Informatics Ethics and Law

Prof. Dr. Eşref ADALI

Ethics in E-commerce

12

E-commerce

- It is known that large firms have been trading in the trade through computer communication since the 1970s. This type of trade is carried out over a private network (VAN: Value Added Network). As a result of the spread of Internet, e-commerce has developed mostly for individual use. E-commerce in this way is developing very fast. E-commerce, which facilitates the shopping process of people, has brought with it different problems.

- Trade has three basic principles:
- Trade requires a safe environment.
- The buyer and seller must trust each other.
- Buying and selling should be happy with shopping.

- Adequate security is provided in e-commerce using EDI documents, which is carried out by large organizations over a closed network VAN, and the parties know each other very well.

TCP/IP Protocol

In Internet, TCP / IP protocol is used. This protocol basically consists of two layers; It consists of Top Layer (TCP: Transfer Control Protocol) and Bottom Layer (IP: Internet Protocol):

Top Layer: The data to be transmitted between computers is divided into packets and the packets are sent to the receiver. The receiver obtains the actual data by combining incoming packets.

Sub Layer: Forwards the packets to be transmitted to the recipient's address.

The top layer contains the Application and Transport layers.

Application Layer: It provides communication between applications on different computers.

Transport Layer: Provides data flow between two computers. This is the move from server to server.

The sub layer includes Internet Layer, Network Access Layer and Physical Layer.

Internet Layer: Source and target computers on networks connected by routers. It provides the transmission of data between.

Network Access Layer: It is considered as the interface that establishes the logical relationship between the computer and the network.

Physical Layer: It is the layer that determines the electrical and physical properties of the communication medium.

Security of TCP / IP Protocol - I

- **SYN Attacks:** In the TCP / IP protocol, computers set up in three stages. The server is in a listening state and waits for a request from the client. The request comes as SYN. The server receiving the request remains in the standby state for about 75 seconds. Generally, the servers are able to meet an average of 5 requests.

  Attackers who aim to engage the server can send a connection request one after the other, preventing them from serving by keeping the server busy. Such attacks, also called SYN deception, exploit the weakness of the TCP / IP protocol.

- **IP Deceit:** In such attacks known as IP deceit, the attacker uses a fake address instead of his own IP address. The attacker sends a fake IP address into the data packet he sends. The IP layer on the receiving side treats the address in the incoming data packet as the actual address.

  IP deceit-like attacks are usually done to disrupt the servers' service (DDos).

- **Estimating the Sequence Number:** The sequence number (Initial Sequence Number: ISN) used in the connection provided in accordance with the TCP protocol is 32 bits long. So it is unlikely to guess this number. If this number produced by the source computer is produced by following a certain rule, it is easier to guess. It is explained that the ISN produced by the Unix kernel is calculated according to a certain rule, so if the ISN used in the previous link is known, the next ISN number can be calculated. Attackers are trying many ISNs to take advantage of this weakness.

- **Resource Forwarding:** It is a situation where the response determines which way should reach which IP to reach. Since today's routers can determine the source router, this issue is no longer a problem.

Security of TCP / IP Protocol - II

- **Capturing the Connection:** In this method, which is called the seizing the connection or the man in between, the attacker gets between the two computers that are in connection. IP spoofing method cannot transfer additional security information such as Unix password, Keyberos and TKP between the two parties. However, in this method, the attacker ensures that the original process continues between the two computers and takes over the connection. In order for the man method in between to work, the man in between must be on the communication path of the two computers in the connection. The man in between transfers the data packets from both sides.

- **Routing Attack:** Routing Information Protocol (RIP), which is not absolutely necessary to be used in the TCP / IP protocol, but is used frequently. RIP identifies the shortest or recommended route on the network. It does not contain the original process in the RIP, so it does not try to verify it.

- Attackers taking advantage of these vulnerabilities can change the addresses that the message packet arrives and goes. In this way, attackers can capture message packets and change their content as desired.

- **ICMP Attack:** The message sent to alert the recipient side is called Internet Control Message Protocol (Internet Control Message Protocol: ICMP). This message is often referred to as pinging. After pinging, the sending side waits for the other party to respond. There is no authentication information in the ICMP message. Therefore, it is easily used in service disruption-type attacks.

- **Domain Name Service Attack:** Domain Name Service (DNS) is widely used in Internet. The process that converts people-friendly domain names to IP addresses understood by Internet Protocol is called DNS, and the servers that perform this process are called DNS servers. Thus, users can easily access web pages and servers. General attackers get the IP address of a server or a web page using the method called Domain Stealing. Then they access the DNS server and change the IP address corresponding to DNS. Thus, they can direct users to a different server or web page.

- **Absence of Unique Identity:** It was predicted that every computer could be given an address with IP method in the first periods when Internet started to be used. However, after a while it was seen that this was insufficient. Today, IP addresses defined temporarily or temporarily are changed by servers or address converters. Therefore, security systems based on location or temporary IP address are weak against attacks.

Secure Electronic Payment

- The main principle of the Secure Electronic Transaction (SET) protocol is that the payment to be made through Internet is not made directly to the seller by the customer, instead the payment is made through an intermediary institution (payment channel).

- SYB is required for both the customer and the seller in the secure payment system. Since SYB is used in the SET, reliable and confidential communication is provided between the customer, the seller and the bank. The payment process is set up securely, is maintained smoothly and prevents counterfeiting. The seller can only decide that the card was stolen or fake because he could not get information about the credit card.

SSL problems:

- SSL protects the customer from ear guests, however, it cannot be said to protect it from counterfeit sellers. Some sales sites can be fake or misleading sites. Such sites are set up to defraud customers. They defraud their customers in two ways:
  - 1- By imitating a reputable dealer or
  - 2- By creating a completely false site.

- 3D security systems have been developed to prevent such frauds. In the three-dimensional security system, a number is sent to the customer's mobile phone at the time of payment by credit card and the customer is asked to enter this number in the field on the payment screen. Thus, it is decided whether the person who wants to pay by credit card is a real customer or not.

SET Protocol

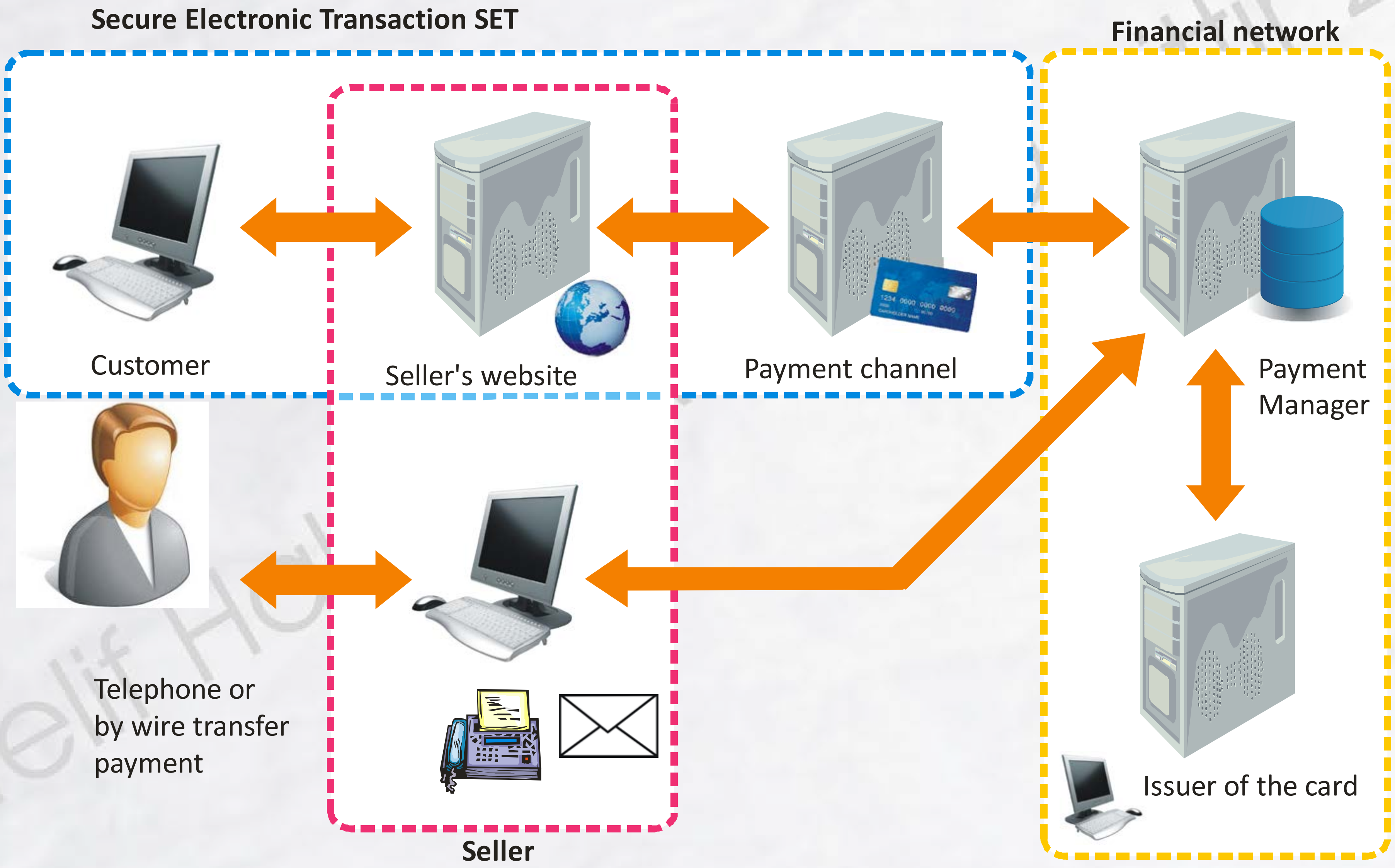
The basic principles are:

- Ensuring confidentiality of order and payment information.
- To ensure the integrity of the data related to the payment process and services.
- To ensure that the customer credit card account is completed.
- To ensure that the seller is hung.

In the SET protocol, a shopping process is defined as 9 steps:

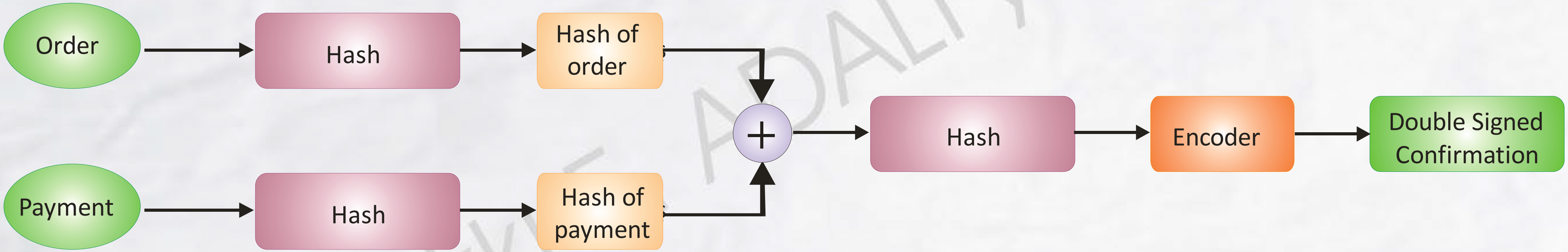
1. The customer connects to the seller's web page.
2. The customer sends two pieces of order and payment information related to what they want to buy. The first one is about shopping and is sent to the seller. The second part is credit card information and this information is sent to the seller to be sent to the bank where the seller is the customer.
3. The seller transmits the credit card information to his bank.
4. The bank of the seller requests the customer's credit card to be approved by connecting to the institution that issued this card.
5. The institution that issued the credit card to the customer sends approval to the bank of the seller.
6. The seller's bank sends confirmation to the seller.
7. The seller completes the order and sends the confirmation information to the customer.
8. It takes the transaction record related to the shopping from the seller bank.
9. The institution that issued the credit card to the customer sends the credit card payment document (receipt or invoice) to the customer.

How the SET Protocol Works



Combining Order and Payment Information

Order and Payment information is in two parts. The first piece is about shopping. We call this piece the order and it is being sent to the seller. The second part is about payment. This piece, which we call payment, contains information about the credit card and is sent to the seller's bank. The seller's payment information should not be seen more clearly, credit card information. These two parts need to be combined to complete a purchase.



Parties' Trust in each other in E-commerce-I

E-commerce over the Internet is divided into three classes:

Business to business e-commerce (B-B): Organizations that use Genelağ instead of VAN know each other, they usually trade for a long time. Therefore, important problems cannot be said.

E-commerce between business to customer (B-C): It is the most common e-commerce application today. Unrecognized organizations and individuals are unrealistic. Therefore, there are problems.

E-commerce between individuals (C-C): There is no evidence that both sides are real. Therefore, it is the most risky e-commerce way.

Business to business

In the trade between big companies on VAN, companies know each other and the communication network they use is closed and secure. Therefore, it is not an important source of problems in terms of ethics and law.

Parties' Trust in each other in E-commerce-II

Business to customer

Generally, problems with little-known e-commerce companies:

- **Sending defective product**: The product that is liked and selected on the e-commerce page is sent to the customer. However, the shipped product may be used, defective, defective or repaired. When the product is sent back, there may be companies that send a new one or those who do not respond at all. It is naive to expect a new and robust product, especially from companies that knowingly send the defective product.
- **Dispatching counterfeit goods**: A product is sent which is very similar to a product with a known appearance. It is certain that senders of counterfeit goods are fraudulent. So it is pointless to send the product back and wait for the actual product to be sent.

Some Far Eastern country companies sell licensed programs (especially operating systems) at cheap rates. The incoming product can be installed on the computer like a licensed product. When researching how such programs can be sold under market prices, the following result was found: Firms producing operating systems give computer hardware manufacturer firms a copy of these programs and give them the right to reproduce. They also define a license number for each replica. It is easy for the vendor to obtain a copy of the operating system program. They prepare their copies on CD or DVD and label them as original. They also add and market license numbers obtained from hardware manufacturers to the package.

- **Sending missing items**: Some products are sold in packs and how many are included in each pack. Fraudsters put less in packs than the number on the web page.
- **Sending counterfeit goods**: We hear people saying that instead of the disc, there is iron mass, instead of medicine, lime instead of medicine, instead of the book, the cover of the book is coming.

Parties' Trust in each other in E-commerce-III

- Banking transactions carried out over Internet can be considered as trade between organization and individual. People invest their money because they trust the banks. In Internet banking, stealing people's money is not an act of the bank. It is the job of robbers who steal client's account information and password.

- There are also events where customers deceive vendors. Generally, there are frauds on credit card payments. Once the structure of the credit card is known, a valid card number can be generated. There are also ready-made programs in Genelağ for this. Ability to generate and shop with a valid credit card number for countries where computerized credit card is not used and 3-D security is not applied.

Evaluation

As a result, whether the seller is reliable or not is very important in s-m type e-commerce. E-commerce firms with known and trusted backgrounds have Security Certificate and often use the SET protocol. Therefore, safe shopping can be done from these companies. Shopping from unknown companies should be avoided. Since individual customers do not need to have SYBs, sellers are required to take measures against counterfeit credit cards.

Parties' Trust in each other in E-commerce-IV

Between individuals

The most risky form of e-commerce is its interpersonal form. Because both sides do not have Security Certificate and it is not expected to happen. There are regulations developed to secure the payment between individuals. These are the organizations that undertake the money transfer between the buyer and seller. After the buyer and seller agree, the buyer sends his money to the intermediary. The intermediary company does not transfer the payment to the seller until the buyer says that he has received the product.

In the interpersonal trade, there may be problems described in the previous section:

- Shipping of defective products
- Sending counterfeit goods
- Submitting missing product
- Sending fake products

Satisfaction of the Parties in E-commerce

For a trade to be considered as a trade and to be sustainable, the buyer and the seller must be happy with the shopping. A customer who knows that there is no security problem always chooses to buy a product from a trusted vendor. Because:

- The seller does not have to go to his place to select the product. In particular, it is sufficient to select products from the e-commerce site, since it is not necessary to manually examine the products that are known and produced in accordance with the measurements. It makes the customer happy to place an order at any time and bring the product to its feet.

- Knowing the guarantee that he can change the product he purchased without any reason, makes it easier and faster to make his shopping decision. It further affects the decision of the seller to be sent back. This convenience opens the way for ordering multiple products. It can send back the dislikes of the products sent within a certain period of time. Thus, he is happy with the feeling that he has brought the products and the seller to his feet.

- In e-commerce, the seller does not need large areas to display the products. It may not even need to store products in its own warehouse. After receiving the order, you can ask the manufacturer. With this method, it provides huge savings from operating expenses. There will be no expenses such as heating, cooling and lighting of the salesperson and the environment required for on-site sales. It is highly profitable to sell products or services with an e-commerce method for an organization whose expenses will be very low.

- With e-commerce, products and services can be sold worldwide. Therefore, the turnover of companies increases thanks to e-commerce. This is also happy for the seller.

Ethical and Legal Issues in E-Commerce-I

Ensuring Security

It is the duty of the public to ensure the security of the trading environment. It is not the duty of customers and sellers to ensure the security of the trade on the general. As described in the relevant section, a lot of work has been done to ensure the security of e-commerce. Unless customers steal their ID and credit card information and passwords, there should be no problem. The events and their evaluations by breaking the security are as follows:

- Stealing the user's credentials and passwords is a type of robbery that is performed by stealing the account information and password used in banking transactions. Some examples were given in Chapter-3 about such robberies are described. The robber ensures that the spy program is installed on the client's computer and thanks to this program, he can learn the account number and password of the client.

- In the cases filed at the end of such robberies, the subject has been much discussed. The customers said that the bank is a reputable and reliable institution, so they should be responsible for the robbery. On the other hand, banks argued that the customer should keep the key information used in entering the bank. In fact, both sides are right. However, the fact that banks are reliable and responsible institutions pushed them to find new and effective solutions to increase security.

- In case of robberies arising from the security of Internet, if the customer does not have an intent or a defect, the sellers are held responsible. They are said to provide the necessary security measures.
- In the meantime, it should not be forgotten that customers can deliberately make robbery in their accounts.

Ethical and Legal Issues in E-Commerce-II

Seller's Reliability

- **Sending a defective product:** If a seller deliberately sends a defective product, it can be said that the seller is a fraudulent. Therefore, it would be an effort to send the product back and ask for a new one. In this case, it is not very meaningful to try the remedy. The first reaction of the seller will be: We sent a solid product; He will say that you broke it. It is very difficult to refute this argument since the customer will not have a neutral witness while taking the product. It is even more difficult to seek rights in court if the seller and the customer are in different countries. If the same company proves to sell similar defective products in the same country, the court may find the culprit.

- **Sending counterfeit goods:** It is clearly fraudulent for a seller to display the original product on the website and send the counterfeit to the customer. The purpose of such sellers to set up an e-commerce site is fraud. Therefore, it is difficult to deal with them by law. They soon close their companies and open a new e-commerce site with a new name.

- **Shipment of missing product:** We can make the same evaluation among sellers who send missing product.

- **Sending counterfeit goods:** Even if the company sends iron mass instead of disk and lime powder instead of medicine, even the fraud title is insufficient.

The reasons that lead the customers to shop from such places;
1- The prices are cheap everywhere;
2- They find products that they cannot find elsewhere.
The customer should think that there is a reason why the product is cheap. In the meantime, it is useful to do research in Internet about the seller. There are two reasons why a product that is not sold elsewhere can be found on this type of site: Either this product is not legally sold or the product they call we sell is fake.

E-ticaretteki Etik ve Hukuk Sorunları-III

Müşterinin Güvenilirliği

Müşteri kılıklı kişilerin satıcıları dolandırdıkları da görülmektedir. Hatta bu tür dolandırıcılıkları örgütlü biçimde yapanlar da vardır. Örneğin Genelağ'daki banka dolandırıcılığı eylemlerinin bazıları örgütler tarafından yapılmaktadır. Bunlarda karşı önlemleri satıcı firmaların almaları gerekir. Soygun amaçlı örgütler genellikle bulundukları ülkenin dışında bu tür soygunları yapmaktadırlar. Böylece yasalardan kaçabilmektedirler.