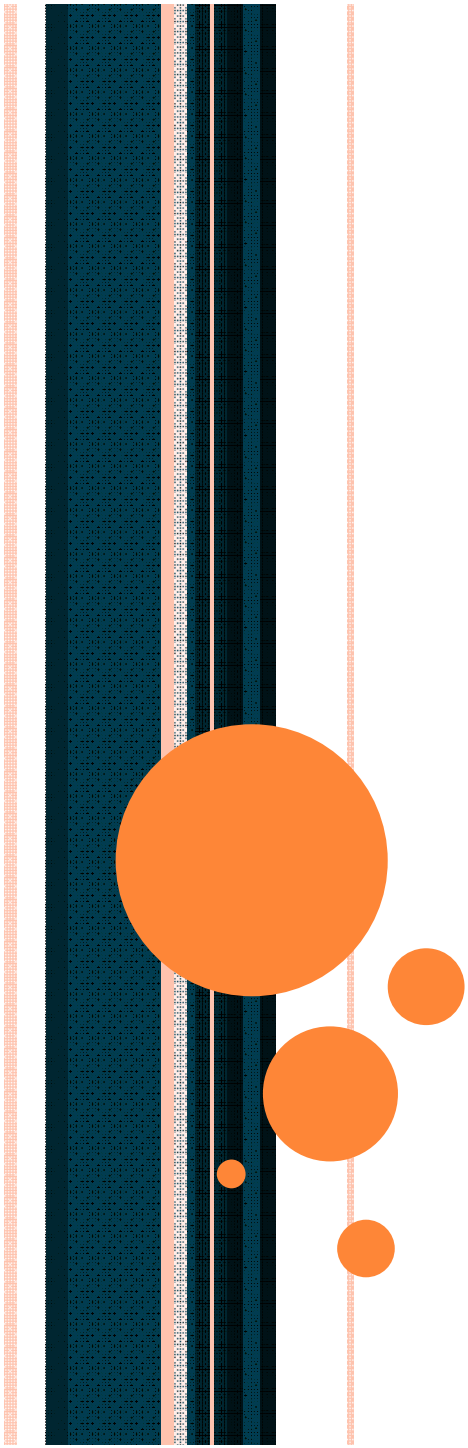


E-COMMERCE SECURITY

Dr. Bhawana Rudra

NITK

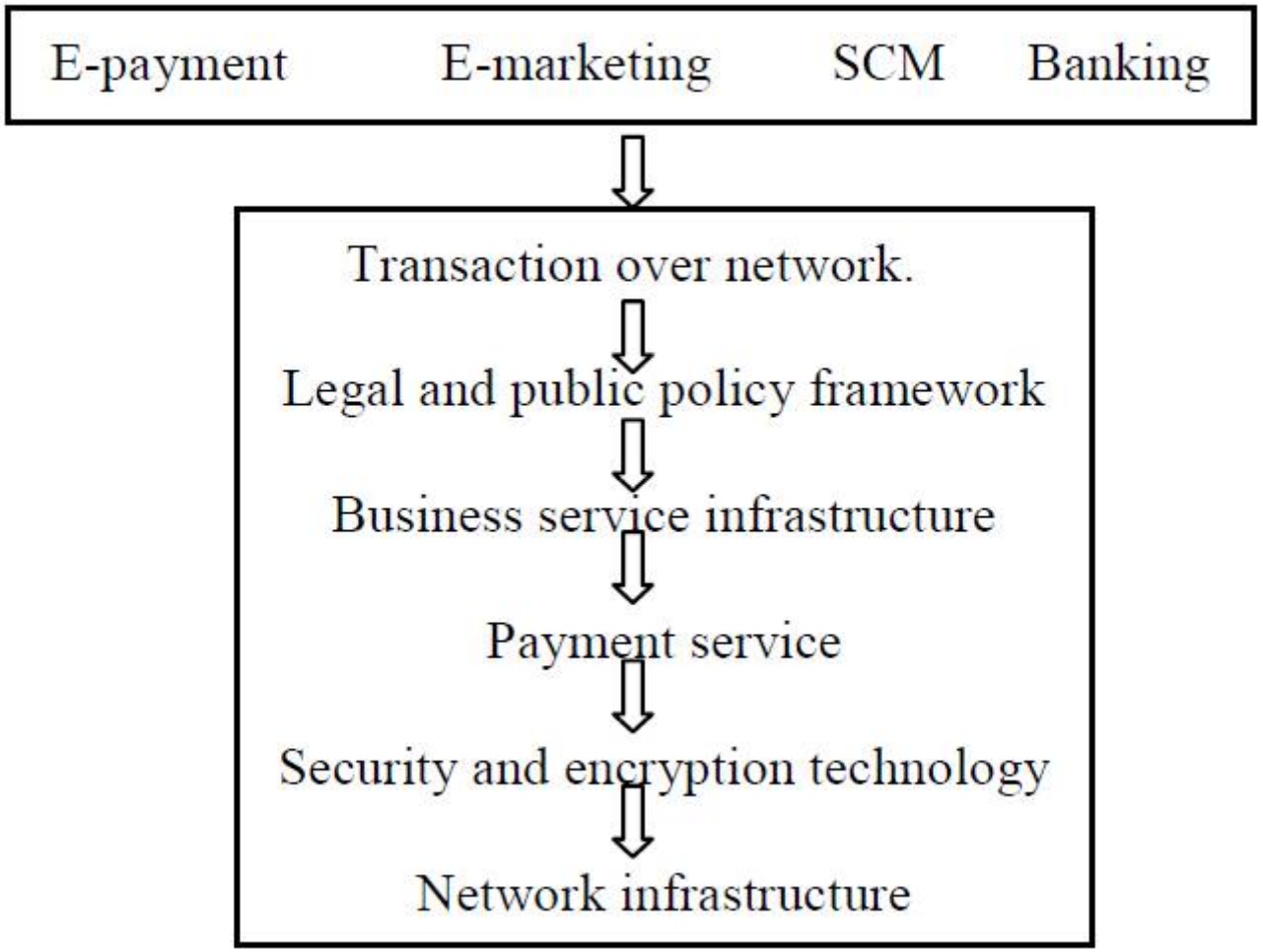
- Disclaimer: The Information and images are taken from various sources of web.

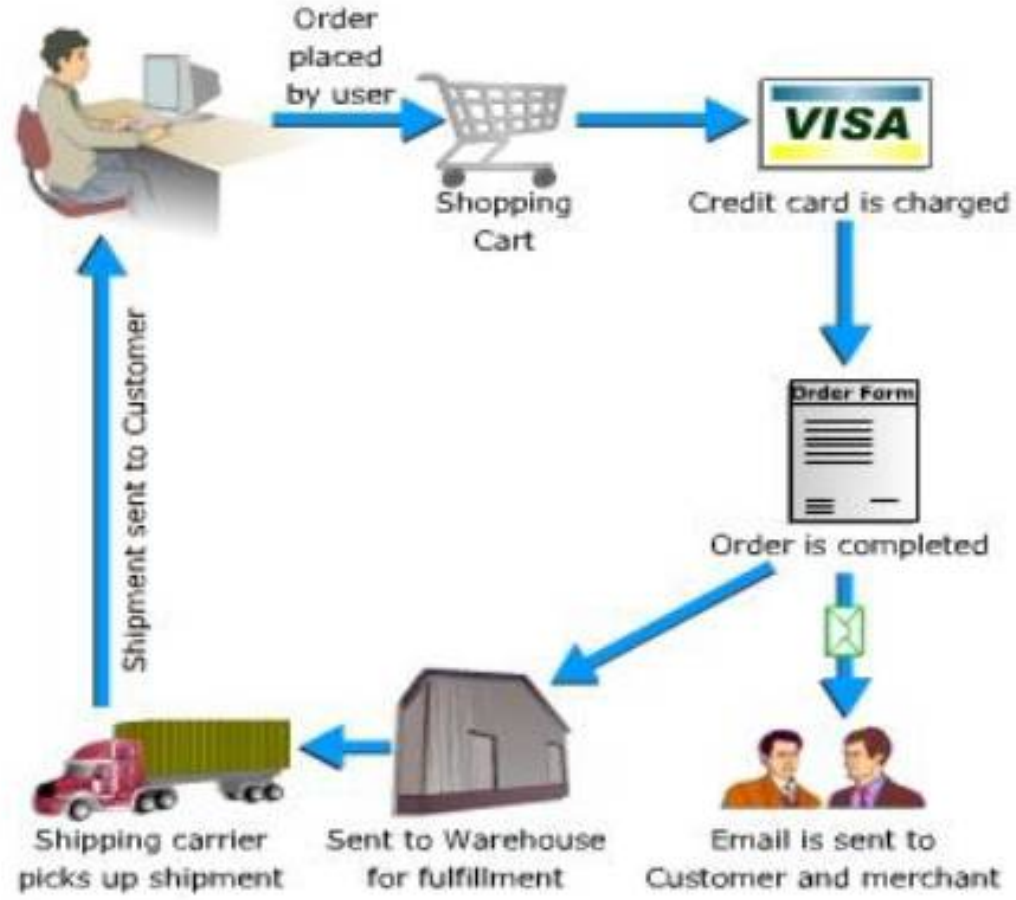
WHAT IS COMMERCE AND E-COMMERCE ?

- **Commerce**--Commerce refers to all the activities the purchase and sales of goods or services.

  --Marketing, sales, payment, fulfillment customer service

- **E-Commerce**--Electronic commerce (E-Commerce) is doing commerce with the use of computers, networks and commerce-enabled software (more than just online shopping)


E-payment
E-marketing
SCM
Banking
Transaction over network.
Legal and public policy framework
Business service infrastructure
Payment service
Security and encryption technology
Network infrastructure


Order
placed
by user
Shopping
Cart
VISA
Credit card is charged
Order Form
Order is completed
Email is sent to
Customer and merchant
Sent to Warehouse
for fulfillment
Shipping carrier
picks up shipment
Shipment sent to Customer

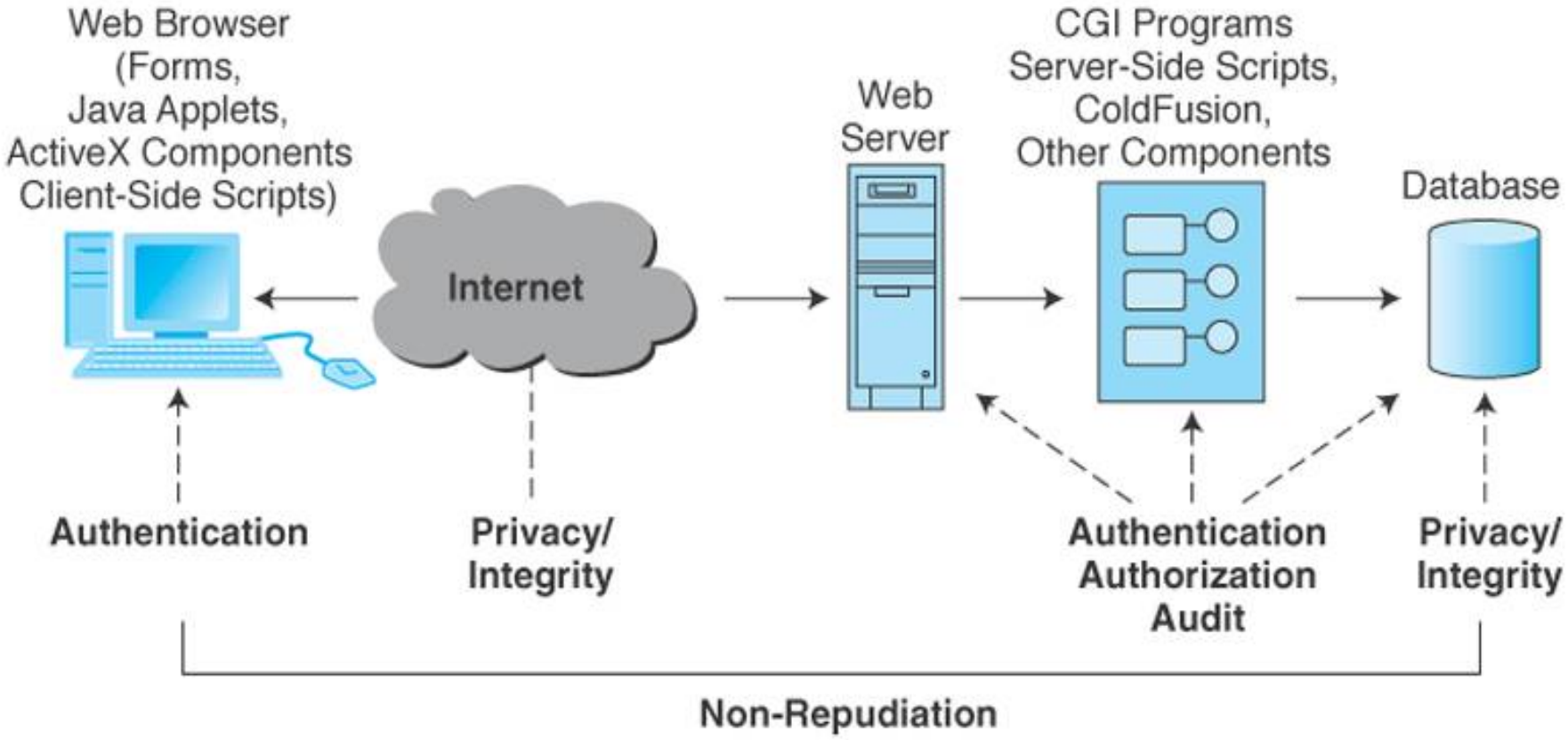
Applications of E-Commerce

- Online Shopping
- Supply chain management
- Video on demand
- Remote banking
- Procurement and purchasing
- Online marketing and advertisement
- Auctions

Advantages of Electronic Commerce

- **Increased sales**
  - Reach narrow market segments in geographically dispersed locations
  - Create virtual communities
- **Decreased costs**
  - Handling of sales inquiries
  - Providing price quotes
  - Determining product availability

Exhibit 12.1 General Security Issues at EC Sites



Source: Scambray, J. et al. *Hacking Exposed 2e*. New York: McGraw-Hill, 2000. Copyright © McGraw-Hill Companies, Inc.

Disadvantages of Electronic Commerce

- Loss of ability to inspect products from remote locations
- Rapid developing pace of underlying technologies
- Difficult to calculate return on investment
- Cultural and legal impediment
- **Payment Security**

Security Threats in the E-commerce Environment

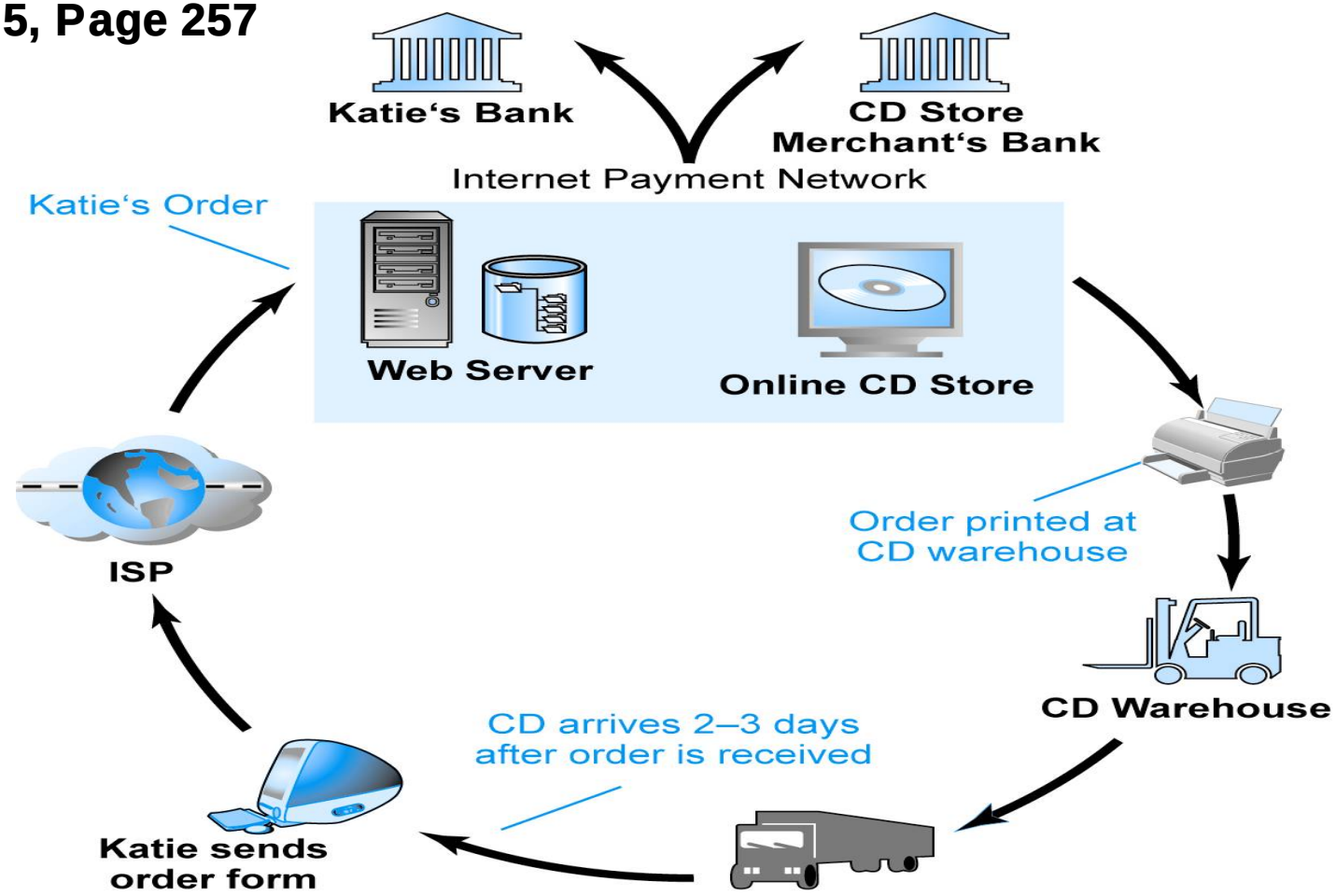
- Three key points of vulnerability:
  - Client
  - Server
  - Communications channel

Security Threats in the E-commerce Environment (cont'd)

- Most common threats:
  - Malicious code
  - Phishing
  - Hacking and cybervandalism
  - Credit card fraud/theft
  - Spoofing (pharming)
  - Denial of service attacks
  - Sniffing
  - Insider jobs
  - Poorly designed server and client software

A Typical E-commerce Transaction

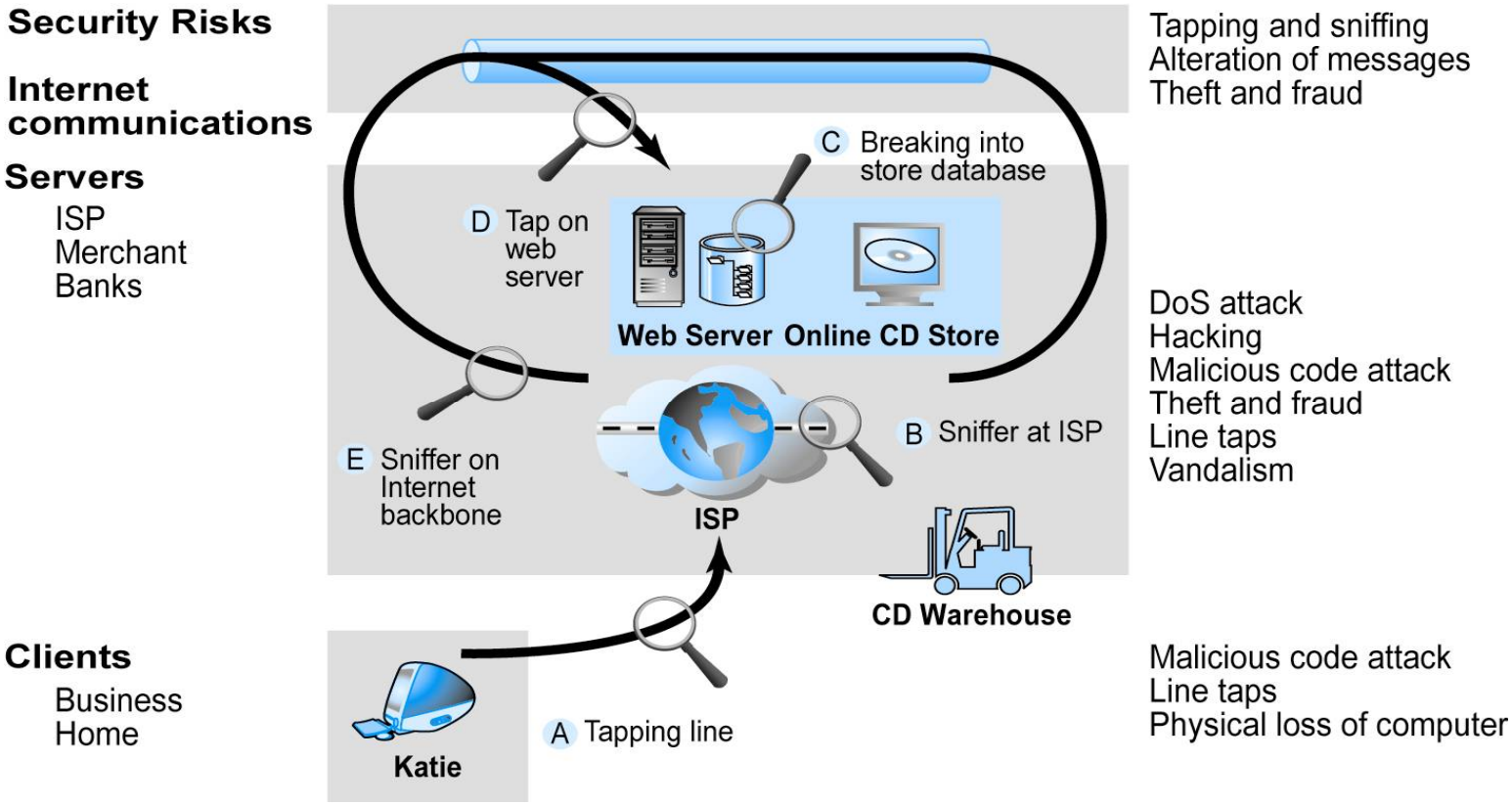
Figure 5.5, Page 257



SOURCE: Boncella, 2000.

Vulnerable Points in an E-commerce Environment

Figure 5.6, Page 258



SOURCE: Boncella, 2000.

E-COMMERCE : CHALLENGES

- Trusting others electronically

  --E-Commerce infrastructure

- Security threats – the real threats and the perceptions
- Network connectivity and availability issues

  --Better architecture and planning

- Global economy issues

  --Flexible solutions

Trusting others electronically: Questions

- Am I connected to the correct web site?
- Is the right person using the other computer?
- Did the appropriate party send the last email?
- Did the last message get there in time, correctly?

E-COMMERCE: SOLUTIONS TRUSTING OTHERS

- **Public-Key Infrastructure (PKI)**
  - Distribute key pairs to all interested entities
  - Certify public keys in a “trusted” fashion

    --The Certificate Authority
  - Secure protocols between entities
  - Digital Signatures, trusted records and non-repudiation

E-Commerce: Security Threats

- Authentication problems
- Privacy problems
- Integrity problems
- Repudiation problems

- **Tricking the consumer:** Some of the simplest and most profitable attacks are supported tricking the consumer, additionally referred to as social engineering methods. These attacks grip surveillance of the shopper's behavior, gathering data to use against the consumer. As an example, a mother's last name may be a common challenge question utilized by varied sites. If one in every of these sites is tricked into giving freely a password once the challenge question is provided, then not only has this web site been give and take, however it is additionally probably that the consumer used identical logon ID and password on alternative sites.
- **Inquiring the consumer's computer:** Lacks of computers are additional to the web monthly. Most users' data of security vulnerabilities of their systems is imprecise at the best. In addition, code and hardware vendors, in their quest to make sure that their merchandise are simple to put in, can ship merchandise with safety features disabled. In most cases, enabling safety features needs a non-technical user to scan manuals written for the engineer. The confused user doesn't plan to alter the safety options. This creates a treasure for attackers.

- **Sniffing the network:** In this theme, the aggressor monitors the information between the shopper's computer and therefore the server. He collects information concerning the consumer or steals personal information, like master card numbers. There are points within the network wherever this attack is additional sensible than others.
- **Guessing passwords:** General attack is to guess a user's secret word. This variety of attack is manual or automatic. Manual attacks are toilsome, and only self-made if the attacker is aware of one thing concerning the consumer. As an example, if the consumer uses their child's name because the password. Automatic attacks have a better probability of success, as a result of the likelihood of guess a user ID/password becomes a lot of vital because the range of tries will increase. Tools exist that use all the words within the lexicon to check user ID/password mixtures, or that attack widespread user ID/password mixtures. The attackers will automatism to travel against multiple sites at only once.

- **Mistreatment denial of service attacks:** The denial of service attack is one among the simplest samples of impacting web site convenience. It involves achieving the server to perform an outsized variety of mundane tasks, prodigious the capability of the server to address the other task.
- **Mistreatment server roots exploits:** Root exploits consult with techniques that gain super user access to the server. This can be the foremost desired kind of exploit as a result of the chances is limitless. Once you attack a consumer or his computer, you can only have an effect on one individual. With a root exploit, you gain management of the merchants and every one the shoppers' info on the location.

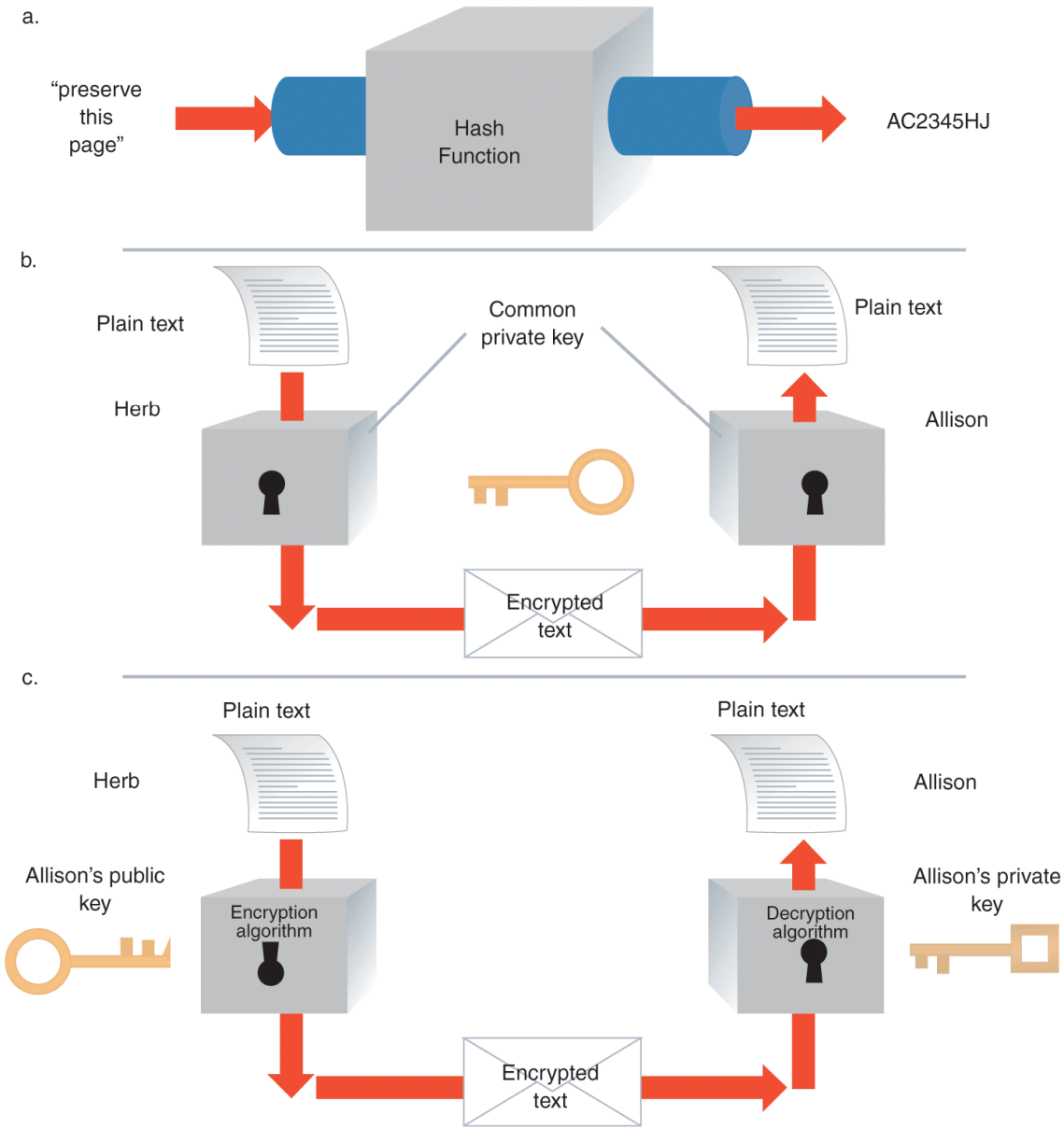


FIGURE 10-10 (a) hash coding, (b) private-key, and (c) public-key encryption

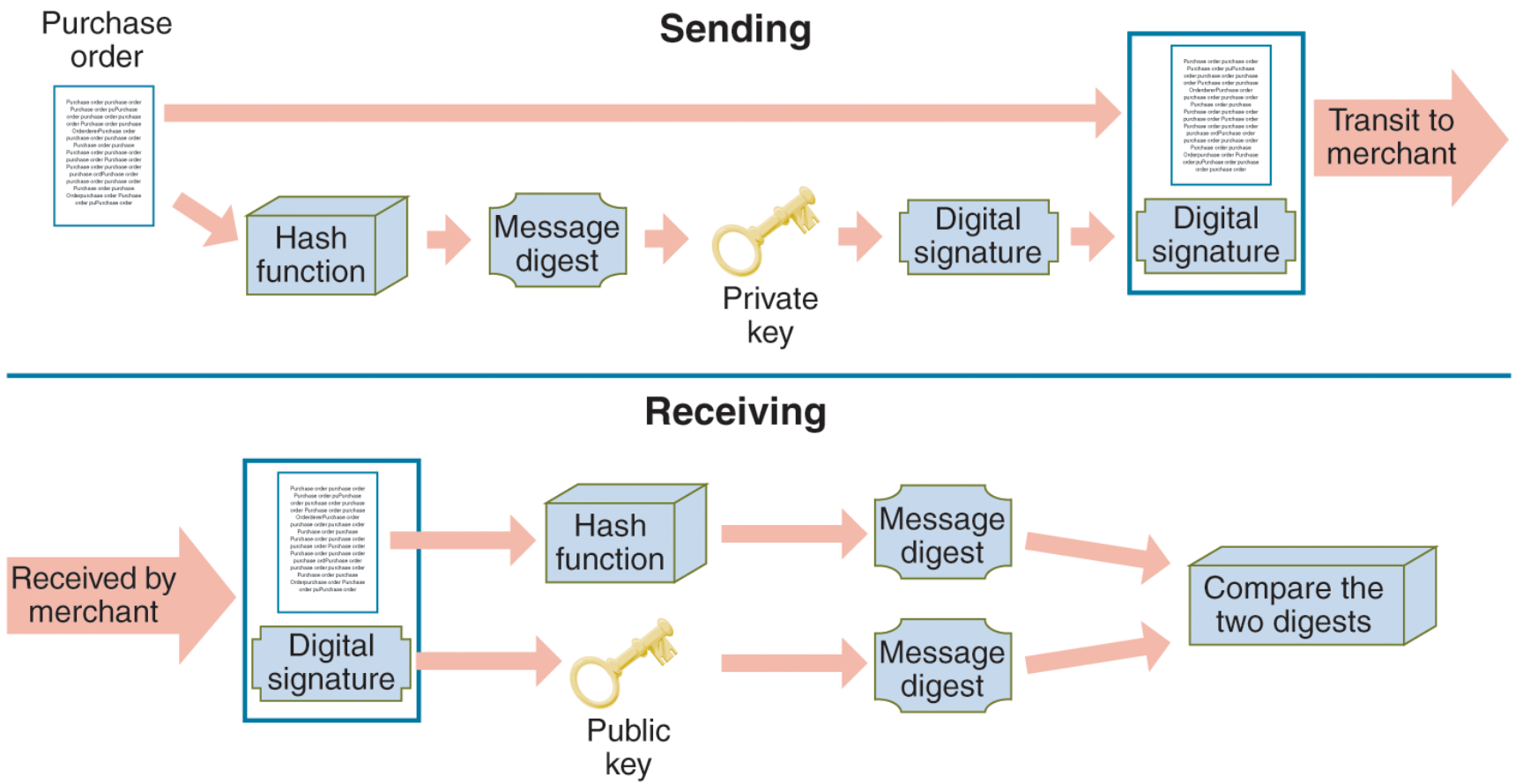


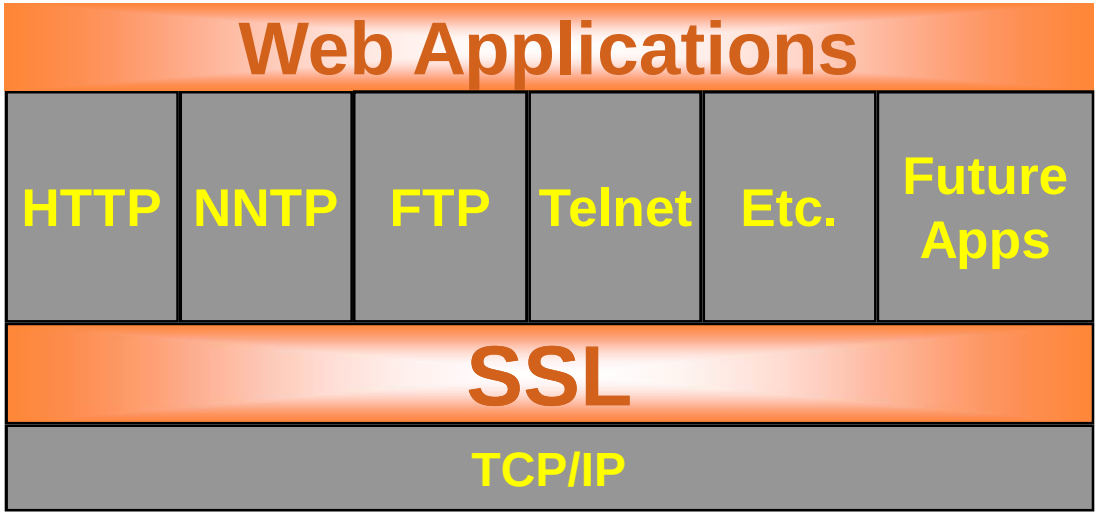
FIGURE 10-12 Sending and receiving a digitally signed message

Secure Protocols

- How to communicate securely:
  - SSL – “the web security protocols”
  - SET – “credit card transaction security protocol”
  - IPSEC – “the IP layer security protocol”
  - SMIME – “the email security protocol”

Secure Socket Layer (SSL)

- Authenticate Client and Server to each other.
  - Operates between application and transport layers



CONTD.....

- Negotiates and employs essential functions for secure transactions
  - Mutual Authentication
  - Data Encryption
  - Data Integrity
  - Data Privacy
  - Send Session messages

SECURED ELECTRONIC TRANSACTIONS (SET)

- Developed by VISA & MasterCard
- SET Specifications:
  - Digital Certificates (Identification)
  - Public Key (Privacy)
- On-Line Shopping Steps:
  - C.H. Obtain Digital Wallets
  - C.H. Obtain Digital Certificates
  - C.H. & Merchants conduct Shopping Dialog
  - Authentication & Settlement Process

E-Commerce: Challenges
Connectivity and availability

- Issues with variable response during peak time
- Guaranteed delivery, response and receipts
- Spoofing attacks
  - Attract users to other sites
- Denial of service attacks
  - Prevent users from accessing the site
- Tracking and monitoring networks

E-Commerce: Challenges Global Economy

- Variable connectivity levels and cost
- Variable economies and cultures
- Taxation and intellectual property issues
- Interoperability between different economies

E-Commerce: Challenges

- Trusting others electronically
  - Authentication
  - Handling of private information
  - Message integrity
  - Digital signatures and non-repudiation
  - Access to timely information

E-Commerce: Challenges

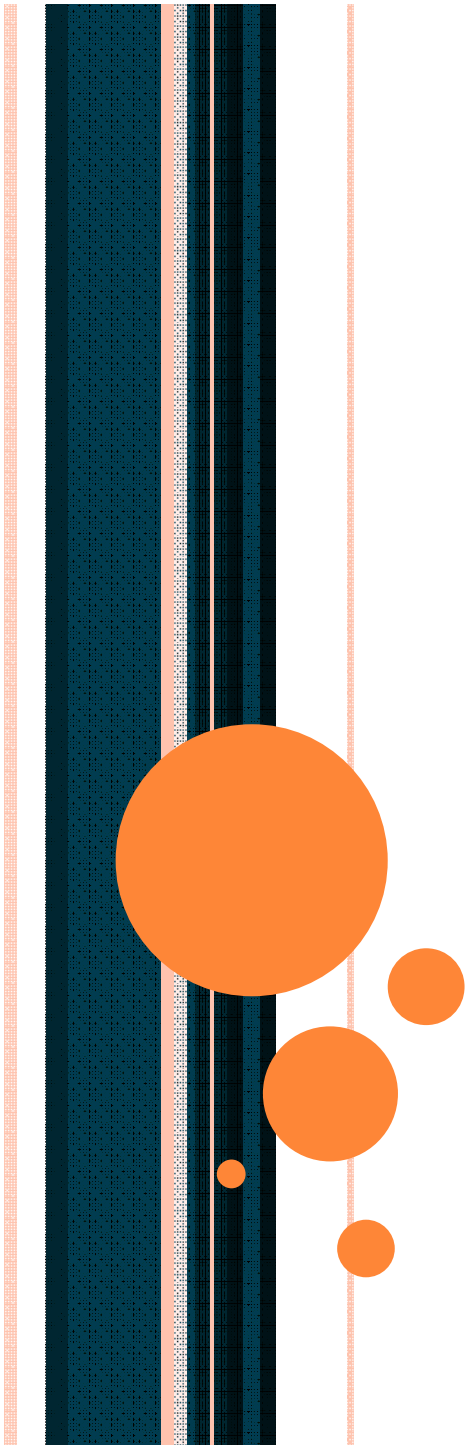
- Trusting others electronically
  - E-Commerce infrastructure
- Security threats – the real threats and the perceptions
- Network connectivity and availability issues
  - Better architecture and planning
- Global economy issues
  - Flexible solutions

E-Commerce: Challenges
Trusting Others

- Trusting the medium
  - Am I connected to the correct web site?
  - Is the right person using the other computer?
  - Did the appropriate party send the last email?
  - Did the last message get there in time, correctly?

REFERENCES

- [1] David J. Olkowski, Jr., “Information Security Issues in ECommerce”, SANS GIAC Security Essentials , March26,2001.
- [2] Paul A. Greenberg, “In E-Commerce We Trust … Not “, Ecommerce Time, February 2, 2001, URL: http://WWW.ecommercetimes.com/perl/story/?id=7194.
- [3] William Stallings, “Cryptography and network Security”, 3rd edition, Prentice Hall,2003.
- [4] Michall E. Whitman and Herbert J. Maiiord, “Information Security”, Thomson, Inc. , 2003.
- [5] Dave Chaffey, “E-Business and E-Commerce”, 2nd , Prentice Hall, 2005
- [6] Mark Merkow . Jim Breithaupt, "Information Security Principles and Practices", Pearson Prentice Hall, 2006.



THANK YOU.....