A Phase Model for E-Commerce Business Models and its Application to Security Assessment*

Manfred Hauswirth, Mehdi Jazayeri
TU Vienna, Distributed Systems Group,
{m.hauswirth, m.jazayeri}@infosys.tuwien.ac.at

Markus Schneider
GMD, Institute for Secure Telecooperation
markus.schneider@darmstadt.gmd.de

Abstract

New e-commerce business models attempt to exploit information technology to overcome the limitations of traditional business models and to lower costs by improving the efficiency of business processes. A basic requirement for their success is security mechanisms against theft or other fraud. The overall security assessment of business models is complicated, however, since the simple customer-vendor model is often augmented by a large number of roles and interactions. This paper presents a simple approach to understanding e-commerce business models by phases in business processes and roles and interactions in each phase. We use our model to categorize several typical new business models and then analyze the specific security requirements of these business models and highlight potential threat scenarios and describe their solutions. The contribution of the paper is in the decomposition approach for e-commerce business models and its application to the systematic assessment of their security requirements.

1. Introduction

The Internet has become the most relevant platform for e-commerce. As in any business the main goal of doing e-business is to make profit under the assumption that every involved party respects the rules that are defined by the legal framework. This assumption is clearly too idealistic since e-commerce suffers from the same possible threats, such as theft or fraud, as non-electronic business. The new business models, however, can only be successful if their technical design and implementation are done in a secure way to prevent such threats.

Early e-commerce systems typically were electronic re-implementations of simple traditional business models with a small number of involved roles. These systems used customized security solutions and mainly considered security issues between two communication partners (2-party security). Current e-commerce business models are far more complex and evolving because they are based on the business cooperation among several partners. The simple customer-vendor model has been augmented by a large number of intermediaries and suppliers which increases complexity due to the higher number of roles and interactions. Unfortunately, 2-party security cannot easily be generalized to *n* interacting parties (n-party security), since more and new security threats are possible (for example, by collusions among parties). Additionally, upcoming domains such as i-commerce (trading of intangible goods) yield new security problems.

Secure and trustworthy commercial relationships require a better understanding of the risks and how they can be addressed technically. To thwart successful attacks potential security holes of the business models must be analyzed carefully in all respects. Such analysis provides the basis for determining the appropriate security methods. At the moment security analysis of business models is done ad hoc and depends heavily on intuition and experience. A systematic and general approach to discover all possible problems and scenarios has not been defined so far.

This paper presents a phase model for e-commerce systems which is applied in a systematic approach to assess the security of e-commerce business models and discusses techniques to overcome possible threats. Section 2 presents the phase model which characterizes the involved business roles and the exchanged artifacts and breaks down the business process into phases. With this model actual business models can be defined by the sequence in which the phases occur and by mapping the phases onto the roles that interact. We then classify currently relevant business models in terms of our model. As a prerequisite for the security analysis of business models Section 3 describes the security threats to be considered. Section 4 then maps the security threats onto our phase model (and thus actual business models), analyzes possible threats for each phase and presents security mechanisms to overcome them. Finally, Section 5 completes the paper with our conclusions.

2. Modeling the business process

In this section we define a general model for e-commerce business models according to [16] which defines a business model for e-commerce as

– an architecture for the product, service and information

*This work was supported in part by the European Commission under contract IST-1999-10288, project OPELIX (Open Personalized Electronic Information Commerce System).

flows, including a description of the various business actors and their roles;
- a description of the potential benefits for the various business actors; and
- a description of the sources of revenues.

First we will describe the involved business actors (roles) and the exchanged artifacts. Then we will define and describe the phases any business model may involve including the possible services, information flows, benefits for the business actors and sources of revenues. Finally we map these phases onto currently relevant business models and describe them in terms of our model. The definition of business models in terms of phases simplifies the investigation of security threats (see Section 4) and facilitates the coverage of possible business models even those not currently in use.

2.1. Business roles and artifacts

Every possible business model can be modeled with three business roles: customers, providers, and intermediaries. A *customer* requests services or products from providers or intermediaries, expects the delivery of the requested product or service, and possibly has to pay for it. A *provider* generates and offers products or services to customers and intermediaries, delivers them according to the negotiated business terms, and may require payment for them. An *intermediary* offers services to customers, providers, and intermediaries and possibly offers products to customers or other intermediaries. A concrete business model can involve any number of any of these roles but at least must consist of a customer and a provider.

The services and products an intermediary offers can be manifold. It can provide search and retrieval services, advertise products or services, group, or aggregate information products, or provide negotiation or payment services. The underlying idea is that customers, providers, or intermediaries can delegate certain functionalities to specialized intermediaries so that they do not have to address certain issues themselves.

In the trading (business) process these actors produce, use, exchange and modify the following main artifacts [7]:

Request: defines a service or product a party is interested in; sent from a customer or intermediary to a provider or intermediary

Offer: defines a service or product of a provider or intermediary (including legal terms and prices); sent from a provider or intermediary to a customer or intermediary

Order: if a party is satisfied with an offer (possibly after a negotiation phase) an order is placed with the offering party; sent from a customer or intermediary to a provider or intermediary

Product: goods (service, information, material goods) which are traded in a business model; sent from a provider or intermediary to a customer or intermediary

A detailed description of the above terminology and a business and domain model for information commerce are given in [7]. Additional optional artifacts will be described together with the models in which they are required.

2.2. Business process phases

A typical business model consists of a combination (of a subset) of the following phases:

Advertising: A party publishes descriptions of the available products to enable other parties to discover products of their interest and browse through available offers. Offers may be legally binding or not. Typical implementations include publishing on web servers (passive), mail/push distribution (active), or active searching and matching (robots, mobile agents).

Negotiation: Once a product of interest is found, negotiating the business terms and possibly the properties of the product can start. Independently of the concrete negotiation process this phase must end with an agreement between the involved parties to continue with the succeeding phases. If no agreement can be reached at all the business process aborts. However, negotiation and advertising can trigger each other mutually: If a party disagrees with an offer it can request new offers or the party issuing the original offer can send new offers.

Ordering: After an agreement on the product and the business terms has been reached, a party may order the product. If the agreement is legally binding, we call it a *contract*.

Payment: If a product requires payment, then monetary values must be exchanged. We consider payment from a high-level point of view due to the arbitrary ways it can be done: It may involve credit card interactions, a bonus point system, micro-payments, or real money transfers, and heavily depends on the applied payment model such as rates, pay-per-use, or flat fees. Since these models involve very different concerns we address the conceptual superset and assume that the applied payment system secures payment transaction in a feasible way.

Delivery: In this phase the involved product is delivered to the requesting parties. Security in this phase heavily depends on whether products are tangible or intangible. Security for tangible goods is provided by non-electronic means whereas for intangible goods additional security issues apply. For example, intangible goods such as programs or documents may be duplicated and sold without the consent of the copyright holder or the product could be tampered with. These scenarios require special consideration. The security problems of intangible goods and an approach to address them are presented in [8].

The possible business models are derived from the above phases by mapping them onto the roles that interact in a certain phase and the sequence in which the phases occur (see Section 2.4).

2.3. The incremental business phases model

In the following we consider an incremental business process in which the provider gradually delegates phases (i.e., functionality) to the intermediary. If a phase is skipped

then the security concerns defined for that phase do not apply; if a phase is performed by the provider instead of the intermediary (as in our incremental model) then the involved security issues were discussed in a previous step; and if the initiative in a phase is reversed, then the security issues can easily be derived.

Depending on the applied business model the sequence of phases may differ from the sequence in the incremental model as discussed below. For example, payment may follow the delivery phase or a product might be delivered to a party without prior advertising, negotiation, and ordering, on the basis of a party's profile and payment is performed after the party accepts the product. In principle any sequence of the presented phases is possible. Also the number of intermediaries involved may differ: One intermediary may be used for all phases or a dedicated intermediary may be used for each phase. For example, one intermediary may be in charge of all phases except for payment which could be done via the services of a credit card company. Our incremental model simplifies the assessment and presentation of security concerns but does not exclude other models as the ones above or violate the general applicability.

In the simplest case all interactions occur directly between the customer and the provider. We call this the *direct model*. At the moment this model is used frequently. It involves 2-party security issues only which are well investigated and standard solutions exist for all phases. However, it is likely to diminish in importance, because it requires the full set of functionalities for all phases at the customer and the provider which may yield "heavy" applications and may necessitate considerable installation efforts on the customer side. The provider is in full control of the whole process but at the cost of having to provide all required functionality. The sources of revenue are clear since only the provider and no intermediaries are involved.

The current trend in e-commerce goes towards the separation-of-concerns paradigm in which specialized intermediaries gradually take over part of the functionality (phases). The benefit for the provider in these models is that it can delegate parts of the process and need not implement it and pays the intermediary for the service(s) it provides. The customer may also benefit because the models may allow the customer to compare prices and products, combine them, or simply order them at a single location.

In the first model—the *A model*—shown in Figure 1 (UML sequence diagram) the intermediary takes over the advertising phase from the provider. To be able to do advertising for a provider the intermediary needs marketing information from the provider such as a description of the provider or individual products or a product catalog. We summarize this class of artifacts under the term *catalog*. Advertising can then be done by putting the catalog on the intermediary's web server or sending its data to customers and other intermediaries or entering into into search engines. The A model is applied frequently in current e-commerce applications and corresponds to *(process) portals* [14] such as Amazon.com and/or *associated partner programs* such as Amazon.com's [1].

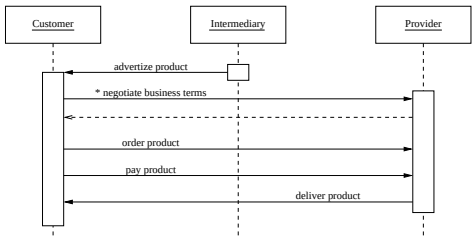

Figure 1. The A model

In the *AN model* the intermediary provides negotiation service in addition to advertising. For the negotiation service the provider must supply the intermediary with an additional artifact—the *pricing and discount model*. This model should enable the intermediary to negotiate with the customer in a meaningful way on behalf of the provider. Depending on the complexity of this model, negotiation can reach from simple discounts for ordering a higher number of products up to sophisticated models based on customer history, customer classification, etc. This heavily depends on the amount of information a provider wants to disclose to the intermediary.

Figure 2 shows the *ANO model* in which the intermediary also does order processing on behalf of the provider additionally to advertisement and negotiation.

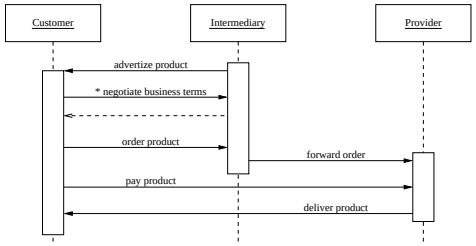

Figure 2. The ANO model

In this model the intermediary additionally requires an *order specification* artifact from the provider where the provider defines the attributes and requirements for a syntactically and semantically correct order. So the intermediary can request all required information from the customer to create and send a correct order that the provider will accept. The intermediary may forward orders immediately to the provider or collect orders and send them to the provider in one message (maybe once a day).

The ANO model and the following ones additionally allow the intermediary to provide higher-level services to the customer. The intermediary may offer combined or syndicated products which the customer may order. This (combined) order may be split by the intermediary into suborders for several providers (including itself) to accomplish the overall order. In this case several providers may interact with the customer in the payment and delivery phases (if these phases are not covered by the intermediary).

In the *ANOP model* the intermediary also provides a payment service on behalf of the provider additionally to advertisement, negotiation, ordering. The intermediary takes care of customers' payment requests and forwards them to

payment service providers in much the same way as described above for orders. The intermediary may also act as a payment gateway which frees customers and providers of supporting many different payment mechanisms and additionally allows them to use best applicable payment services. For example, the customers may pay the intermediary using a micro-payment protocol and the intermediary accomplishes payment with its providers via a macro-payment protocol after having accumulated a large number of customer payments to keep transaction costs low.

Finally, Figure 3 shows the *ANOPD model* in which the intermediary also takes over the delivery and thus is the single interaction partner of the customer on behalf of the provider. This is a degenerate case of the direct model.

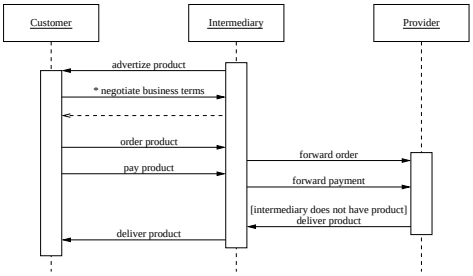

Figure 3. The ANOPD model

Typical delivery mechanisms are: download, email, or push. Physical shipment is outside the scope of our model because we are concerned with intangible (information) products. The intermediary may also act as a delivery gateway. For example, the intermediary may provide a uniform delivery service for its customers via WWW download and have multiple different delivery channels for its providers. A problem in this model is that the intermediary has a physical copy of the product which it may exploit to produce unlicensed copies and sell them. This is a general problem of intangible goods and will be discussed in Section 4. The ANOPD model also allows the intermediary to act in a new role. It can combine products of several providers autonomously and create, offer, and sell combined products. Thus the intermediary becomes a kind of provider itself (*value-adding reseller*, *content syndicator*). However, it is unclear where to exactly draw the line between an intermediary and a provider in this case.

As stated at beginning of this section phases in the incremental model may be left out. As an example, we will also evaluate the security of the *ANOD model* in Section 4. This practically highly relevant model is similar to the ANOPD model but payment is done directly between the customer and the provider. Such a configuration is applicable if, for example, the provider does not have enough network bandwidth to distribute its products to a high number of consumers and for this purpose uses a feasible intermediary but does not want to hand over payment to the intermediary.

2.4. Mapping of business models

In the previous section we have already identified some correspondences of our model with well-known e-commerce models and architectures. The *e-shop model* and *portal* (for one provider) correspond to the *direct model*. A *(process) portal* [14] and the *associated partner* model, e.g., [1], can be mapped onto the *A model*. Several others, such as (process) vortex, dynamically trading processes, third-party marketplace, (value-adding) reseller, or virtual communities, require special consideration since no simple 1:1 mapping can be defined for them.

The *(process) vortex* architecture [14] is similar to a portal. The difference is that in a vortex marketplace the interactions between customers and providers occur through a third-party (the intermediary). A vortex would correspond to the *AN model* and the subsequent models (depending on the service level of the vortex). The *dynamically trading processes* model [14] extends the vortex model. In this model neither business processes nor the set of possible interactions are predefined. Instead a unique process can be dynamically constructed on a per customer basis. Dynamically trading processes have the same mapping as the vortex since they only add higher flexibility to the vortex model but do not extend it otherwise.

A *third-party marketplace* architecture can be mapped onto all our models other than the direct model and denotes a wide range of architectures. Depending on the services that an intermediary provides it defines a more advanced marketplace. The *(value-adding) reseller* and *(content) syndicator* models correspond to our ANOPD model whereas the concept of *virtual communities* is orthogonal to our models and simply depends on whether such a service is provided by the intermediary or producer.

3. Security threats and solutions

Before the design of a secure system the business model has to be analyzed to identify what has to be protected against which potential attacker and which parts need not be secured because the parties trust each other. The result is the *trust model* which is the basis for any further steps. To enable an analysis, we have to consider the capabilities, skills, and time the attacker is assumed to have. Then critical points have to be determined, the values for all involved parties and the possibilities for dishonest parties to achieve advantages illegally must be identified. Other problems with dishonest parties to be regarded concern the infliction of losses to other parties, e.g., denial of service. In such cases, the advantages are indirect: causing problems for a competitor can have positive influence on the attacker's own business. Another aspect to be considered in a trust model are potential collusions of involved parties. Even if security concepts resist attacks that were performed by individual attackers they can become dramatically insecure if attackers exploit their common power. In reality, the strength and restrictiveness of the trust model to be chosen is not only driven by security aspects. Because security can often be expensive, the expenditure for security has to be compared with expected losses.

Security methods can be classified into those providing prevention of attacks (e.g., encryption of information) and

those for detection of attacks (e.g., verification of signature forgery). Furthermore, consequences for attackers have to be defined clearly. This must be accomplished by laws and regulations within a legal framework since technical security is not sufficient for a secure business environment. Additionally, an *arbitrator* is needed who has the authority to impose these consequences based on the evaluation of some evidence provided by the detection mechanisms. A party A which is in conflict with party B can convince an arbitrator of B's fault only if it can present an evidence which can be only created by party B. Presenting information that can also be created by other parties, e.g., A, is insufficient for this purpose. Therefore, the technical design must include special mechanisms whenever a business interaction requires convincing means to prevent malicious parties from infringing the business or legal rules. Additionally, trusted third parties (TTP) such as certification authorities or time stamping authorities, are frequently necessary in security concepts.

Actions of malicious parties are categorized under the summarizing terms *privacy infringement* and *fraud*.

Privacy infringement: This category denotes actions by which malicious parties intend to find out information about other parties. Such attacks can hardly be detected by the victims. Considering a business relation we have to distinguish if the privacy infringement is performed by a party which is involved in the business relation or which does not participate in the business relation. Inside a business relation the involved partners in general have to reveal information to each other to a certain degree. For example, a customer may have to provide name and address, the knowledge of a customer's buying preferences can be exploited for identifiable customer profiles for data mining and direct marketing purposes. Studies have shown that users want to reveal as little personal information as possible because they fear loss of privacy and potential misuse [6, 17].

Two approaches exist for avoiding misuse of personal data such as collecting, processing or passing it to other parties: regulation by legal framework, e.g., [4], and technologies which constrain or fully avoid unauthorized insight into personal data. Solely relying on a legal framework is an insufficient protection since this is equivalent to trusting that other parties will follow the rules. Furthermore, in an international context the legal framework is still very heterogeneous. Technologies that hide personal data from interacting business partners are not developed to an extent to be used in real trading scenarios. Technologies which provide anonymity exist and can be used to surf the Internet or to hide all identifiable information from the communication partner in emails, e.g., [5, 13, 15], but cannot be used in business relations that are based on contracts.

Beside this intra-business protection also protection against parties not participating in the business relationship must be considered, e.g., a wiretapper who is interested in what a specific person buys or how often a vendor sells a specific product. This problem can be easily solved by encrypting messages. Several encryption methods and ways for exchanging cryptographic keys can be used here [9].

Fraud: In this classification fraud covers different intentions of malicious parties that can either be inside or outside the business relationship. It comprises masquerading of parties, manipulation of messages, repudiation of binding agreements, and theft of goods. Secure systems must be able to detect such attacks immediately and they should provide the victim with enough evidence to identify the malicious party undoubtedly to convince an arbitrator.

In masquerading attacks, malicious parties claim to have some other party's identity. Examples are sending messages with forged sender address, or using services and charging it to some other party's account. The solution to this well-known problem is authentication, where we have to distinguish between data origin authentication and entity authentication. Data origin authentication provides the receiver of a message with the identity of the party which originated the message. However, this does not prevent an attack in which a malicious party copies an authenticated message and resends it later claiming the identity of the originator. This security hole can be fixed by applying entity authentication which guarantees both the identity of the communication partner and that he/she really sent the received message. Authentication methods can also be classified according to whether they provide the receiver with an evidence to convince a third party or not.

Manipulation of messages is another security problem in business relationships that has to be prevented. E.g., an attacker who is not involved in the business relationship could increase the prices in offers on their way to a customer to dissuade him/her. The motivation to manipulate messages can be for profit or simply wanting to be detrimental to others. To prevent manipulation methods for verifying the integrity of exchanged messages are applied. Again we can distinguish two cases: Is it sufficient to detect manipulation at all or should the detection also provide an evidence to convince a third party of the integrity and validity of a document? In the second case this additionally means that the originator of a valid document cannot claim that the document was changed at a later time. This already touches the problem of repudiation of binding agreements. In business relations agreements are often binding. E.g., a party should not be able to claim not having placed a certain order if it actually did, or it should not be possible that a party falsely claims having received an order from another party. In both cases, the ordering party would repudiate what the receiver claims. A conflict in which a party repudiates having agreed to some business details requires evidence that can be used to convince a third party or to identify the dishonest party. A solution to this problem are unforgeable digital signatures as first sketched in [3]. A digital signature of a message is a number which depends on a secret key that is only known to the signer, and on the content of the message that is signed. The validity of the signature can be verified easily by everyone using the signer's public key and without knowing the secret.

Whenever commercial goods are traded the possibility of theft must be considered. This problem is well-known in the tangible world and measures are taken to avoid it. In the

area of i-commerce dealing with intangible goods the situation is different and much more complicated. Digital goods can be copied easily at nearly no costs and without loss of quality. An original and its copies are identical and cannot be distinguished. Illegal copying and redistribution of intangible goods is hard to detect because in contrast to theft in the tangible world the original is still available to its rightful owner afterwards. Two approaches exist to cope with this piracy problem: preventive methods using tamper-resistant hardware and repressive methods based on fingerprinting the intangible goods.

The approach based on special tamper-resistant hardware modules has shown its limitations because of practical and effectiveness reasons. Although fingerprinting cannot make copying data technically impossible, it can prevent malicious parties from redistributing information goods. The goal of fingerprinting is to embed invisibly some information into each copy to make it unique [10]. This information can be used later to identify the buyer of a copy. If an illegal copy is found the seller can trace the copy back to the buyer who has redistributed the copy. Fingerprints in information goods have to fulfill several requirements: They should not harm the functionality or representation of the data they are embedded in, buyers or a certain number of colluding buyers must not be able to locate the marks, marks must not be deleted by processing and compression, and must not be corrupted by embedding new fingerprints.

If it is sufficient for a seller to know which buyer has redistributed an illegal copy the seller can fingerprint each sold copy on his/her own. But if he/she also wants an evidence for a third party to prove that an illegal copy was redistributed by a specific buyer, then the seller is not allowed to know the fingerprinted copy at the time of selling it. If the seller has the fingerprinted copy he/she could illegally distribute it after having sold it to an honest buyer and then claim that this buyer has redistributed it. On the other hand, he/she must be able to identify the buyer if he/she finds a copy one day at an unexpected party. These properties are provided by asymmetric fingerprinting as described in [11, 12]. Unfortunately, the case in which a malicious buyer redistributes an asymmetrically fingerprinted copy cannot be distinguished from the case in which some other party steals an asymmetrically fingerprinted copy from an honest buyer.

The methods described above are basic technical means to avoid privacy infringement and fraud. Beside these technical means organizational means are also necessary [2].

4. A security view on business processes

In this section we show security problems in complex business processes involving three parties and describe *possible* solutions. The well-known direct model of two interacting parties will not be discussed. In the discussion of the considered models—A, AN, ANO, ANOP, and ANOD—we assume as little trust as possible and that all communication is encrypted by default to prevent wiretapping. We also address the issue of non-repudiation, which is required to obtain binding messages, wherever reasonable.

4.1. The A model

In this model the intermediary I only performs advertising on behalf of the provider P. If I's marketing efforts are successful, the costumer C starts to negotiate with P. Therefore, P has to provide its catalog cat at I's disposal before I can start marketing. cat has a validity period starting at time t_1 and ending at t_2 which have to be communicated to I. For reasons of authentication, integrity verification, and conflict resolution by third parties, P creates a digital signature $sig_P(cat, I, t_1, t_2)$ that depends on cat, I, t_1, and t_2, and passes the signature to I. After positive verification of the signature, I creates $sig_I(cat, P, t_1, t_2)$ and replies it to P. This signature is a confirmation that I really received cat and is informed about the validity period. The signature also depends on P so that no other party $\tilde{P}$ providing the same products can claim having a confirmation of I. If P distributes different catalogs cat_1 and cat_2 to different intermediaries I_1 and I_2, I_1 and I_2 should be prevented from exchanging the catalog. Therefore, P's signature depends on the receiver I. Both parties, P and I, should store the received signatures because they can be used as evidences in case of malicious actions by some party. The evidences can be verified by a third party (e.g., an arbitrator) to identify a dishonest party. E.g., since P has stored $sig_I(cat, P, t_1, t_2)$, I cannot advertise expired offers.

Having received P's catalog, I can start with the marketing activities. In general, P and I can cooperate in two ways: (1) P pays a constant amount of money to I for its advertising service, or (2) P pays a commission to I for each sale resulting from I's advertising activities. In the first case, P and I have a contract that guarantees I a fixed income. The second case is more attractive for P since it motivates I to do good advertising and P needs not check if or how I is doing its job.

Whenever I gives any advertising information to C it should be digitally signed. This is necessary for several reasons: (1) it can be used for an integrity check; (2) it can be used as proof if I does not work properly; and (3) it can be used for the authentication of I and for the assignment of the commission.

The third point is essential in this model. The identity of I has to be forwarded by C to P while negotiating or ordering. Then, P knows which intermediary deserves the commission. Therefore, the information referencing I as the intermediary has to be protected against modification by a malicious party $\tilde{I}$ that could replace the reference to I by a reference to itself: A digital signatures of I could be deleted and replaced by a new signature of another parties. The strategies to avoid this attack depend on the power of the assumed adversary. In case the adversary is an external party that tries to replace I's signature by its own signature, it suffices to encrypt the communication between I and C. In the case that the adversary has the power of I's Internet service provider, the situation is more complicated. Here I should ask C to confirm that its signed advertisement has

reached C properly. If I does not receive C's confirmation, it may become distrustful. In reality, there are several examples in which the information for the identification of the intermediary is transmitted without protection.

The low protection level in real business relationships may be due to further weak assumptions which are inherent in the A model: In the A model I must trust P. Since I does not see any order or contract negotiated between C and P, I does not know if C really buys and how much it pays. Thus I has to trust that P is honest and provides I with proper sales information. Of course, I could ask C for a signed and unique purchase confirmation which indicates the price and also holds a signed and unique receipt from P. But it is questionable if such a scheme would work in practice because C gains no benefit from its additional work. Even if such a scheme was introduced, P could collude with C to achieve a win-win situation by offering goods at a lower price if C did not inform I about the purchase.

So far we have only described the potential for any kind of fraud in the A model. The second issue to consider is privacy infringement. As long as I gets no information if C and P are doing business with each other there are no data concerning C that can be collected, processed, or used by I for other purposes. Even if I receives information specifying how much money C spends while doing business with P it does not know which products C is buying.

In summary the A model has some advantages in the area of privacy protection: While providers get insight into the personal data of costumers, no other parties can learn about the costumers' interests or collect personal data of the customer. The A model is based on a trusted relation between the intermediary and the provider. The intermediary should not cooperate with the provider if it does not trust the provider. Thus, it is questionable if the A model should be applied for ad-hoc business cooperations. On the other hand, introducing security instead of trust would have a negative impact on potential privacy infringements.

4.2. The AN model and the ANO model

In these models the intermediary I performs advertising and negotiation. In the AN model the ordering is done by C, whereas in the ANO model, I is also responsible for forwarding the order as a signed contract to P. In both models P provides I with a pricing and discount model pdm, in addition to the catalogue cat, to enable negotiation by I. Both, cat and pdm, and their validity periods have to be signed by P similarly to the signing described in the A model to avoid the attacks described above. The same applies to the advertising phase: All advertising messages should be digitally signed by I. If C is interested in some product, it can start to negotiate about the final price or other negotiable properties. All messages that are exchanged in the negotiation phase before the final contract should be protected against modification and also be checked if they are created and sent by the claiming party. If both negotiating partners finally agree and C intends to purchase they finish the negotiation with a binding contract. Therefore, I and C sign the contract which includes all the relevant business parameters such as description of the good, price, identity of both I and C, date, constraints for delivery, and more. This will be done by filling in and signing an order form provided by P. In the AN model, the contract is sent to P by C, while in the ANO model it is forwarded by I. The contract and the signature can be verified by P and additionally it can check whether I followed the rules. If not, P can can prove I's fault by showing I's confirmation signature on the pdm and I's signature on the contract. If I did act properly it can nullify any false accusation through P's signature on the pdm and the contract signed by I and C.

In the ANO model, after having forwarded the signed contract, I requires P to send the commission. All contracts have to be uniquely identifiable (e.g., by a unique number) because copies of the same contract will not be accepted by P. This prevents an intermediary from sending a contract twice. Upon receipt of the commission, I must send a confirmation of having received it for each specific contract to P. This confirmation protects P against multiple commission claims. If a malicious I requests the commission multiple times and refuses to send the payment confirmation P can prove the money transaction via a trustworthy payment authority. Thus I can be forced to send the payment confirmation. As long as P has no evidence that proves the payment of the commission it will lose a conflict with I and has to pay. Since I has a proof for every good P sold as a result of I's activities, this model also works even if I does not trust P. There is also no obvious possibility for a collusion between P and C.

In the AN model, after C has sent the signed contract to P, I waits for the commission from P. Having received it, I has to confirm the receipt of each payment as in the ANO model. In AN model, it is still possible that C changes its mind after having signed the contract—of which I holds a copy—and does not send the signed contract as an order to P. In this case, I would wait a certain time for the commission, and then would inquire P about the commission. At this stage, I cannot know if C did not send the contract or if P tries to cheat or simply failed to send the commission to I. In all cases I can show a copy of the contract to P, and as long as P has no confirmation from I for the payment of the commission for that specific contract, P would have to pay. In the case that C changed its mind and did not send the contract to P, P can use the copy of the contract provided by I and deliver the goods which C has confirmed in the contract. This model also works if I does not trust P. But in case of not receiving the commission in time, he does not know whose fault—P's or C's—it was. The delivery and payment in both models are handled between C and P as in the well-known direct model and thus require no further discussion.

Regarding privacy aspects, the properties of the AN and the ANO model are equivalent. In both models I gains considerable insight into the costumers' personal data, their interests and activities. I knows all products C is interested in and how much it is willing to pay for them. This knowledge not only derives from the interaction with C during

marketing, negotiation, and contracting: Since I has access to the pdm it can categorize customers probably enriched with further properties that can be critical from a privacy protection point of view. Since I can act as an intermediary for several providers $P_1, \ldots, P_n$ it can aggregate and concentrate lots of personal data.

Summarizing the properties of the AN and the ANO models, we see that there is a larger potential for privacy infringement but a much more balanced trust model for the business process. The AN and ANO models can be applied even if there is no trust between I and P. However, since C has the possibility to change its mind after signing a binding contract which implies some further workflow for conflict resolution, the ANO model seems to be preferable.

4.3. The ANOP model

The ANOP model is similar to the ANO model. The difference is that I is also involved in the payment process. C sends the payment to I after ordering. Thus, I can directly withhold the commission it is entitled to. The rest of the money is forwarded to P together with the order and the signed contract. Having received this artifacts P can deliver the ordered good(s) to C. To enable proper cooperation in the ANOP model, the same prerequisites as in the ANO model have to be fulfilled (e.g., provision of cat and pdm). The security requirements for the early phases in this model are clear by the discussion of the previous models.

Let us suppose now that I has received the signed order from C and C replied the confirmation to it. Since I receives the money directly from C in the ANOP model, there is no necessity for I to collect evidences in order to proof its claim for the commission resulting from its activities. Upon the receipt of the payment, I has to confirm the receipt to C with a digital signature referencing undeniably the payment to the unique order. Thus, C gets an undeniable proof that it paid for a certain order if some conflict arises later. Of course, a dishonest $\tilde{C}$ could try to cheat by claiming the money transfer without actually having done it and accuse I of not having sent the confirmation. Similarly, a dishonest $\tilde{I}$ could refuse to send the confirmation to C after receipt of the money. All these problems can be solved easily with the help of the involved payment authorities that have registered all money transactions.

After deducting the commission, I forwards the rest of the payment to P with an undeniable reference to the concerned order. The unique order containing C's address and the description of the ordered good(s) which is also signed by I can be send in parallel to the payment or before. Thus, P knows where the ordered good(s) have to be delivered to. In any case, the receipt of the undeniable order and the receipt of the payment have to be confirmed undeniably to I by P. Thus P cannot claim later having received different data. Since both P and I hold evidences, i.e., signed confirmations, about the exchanged messages all responsibilities for intentional or unintentional faults can be assigned easily. Other problems concerning payment and confirmation can be solved with the help of payment authorities. After P has verified all data it has received from I it can deliver the ordered goods to C. In case C complains that it did not receive the goods, the dishonest party can be identified (e.g., $\tilde{I}$ did not forward the money and order, or $\tilde{P}$ received the money but did not deliver the goods) because this party does not have the necessary evidences.

From the privacy point of view the ANOP model is comparable with the ANO model. Here I also gains considerable insight into C's personal data. I can learn the same things about C as in the ANO model. Like in the ANO model, the ANOP model is based on a balanced trust model. The ANOP model can be applied even if there is no mutual trust between I and P. One advantage of the ANOP model over the ANO model is that potential doubtful intermediaries can be convinced easier to participate in such business cooperations. They obtain money directly from the costumer and do not have to wait for their commission from the provider. Conversely there is no risk for the producer, since it can keep the good(s) until receiving the money. The ANOP model seems to be attractive if P cannot fulfill some requirements concerning payment, e.g., P accepts only one or a few payment systems while I offers a variety of payment systems.

4.4. The ANOD model

In the ANOD model I performs the delivery of the ordered good after the reception of the order while C transfers the payment to P. Therefore, P has to provide I with the good(s). Let us assume that the earlier phases are secured as in the ANO model and both C and I hold a signed copy of the order. In the ANOD model I knows exactly how much was sold resulting from its activities and also has undeniable proofs by the orders that are signed by the costumers. Thus there is no possibility for a dishonest $\tilde{P}$ to claim that it sold less products via I's activities. Therefore, I non-repudiably forwards each received order to P and waits for a confirmation. (Later, we will also need the forwarding of the order and the confirmation of receipt for copyright protection. There these non-repudiable messages are used for informing P about the identity of legal buyers.) Thereby, P knows which costumer ordered which product at what price via which intermediary. Meanwhile, C can send the payment to P accompanied with its order. Upon receipt of the payment P sends a confirmation of receipt to C. If a dishonest $\tilde{C}$ refuses to send its payment P can enforce the payment by using the copy of the order with $\tilde{C}$'s signature. Problems related to dishonest claims concerning payment and the confirmation can be solved via trustworthy payment authorities.

Further security aspects concerning the provision of goods to I and delivery depend on the kind of goods. In this context we classify them as tangible or intangible. In the case of tangible goods, P has to provide each piece to I physically. After the receipt of the order I can deliver the good(s) itself or via a delivery service. In both cases, C confirms the receipt of the good(s) and replies the confirmation to I so that C later cannot claim that I did not deliver.

For the sake of simplicity assume that the delivery service is trustworthy. If C refuses to pay and claims that I did not deliver the good(s) P asks I to show C's confirmation of delivery. If C is dishonest and I provides P with C's confirmation of delivery P can force C to pay. If I cannot show C's confirmation P can force I to deliver.

In the case of intangible goods they can be delivered electronically. We assume that I holds one copy of each intangible information product in its database which it uses to create the copies of the products to be delivered. If delivery is done electronically a dishonest $\tilde{C}$ can receive the good(s) without replying a confirmation and claim that it never received the good(s)s from I. In this situation it is not possible for P to decide who—I or C—cheats. A malicious $\tilde{C}$ could refuse to pay. In this case, P would ask I to send the good(s) or to send the same copy again as before. Even if I delivered the good(s) before it requires no costs for I to send the same copy twice which is in contrast to the case of tangible good(s). If such a conflict arises the delivery could be done under the observation of P or any other trustworthy party. Thus C can be forced to pay.

A serious problem with intangible goods stems from piracy and copyright infringement. Since digital goods can be copied at no costs without loss of quality, illegal copies are very attractive for pirates. Since the ANOD model comprises three parties—P, I, and C—that trade with digital goods, and since two parties—I and C—can deal with illegal copies, a special special protection mechanism is needed. This mechanism should help P to identify the party which has distributed illegal copies of P's good(s). Furthermore, the identifying information must also be sufficient to convince third parties of the identity of the malicious party. Therefore the marked copy which is distributed legally has to be unknown to the distributor. If not the distributor could give a copy to some other party and accuse the legal receiver having redistributed it. The mechanism to overcome these problems is offered by the double application of asymmetric fingerprinting.

The concept of asymmetric fingerprinting of digital good(s) was already presented in the previous section. In the following we restrict our discussion to those kind of intangible goods to which asymmetric fingerprinting can be applied, e.g., multimedia content. In a first step, while P provides its product to I, the product is marked by asymmetric fingerprinting. If I redistributes this product legally to C upon C's order, the copy which is delivered gets a second asymmetric fingerprint. Both asymmetric fingerprints do not interfere with each another. Furthermore, I informs P that C ordered a copy of a specific good by forwarding C's order, and P confirms the receipt of this information as described above.

If P finds a copy of a digital good at some $\tilde{C}$ it can check by the information provided by I if $\tilde{C}$ is a legal buyer of the good. If $\tilde{C}$ is not known as a legal buyer P can analyze the copy and prove to third parties that it stems from I's copy. Here the first asymmetric fingerprint in the copy is exploited. But even if some illegal copy turns up which can be traced back to I it is not clear at this time which party is malicious. There are two possibilities: (1) I is malicious, because he has redistributed an illegal copy to $\tilde{C}$. This implies that I has not informed P that $\tilde{C}$ is a legal buyer. Or (2) I has delivered a legal copy to a malicious C which has redistributed an illegal copy to $\tilde{C}$.

If I acted honestly it has informed P about the identity of the legal buyer C. Now, I can analyze the copy found by P and prove to third parties that it stems from C's copy. Furthermore, I has P's confirmation that I informed it about C to be a legal buyer. This proves that I is honest. Additionally, P can verify itself if it knows C to be a legal buyer. In this case, C will be accused for redistribution of illegal copies. Here the second asymmetric fingerprint in the copy is exploited. If I cannot prove to third parties that the found copy once belonged to a certain customer who was announced to P by I to be a legal buyer, I will be accused.

Concerning privacy problems, the ANOD model shows the same properties as the previously considered ANO and ANOP model.

To summarize the ANOD model we see that it is also based on a more balanced trust model. Like in the ANO and the ANOP case, the ANOD model can also be applied if there is no mutual trust between I and P. Since the intermediary has access to the digital goods, this model requires special mechanisms to cope with copyright protection problems. Here it also has to be considered that the costs for copyright protection and possibly necessary conflict resolution must be in relation to the value of the traded goods. This implies that the value of the traded goods has an impact on the applicability of the ANOD model. Besides P, I gains considerable insight into C's personal data. The ANOD model is attractive when a special delivery arrangement is required that can not be provided by P, e.g., delivery of large data packages when P only has access to limited network bandwidth.

4.5. Comparison of the models

The previous discussion shows that models with better privacy protection have more potential for fraud (A model) and vice versa (AN, ANO, ANOP, and ANOD models). The A model can only be applied if the intermediary trusts the provider. In contrast the AN, ANO, ANOP, and ANOD model do not require mutual trust between intermediary and provider. This distinction may considerably influence the decision whether two parties start a business cooperation without knowing each other. In the ANOP and ANOD models, the intermediary offers special functionalities (payment, delivery) to the provider. These models are attractive if the provider cannot fulfill special requirements related to these functionalities. The A, AN, ANO, and ANOP model are applicable to tangible and intangible goods, whereas in the ANOD model precautions for securing intangible goods are required. The value of the traded intangible goods has an impact on the applicability of the ANOD model.

5. Conclusions

The success of business models in e-commerce depends on how well they support secure business interactions among the business actors. Due to the complexity of the new models, which involve a higher number of roles and interactions, security must be based on a systematic analysis that clearly exposes the possible threats and supports an overall security assessment of the intended model before it is deployed. On the basis of such analysis, it is possible to apply, combine, or augment standard security mechanisms to achieve the required level of security.

In this paper we have presented a systematic approach for the assessment of business model security. As the basis for a security analysis we have broken down the business process into 5 phases: advertising, negotiation, ordering, payment, and delivery. We have presented a 3-party model (customer, intermediary, provider) for modeling interactions in e-commerce business models, described their possible roles in the phases, and the exchanged artifacts. We then mapped this generally applicable unified model onto the common e-business models and concepts.

We analyzed the security concerns of each phase with respect to mappings of the phases onto the different parties in our model. This analysis facilitates overall security assessment of specific business models. The 5-phases/3-party model allows a designer to classify a business model and assess its security. We have analyzed business processes on a conceptual level, discussed their security problems, and have provided conceptual proposals for addressing the security issues if technically possible.

As a main result of our security analysis we have demonstrated the impact of assigning different phases to different parties on the security level that is objectively achievable. The level of security that can be achieved depends on the party that performs a certain phase. For example, different security levels are possible depending on whether negotiation is done by the intermediary or the provider. As a result, depending on which party performs a given phase, different security mechanisms must be applied.

In some models, correct operation depends on trust and cannot be secured in an objective way, i.e., some parties must always be honest for the model to work. For example, the A model—portal, associated partners—can only work correctly if the intermediary is trustworthy (but no mechanism exists to enforce this). In several other models we have analyzed, objective security is possible. This distinction may heavily influence the choice of possible business partners since it defines whether a business party can potentially defraud another party or such fraud may be prevented by security mechanisms.

If a 2-party business model is extended to an n-party model then the security issues cannot be addressed by solely applying standard security mechanisms such as authentication, signatures, or secure payment methods. Instead the overall security of the n-party model heavily depends on the assignment of phases among the partners. Additional security issues emerge depending on a concrete assignment even as the security issues of a 2-party model must still be addressed adequately.

Our results show that many intrinsic security issues exist in common e-business models which are addressed only to a limited extent in current e-business sites. Assessment of these problems and the application of adequate solutions may determine the success of e-business sites in the long run. Such assessment may be made systematically on the basis of our phase model.

References

[1] Amazon.com Associates Program, Amazon.com, 2000, http://www.amazon.com/exec/obidos/subst/associates/join/associates.html/ref=as_gw_sf/104-2151277-1127609

[2] R. Anderson: Why Cryptosystems Fail, Comm. of the ACM, Vol. 37, No. 11, 1994

[3] W. Diffie, M. Hellman: New Directions in Cryptography, IEEE Trans. Inf. Th., Vol. 22, No. 6, 1976

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with the Regard to the Processing of Personal Data and on the Free Movement of such Data, Official Journal of the European Communities, No. L281, 1995

[5] D. Goldschlag, M. Reed, P. Syverson: Hiding Routing Information, Proc. Information Hiding, Springer, LNCS 1174, 1996

[6] D. Hoffman, T. Novak, M. Peralta: Building Consumer Trust Online, Comm.of the ACM, Vol. 42, No. 4, 1999

[7] M. Jazayeri, I. Podnar: A Business and Domain Model for Information Commerce, To appear in Proc. HICSS, 2001, Maui, Hawaii

[8] D. Konstantas, J.-H. Morin: Trading digital intangible goods: the rules of the game, Proc. HICSS, 2000, Maui, Hawaii

[9] A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, 1997

[10] F. Petitcolas, R. Anderson, M. Kuhn: Information Hiding - A Survey, Proc. of the IEEE, Vol. 87, No. 7, 1997

[11] B. Pfitzmann, M. Schunter: Asymmetric Fingerprinting, Eurocrypt '96, LNCS 1070, Springer, 1996

[12] B. Pfitzmann, M. Waidner: Asymmetric Fingerprinting for Larger Collusions, Proceedings, 4th ACM Conf. on Computer and Communications Security, Zurich, 1997

[13] M. Reed, P. Syverson, D. Goldschlag: Anonymous Connections and Onion Routing, IEEE Journal on Selected Areas in Communications – Special Issue on Copyright and Privacy Protection, 16(4), 1998

[14] A.P. Sheth, W.v.d. Aalst, I.B. Arpinar: Processes Driving the Networked Economy, IEEE Concurrency, Vol.7, No.3, 1999

[15] P. Syverson, M. Reed, D. Goldschlag: Private Web Browsing, Journal of Computer Security, Vol. 5, No. 3, 1997

[16] P. Timmers: Business Models for Electronic Commerce, EM – Electronic Markets, Vol.8, No.2, 1998

[17] H. Wang, M. Lee, C. Wang: Consumer Privacy Concerns about Internet Marketing, Comm. of the ACM, Vol. 41, No. 3, 1998