ECOMMERCE SECURITY

DR. SHAZIA KHAN

TABLE 5.2 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

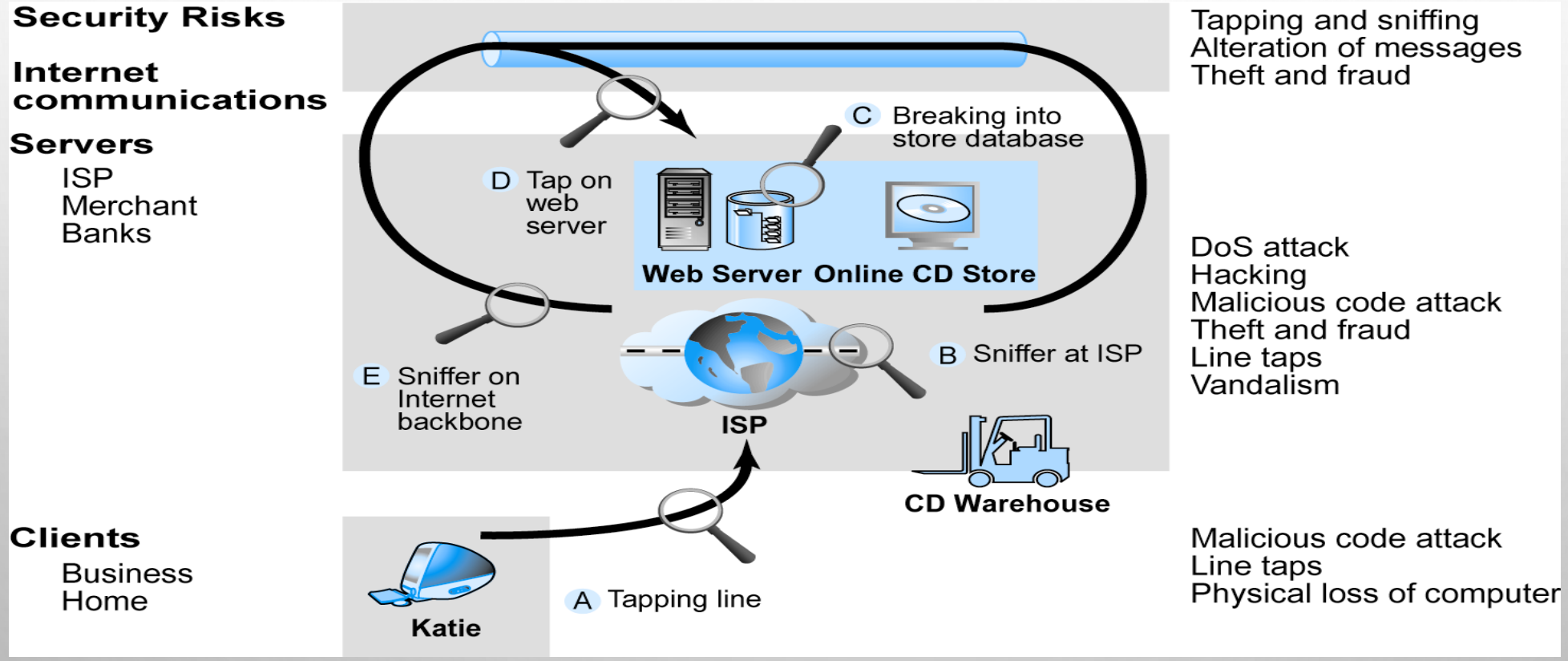
DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

- THREE KEY POINTS OF VULNERABILITY:
  - CLIENT
  - SERVER
  - COMMUNICATIONS CHANNEL

VULNERABLE POINTS IN AN E-COMMERCE ENVIRONMENT

FIGURE 5.6, PAGE 267



SOURCE: Boncella, 2000.

MOST COMMON SECURITY THREATS IN THE E-COMMERCE ENVIRONMENT

- MALICIOUS CODE (VIRUSES, WORMS, TROJANS)
- UNWANTED PROGRAMS (SPYWARE, BROWSER PARASITES)
- PHISHING/IDENTITY THEFT
- HACKING AND CYBERVANDALISM
- CREDIT CARD FRAUD/THEFT
- SPOOFING (PHARMING)/SPAM (JUNK) WEB SITES
- DOS AND DDOS ATTACKS
- SNIFFING
- INSIDER ATTACKS
- POORLY DESIGNED SERVER AND CLIENT SOFTWARE

MALICIOUS CODE

- VIRUSES: HAVE ABILITY TO REPLICATE AND SPREAD TO OTHER FILES; MOST ALSO DELIVER A "PAYLOAD" OF SOME SORT (DESTRUCTIVE OR BENIGN); INCLUDE MACRO VIRUSES, FILE-INFECTING VIRUSES, AND SCRIPT VIRUSES
- WORMS: DESIGNED TO SPREAD FROM COMPUTER TO COMPUTER
- TROJAN HORSE: APPEARS TO BE BENIGN, BUT THEN DOES SOMETHING OTHER THAN EXPECTED
- BOTS: CAN BE COVERTLY INSTALLED ON COMPUTER; RESPONDS TO EXTERNAL COMMANDS SENT BY THE ATTACKER

UNWANTED PROGRAMS

- INSTALLED WITHOUT THE USER'S INFORMED CONSENT
  - BROWSER PARASITES: CAN MONITOR AND CHANGE SETTINGS OF A USER'S BROWSER
  - ADWARE: CALLS FOR UNWANTED POP-UP ADS
  - SPYWARE: CAN BE USED TO OBTAIN INFORMATION, SUCH AS A USER'S KEYSTROKES, E-MAIL, IMS, ETC.

PHISHING AND IDENTITY THEFT

- ANY DECEPTIVE, ONLINE ATTEMPT BY A THIRD PARTY TO OBTAIN CONFIDENTIAL INFORMATION FOR FINANCIAL GAIN
  - MOST POPULAR TYPE: E-MAIL SCAM LETTER
  - ONE OF FASTEST GROWING FORMS OF E-COMMERCE CRIME

HACKING AND CYBERVANDALISM

- HACKER: INDIVIDUAL WHO INTENDS TO GAIN UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS
- CRACKER: HACKER WITH CRIMINAL INTENT (TWO TERMS OFTEN USED INTERCHANGEABLY)
- CYBERVANDALISM: INTENTIONALLY DISRUPTING, DEFACING OR DESTROYING A WEB SITE
- TYPES OF HACKERS INCLUDE:
  - WHITE HATS
  - BLACK HATS
  - GREY HATS

CREDIT CARD FRAUD

- FEAR THAT CREDIT CARD INFORMATION WILL BE STOLEN DETERS ONLINE PURCHASES
- HACKERS TARGET CREDIT CARD FILES AND OTHER CUSTOMER INFORMATION FILES ON MERCHANT SERVERS; USE STOLEN DATA TO ESTABLISH CREDIT UNDER FALSE IDENTITY
- ONE SOLUTION: NEW IDENTITY VERIFICATION MECHANISMS

SPOOFING (PHARMING) AND SPAM (JUNK) WEB SITES

- SPOOFING (PHARMING)
  - MISREPRESENTING ONESELF BY USING FAKE E-MAIL ADDRESSES OR MASQUERADING AS SOMEONE ELSE
  - THREATENS INTEGRITY OF SITE; AUTHENTICITY
- SPAM (JUNK) WEB SITES
  - USE DOMAIN NAMES SIMILAR TO LEGITIMATE ONE, REDIRECT TRAFFIC TO SPAMMER-REDIRECTION DOMAINS

DOS AND DDOS ATTACKS

- DENIAL OF SERVICE (DOS) ATTACK
  - HACKERS FLOOD WEB SITE WITH USELESS TRAFFIC TO INUNDATE AND OVERWHELM NETWORK
- DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK
  - HACKERS USE NUMEROUS COMPUTERS TO ATTACK TARGET NETWORK FROM NUMEROUS LAUNCH POINTS

OTHER SECURITY THREATS

- SNIFFING: TYPE OF EAVESDROPPING PROGRAM THAT MONITORS INFORMATION TRAVELING OVER A NETWORK; ENABLES HACKERS TO STEAL PROPRIETARY INFORMATION FROM ANYWHERE ON A NETWORK
- INSIDER JOBS: SINGLE LARGEST FINANCIAL THREAT
- POORLY DESIGNED SERVER AND CLIENT SOFTWARE: INCREASE IN COMPLEXITY OF SOFTWARE PROGRAMS HAS CONTRIBUTED TO INCREASE IS VULNERABILITIES THAT HACKERS CAN EXPLOIT

TECHNOLOGY SOLUTIONS

- PROTECTING INTERNET COMMUNICATIONS (ENCRYPTION)
- SECURING CHANNELS OF COMMUNICATION (SSL, S-HTTP, VPNS)
- PROTECTING NETWORKS (FIREWALLS)
- PROTECTING SERVERS AND CLIENTS

TOOLS AVAILABLE TO ACHIEVE SITE SECURITY