Resilience as a new Enforcement Model for IT Security based on Usage Control

Sven Wohlgemuth
System Security Lab
Center for Advanced Security Research Darmstadt (CASED)
Darmstadt, Germany, 64293
Email: sven.wohlgemuth@trust.cased.de

***Abstract*—Security and privacy are not only general requirements of a society but also indispensable enablers for innovative IT infrastructure applications aiming at increased, sustainable welfare and safety of a society. A critical activity of these IT applications is spontaneous information exchange. This information exchange, however, creates inevitable, unknown dependencies between the participating IT systems, which, in turn threaten security and privacy. With the current approach to IT security, security and privacy follow changes and incidents rather than anticipating them. By sticking to a given threat model, the current approach fails to consider vulnerabilities which arise during a spontaneous information exchange. With the goal of improving security and privacy, this work proposes adapting an IT security model and its enforcement to current and most probable incidents before they result in an unacceptable risk for the participating parties or failure of IT applications. Usage control is the suitable security policy model, since it allows changes during run-time without conceptually raising additional incidents.**

***Keywords*—resilience, security and privacy, usage control, identity management, data provenance**

I. Resilience and IT

Resilience is gaining importance as a core concept for improving sustainable welfare and safety of a society. Instead of unilaterally reducing the vulnerabilities of a (sub)system, resilience aims to achieve equilibrium of a system by constantly adapting its dependencies to incidents of any kind [1]. A statement on the resilience of a system corresponds to a particular incident and the systems ability to recover within a certain response time, as well as the composite costs and risks [2]. Current initiatives, e.g. IBM with *Smarter Planet* [3], Europe within *Horizon 2020 – A Digital Agenda for Europe* [4], and Japan with the *Declaration to be the World's Most Advanced IT Nation* [5], propose to predict incidents as well as to react to them under real-time conditions with Big Data analytics and Cyber-Physical Systems (CPS) [6], [7].

A. IT Support for Resilience

Both Big Data analytics and CPS contribute to adaptive IT systems. Big Data analytics aims to predict and detect changes and incidents by deriving this information from a huge amount of data (*volume*) from different sources (*variety*) under real-time conditions (*velocity*). *Variety* in particular implies the disclosure of data to third parties and their aggregation for these analytics as their secondary use. The anticipated contribution of Big Data analytics to an adaptive IT system is to adapt a system model to real states and state transitions of a society's social infrastructures. Sensors collect and disclose data acting as a data provider to a Big Data service provider. Acting in the role of a data consumer, these service providers aggregate data from different sources and derive information from these data by means of secondary use with machine learning algorithms. This information is, in turn, disclosed to third parties, e.g. actuators, who use the information to decide and act as a data consumer.

CPS have the potential to achieve availability of required functionality for IT systems. They follow the system paradigm of *Autonomic Computing* [8], whereas *Embedded Systems*, *Mobile Computing*, *Cloud Computing*, and minimal interoperability with standardization for their software interfaces already exist. Examples for IT support with Big Data analytics and CPS for improving resilience are a sustainable energy supply, health care for an ageing society, intelligent transportation systems, the production of personalized services and goods, and public security.

Information must be reliable, i.e. at least authentic and available according to the minimum required *volume* [9]. Authenticity of derived information is always subject to a given error probability. This is conceptually the fact, since statistical models of machine learning schemes depend on their context, i.e. an IT application [10]. The usage of information in a different context to derive further information has the impact of falsifying (training) data for machine learning, which in turn increases error probability [11], [12].

B. Improvement by Spontaneous Information Exchange

The current proposal is a spontaneous information exchange between public and private service providers, e.g. as stated by the European Directive 2009/140/EC [13], in order to increase the amount of authentic information relating to a given incident and to take previously unknown incidents into account. Other approaches consider an information exchange between official and non-official parties, i.e. citizens, via social networks [14]. In respect of IT business applications, it has been shown that decision support based on Big Data analytics and sharing information within an organization using social media results in higher productivity compared to their competitors running standardized IT systems and processes only [15]. However, concerns regarding the lack of verification of the authenticity and availability of information, as well as its confidentiality, hinder an information exchange with non-official parties. For instance, the U.S. Department of Homeland Security reports these concerns as reasons for refraining from

DOI 10.1109/SPW.2014.14

integrating social networks for response to and recovery from a natural disaster [16]. For Germany, a concern of threats by misuse of personal data is the main reason why the majority of the population refrains from participating in Internet applications [17].

C. Threats resulting from inevitable Dependencies

An exchange of information establishes a dependency between the IT systems of the parties while at the same time creating an unwanted vulnerability. An incident can propagate via dependencies and violate confidentiality, integrity, and the required availability of information. This threat arises not only because of cyber attacks but also due to software bugs, hardware failure, system configuration, accidents, and human error [18], [19]. Figure 1 shows two cases for the origin of an incident. Case 1 refers to incidents without a dependency between IT systems, e.g. by an attack as considered by current threat analysis of IT security. Case 2 refers to propagation of an incident via dependencies of two information exchanges by a shared IT system. Examples for a security vulnerability caused by a dependency are covert channels and escalation of rights. Unfortunately, it is impossible to automatically detect all dependencies of an IT system [20].

This threatens participation in an information exchange, e.g. for incident reporting. In the case of a breach of confidentiality at a trusted party acting in the role of a data consumer, the reporting party, as a data provider, would be harmed twice: firstly by the incident and secondly by a loss of reputation due to the leakage of the confidential report. If the origin and cause of this incident breaching confidentiality and, hence, integrity of a trusted party is unknown, the accountability of the incident remains uncertain. This, in turn, could result in the compromised trusted party in the role of a data consumer being treated as an attacker. Hence, the key issue to be solved for a spontaneous information exchange is controlled data processing according to the individual security interests of the parties.

D. Current Approach for IT Security

The approaches for developing "secure" IT systems to improve security and privacy are *Security by Design* and *Privacy by Design*, respectively. Their widespread procedures improve the implementation of a security enforcement model, while leaving the threat and security enforcement model as specified in the beginning of the development process unchanged [21]. However, spontaneous information exchange leads to an adaptive IT systems which leads to continuous changes in its model during run-time. A model would only represent the states which have already passed and is incomplete in respect of the dependencies of the adaptive IT system. For a partial IT system, which doesn't change over an adequate timespan, a non-adaptive model still reflects the states and state transitions of the corresponding partial IT system.

Even though if the threat and security model of an adaptive IT system would not adapt to vulnerabilities and incidents, which are raised by a spontaneous information exchange, minimizing the impact of incidents towards an acceptable risk may still be possible. Nowadays, two security paradigms are under discussion: *control* [4] and *transparency* [22]. Even though

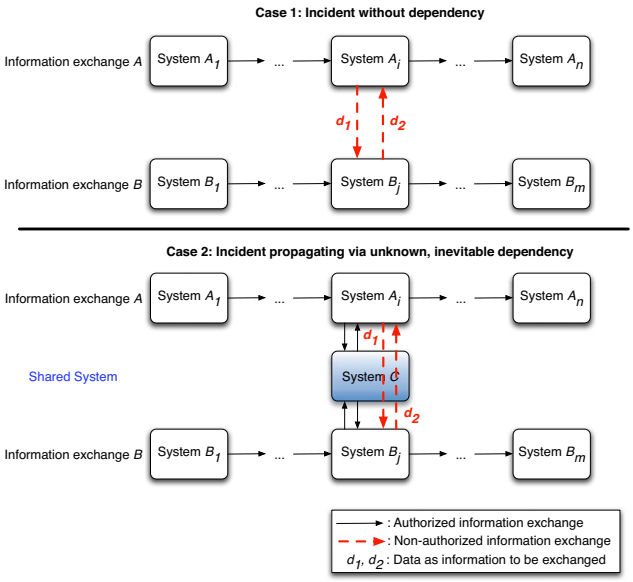

Fig. 1. Dependencies and propagation of an incident.

their approach differs in preventing incidents vs. tolerating them, they have their focus on a static security model in common. Although these approaches achieve security and privacy in some cases, they are not suitable in general. Actually, the deployment of security enforcement mechanisms raises new vulnerabilities in adaptive IT systems. Control with *Privacy-Enhancing Technology (PET)* enforces security and privacy according to a pre-defined threat model by reducing information and impeding its use for other IT systems after access has taken place. This in turn threatens availability of information. Transparency with *Transparency-Enhancing Technology (TET)* enforces security and privacy by re-constructing the current model of this information exchange without taking passive incidents into account. This in turn threatens confidentiality of information.

E. Contribution

The contribution of this work is to show that the current model of IT security is not generally suitable for achieving security and privacy in adaptive IT systems, which are proposed to improve resilience of a society. This work suggests adapting resilience on IT security to improve security and privacy in respect of incidents of any kind by adapting both the threat model and the usage of security mechanisms to current and expected incidents. A risk-based comparison of parties' and their IT system's trustworthiness and the exchange of incident reports on IT security during run time should support a continuous improvement of trust relationships.

II. Trustworthy Information Exchange

In computer science a trustworthy information exchange means a reduction of vulnerabilities in the participating IT systems and their communication in order to reduce the effect of any incident [23]. It also means that parties can formalize a security policy describing their individual security interests and negotiate on an agreed-upon security policy

reflecting a compromise or equilibrium respectively [24]. In such multilateral IT security models protection goals, such as accountability and unobservability, become an important part of *balanced* security [25]. Technically enforcing accountability and unobservability can be achieved by encryption and authentication schemes which support pseudonymity, e.g. by cryptographic key systems [27] and identity management [26]. These approaches depend on confidentiality and integrity of the private key, its accountability to the identity of the given party, and on integrity and consistency of a public key exchange. Although trusted run-time environments exist [28], security of a cryptographic key exchange without a trusted third party (TTP) has not yet been demonstrated [29].

A. Extension of the Communication Model and Isolation

Introducing a third party extends the communication model of an information exchange. In practice, the role of a third party acting as an intermediary for an information exchange is manifold. For incident reporting, according to Article 13a [13], they should coordinate security activities for prevention, response and recovery. Intermediaries also establish relationships between data providers and data consumers by deriving information based on data collected with their consent. Successful examples of this are loyalty card programs in the field of customer relationship management (CRM) or social networks sites. Furthermore, intermediaries can contribute to the usability of an information exchange to enforce the participants' individual security interests. Usability studies of security tools, e.g. SSL [30] and PGP [31], show that their user interfaces and security concepts are too technical and not intuitive, with the result that, as observed in Germany, over 70% are willing to delegate responsibility for their security to a TTP [17].

According to the widely used IT security model of access control and its enforcement by authentication with identities, identity management systems following the scheme of David Chaum [26] enforce accountability and unobservability of transactions. Together with PKI for systems and cryptographic protocols for a secure end-to-end communication channel, a precondition is given for a trustworthy information exchange via a third party. Figure 2 shows the current trust model from the view of *Alice* when using a third party *Charlie* for a spontaneous information exchange between *Alice* and *Bob*. In this example the information is the public cryptographic key pk_{Alice}.

Since a third party has changing dependencies to parties of different information exchanges, propagation of an incident represents a threat. Hence, introducing a third party also introduces a vulnerability in the form of a possible *man-in-the-middle*. According to Article 13a incident reports in 2013, third party failure has a high impact. Most of the observed incidents have their direct cause in system overload, power cuts, and software bugs [19]. The IT security report for Germany in 2011 [18] shows a trend from direct attacks to indirect ones via dependencies to the affected IT system. The report forecasts an increase in attacks by botnets, identity theft, security vulnerabilities, and malware. SCADA, mobile communications, interfaces and storage media, or Cloud Computing systems – all of which are considered to be part of future CPS – show an increased risk potential.

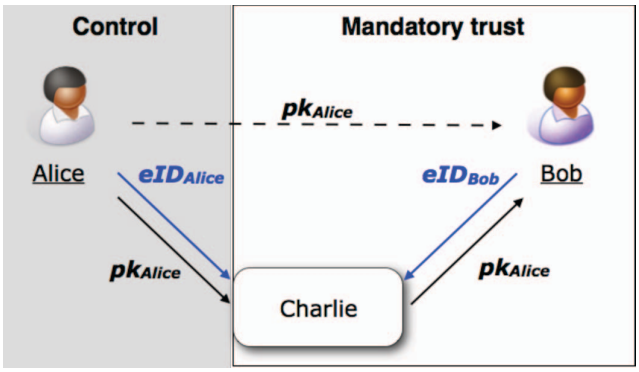

Fig. 2. Information exchange via a third party in the unilateral trust model.

In order to protect information in the case of its disclosure to a third party, the security approach is isolation of the information exchange. Isolation as information flow control can be seen as a special sort of privacy, where an information exchange should not come in contact with other information exchanges, and at the provider of the information exchange services should not know what information is used in the service or the purpose for which the service is being used by its service consumers [32]. The following investigation of security policy models discusses their suitability for spontaneous information exchange, i.e. developing "secure" adaptive IT systems.

B. Security Policy Models

Mandatory access control (MAC) security models, e.g. Biba, Bell-LaPadula, and the Chinese Wall Security Policy, are in widespread use [33]. They model information flow control to protect data by the use of labels and a pre-defined order. This pre-defined order, classifying data and subjects into access classes, formalize confidentiality or integrity, respectively. However, availability is threatened in adaptive IT systems if a MAC policy is deployed. The pre-defined order of the security policy would have to be implemented for service providers, resulting in confidentiality of the data on the one hand, but to a restriction of the availability of the services, on the other hand. For instance, a service of a given service provider *Charlie* would only be able to read the data of a user *Alice* but neither would be able to read data of another user *Bob*. In the case of the Chinese Wall Security Policy, access authorization depends on the access history of this information and its classification to a security class. After granting access to a given user *Charlie* to information of *Bob*, *Charlie* would not get access to a user *David*, who competes with *Bob*. It follows that *Charlie* can't support an information exchange between *David* and *Alice*. Hence, a security configuration based on MAC may lead to an incident regarding the availability of information in adaptive IT systems due to the concept of MAC.

Discretionary access control (DAC) is more flexible in that authorizations are granted to the identity of requestors and not according to security classes. However, they are not precise enough for a trustworthy spontaneous information exchange. Granting access to data for given exchanges needs to define a group or role, respectively, for the parties. This, in turn, would grant access to parties to an information exchange, who

are not participating in it. This is, in turn, a vulnerability for confidentiality and integrity of information.

Distributed usage control, however, grants authorizations on information and on data processing to any identity and role through obligations without restricting the availability of information [34]. This allows changes in the security model, e.g. granting or revoking authorizations to parties during run-time without creating an additional vulnerability in the model's specification due to the concept of usage control. This means that a usage control security policy model for an adaptive IT system can model incidents and their propagation, which could occur during run-time. In respect of enforceability, the classification of obligations according to the criteria time and distribution shows that obligations are, in general, not enforceable but can become so at run-time [35]. Non-observable obligations can be transformed into more strict and observable obligations; however, this implies the drawback of restricting the availability of information. In the following, this work discusses whether enforcement mechanisms for obligations through control and transparency raise additional incidents or vulnerabilities for adaptive IT systems.

C. Control using PET

Control of data processing with PET enforces obligations by impeding the availability of the information for a secondary use. Anonymization schemes decrease utility of the information by obscurity [36]. Encryption schemes protect information before access has taken place [37]. However, if a trusted party is host to the cryptographic encryption keys, they are alsol vulnerable due to dependencies. Furthermore, after decryption, protection is no longer provided. Identity management, with anonymized credentials, doesn't consider disclosure of information to third parties. In that case, their use would lead to a loss of control of his identity for the corresponding data provider due to the all-or-nothing principle [38]. Schemes of homomorphic encryption enforce confidentiality and integrity with availability of information. Their general suitability is uncertain, however, due to the computing performance required for their cryptographic scheme and a mismatch in abstraction of the protected information [39]. Concluding, the use of PET restrict availability of information and thus create an incident for adaptive IT systems. A breach of confidentiality by a dependency, e.g. a passive incident like eavesdropping, using PET to act with pseudonyms instead of a master identity impedes observability and re-identification. The non-linkable delegation of rights and their revocation contributes to developing "secure" adaptive IT systems, since they enforce unobservability and accountability for a spontaneous disclosure of data to third parties and their adaptation to changes in the security policy for this isolation. The assumption of the cryptographic protocols for a non-linkable delegation of rights is a trustworthy third party as a data provider [32].

D. Transparency using TET

TET aims to detect an anomaly of an enforcement and its origin to decide on its accountability. This can be used to check whether an incident at a data provider has occurred. Monitors observe data flows of an IT system and log them for a data protection audit [40]. Data leakage prevention is an example for monitoring which aims at confidentiality of data usage. However, a monitor cannot consider more than one trace and is vulnerable to covert channels as seen by virtualization in Cloud Computing [41]. If integrity, rather than confidentiality has the highest priority for an information exchange fault tolerance is an option. Consensus protocols achieve fault tolerance by running redundant systems in parallel, preferably with different implementations. They assume channels between systems. Unfortunately, it is impossible for consensus protocols to result in a consensus in the asynchronous model – preferable for CPS to avoid blockage of services due to delayed message delivery – if only one of the participating systems fails during the protocol run [42]. Adding extensions as randomization, failure detectors, and strong primitives for shared-memory lead to consensus protocols coping with failed systems due to non-malicious causes, while adding time restriction enhances consensus protocols to cope with incidents with a malicious cause [43]. Restricting time assumptions means that the asynchronous model becomes a synchronous model, at least for the systems participating in the consensus protocol. Consensus protocols for the synchronous model can cope with failed systems, even if they send different messages to other systems. Their impossibility result for a system without assuring the authentication of the parties is that a consensus protocol is correct as long as $t < n/3$ of n systems have failed [44]. However, this restricts availability of information for dependent IT systems, which don't participate in the consensus protocol.

Latest research on TET aims at detecting anomalies by evidence without restricting availability. Secure logging and evidence [45] increases transparency regarding data usage in separated IT systems and enforces access to logged data to authorized identities only. Process mining extends secure logging on control traces between IT systems [46]. The assumptions are completeness of logged events, as well as that confidentiality, integrity and origin of logged data is assured, whereas anomalies are detected by falsification of logs according to the corresponding data usage policy [47]. Data provenance is a variation of process mining. Data provenance documents the history of data to result in the direct acyclic graph of its data traces [48]. Realizations are inversion of data traces and annotation of data. Inversion depends on knowledge of the executed control traces and the output data. This relates to the same completeness assumption as for secure logging and process mining. Annotation labels data so that data traces can be re-constructed if a mapping to the processed data exists. However, current means for data provenance either assume centralized monitoring of the complete information exchange or are suitable for some kind of data without the derived information. Furthermore, data provenance can detect an information leakage and its cause only if the leaked information has been found together with evidence on its history [49]. The latter represents a vulnerability for a misuse of data. Since, this cannot be completely detected with TET, this vulnerability remains and threatens participation in adaptive IT systems, e.g. as the survey on Internet user groups in Germany shows [17].

E. Adapting Resilience to IT Security

A mix mode of PET and TET would complementarily achieve unobservability and accountability in adaptive IT systems. In order to adapt to incidents during run-time including those originating from the use of PET or TET, this mode of

operation should be constantly checked as to whether their deployment raises an additional incident or if information leakage might become most probable in a future information exchange. Adapting both the threat and security model, as well as its enforcement to incidents of any kind relates to the purpose of resilience for social infrastructures. This work proposes resilience as a new enforcement model for IT security in that vulnerabilities and incidents regarding isolation, i.e. security and privacy for an information exchange, are detected and predicted during run-time to achieve equilibrium of the individual security interests of the parties to an information exchange. The starting point for developing "secure" adaptive IT systems is the availability of acceptable secure IT sub systems, e.g. certified IT systems, and an initial threat and security model. The models should be refined during run-time in addition to the deployment of security enforcement mechanisms. Similar to incident reports and their exchange, evidence on anomalies of isolation should be derived and exchanged to predict known vulnerabilities and detect previously unknown vulnerabilities.

III. Evidence on Evolution of Isolation

In order to measure anomalies in an information exchange, both data providers and data consumers should derive $evidence_{ISOLATION}$ on the isolation of their information exchange. For data providers and data consumers approaches are required that allow both to balance the benefit and the level of service, respectively, the security or privacy risk associated with information exchange. Depending on their role, this evidence should be used to get a statement on the information before it has been disclosed or used for further data processing. In respect of a data provider, $evidence_{ISOLATION}$ should be used to *ex post* enforce an information exchange, which has already happened, and to *ex ante* enforce isolation by predicting anomalies and usage of an acceptable PET. Among other incentives for an information exchange, a data provider can use $evidence_{ISOLATION}$ to decide on the usage of a PET with a view to its implied side effects. In respect of a data consumer, $evidence_{ISOLATION}$ should be used to detect an anomaly in an information exchange before this information is processed further. This, in turn, should lead to the selection of a TET, e.g. a consensus protocol. In accordance with $evidence_{ISOLATION}$, this data consumer can inform the previous data providers in this information exchange about evidence of an anomaly in their data processing. This, in turn, should support an *ex post* enforcement of an isolation. This is *ex ante* enforcement on security of their own data processing. Additionally, for both provider and consumer, $evidence_{ISOLATION}$ should be used to improve one's own threat and security model. Either each party, or a third party acting on their behalf, can derive and access $evidence_{ISOLATION}$ on isolation and, in addition, on the reliability of an information exchange. Figure 3 illustrates the view of each party in an information exchange, where *Alice* is the first data provider and *Bob* the last data consumer.

Returning to the key exchange example for a spontaneous information exchange. The problem of deriving $evidence_{ISOLATION}$ on information also relates to a statement on the authenticity of a given public key in a PKI as seen by the example of exchanging pk_{Alice}. This, in turn, relates to checking the enforcement of rights in the direct graph of a

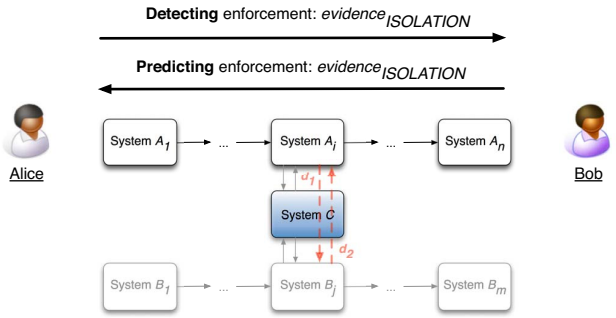

Fig. 3. Same evidence for *detecting* and *predicting* enforcement.

data disclosure to third parties, which is similar to deriving a statement on authenticity of a given public key, e.g. pk_{Alice}, by checking its certification path. For a PKI the set of statements for deriving a statement on authenticity consists of an initial set of authentic keys, certificates on keys, trust in following a certification, and recommendations for trusting others, all with an error probability [50]. These statements for a general information exchange are evidence of an initial set of authentic statements, such as the electronic identities of parties as data provider and data consumer, certification as evidence of the secure data processing of their IT system, trust statements as an evidence of their future data processing, and recommendations as rights for processing the given information delegated by the data subject or data owner, respectively.

Two kinds of evidence need to be derived to get $evidence_{ISOLATION}$, i.e. evidence on the output of a party as a data provider by $evidence_{INFORMATION}$ and on the internal data processing of a party by $evidence_{DATA\ TRACE}$. Considering $evidence_{INFORMATION}$ exclusively is sufficient, if it shows that the resulting information corresponds to that which is expected. If $evidence_{INFORMATION}$ indicates faulty data, the data processing of this party needs to be checked for an anomaly. In general, it can be assumed that the internal data trace of another party's IT system is unknown. A combined assessment of $evidence_{INFORMATION}$ and $evidence_{DATA\ TRACE}$ results in one of the following four cases:

1) $\mathbf{evidence_{INFORMATION}}$ and $\mathbf{evidence_{DATA\ TRACE}}$ match both expectations for isolation:
   The system for this information exchange has followed the obligations on data processing. There is no evidence for a violation of an obligation on the information exchange up to the last data provider's system and the disclosure to the next system of the recipient of this information exchange as a data consumer. A probability for the existence of information leakage depends on the dependency of the data provider's IT system on other IT systems.
2) $\mathbf{evidence_{INFORMATION}}$ indicates an anomaly in the expected information and $\mathbf{evidence_{DATA\ TRACE}}$ matches the expected isolation:
   Regarding the information exchange, this case is identical to case (1). Here, the resulting data

represents a previously unknown authentic result. The set of expected authentic results should be refined according to this new information.

3) $\mathbf{evidence}_{\mathrm{INFORMATION}}$ matches expectations for valid information and $\mathbf{evidence}_{\mathrm{DATA\ TRACE}}$ indicates an anomaly:
The data trace of the data provider appears to have violated obligations with an active incident. This service must be checked in detail. Confidentiality of the data is not guaranteed. Authenticity of resulting information should be checked additionally by other means. If this check results in faulty information, the classification mechanism should be revised and the data provider's security configuration or security mechanism should be modified or replaced. If no vulnerability can be found with this party, this is evidence that the party has violated the isolation policy. Hence, this party has conducted a man-in-the-middle attack and should be excluded from the system.

4) $\mathbf{evidence}_{\mathrm{INFORMATION}}$ and $\mathbf{evidence}_{\mathrm{DATA\ TRACE}}$ both indicate an anomaly:
The data provider's IT system does not achieve integrity and confidentiality for this information similar to case (3). Since $evidence_{INFORMATION}$ confirms the indication of $evidence_{DATA\ TRACE}$ for a compromised data provider's security configuration or security mechanism. The same activities as for case (3) should be conducted.

Considering these four cases, enforcement of an isolation for an information exchange is viewed as *brittle*, if case (1) or (2) applies and an additional failure of one of the parties or their IT system, respectively, would result in a faulty information exchange or no information exchange at all. If one more IT system of a brittle information exchange also fails, this information exchange becomes critical in authenticity or availability of information. However, if replacement of a failed party is possible within the available time for response and for lower expected risk on achieving isolation, the information exchange can return to its brittle state. Even if the affected information exchange is able to adapt to failures of its parties but the obligations on isolation cannot be enforced with all means and with acceptable risks, e.g. due to restricting non-availability of information for other critical services, it is in a state of no return and finally fails.

IV. ICT Resilience

ICT Resilience is the signaling and screening architecture for the proposal of resilience for enforcing multilateral IT security. It should automatically derive evidence of anomalies in an information exchange and evaluate them according to the individual security interests of the parties. If it detects an anomaly above the given risk threshold for an information exchange, it should automatically modify the affected information exchange by replacing the failed security configuration or system. Control means that the real identity of data owners and service consumers remain unobservable. Therewith, *ICT Resilience* needs identity management which supports pseudonymity. Together with a specification of the isolation policy and granting access to trustworthy parties in accordance, this is called *Privacy Control*. A data provenance scheme should derive evidence of anomalies of an isolation. This component is called *Privacy Forensics*. A risk assessment of this evidence should result in a qualitative statement regarding the evidence and subsequent isolation of current and future information exchanges. According to this risk assessment, data owners and service consumers can decide in accordance with their threshold of acceptable risks, whether this information exchange can be seen as reliable or not.

A. Usage Control Policy Toolbox

Isolation and anti-isolation patterns aim at certifiable metrics for isolation of an information exchange. Patterns specify an incident-specific information exchange and risk scenarios, respectively. An isolation pattern specifies the expected isolation. It formalizes the authorized identities and data processing purpose for a requested information exchange, together with security mechanisms for enforcement of obligations and classes of expected results. Isolation patterns will be checked for hidden dependencies and specified during run-time. Anti-isolation patterns formalize classes of anomalies regarding expected information and data traces. Isolation in real-time requires the delegation and revocation of rights. The set of patterns should be extensible to accomodate new detected patterns during run-time for previously unknown incidents and results.

B. Privacy Control

Privacy Control aims at self-protection against information leakage. The real identities of data providers should remain unobservable when information is going to be disclosed to third parties. This requires, e.g., identity management supporting pseudonymity as well as non-linkable delegation and revocation of rights. Pseudonymity should be revocable should provable fraud occur. The experimental system DREISAM extends identity management by non-linkable delegation of rights [38]. Initiatives for interoperability between identity management systems exist, among others, with *Storck*[1], *FutureID*[2], *Kantara Initiative*[3], *OpenID*[4], *Identity Commons*[5], and the proposal for a European regulation on electronic identification and trust services for electronic transactions in the internet market [51].

C. Privacy Forensics

Privacy Forensics aims at deriving evidence on isolation by the most probable data provenance history and its classification to an anomaly pattern. 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 experimental data provenance system DETECTIVE presents data provenance based on identities while retaining their pseudonymity [49].

[1] https://www.eid-storck.eu
[2] http://www.futureid.eu
[3] http://kantarainitiative.org
[4] http://openid.net/
[5] http://www.identitycommons.net/

D. IT Risk Analysis

IT risk analysis aims at evaluating aims at evaluating and combining $evidence_{INFORMATION}$ and $evidence_{DATA\ TRACE}$ to $evidence_{ISOLATION}$ to result in a qualitative (or quantitative) statement on isolation, on information exchanges and, thus, on security and privacy in the adaptive IT system. A database should be developed to aggregate this evidence together with isolation and anti-isolation patterns for a continuous learning according to given incidents as well as to run simulations to predict balanced enforcement of isolations and incidents. The corresponding security policies and compromises can be decided according to the risk preferences of all the participants.

E. System Evolution

System Evolution aims at automatic improvement of the security configuration for an isolation and replacement of compromised IT systems or parties, respectively. A snapshot of the current traces at the time of a replacement should be made so that the newly integrated part can be reset in case of their replacement in the future. A removal of systems implies revocation of rights, which can be enforced by revocation mechanisms for credentials. In the case of accessed data, information has to be removed along the subsequent data trace or at least made useless. Data provenance with machine learning schemes can support auditing to determine whether this information has indeed been removed.

This proposal doesn't claim to be the only correct approach for achieving *ICT Resilience*. It is a starting point for further work. However, it is expected that these components of *ICT Resilience* will not be subject to change over short periods and won't have dependency on the data processing state transitions of an information exchange. A model of their state transitions can be verified and their implementation can be certified to ensure robust components. Development of secure schemes for data provenance and fault-tolerant machine learning is the topic of current research.

V. Discussion

ICT Resilience should measure isolation of an information exchange according to obligations for isolation with unobservability of its parties. This measurement will result in a risk score for the privacy of parties as data providers and in a risk score for the security of parties as data consumers. Depending on the purpose of an information exchange, e.g. business transaction, such as benchmarking or emergency situation seriously threatening safety, the acceptable risk scores will vary. Whereas for one situation – business transaction such as benchmarking – *Privacy Control* with a homomorphic encryption scheme may be a low risk solution including consequences for dependent systems, another situation – emergency activities as a response to natural disasters – has a higher priority for security than for privacy, resulting in getting as much data as possible to evaluate the integrity of isolation, i.e. *Privacy Forensics* without unobservability.

A measurement of privacy and security risks by *ICT Resilience* should illustrate the suitability of these approaches for achieving reliable information exchanges which also take the consequences for dependent systems into account. Therewith, isolation patterns should be classified according to their suitability for exemplary situations in application domains. As the next step, change of these patterns should be simulated to predict the evolution of an affected isolation and its dependencies on other data processing. Simulations should run risk scenarios including expected dependencies. The aim is not to find the balance of accountability and unobservability for a global equilibrium, but rather to identify a set of isolation strategies for local equilibriums.

VI. Conclusion

A next step is to develop an experimental test bed for *ICT Resilience* to concretize and prioritize open issues for its realization. As reliability of an information exchange depends on enforcement of obligations for its isolation, privacy is evidence for this reliability. Participating as a sensor may infringe other people's privacy, namely if they are part of sensor data and predications are made about their behavior without their being aware of it. Since security and privacy cannot only be guaranteed by technology other means should foster the participation of individuals and the reliability of their information exchange. Data protection acts are one option. Since they don't treat anonymized data as personal data and, hence, don't regulate their usage for statistics, which, however, can become personal data by their aggregation and derivation of inferences, regulation for usage control of anonymized personal data is another open issue.

Acknowledgment

This work has, in part, been funded by the German Federal Ministry of the Interior under project funding reference number B3.50-0006/12:1/060253208. The responsibility for the content of this publication lies with the author. I would like to thank Isao Echizen, Hiroshi Maruyama, Kazuhiro Minami, Günter Müller, Stefan Sackmann, Matthias Schunter, Noboru Sonehara, A Min Tjoa, and Michael Waidner for discussions and their comments.

References

[1] C. S. Holling, "Understanding the Complexity of Economic, Ecological, and Social Systems," *Ecosystems*, vol. 4, no. 5, pp. 390–405, 2001.

[2] Y. Y. Haimes, "On the Definiton of Resilience in Systems," *Risk Analysis*, vol. 29, no. 4, pp. 498–501, 2009.

[3] IBM Corporation, "A mandate for change is a mandate for smart," https://www.ibm.com/smarterplanet/global/files/us__en_us__overview__68655_08_522_11092012.pdf, 2008.

[4] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT, 2010.

[5] Prime Minister of Japan and His Cabinet, "Declaration to be the World's Most Advanced IT Nation," Strategic Headquartes for the Promotion of an Advanced Information and Telecommunications Network Society, Tech. Rep., 2013.

[6] 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.

[7] W. Wahlster and G. Müller, "Placing Humans in the Feedback Loop of Social Infrastructures – NII Research Strategies on Cyber-Physical Systems," pp. 520–529, 2013.

[8] J. O. Kephart and D. M. Chess, *The Vision of Autonomic Computing*. IEEE Computer Society Press, 2003, vol. 36, no. 1.

[9] 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*, vol. 21, no. 2, pp. 83–97, 2011.

[10] P. Domingos, "A Few Useful Things to Know About Machine Learning," *CACM*, vol. 55, no. 10, pp. 78–87, 2012.

[11] B. Biggio, B. Nelson, and P. Laskov, "Poisoning Attacks against Support Vector Machines," in *29th Int. Conf. on Machine Learning*, 2012.

[12] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubenstein, and J. Tygar, "Adversarial Machine Learning," in *4th ACM Workshop on Security and Artifical Intelligence*. ACM, 2011, pp. 43–58.

[13] 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*, vol. L 337, pp. 37–69, 2009.

[14] K. Riemer, C. Steinfield, and D. Vogel, "eCollaboration: On the nature and emergence of communication and collaboration technologies," *Electronic Markets*, vol. 19, no. 4, pp. 181–188, 2009.

[15] A. McAfee and E. Brynjolfsson, "Investing in the IT That Makes a Competitive Difference," *Harvard Business Review*, 2008.

[16] U.S. Department of Homeland Security, "National Preparedness Report," U.S. Department of Homeland Security, Tech. Rep., March 2013.

[17] DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet, "DIVSI Milieu Study on Trust and Security on the Internet – Condensed version," https://www.divsi.de/sites/default/files/DIVSI_Milieu_Study_Summary.pdf, 2012.

[18] Federal Office for Information Security (BSI), "The IT Security Situation in Germany in 2011," Federal Office for Information Security (BSI), Tech. Rep., 2011.

[19] M. Dekker, C. Karsberg, and M. Lakka, "Annual Incident Reports 2012 – Analysis of Article 13a incident reports," European Union Agency for Network and Information Security (ENISA), Tech. Rep., 2013.

[20] C. Wang and S. Ju, "The Dilemma of Covert Channels Searching," in *Information Security and Cryptology - ICISC 2005*, ser. LNCS, no. 3935. Springer, 2005, pp. 169–174.

[21] S. Lipner and M. Howard, "The Trustworthy Computing Security Development Lifecycle," http://msdn.microsoft.com/en-us/library/ms995349.aspx, 2005.

[22] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information Accountability," *CACM*, vol. 51, no. 6, pp. 82–87, 2008.

[23] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[24] K. Rannenberg, A. Pfitzmann, and G. Müller, "IT Security and Multilateral Security," in *Multilateral Security in Communications – Technology, Infrastructure, Economy*. Addison-Wesley-Longman, 1999, pp. 21–29.

[25] U. Jendricke and D. G. tom Markotten, "Usability Meets Security - the Identity-Manager As Your Personal Security Assistant for the Internet," in *Proceedings of the 16th Annual Computer Security Applications Conference*, ser. ACSAC '00. IEEE Computer Society, 2000, pp. 344–354.

[26] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *CACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[27] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management — A Consolidated Proposal for Terminology," TU Dresden and ULD Kiel, Anon Terminology v0.34, 2010.

[28] N. Asokan, L. Davi, A. Dmitrienko, S. Heuser, K. Kostiainen, E. Reshetova, and A.-R. Sadeghi, *Mobile Platform Security – Synthesis Lectures on Information Security, Privacy, and Trust*. Morgan & Claypool Publishers, 2013.

[29] E. Freire, D. Hofheinz, E. Kiltz, and K. Paterson, "Non-Interactive Key Exchange," in *PKC 2013*, ser. LNCS, vol. 7778. Springer, 2013, pp. 254–271.

[30] M. Waidner, "Open Issues in Secure Electronic Commerce," IBM Corporation, Tech. Rep., 1998.

[31] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *SSYM'99 8th USENIX Security Symposium*, vol. 8, 1999, pp. 169–184.

[32] N. Sonehara, I. Echizen, and S. Wohlgemuth, "Isolation in cloud computing and privacy-enhancing technologies," *Special focus "Sustainable Cloud Computing" of BISE*, vol. 3, no. 3, pp. 155–162, 2011.

[33] P. Samarati and S. de Capitani di Vimercati, "Access control: Policies, models, and mechanisms," in *FOSAD 2000*, ser. LNCS, vol. 2171. Springer, 2001, pp. 134–196.

[34] A. Pretschner, M. Hilty, and D. Basin, "Distributed usage control," *CACM*, vol. 49, no. 9, pp. 39–44, 2006.

[35] M. Hilty, D. Basin, and A. Pretschner, "On obligations," in *ESORICS'05*, ser. LNCS, no. 3679. Springer, 2005, pp. 98–117.

[36] L. Sweeney, "k-anonymity: a model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[37] M. Beiter, M. C. Mont, L. Chen, and S. Pearson, "End-to-end policy based encryption techniques for multi-party data management," *Computer Standards & Interfaces*, vol. 34, no. 4, pp. 689–703, 2014.

[38] S. Wohlgemuth and G. Müller, "Privacy with Delegation of Rights by Identity Management," in *ETRICS 2006*, ser. LNCS, no. 3995. Springer, 2006, pp. 175–190.

[39] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *3rd ACM Workshop on Cloud Computing Security*, ser. CCSW'11. ACM, 2011, pp. 113–124.

[40] G. Karjoth, M. Schunter, and M. Waidner, "Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data," in *PET'02 2nd International Conference on Privacy-Enhancing Technologies*. Springer, 2002, pp. 69–84.

[41] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *16th ACM CCS*, ser. CCS'09. ACM, 2009, pp. 199–212.

[42] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *Journal of the ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[43] F. Gärtner, "Fundaments of Fault-Tolerant Distributed Computing in Asycnhronous Environments," *ACM Computing Surveys*, vol. 31, no. 1, pp. 1–26, 1999.

[44] B. Pfitzmann and M. Waidner, "Unconditional Byzantine Agreement for any Number of Faulty Processes," in *STACS'92*, ser. LNCS, no. 577. Springer, 1992, pp. 339–350.

[45] S. Sackmann, J. Strücker, and R. Accorsi, "Personalization in privacy-aware highly dynamic systems," *CACM*, vol. 49, no. 9, pp. 32–38, 2006.

[46] W. V. der Aalst, "Process mining," *CACM*, vol. 55, no. 8, pp. 76–83, 2012.

[47] R. Accorsi, "A secure log architecture to support remote auditing," *Mathematical and Computer Modelling*, vol. 57, pp. 1578–1591, 2013.

[48] P. Buneman, S. Khanna, and W. C. Tan, "Why and Where: A Characterization of Data Provenance," in *ICDT 2001*, ser. LNCS, no. 1973. Springer, 2001, pp. 316–330.

[49] S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy," in *SEC 2010*, ser. IFIP AICT 330. IFIP, 2010, pp. 241–252.

[50] U. Maurer, "Modelling a Public-Key Infrastructure," in *European Symposium on Research in Computer Security — ESORICS '96*, ser. LNCS, vol. 1146. Springer, 1996, pp. 325–350.

[51] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internet market," 2012.