-time. In contrary to the rigorous aim of strictly enforcing *safety* properties, adaptive user-centric security aims at an acceptable enforcement of an equilibrium between *safety*

and *liveness* requirements according to the risk tolerance of the given user. An adaptation component configures and enforces individual security interests on behalf of the user as far as desired and possible. Starting point is the electronic identity (eID) of a user as his electronic representation in the Internet.

2 Adaptation to the User

Security mechanisms need to be used and configured without loss of information according to the privacy policy of an information exchange. The basics are a *user model* supporting the target user groups, establishment of *trust domains* with specific *safety* and *liveness* requirements, and a *measurement on authenticity of information* of an exchange. An adaptive user interface should prevent privacy vulnerabilities due to an interaction with the given user as far as possible according to the user model and privacy policy of an information exchange. It considers user interactions for the security configuration of an IT system and scale its enforcement according to the privacy expectations of the user and properties of the security mechanisms. Depending on the results of a measurement, a change in the privacy policy for the isolation and the usage of security mechanisms should improve security and privacy and remain the information exchange acceptable or at least brittle, which means that an additional incident will turn the IT risk to be unacceptable for the affected user.

2.1 Security-relevant User Interactions

The user interface of security tools must fulfil two requirements. On the one hand, it should offer the user all the necessary information about the configuration of security mechanisms, and on the other hand the user should interact with it as few as possible for achieving the goal of his activity with an IT service. Usability studies for security tools [46,49] show that their current user interfaces threaten an enforcement of a policy, since the user interfaces are driven by IT security concepts. A user has to learn these technical concepts and adapt to it.

In order to configure all IT security protection goals, a user needs to explicitly configure *accountability* and *unobservability* by his eID. Due to dependencies of IT security protection goals, *confidentiality* can be controlled by the IT system. Integrity can be automatically controlled so that a user interaction needs only take place in case of a non-acceptable anomaly of *integrity* [28]. In addition to this configuration by *safety* requirements of a privacy policy, its *liveness* requirements define obligations on the availability of data according to the purpose of data processing, storage, their further disclosure and removal [30].

In case of *accountability* and *unobservability*, an IT security situation depends on the user's configuration, otherwise it is user-independent. If the current vulnerability is part of the system's threat model, the IT security situation is independent on a manual user's decision, otherwise dependent. If an information exchange depends on the

context, the IT system can control enforcement of the privacy policy as long as the threat model considers the current security vulnerability under investigation. If the context has no dependency to the privacy policy, e.g. integrity can always be assured without raising an additional vulnerability, the situation is context-independent. These dependencies result in four classes of an IT security (Table 1).

	Context-independent Privacy Policy	**Context-dependent Privacy Policy**
User-independent Configuration	**Class 1:** No user interaction necessary, totally controlled by the IT security system	**Class 2:** Controlled by the IT security system, if situation can be detected; otherwise user interaction necessary
User-dependent Configuration	**Class 3:** User interaction necessary for initial configuration, then totally controlled by the IT security system	**Class 4:** User interaction necessary, controlled by the user

Table 1 Classes of IT security situations.

2.2 Scalability for Enforcement of a Privacy Policy

Starting point for a user-centered enforcement of a privacy policy is identity management to achieve *accountability* with the digital representation of a user [43]. Identity management systems according to Chaum [9] and with anonymous credentials [23] are suitable for the enforcement of an adaptable user-centered security model, since they support *accountability* and *unobservability* by authentication with pseudonyms without raising any vulnerability by contradicting with a *liveness* requirement of an information exchange. Even though identity management supports end-to-end security of an information exchange by authentication to an intermediary, dependencies between the IT systems of participants in a data-centric service imply at the same time a vulnerability of non-observable traces between these IT systems. A compromise of participants and their IT system can thus not be ruled out. Dependencies need to be considered for the user, threat, and IT security model as well as for enforcement.

Regarding enforcement, these vulnerabilities relate to the threat model of Dolev and Yao [15], in which security is based on perfect security of cryptographic public key protocols, secure and available public directory of cryptographic public keys, and confidentiality of cryptographic secret keys. Since identity management ensures authenticity of identity but not of exchange information, e.g., such as the necessary cryptographic public key for cryptographic protection of an information exchange, either an authentic pre-key sharing or an authentic key exchange via a third party is required to enforce IT security. A third party as an intermediary in information exchanges is in particular threatened by hidden dependencies, as IT security analysis for IT systems of data-centric services show. The concluding approach is *ICT Resilience*, which takes dependencies and incidents of any kind for IT security into account [53]. So that additional vulnerabilities don't arise when formalizing the IT security model

and its policies for an information exchange, the privacy policy model for adaptive user-centered security in general is usage control. Usage control considers obligations and does not raise additional vulnerabilities by its concept.

Enforcement of privacy and security policies, respectively, differs according to their enforceability in static analysis of the IT system, enforcement by a monitor, and by re-writing [27] whereas the approach differs in preventing, tolerating, removing, or forecasting vulnerabilities [6]. According to different security interests of the participants, their self-protection requires *Privacy-Enhancing Technologies (PET)*, *Transparency-Enhancing Technologies (TET)*, or a mixed mode of their operation.

Scalability for IT security requires a semantically accurate mapping of the required *safety* and *liveness* properties to different user interfaces for configuring privacy policies and their enforcement by the IT security architecture with its different security mechanisms PETs and TETs. Thereby, scalability may not raise by itself a vulnerability across these IT security abstraction layers. Dependencies between these layers should be minimized so that changes within one layer does not affect internals of the other layers. The Model-View-Controller (MVC) software pattern for user interfaces [21] to enhance usability for non-experts, e.g., as deployed for film production processes [29], is suitable for *Adaptive User-Centered Security*. It considers dependencies only between abstraction layers but not across their internal state transitions.

2.3 System Evolution Cycle

The system evolution cycle aims at adapting an IT security system to changes, vulnerabilities, and incidents during run-time. Figure 1 shows the process of adaptation.

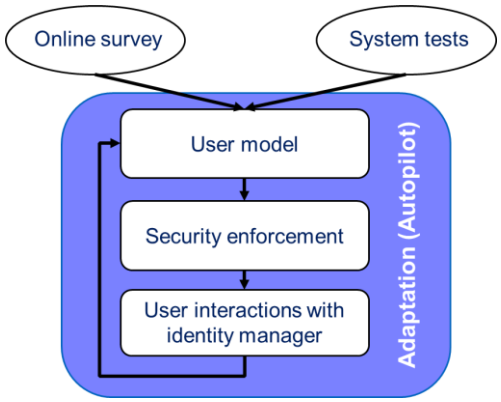

Figure 1 Procedure for continuous adaptation of IT security enforcement.

User modeling gets input from two sources: From the initial evaluation and modelling by a user survey and from system tests. For the Internet usage in Germany, the study on trust and security on the Internet [14] is a starting point for the user modelling. System tests during run-time derive an evidence on anomalies of a policy violation on

isolation and their *information accountability* [48] in combination for using security mechanisms for *unobservability*. In order to detect evidence on anomalies in information, a system test predicts and re-constructs the provenance on this information to be derived or on derived information, respectively. The idea is to classify information and their provenance to patterns, since this kind of monitoring does not change the state of the observed IT system. Patterns represent categories of enforcement with isolation patterns and vulnerabilities as well as incidents by anti-isolation patterns with machine learning algorithms. This requires log data as observation by sensors on the provenance of the information under investigation. The adaptation component initializes this system evolution cycle and continuously re-configures the IT security architecture while evaluating evidences of system tests and user's interactions.

2.4 Adaptive System Model for IT Security

The MVC software pattern allows a scalable adaptation of the IT security architecture to the given user model, system model, and available security mechanisms. According to the current approach of *Privacy by Design*, the IT security architecture with its security mechanisms for controlling isolation follows immediately after the specification of the IT security model. The consequence is a direct dependency between the state transitions of the model with a security mechanisms for their enforcement. A change of such a dependency requires a change in the model or security architecture with a re-validation of its security. The adaptation component aims exactly at a continuous re-validation of isolation. This give a view to the user on his privacy during run-time. According to the MVC software pattern, the adaptation component is an abstraction layer between then concrete IT system architecture and state of the isolation and the adaptive user interface with its user and security model (Figure 2).

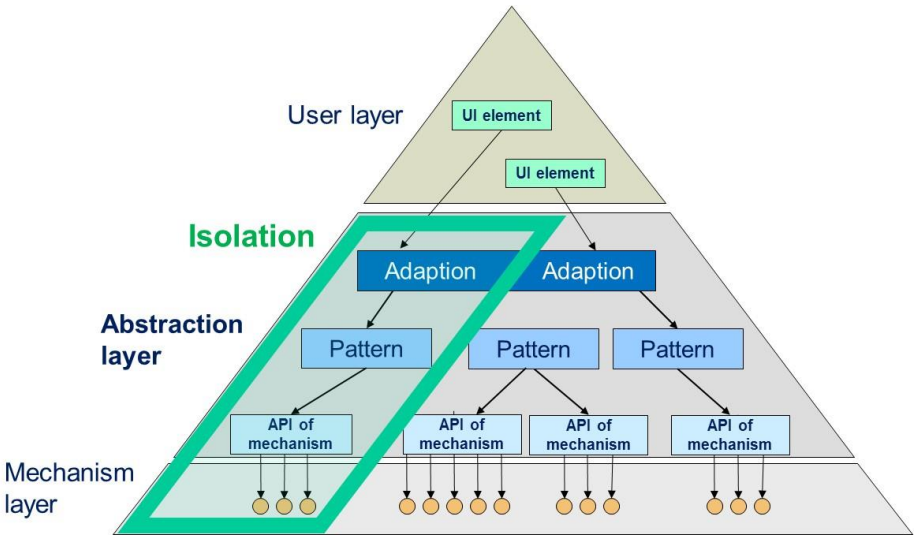

Figure 2 3-Layer-Security-Model introducing abstraction for user-centered isolation.

This model introduces user-centered isolation for an information exchange across the layers and isolation patterns on combining suitable, available security mechanism according to different classes of isolation and its expected results. Isolation refers to an information exchange between a user and his trust relationships to the other participants and their IT systems according to a 'balanced' IT privacy policy of their interests. In this context, isolation of an information exchange is seen as a special sort of privacy, which refers to a controllable data processing for this information exchange [44]. Measurement of accountability of information derives an evidence on enforcement of a given isolation.

A certified isolation pattern can then be used for an equivalent scenario of an information exchange as well as for an exchange with other users. This allows the adaptation component to re-configure the IT system configuration according to a given user. System-centered isolation patterns complements it. They formalize a deployment of security mechanisms to enforce an isolation with acceptable risk according to the current and possible future states of the given IT system. If a previously unknown requirement, vulnerability, or incident occurs, the adaptation component can simulate deployment of known isolation patterns on this new situation, improve them, or develop a new isolation pattern. This results in a new view on the required isolation.

3 Adaptive User-Centered View on Information Exchange

A view on isolation derives a statement on the likelihood for authenticity and accountability of information, i.e. anomalies in the specified isolation and accountability of the data processing. A view differs in the model of a user including his trust assumptions and knowledge about suitable isolation patterns as well as evidence on their enforcement. Concerning a data provider, the view results in a prediction of the expected isolation; concerning a data consumer, the view results in detecting whether isolation of received information has been enforced and it can be seen as authentic.

3.1 IRiS: User-Centered IT Risk Analytics

An evaluation library called IRiS (Information exchange Risk Screening) derives a statistical evidence on authenticity on the data processing and resulting information for a user-centered view on this IT system. IRiS extends data mining capability with two mechanisms to record information flows and to reconstruct events, which have led to a deviation from acceptable states. The third extension is to incorporate *liveness* concepts that allow a usage in planning mode, i.e. prediction on isolation of an information exchange. IRiS consists of an IT risk analyzer (IRiS Analytics) and a database (IRiS Knowledge Database). The adaption component queries the IRiS Analytics whether the current isolation is acceptable according to the corresponding user and his membership to a group of the user model. The IRiS Analytics derives a statistical statement on the current information exchange from user's known statements about the participants in this data processing and isolation patterns for the expected isola-

tion. The IRiS Knowledge Database stores this knowledge of the user and extends it with discovered isolation patterns and anomalies during run-time.

The challenge for IRiS IT risk analyzer whether information and, in turn, its data processing can be seen as being authentic is the same as in a PKI in providing a statement on the authenticity of a cryptographic public key. Irrespectively on the organizational model of a PKI, the evaluation model of Maurer [33] derives with propositional logic a user-centered view. Trust assumptions of a user *A* in other participants' enforcement of certification of the PKI, here isolation of the information exchange, is taken into account. Statements of a view refer to the cryptographic key of another participant *X* ($Aut_{A,X}$) known to the user *A* and taken as being authentic as well as on his belief in *X*, that is expressed by a trust statement ($Trust_{A,X,i}$).

Still, cryptographic key certificates and recommendations need to be considered to obtain the user's trust in this view on an information exchange. A cryptographic key certificate issued by a participant *X* in the role of a certification authority (CA) on enforcement of isolation and this, in turn, on the reliability of the IT system of another participant *Y* ($Cert_{X,Y}$). A recommendation expresses a belief *i* of a participant *X* in a participant *Y* ($Rec_{X,Y,i}$) in that *Y* enforces the certification policy and, hence, can be trusted, i.e. privacy policy for this information exchange. Figure 3 illustrates an exemplary view of a user *X=Alice* on the exchange of information from a user *Y=Bob* with the intermediaries and statements of user *C=System 3* and *D=System 4*. The red arrow represents the requested statement whether *Alice* can consider the information from *Bob* as being authentic ($Aut_{Alice,Bob}$). The blue arrows represent the statements for the information exchange via *System 3* on authenticity of data processing ($Aut_{Alice,System\ 3}$), certification ($Cert_{System\ 3,Bob}$), and trust ($Trust_{Alice,\ System\ 3,2}$). The black arrows represent statements known to *Alice* on an exchange of the same information via participant *System 4*: $Aut_{Alice,System\ 4}$, $Cert_{System\ 4,Bob}$, $Cert_{System\ 3,System\ 4}$, and $Trust_{Alice,System\ 4,1}$.

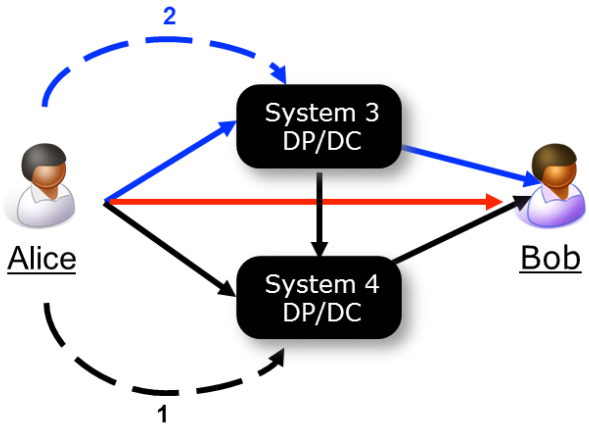

Figure 3 Exemplary view of a user Alice on an information exchange according to [Maurer 1996].

The aim of IRiS Analytics is to derive the statement $Aut_{A,B}$, here $Aut_{Alice,Bob}$, by the following rules [33] from the view of *A=Alice*.

- $\forall X,Y: \quad Aut_{A,X}, Trust_{A,X,1}, Cert_{X,Y} \rightarrow Aut_{A,Y}$ (1)
- $\forall X,Y,i \geq 1: \quad Aut_{A,X}, Trust_{A,x,i+1}, Rec_{X,Y,i} \rightarrow Trust_{A,Y,i}$ (2)
- $\forall X,Y,1 \leq k < i: Trust_{A,X,i} \rightarrow Trust_{A,X,k}$ (3)
- $\forall X,Y,1 \leq k < i: Rec_{A,X,i} \rightarrow Rec_{A,X,k}$ (4)

Concerning the example, *Alice* considers the information from *Bob* as authentic, since $Aut_{Alice,Bob}$ can be derived by one of the data traces in the directed graph of the data traces for this information. Afterwards IRiS Analytics checks whether the received information matches with acceptable probability to a cluster of expected valid information or it validity in case this information is the cryptographic public key of *Bob* or a certified statement of a credential. In case of information, a data clustering scheme should assign this information to a cluster of expected results according to the privacy policy and isolation patterns known to *Alice*. In case of a cryptographic public key, its validity will be checked according to the privacy policy on its authorized usage, timeliness, and revocation to grant access on *Alice*'s IT system [7].

IRiS Analytics checks security vulnerabilities as dependencies of the given instance of the workflow 'Information exchange' between the participating IT systems as a Black Box [3] and, if necessary and possible, additionally their internal data traces with a White Box test scheme [17]. The former evaluation results in $evidence_{INFORMATION}$; the evaluation of the workflow instance results in $evidence_{DATA\ TRACE}$. Their combination contributes together with the statement $Aut_{A,X}$ on $evidence_{ISOLATION}$ [52]. However, even though if a data trace between nodes or a node itself is faulty, a data trace of another information exchange might be acceptable correct. Taking several data traces for exchanging the same information into account results, in turn, in a consensus on $Aut_{A,X}$. The evaluation model of [33] considers dependencies and incomplete knowledge about enforcement, which is the case for data traces of hidden dependencies, by a confidence parameter derived from a probability distribution on the set of possible initial views of a user.

The IRiS Database stores this knowledge including user interactions and system configurations of instances of the workflow 'Information exchange'. Since the outcome and costs of reconstructing archived information with the configuration of the corresponding instance are difficult to estimate, an approach is to emulate their reconstruction in possible future data processing environments using software [41]. The aim is to identify clearly defined and controllable preservation strategies, which should be integrated in current business processes. Detected and robust patterns from other trustworthy participants should extend this knowledge as well as the robust isolation patterns of this user should be publicly available and exchanged with others. This information should be exchanged via an already established isolated channel, e.g. a proven trustworthy intermediary of an eID infrastructure. Since information leakage might occur due to a hidden dependency, isolation patterns should be anonymized

before their disclosure while remaining accountable to detect the cause of such an information leakage. An approach is a k-anonymization scheme, which tags anonymized information by the procedure of their anonymization [32]. This evaluation considers colluding data consumers, as given by an incident propagation, with the aim of non-authorized re-identification of the related identity to this information.

3.2 Retrieving and Re-Writing Data Traces

IRiS Analytics derives a view on an IT system and exchange of personal information, which is built with the IT systems of the participants in an information exchange and eventually needs to be modified or dissolved during run-time. If a non-acceptable evidence on an anomaly derived by a system test or a new requirement from the user model occurs, a re-writing of the workflow [47], the IT system [27], or both is required in advance or during an information exchange, respectively, to prevent more severe incidents. Retrieving and re-writing data traces may not raise an additional vulnerability in enforcing the user's security interests on *accountability* and *unobservability*. Since these mechanisms consider isolation as a kind of privacy, they are called *Privacy Foren*sics and *Privacy Control*.

Privacy Forensics aims at detecting evidence on isolation by the most probable data provenance history and its classification to an anomaly pattern. Information is tagged with a label, which represents the data providing and data consuming parties together with the corresponding privacy policy for this isolation. The provenance of information, and in general data, *d* consists of the data provider's, data consumer's, and the user's identity as well as a pointer to the privacy policy. The privacy policy is indirectly part of a tag by a link to it. This, in turn, allows the user to modify the privacy policy and the IT system, if the purpose of the data's usage changes or a severe vulnerability and incidents occurs. The tag should stick to *d*, so that $d^*=(d, tag)$ can be disclosed further while assuring the integrity of the relationship within d^*. If d^* is disclosed further, the tag has to be updated by adding the new role of this now data providing participant and adding the identity of the new data consumer. The sequence of tags for the same personal information thus constitutes its data trace.

Tagging of data requires authentic information for testing and to reduce the statistical error rate of the applied machine learning scheme. So that the necessary (personal) data as log data don't violate the protection goal *unobservability*, each log data is encrypted and related log data for deriving an evidence on isolation of a given information exchange are linked by a chain of cryptographic hash values. Linked log data represent a log view on a data provider's information. Each log view is individualized to the identity of the corresponding data provider. Collection and retrieval log views depend on a trusted execution environment to which the data provider or an authorized participant, e.g. an auditor, authenticates with his identity to get access [2]. Since internal traces of a sub IT system are not known, but labeled evidence exists by the specification of this data processing, supervised machine learning can be useful for deriving $evidence_{DATA\ TRACE}$. Since not all kind of data can be annotated, mechanisms

of unsupervised machine learning should also be researched to establish their suitability. The derived data provenance has some safety and liveness properties, which are expressed by a policy as its *detector* [27]. If this policy is not equivalent to the privacy policy of the expected isolation, an anomaly has been detected.

Privacy Control aims at re-writing the 'code' according to changes in the privacy policy and supporting at the same time self-protection against information leakage. The main identity of users as data providers remains unobservable, when the eID infrastructure supports pseudonymity as well as non-linkable delegation and revocation of rights [44]. Pseudonymity should be revocable should provable fraud have occurred. According to distributed trust management [7], an orchestration according to authorizations can be done by delegation and revocation of rights with credentials. Credentials are a representation of access rights, which are delegated to service providers to obtain access to personal data in agreement with the individual in question. Anonymized credential schemes achieves unobservability in the issuing and showing protocols [8]. The individual (in the role of the data subject) specifies these access decisions by delegating the access rights together with obligations or using these access rights to the requesting service provider (in the role of a data consumer). To obtain a user's agreement for each disclosure of his personal data to a third party, it should be possible to delegate and revoke rights for isolating an information exchange. Thereby, a delegation of rights defines a collaboration between service providers including the exchange of given user's personal data between them.

4 Adaptive Identity Management System

Preliminary work of the author exists as partial identities for security-relevant user interactions, *Privacy Control*, and *Privacy Forensics*.

4.1 *iManager*: User Interactions and Personal IT Security Tool

iManager as an eID client for mobile use introduces partial identities for user interaction and a concept for automatic configuration of security mechanisms [50]. It offers interfaces to the user, security mechanisms, and applications of a mobile device. The access to personal data and to cryptographic keys is exclusively possible by using the identity manager. An application's request to these data will be checked by the identity manager to see whether the user has granted authorization to this access on personal data. Based on a *security platform* with the necessary security mechanisms in order to protect the communication, the personal data and the privacy of the user, the components *identity configuration*, *identity negotiation*, and *confirmation of action* are responsible for managing partial identities. The concept of partial identities for security-relevant user interactions and its implementation for the *iManager* has been developed according to the software development process model of *User-Centered Security Engineering (UCSec)* [22]. *UCSec* combines usability engineering for development of user interfaces with security engineering.

4.2 *DREISAM*: Non-Linkable Delegation of Rights for *Privacy Control*

DREISAM extends an eID infrastructure for an unobservable delegation and revocation of rights to third parties [44]. The higher cryptographic protocols of *DREISAM* combine the mechanisms for delegation of rights by credentials with mechanisms for enforcing non-linkability for unobservability when using credentials. Anonymous credentials make use of a cryptographic commitment scheme for binding authorizations to a cryptographic key and of zero-knowledge proofs for showing this relationship without revealing any identifying data. Since a user would lose control on his identity, if he would use anonymous credentials for delegation, a proxy credential replaces sharing of individual's master identity. It represents to the certification authority (CA) the individual's delegation request for a certain right to a service provider. If the service provider gets a proxy credential, he has the individual's authorisation to get the requested access right by means of an anonymous credential. The CA logs requests from users and service providers with the issued proxy and anonymous credentials in the delegation list. The CA uses this list for checking service providers' requests for anonymous credentials and for resolving disputes between participants.

4.3 *DETECTIVE*: Data Provenance Protocols for Privacy Forensics

DETECTIVE is an experimental data provenance system with the aim of privacy-preserving tracing disclosure of data to third parties even in case of covert channels [51]. *DETECTIVE* makes use of cryptographic commitments and of a symmetric digital watermarking algorithm but without the need of a trustworthy data provider or a TTP regarding the embedding and checking of data provenance information. Cryptographic commitments link the identities of the participating service providers in any disclosure of personal data. Digital watermarking is used to tag the corresponding personal data with this link. Since users do not take part in the disclosures of personal data, users give their authorization in advance, e.g. by using *DREISAM*. *DETECTIVE* operates in the three phases (1) definition of the collaborating service providers of a business process by obligations and their delegation according to the privacy policy, (2) documenting disclosures of personal data to third parties by adding data provenance as a digital watermark, and (3) checking the enforcement of the obligations by comparing the delegated rights with the data provenance information of the found personal data.

5 Related Work

Adaptation of IT security enforcement is considered for user interfaces and on getting access on data, but without proposing a concept for adaptation in general and in case of an information exchange. Recent work configures screen locking of a device for non-authorized access via the GUI according to the current physical environment of the (mobile) device. The physical environment represent the context on which a machine learning scheme derives a classification and classify the current context. The focus is on data disclosure, i.e. on data collection, of location data [34].

Adaptation of security-relevant user interactions on IT security considers the design of a GUI, which addresses different level of user risk [12]. A dialogue adaptation engine tracks user's behavior, generates security dialogues, and provides feedback to the user. It uses collected security information to alter the behavior of the dialogs. Security information is stored in data stores, which is decision risk, user performance, and environmental data. Decision risk data are executions with high risks, user performance data refers whether a user differentiates between non-risk and risky operations, and environmental data are other external data. However, there is no assurance that this systems runs as expected, since it assumes an IT system without vulnerabilities. It has been shown that a misuse of GUI elements by introducing hidden GUI elements is possible and an exploit of this vulnerability results in information leakage. Approaches for detecting security vulnerabilities by assessing a GUI consider certain classes of vulnerabilities and user group, but not a general user and threat model [29,35].

6 Conclusion

Adapting an IT system of an information exchange to security vulnerabilities during run-time to acceptable enforce individual security interests would improve security and privacy by reducing security vulnerabilities in an isolation. However, this inherits a *privacy paradoxon*. Whereas PETs should impede a privacy violation by restricting availability personal information, they impede at the same time a detection of security vulnerabilities in isolation of an information exchange and, hence, threaten privacy as understood by isolation of an information exchange. On the one side, accountability of information with *TETs*, as demanded with transparent, accountable data flow tracking by the *Big Data and Privacy 90-day review* of The White House [19], requires authentic personal information to reduce the error rate of an adaptation. On the other side, usage of personal information according to an isolation, hence security and privacy, is threatened by hidden dependencies such as an exploit of a covert channel for an information leakage and modification of information. The proposal for *Adaptive User-Centered Security* should contribute to identify and enforce an equilibrium in such a multilateral settings between the individual security and privacy interests of participants in an information exchange, among others on security incidents.

7 Acknowledgement

Basics of this work was funded by the German Research Foundation (DFG) within the priority program 'Security in the Information and Communication Technology' (SPP 1079) under coordination of Günter Müller. I would like to thank all members of the corresponding project group 'ATUS – A Toolkit for Usable Security', Isao Echizen and Stefan Sackmann for the discussions on resilience and IT risk in social infrastructures, and the reviewers of CD-ARES 2014 for their valuable comments.

References

1. acatech. Cyber-Physical Systems. Driving force for innovation in mobility, health, energy and production. acatech - National Academy of Science and Engineering, acatech POSITION PAPER, 2011.
2. R. Accorsi. A secure log architecture to support remote auditing. Mathematical and Computer Modelling 57, Elsevier, 1578—1591, 2013.
3. R. Accorsi, A. Lehmann, and N. Lohmann. Information leak detection in business process models: Theory, application, and tool support. Information Systems, Elsevier, 2014.
4. B. Alpern and F.B. Schneider. Defining Liveness. In: Information Processing Letters 21(4), 181—185, 1985.
5. R.J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems 2nd edition, John Wiley & Sons, 2008.
6. A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing 1(1), IEEE Computer Society, 11—33, 2004.
7. M. Blaze, J. Feigenbaum, and J. Lacy. Distributed Trust Management. IEEE Symposium on Security and Privacy, IEEE Computer Society, 164—173, 1996.
8. J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. Advances in Cryptology – Eurocrypt 2001, LNCS 2045, Springer, 93—118, 2001.
9. D. Chaum. Security without Identification: Transaction Systems to make Big Brother Obsolete. CACM 28(10), ACM, 1030—1044, 1985.
10. M.R. Clarkson and F.B. Schneider. Hyperproperties. Journal of Computer Security 18(6), IOS Press, 1157—1210, 2010.
11. Court of Justice of the European Union. Judgment of the Court (Grand Chamber) of 13 May 2014 (request for a preliminary ruling from the Audiencia Nacional – Spain) – Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez (Case C-131/12), 2014.
12. F. De Keukelaere, S. Yoshihama, S. Trent, Y. Zhang, L. Luo, and M.E. Zurko. Adaptive Security Dialogs for Improved Security Behaviors of Users. Human-Computer Interaction – INTERACT 2009, LNCS 5426, Springer, 510—523, 2009.
13. M. Dekker, C. Karsberg, and M. Lakka. Annual Incident Reports 2012 – Analysis of Article 13a incident reports. European Union Agency for Network and Communication Security (ENISA), 2013.
14. DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet. DIVSI Milieu Study on Trust and Security on the Internet – Condensed version, 2012.
15. D. Dolev and A.C. Yao. On the Security of Public Key Protocols. SFCS'81, IEEE Computer Society, 350—357, 1981.
16. C. Eckert. IT-Sicherheit: Konzepte, Verfahren, Protokolle 8th edition, Oldenbourg, 2013.
17. W. Enck, P. Gilbert, B.-G. Chun, L.P. Cox, J. Jung, P. McDaniel, and A.N. Sheth. TaintDroid: An Information Flow Tracking System for Real-Time Privacy Monitoring on Smartphones. CACM 57(3), 99—106, 2014.
18. European Commission. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. Official Journal of the European Communities, L 337, 37—69, 2009.

19. Executive Office of the President. Big Data: Seizing Opportunities, Preserving Values. The White House, 2014.
20. Federal Office for Information Security (BSI). The IT Security Situation in Germany in 2011, 2011.
21. E. Gamma, R. Helm, R.E. Johnson, and J. Vlissides. Design Patterns. Elements of Reusable Object-Oriented Software. Prentice Hall, 1994.
22. D. Gerd tom Markotten. User-Centered Security Engineering. 4:rd EurOpen/USENIX Conference – NordU 2002, 2002.
23. D. Gerd tom Markotten, S. Wohlgemuth, and G. Müller. Mit Sicherheit zukunftsfähig. PIK Sonderheft Sicherheit 2003 26(1), De Gruyter, 5—14, 2003.
24. M. Gilliot, V. Matyas, and S. Wohlgemuth (eds.). Privacy and Identity in Kai Rannenberg, Denis Royer, and André Deuker (eds.) The Future of Identity in the Information Society (FIDIS) – Challenges and Opportunities. Springer, Heidelberg, 2009.
25. K. Holzinger, A. Holzinger, C. Safran, G. Koiner, and E. Weippl. Use of Wiki Systems in Archaeology: Privacy, Security and Data Protection as Key Problems. ICE-B 2010 - ICETE, IEEE, 120—123, 2010.
26. A. Holzinger, K.-H. Struggl, M. Debevc. Applying Model-View-Controller (MVC) in Design and Development of Information Systems: An example of smart assistive script breakdown in an e-Business Application. ICE-B 2010 - ICETE, IEEE, 63—68, 2010.
27. K.W. Hamlen, G. Morrisett, and F.B. Schneider. Computability Classes for Enforcement Mechanisms. ACM Transactions on Programming Languages and Systems 28(1), ACM, 175—205, 2006.
28. U. Jendricke and D. Gerd tom Markotten. Usability Meets Security – the Identity-Manager As Your Personal Security Assistant for the Internet. ACSAC ’00, IEEE Computer Society, 344—354, 2000.
29. T. Kajiyama and I. Echizen. Evaluation of an Improved Visualization System for Helping Children Identify Risky Websites. ARES 2012, IEEE Computer Society, 495—498, 2012.
30. G. Karjoth and M. Schunter. A Privacy Model for Enterprises. In: CSFW’02 Proceedings of the 15th IEEE Workshop on Computer Security Foundations, IEEE Computer Society, 271—281, 2002.
31. P. Kieseberg, H. Hobel, S. Schrittwieser, E. Weippl, and A. Holzinger. Protecting Anonymity in the Data-Driven Medical Sciences. Interactive Knowledge Discovery and Data Mining: State-of-the-Art and Future Challenges in Biomedical Informatics, LNCS 8401, Springer, 303—318, 2014.
32. P. Kieseberg, S. Schrittwieser, M. Mulazzani, I. Echizen, and E. Weippl. An algorithm for collusion-resistant anonymization and fingerprinting of sensitive microdata. Special issue Security and Privacy in Business Processes 24(2), Electronic Markets, Springer, 2014.
33. U. Maurer. Modeling a Public-Key Infrastructure. ESORICS 1996, LNCS 1146, Springer, 325—350, 1996.
34. M. Miettinen, S. Heuser, W. Kronz, A.-R. Sadeghi, and N. Asokan. ConXsense – Context Profiling and Classification for Context-Aware Access Control. ASIACCS 2014, ACM, 2014.
35. C. Mulliner, W. Robertson, and E. Kirda. Hidden GEMs: Automated Discovery of Access Control Vulnerabilities in Graphical User Interfaces. IEEE Symposium on Security and Privacy 2014, IEEE Computer Society, 149—162, 2014.
36. B. Otto, Y.W. Lee, and I. Caballero. Information and data quality in business networking: a key concept for enterprises in its early stages of development. Electronic Markets 21(2), 83—97, 2011.

37. H. Orman and R. Schroeppel. Positive Feedback and the Madness of Crowds. Proceedings of the 1996 Workshop on New Security Paradigms. 134—138, 1996.
38. A.S. Patrick, P. Briggs, and S. Marsh. Designing Systems That People Will Trust". Security and Usability: Designing Secure Systems that People Can Use, O'Reilly, 2005.
39. L.A. Pineda, I.V. Meza, and L. Salinas. Dialogue Model Specification and Interpretation for Intelligent Multimodal HCI. IBERAMIA 2010, LNCS 6433, Springer, 20—29, 2010.
40. K. Rannenberg, A. Pfitzmann, and G. Müller. IT Security and Multilateral Security. Multilateral Security in Communications – Technology, Infrastructure, Economy, Addison-Wesley-Longman, 21—29, 1999.
41. K. Rechert, D. von Suchodoletz, I. Valizada, T.J. Cardenas, and A. Kulzhabayev. Take care of your belongings today – securing accessibility to complex electronic business processes. Special issue Security and Privacy in Business Processes 24(2), Electronic Markets, Springer, 2014.
42. K. Riemer, C. Steinfeld, and D. Vogel. eCollaboration: On the nature and emergence of communication and collaboration technologies. Electronic Markets 19(4), Springer, 181—188, 2009.
43. J.H. Saltzer and M.D. Schroeder. The Protection of Information in Computer Systems. IEEE 63(9), IEEE, 1278—1308, 1975.
44. N. Sonehara, I. Echizen, and S. Wohlgemuth. Isolation in Cloud Computing and Privacy-Enhancing Technologies – Suitability of Privacy-Enhancing Technologies for Separating Data Usage in Business Processes. Special focus Sustainable Cloud Computing of Business Information Systems Engineering (BISE) 3(3), Gabler, 155—162, 2011.
45. W. Wahlster and G. Müller. Placing Humans in the Feedback Loop of Social Infrastructures – NII Research Strategies on Cyber-Physical Systems. Informatik Spektrum 36(6), Springer, 520—529, 2013.
46. M. Waidner. Open Issues in Secure Electronic Commerce, 1998.
47. Q. Wang and N. Li. Satisfiability and Resiliency in Workflow Authorization Systems. ACM Transactions on Information and System Security 13(4), ACM, 40:1—40:35, 2010.
48. D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G.J. Sussman. Information Accountability. CACM 51(6), ACM, 82—87, 2008.
49. A. Whitten and J.D. Tygar. Why Johnny can't encrypt: A Usability Evaluation of PGP 5.0. SSYM'99, USENIX Association, 1999.
50. S. Wohlgemuth, D. Gerd tom Markotten, U. Jendricke, and G. Müller. DFG-Schwerpunktprogramm Sicherheit in der Informations- und Kommunikationstechnik. it – Information Technology 45(1), Oldenbourg, 46—54, 2003.
51. S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller. Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy. 25th IFIP International Information Security Conference Security & Privacy – Silver Linings in the Cloud (SEC) 2010, IFIP AICT 330, IFIP International Federation for Information Processing, 241—252, 2010.
52. S. Wohlgemuth. Resilience as a new Enforcement Model for IT Security based on Usage Control. 5th International Workshop on Data Usage Management, IEEE CS Security & Privacy Workshop (SPW 2014) within 35th IEEE Symposium on Security and Privacy (S&P) 2014, IEEE Computer Society, 2014.
53. S. Wohlgemuth, S. Sackmann, N. Sonehara, and A Min Tjoa. Security and Privacy in Business Networking. Special issue 'Security and Privacy in Business Networking' of Electronic Markets 24(2), Springer, 2014.
54. M.E. Zurko. User-Centered Security: Stepping Up to the Grand Challenge. In: Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE Computer Society, 187—202, 2005.