Technical University of Vienna
Information Systems Institute
Distributed Systems Group

A phase model for e-commerce business models and its application to security assessment

Manfred Hauswirth, Mehdi Jazayeri
and Markus Schneider
M.Hauswirth@infosys.tuwien.ac.at
M.Jazayeri@infosys.tuwien.ac.at
markus.schneider@darmstadt.gmd.de

TUV-1841-00-04 June 5, 2000

New e-commerce business models attempt to exploit information technology to overcome the limitations of traditional business models. The usual motivation is to lower costs by improving the efficiency of business processes. One of of the basic requirements for the success of these business models is security mechanisms against theft or other fraud. Early e-commerce systems used customized security solutions. With the rapid increase in the numbers of such systems, however, developing customized security mechanisms for each system is not a viable solution. Another reason against the use of customized security solutions is the complexity of the new business models and their continuous evolution. The complexity of the models stems from an increase in the number of roles and interactions. The simple customer-vendor model is often augmented by a large number of third-party intermediaries, complicating the overall security assessment of e-commerce business models. To address these problems, this paper presents a simple approach to understanding e-commerce business models by phases in business processes and roles and interactions in each phase. A concrete business model is defined by mapping it onto a certain sequence of phases. We use our model to categorize several new business models of current interest to the business community. We 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.

Keywords: E-commerce, modeling, security assessment

Argentinierstr. 8/184-1
A-1040 Vienna, Austria
phone: +43 1 58801-4470
fax: +43 1 5058453
URL: http://www.infosys.tuwien.ac.at/

A phase model for e-commerce business models and its application to security assessment*

Manfred Hauswirth[1], Mehdi Jazayeri[1] and Markus Schneider[2]

[1]Technical University Vienna, Information Systems Institute,
Argentinierstr. 8, A-1040 Vienna, Austria
[2]GMD - German National Research Center for Information Technology,
Institute for Secure Telecooperation,
Dolivostr. 15, D-64293 Darmstadt, Germany
{m.hauswirth|m.jazayeri}@infosys.tuwien.ac.at,
markus.schneider@darmstadt.gmd.de

Abstract. New e-commerce business models attempt to exploit information technology to overcome the limitations of traditional business models. The usual motivation is to lower costs by improving the efficiency of business processes. One of of the basic requirements for the success of these business models is security mechanisms against theft or other fraud. Early e-commerce systems used customized security solutions. With the rapid increase in the numbers of such systems, however, developing customized security mechanisms for each system is not a viable solution. Another reason against the use of customized security solutions is the complexity of the new business models and their continuous evolution. The complexity of the models stems from an increase in the number of roles and interactions. The simple customer-vendor model is often augmented by a large number of third-party intermediaries, complicating the overall security assessment of e-commerce business models. To address these problems, this paper presents a simple approach to understanding e-commerce business models by phases in business processes and roles and interactions in each phase. A concrete business model is defined by mapping it onto a certain sequence of phases. We use our model to categorize several new business models of current interest to the business community. We 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. Vendors and customers of various market segments are trading via the Internet using a number of different business models. Additional new business models emerge due to the dynamics in e-commerce and new demands in the electronic markets. Of course, the main goal of doing business is to make profit under the assumption that every involved party respects the rules that are defined by the legal framework (if such a framework already exists and if it is applicable to the trans-national character of e-commerce). As in real life this assumption is clearly too idealistic: Experience shows that e-commerce suffers from the same possible threats, such as theft or fraud, as non-electronic business. Even worse the possibilities of the electronic environment sometimes make it easier to commit illegal actions at a larger scale. The new business models, however, can only be successful if their technical design and implementation are done in a secure way to prevent threats. Thus, beside base technologies, such as exchange formats, interaction protocols, and payment systems, security is a main issue in e-commerce [15].

In early e-commerce systems the business models were quite simple. Typically they were electronic re-implementations of traditional models with a small number of involved roles, for example, customer-vendor, customer-vendor-bank. These systems used customized security solutions and considered mainly peer-to-peer security, i.e., security issues between two communication partners (2-party security). With the rapid explosion of such systems, developing security mechanisms from scratch each time is no longer a

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

viable solution. Additionally, 2-party security cannot easily be generalized to *n* interacting parties (n-party security), because with the number of interacting parties also a much higher number of security threats is possible (for example, by collusions between parties).
This is especially true because the new business models are complex and evolving because they are based on the business cooperation between several partners. The complexity derives from an increase in the number of roles and interactions. The simple customer-vendor model has been augmented by a large number of intermediaries and suppliers. The new business processes frequently have a higher complexity and have no corresponding analogs in the real world, i.e., they are not re-implementations of traditional business models. Furthermore, new techniques such as sophisticated user profiling are introduced. A security model must apply to all roles and interactions and support the integration of specific security solutions based on the specific requirements of the e-commerce business model.
As in the tangible world e-business is done in phases: advertising, negotiation (ends with a contract), ordering, payment, and delivery (relevant mainly for businesses involving intangible goods). Depending on the concrete business model phases may be left out or their order may be changed. For example, payment could be done before or after delivery. The business models themselves are defined by mapping these phases onto the parties interacting in a business model, i.e., which parties interact in which phase of the model.
With the new business models, which involve more parties and more complex interaction, and the upcoming domain of i-commerce (trading of intangible goods such as information or software), new security problems arise for which technical solutions exist but have received little attention so far. Secure and trustworthy commercial relationships require a better understanding of the risks and how they can be addressed technically. Once an attack is successful and becomes public, the harm resulting from the loss of reputation can be much higher than possible direct monetary losses caused by the attack. To prevent successful attacks the important questions to be answered are:

- What are the potential security holes of the new business models?
- What are the differences for these business models from a security point of view if dealing with tangible and intangible goods?
- Can these problems be solved under simple assumptions in the trust model?
- Can these problems be solved under harder assumptions in the trust model (for example, colluding partners)?
- What are the security methods to solve these problems?

A systematic and general approach to discover all possible problems and scenarios has not been defined so far. At the moment security analysis of business models is done ad hoc and heavily depends on intuition and experience. Answers to the previous questions can only be given for the new business models in a general form. Specific variants of business models may yield new security problems.
This paper presents a phases model for e-commerce systems which is applied in a systematic approach to assess the security of an e-commerce business model and discusses techniques to overcome possible threats. Section 2 presents the phases model. We describe the involved business roles and the exchanged artifacts. Then we break down the business process into phases (advertising, negotiation, ordering, payment, and delivery) and describe them. The actual business models are derived by mapping the phases onto the roles that interact in a certain phase and the sequence in which the phases occur. At the end of this section we classify the currently relevant business models in terms of our model. As a prerequisite for a security analysis of business models Section 3 describes the security threats to be considered. Section 4 then maps the security threats onto the business process phases (and thus onto the business models), analyzes possible threats for each phase and presents security mechanisms to overcome them. This allows us to define the security threats for a specific business model and how they can be addressed. Finally Section 5 rounds out the paper with our conclusions.

2 Modeling the Business Process

According to [18] a business model for e-commerce is defined as

- an architecture for the product, service and information 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.

In this section we define a general model for e-commerce business models according to this definition. The definition will be done in several steps: First we will describe the involved business actors and their possible roles and the exchanged artifacts. Then we will define and describe the phases every business model may involve including the possible services, information flows, benefits for the business actors and sources of revenues. In the final step we map these phases onto the 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 that will be done in Section 4. Additionally the phase model facilitates to cover all possible business models even if they are currently not used.

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, order, enhance, or aggregate information products, or provide mediation, negotiation, delivery, security, 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 (e.g., a credit card company offers electronic payment services for customers and providers).
In the trading (business) process between these actors the following main artifacts are produced, used, exchanged, and modified [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, tangible or intangible) 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 required in special types of models 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, negotiation, ordering, payment, delivery.
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. Advertising can be implemented in many different ways. For example, offers could be published on a web server waiting for parties to access them, they can be actively distributed via mailing lists or push systems, or they can be gathered by an active search component (mobile agents) which was equipped with a searching party's criteria.
Negotiation: Once a party has found a product of interest it can start negotiating the business terms and possibly the properties of the product. In the simplest case no negotiation takes place at all (because the

provider's offers are not negotiable or because the customer is satisfied with the offer) and the requesting party accepts the offer. Independently of the concrete negotiation process the negotiation phase ends with an agreement between the involved parties as a necessary prerequisite for the following phases. Negotiation and advertising can trigger each other mutually: If no agreement can be reached a party 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, i.e., some kind of payment occurs. 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. For example, the full price of the product could be paid at once or in rates, a flat-fee may be paid for a service, or a pay-per-use fee may be due for each use of a product. Since these models involve very different concerns we address the conceptual superset of their security issues but do not go into detail with the applied payment systems and assume that the payment transaction itself is secured in a feasible way.

Delivery: In this phase the involved product is delivered to the requesting parties. Security in the delivery phase heavily depends on the nature of the product. For tangible goods the security precautions well-known from non-electronic commerce systems apply. For intangible goods, however, new security issues must be taken into consideration. For example, intangible goods such as programs or documents may be duplicated by a malicious party and distributed or sold without the knowledge or consent of the copyright holder (copyright infringement, fraud); a party may have the permission of the copyright holder for licensed production but pays the license fee for a subset of the copies only; the product could be tampered with on its way to the receiving party; or the product may never reach the intended recipient due to theft or simply because of technical problems (network failure, system crash). These scenarios require special consideration to obtain security standards for intangible goods which are comparable to tangible goods. 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. For example, if advertising is mapped onto the customer and the intermediary, but all other phases are done directly between the customer and the provider, as shown in Figure 2, then this defines the *associated partner* business model.

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. This simplifies the presentation but does not exclude other models or violate the general applicability of the approach because it facilitates to model the superset of possible security concerns and abstracts from the initiating party: 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 of the incremental model and must be applied; and if the initiative in a phase is reversed, then the security issues can easily be derived from the original phase in the incremental model.

Depending on the applied business model the sequence of phases may differ from the sequence in the incremental model as discussed below. For example, the advertising and negotiation phases will occur in the order given below and the sequence of the following phases may be changed. In another business model a product might be delivered to a party without prior advertising, negotiation, and ordering, on the basis of a party's profile. In such a model, the receiving party may test the product; send it back if it is not interesting, or in case it is, enter into the negotiation and payment phases afterwards. Some business models may require payment to follow the successful delivery of the product.

In principle any sequence of the phases is possible depending on the business model. We use the incremental model as a special configuration without constraining generality to enable easier assessment of the security concerns. Also the number of intermediaries involved may differ. For each phase in the process a dedicated intermediary may be used. For example, one intermediary may be in charge of advertising, negotiation, and ordering, payment may be done via the services of a credit card company, and delivery would

be provided by a specialized logistics company. However, this does not have an impact on the general applicability of our model.
Figure 1 shows the simplest model (UML sequence diagram [14]) where all interactions occur directly between the customer and the provider (for clarity reasons the UML diagrams are not complete but focus on the main interactions and data flows).

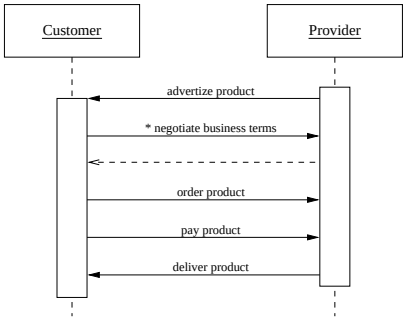

Fig. 1. Direct model: customer and provider do not employ an intermediary

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 (if the phases are supported by software and do not simply rely on the user filling out web forms and thus driving the process via the input data). This model is typically known as *e-shop model* or *portal*, if the portal is focussed on the products of one provider. Since many of the terms denoting such models are rather fuzzy, overloaded, and imprecise we introduce our own terminology with exact definitions and then relate this terminology to the common current terms (this may be a m:n mapping). In our terminology we call the model given in Figure 1 the *direct model* of e-commerce. In the direct model the provider is in full control of the whole process 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 2 the intermediary takes over the advertising phase from the provider.

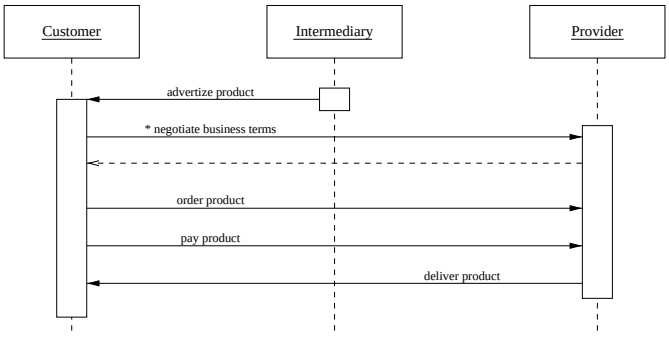

Fig. 2. A model: intermediary advertises

To be able to do advertising for a provider (typically one intermediary will do this for many providers) the intermediary needs marketing information from the provider. Marketing information can be of very different quality. For example, it may be a description of the provider or individual products, or a product catalog (with or without pricing information). We summarize this class of artifacts under the term *catalog*.

On the basis of the catalog's information the intermediary can advertise the products of the provider in many ways. For example, (parts of) the catalog can be put on the intermediary's web sever, sent to customers and other intermediaries via email, push systems, or ICE [20], and entered into search engines.
The A model is applied frequently in current e-commerce applications. Successful sites like Amazon.com are based on this model: Amazon.com advertises the books and CDs of various publishers on its web site and via links that third-parties can put on their web sites which refer to Amazon.com's web site or specific parts (products). The A model corresponds to *(process) portals* [16] such as Amazon.com and/or *associated partner programs* such as Amazon.com's [1].
In the *AN model* shown in Figure 3 the intermediary provides negotiation service additionally to advertising.

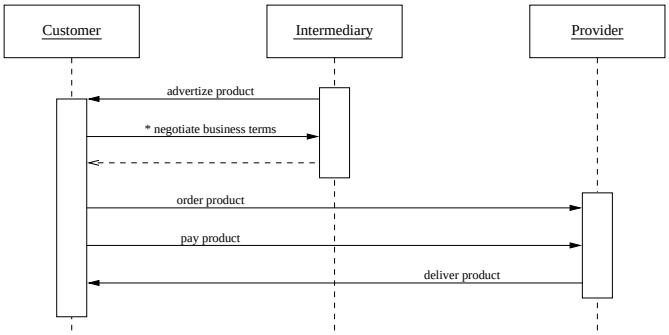

Fig. 3. AN model: intermediary advertises and negotiates

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 and completeness 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, order size, payment procedure, etc. This heavily depends on the amount of information a provider wants to disclose to the intermediary.
Figure 4 shows the *ANO model* in which the intermediary also does order processing on behalf of the provider additionally to advertisement and negotiation.

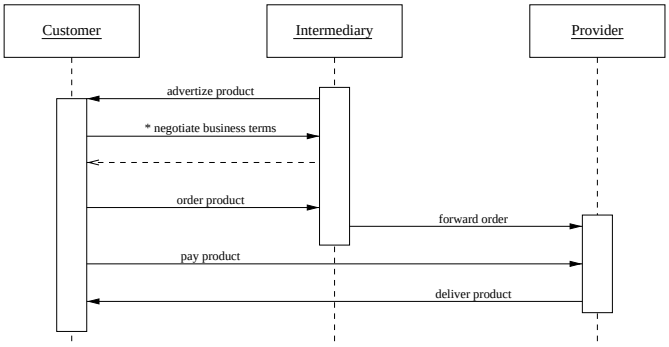

Fig. 4. ANO model: intermediary advertises, negotiates, and processes orders

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. With this information at hand the intermediary can request all required information from the customer to create and send a correct order that the provider will accept. Figure 4 does not define whether each order is sent immediately to the provider: It is also possible that the intermediary collects orders and sends 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 sub-orders 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).
Figure 4 depicts the *ANOP model* in which the intermediary provides a payment service on behalf of the provider additionally to advertisement, negotiation, ordering.

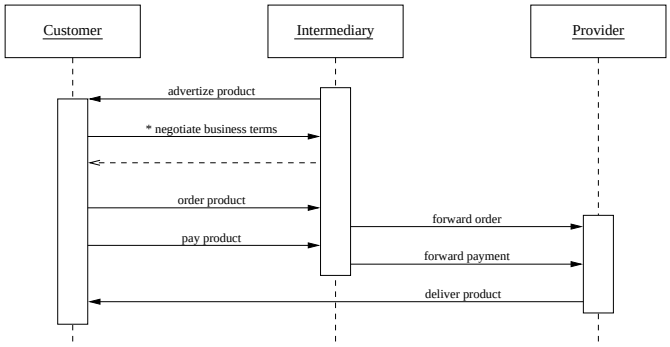

Fig. 5. ANOP model: intermediary advertises, negotiates, and processes orders and payment

Due to the number of available payment services the intermediary may also act as a payment gateway in this configuration. Any combination of payment services and payment processes can be used here. For example, the customers may pay the intermediary using a micro-payment protocol such as Millicent and the intermediary accomplishes payment with its providers via a macro-payment protocol such as SET after having accumulated a large number of customer payments to keep SET transaction costs low. This separation frees the customer and the provider to support a large number of different payment mechanisms.
Finally, Figure 6 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.

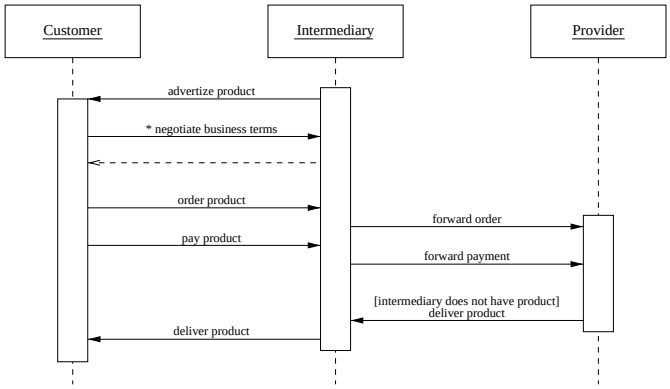

Fig. 6. ANOPD model: intermediary advertises, negotiates, processes orders and payment, and delivers

Typical delivery mechanisms are (as in all other configurations): download (the customer gets a user name and a password and can download the product from a web or FTP site), email (the product is mailed to the customer), push (the customer receives the product via a push system; this is useful for products which evolve over time such as news or stock quotes), or physical shipment via courier services. The last case is relevant especially if tangible goods (CDs, books, furniture, wine, etc.) must be shipped. This type of shipment is outside the scope of our model.
Additionally the intermediary may 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 including licensed production. This may dramatically simplify delivery for the customer and still support the use of sophisticated delivery mechanisms between the intermediary and its providers. Several delivery arrangements are possible in the ANOPD model: The intermediary may request

the product from the provider every time it needs to deliver it; the intermediary may have the product on stock and request a certain quantity from the provider only if its stock goes below a certain threshold, or the intermediary may be licensed to "produce" the product (licensed production). Production in this context actually means that the intermediary may add a valid serial number to the product or has been provided with the unfinished product and some software to create the final product. In any of those delivery arrangements new security problems are introduced. Since the intermediary physically has the product, it may produce unlicensed copies and sell them. This is a general problem with intangible goods and will be discussed in Section 4. A possible solution for part of this problem is the application of double fingerprinting by the producer and the intermediary.
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. For example, the intermediary may combine stock quotes with analyses and sell this new kind of information. 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 in order not to constrain its generality. As an example, we also consider the *ANOD model* where the delivery is taken over by the intermediary while payment still is done between the customer and the provider and evaluate its security in Section 4. We have chosen this example because of its high relevance in real configurations. For example, the provider may not have enough network bandwidth to efficiently distribute its information goods to a high number of consumers while the intermediary has but it may not want to hand over payment to the intermediary. In this case the ANOD model would be applied.

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* and the *associated partner* model 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 [16] 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 [16] 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 [16]. 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

Security is widely understood as a key point for the acceptance of e-commerce. Parties that are involved in business relationships gain security by applying technical and organizational means. 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 caused by certain security holes. If security costs exceed the estimated losses, security solutions cannot be justified economically.

Security methods can be classified into those providing prevention of attacks (e.g., encryption for concealment of information) and those for detection of attacks (e.g., verification of message integrity or 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. These concepts either always use TTPs or the TTPs are used only when some party cheats.

Actions of malicious parties which should be prevented in business processes 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, or the offering party may have to reveal its price model which could be interesting for a competitor. Studies have shown that users want to reveal as little personal information as possible because they fear loss of privacy and potential misuse [6, 19].

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 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 so far as 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, 17], but can not 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 exchanging encrypted 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. The motivation for masquerading in business relationships may be for profit or simply being detrimental to others. 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 was really sending the received message. Authentication methods can also be classified according to whether they can be used as evidence to convince a third party or not. If they can be used they already have the quality for the introduction of non-repudiation, as will be discussed below. E.g., a message authentication code (MAC) would be no sufficient evidence to convince third parties undoubtedly that a message originated from a claiming party, whereas a digitally signed message would [9].

Manipulation of messages is another security problem in business relationships that has to be prevented. E.g., an attacker that 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 is also simply being detrimental to others or for profit. 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 sufficient 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 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 the seller can fingerprint each sold copy on his own. But if he also wants an evidence for a third party to proof 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 would have 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 must be able to identify the buyer if he 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 very briefly described above are the basic technical means to avoid privacy infringement and fraud in business processes. Beside these technical means also organizational means and the careful assignment of responsibilities in organizations—which are beyond the scope of this paper—are necessary [2].

4 A Security View on Business Processes

In this section we show security problems in complex business processes involving three parties. The well-known direct model of two interacting parties (provider and costumer) need not be discussed: The application of digital signatures in offers and orders makes them verifiable for authenticity, integrity and non-repudiation purpose, and secure payment systems and copyright protection (e.g. fingerprinting) exist (intangible goods). Our discussion of security issues in 3-party models describes *possible* solutions—we do not claim that the presented solutions are the only ones.
In the discussion of the models we assume as little trust as possible and that security is based on technical means. We also address the issue of non-repudiation, which is required to obtain binding messages, wherever possible. In general, we assume that all communication shown in the following subsections will be encrypted to prevent external parties from wiretapping.
In the following, we discuss the A, AN, ANO, ANOP, and ANOD models. In all these models, three parties are involved for the execution of the 5 phases. Since in the ANOPD model requires only 2 parties interact in these phases the basic security issues are already covered as in the direct model.

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 intentional 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 and afterwards claim that P required this.
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. From a security point of view the first case is not interesting. 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 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 spends there. 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 ANO model, I is also responsible for forwarding the order as a signed contract to P. In the AN model the ordering is done by C himself. 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 a contract or order form which is provided by P. In the AN model, the contract is sent to P by C, while in the ANO model it is sent by C and forwarded by I. The contract and the signature can be verified by P and additionally it can check whether I followed the rules of the pdm. If not, for example, because I's offered price was to low, 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 or timestamp) because copies of the same contract will not be accepted by P. This prevents an intermediary from sending a contract multiple times. 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 for the same contract. 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 the commission. 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 as in the previous model.

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 signing 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 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 requires 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 also act as an intermediary for several providers $P_1, \ldots, P_n$ it can aggregate and concentrate lots of personal data which can be of high relevance for I's own core business.

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. To build up such a business relationship it is not even necessary that they know each other. 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 and request the money again. All these problems can be solved easily with the help of the involved payment authorities that have registered all money transactions. To illustrate this, consider the case that I claims that C did not pay after the placement of the order. C would react by claiming that it paid but did not receive a confirmation from I. In this situation it is not clear who tries to cheat. This problem can be solved easily by means of trustworthy payment authorities. Suppose that C has paid and a malicious $\tilde{I}$ tries to cheat by claiming that C did not pay and does not reply the payment confirmation. In this case C can get a confirmation from its payment authority that proves the payment. With this confirmation $\tilde{I}$ is forced to send the payment confirmation. In the other case in which a dishonest $\tilde{C}$ did not pay the requested amount it can never get a confirmation of an honest payment authority. Being unable to get such a confirmation would force $\tilde{C}$ to pay. Afterwards I will confirm the

receipt of the payment. Thus the intervention of a trustworthy payment authority assures that I receives the payment and C receives the confirmation in both cases.
After deducting the commission, I forwards the rest of the payment to P with a clear and 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. If I later denies having sent the message, P can use the accompanying evidence as proof against I. 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 as already described above.
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 keeps 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 ordered good(s) in advance. 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 from all the orders it received 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 that P has received a copy of each specific order. (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 his 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 as explained in the ANOP model.
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 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 by via a delivery service if the ordered good(s) are on stock. 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. I or the delivery service do not hand over the tangible good(s) if they do not receive a confirmation by C. Thus, as long as I has no confirmation of delivery from C it is enforced to 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 multiple time 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 the infringement of copyright. 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—I or C—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. 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. It is required that the two asymmetric fingerprints do not interfere with each another.

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 him about C to be a legal buyer. This proves that I is honest. Additionally, P can verify itself if C is known to him as 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. There are no special or one-way trust prerequisites that are necessary for the 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 is responsible for delivery and 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. To be worth the effort the additional costs caused by these mechanisms must be much lower than the costs of the 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

In the previous sections we have discussed different business models involving 3 parties from a security point of view. We have analyzed the potential for privacy infringement and fraud for these models and have shown the minimal mechanisms to secure them. The discussion shows that model 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 reasonably 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 (copyright infringement) 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 the 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 partners 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. Ross Anderson: Why Cryptosystems Fail, Communications of the ACM, Vol. 37, No. 11, November 1994
3. W. Diffie, M. Hellman: New Directions in Cryptography, IEEE Transactions in Information Theory 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, November, 1995,
5. D. Goldschlag, M. Reed, P. Syverson: Hiding Routing Information, Proceedings, Information Hiding, Springer Verlag, LNCS 1174, 1996
6. D. Hoffman, T. Novak, M. Peralta: Building Consumer Trust Online, Communications of the ACM, April 1999, Vol. 42, No. 4
7. M. Jazayeri, I. Podnar, A Business and Domain Model for Information Commerce, Technical report TUV-1841-00-02, Technical University of Vienna, Distributed Systems Group, May 2000, http://www.infosys.tuwien.ac.at/reports/repository/TUV-1841-00-02.ps
8. D. Konstantas, J.-H. Morin: Trading digital intangible goods: the rules of the game, Proceedings of the Hawai'i International Conference On System Sciences, January 4-7, 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, Proceedings of the IEEE, Vol. 87, No. 7, July 1997
11. B. Pfitzmann, M. Schunter: Asymmetric Fingerprinting, Eurocrypt '96, LNCS 1070, Springer Verlag, 1996
12. B. Pfitzmann, M. Waidner: Asymmetric Fingerprinting for Larger Collusions, Proceedings, 4th ACM Conference 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 Protetction, 16(4), May 1998
14. J. Rumbaugh, I. Jacobson, G. Booch: Unified Modeling Language Reference Manual, Object Technology Series, Addison-Wesley, Reading, Mass. and London, 1999
15. D. Schoder, R.E. Strauss, P. Welchering: Electronic Commerce Enquête 1997/98, Survey on the Business of Electronic Commerce for Companies in the German Speaking Area, Stuttgart: Konradin, Executive Research Report, 1998
16. A.P. Sheth, W. van der Aalst, I.B. Arpinar: Processes Driving the Networked Economy, IEEE Concurrency, Vol.7, No.3, 1999
17. P. Syverson, M. Reed, D. Goldschlag: Private Web Browsing, Journal of Computer Security, Vol. 5, No. 3, 1997
18. P. Timmers: Business Models for Electronic Commerce, EM – Electronic Markets, Vol.8, No.2, 1998
19. H. Wang, M. Lee, C. Wang: Consumer Privacy Concerns about Internet Marketing, Communications of the ACM, March 1998 / Vol. 41, No. 3
20. A.N. Webber, A.C. O'Connell, A.B. Hunt, A.R. Levine, A.L. Popkin, A.G. Larose: The Information and Content Exchange (ICE) Protocol, World Wide Web Consortium (W3C), 26 Oct. 1998, http://www.w3.org/TR/1998/NOTE-ice-19981026