

מסחר אלקטרוני – נושא 12

אבטחת מידע ברשת

מרצה: שי שקרוב

הסוחרים משלמים – דיון כיתתי

- מדוע נהלים של אבטחת עסקאות בכרטיסי אשראי הקיימים בשוק המסורתי אינם ישימים בשוק המקוון?
- מהן הטכניקות הזמינות לסוחרים להפחתת הונאות כרטיסי האשראי ברשת?
- מדוע הסוחרים נאלצים לשאת בסיכוני הרכישה בכרטיסי אשראי ברשת ולא הבנקים?
- מהם הצעדים הנוספים אותם יכולים לנקוט הסוחרים כדי להפחית את הונאות כרטיסי האשראי באתריהם?
- מדוע הסוחרים מסרבים להוסיף אמצעי אבטחה נוספים?



סביבת אבטחת המידע בסחר אלקטרוני: היקף הבעיה

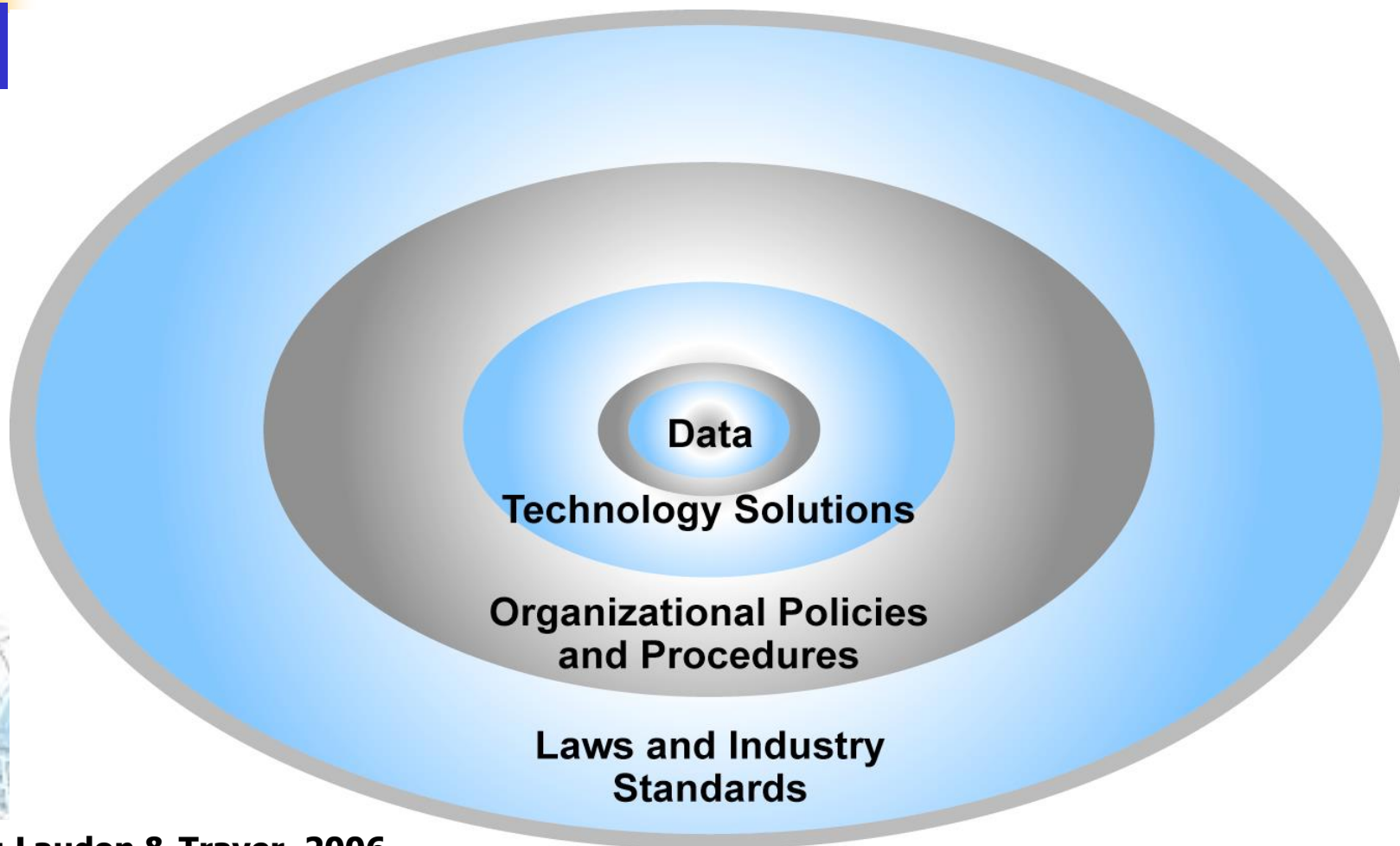
- ההיקף המדויק של הפשיעה ברשת אינו ידוע
- היקף ההפסדים משמעותי אך יציב
- ללקוחות: ישנם סיכוני הונאה חדשים הכרוכים בהפסדים שאינם מבוטחים

■ Symantec: ממוצע של 57 התקפות על עסק ביום בתקופה 7/2004-6/2005

■ לפי סקר של Computer Security Institute לשנת 2005:

- 56% מהמשיבים דיווחו על פריצות למחשביהם בשנה האחרונה;
- מתוכם 91% דיווחו על הפסד פיננסי כתוצאה מהפריצה
- מעל 35% חוו התקפות של denial of service
- מעל 75% זיהו התקפת וירוסים

סביבת אבטחת המידע בסחר אלקטרוני



Source: Laudon & Traver, 2006

ממדים של אבטחה בסחר אלקטרוני

- שלמות: היכולת להבטיח שמידע המוצג באתר האינטרנט או המועבר באינטרנט לא עבר שינוי ע"י גורם שאינו מורשה.
- הכרה בעסקאות: היכולת להבטיח שהצדדים לעסקה לא יתכחשו לה.
- אותנטיות: היכולת לזהות את הגורם איתו מתבצעת העסקה באינטרנט
- סודיות: היכולת להבטיח שרק מי שמורשה יצפה במידע המועבר באינטרנט
- פרטיות: היכולת לשלוט בשימוש במידע הפרטי המועבר ע"י הלקוח
- זמינות: היכולת להבטיח שאתר הסחר האלקטרוני יתפקד כמתוכנן

ממדים של אבטחה בסחר אלקטרוני מנקודת המבט של הסוחר ושל הלקוח

ממד	מבט לקוח	מבט סוחר
שלמות	האם המידע שהעברתי או קיבלתי שונה?	האם המידע המוצג באתר שונה? האם המידע שהתקבל מהלקוח תקף?
הכרה בעסקאות	האם הצד השני יוכל להתכחש להזמנה?	האם הצד השני יוכל להתכחש להזמנה?
אותנטיות	ממי אני מזמין? כיצד אני יכול להיות בטוח שאכן זה הוא?	מהי הזהות האמיתית של הלקוח?

ממדים של אבטחה בסחר אלקטרוני מנקודת המבט של הסוחר ושל הלקוח

ממד	מבט לקוח	מבט סוחר
סודיות	האם מישהו אחר מלבד הנמען יוכל לקרוא את המסר?	האם מידע חסוי זמין למי שאינו מורשה לראותו?
פרטיות	האם אני יכול לשלוט בשימוש במידע שהעברתי על עצמי?	איזה שימוש ניתן לעשות במידע אישי שהועבר אליי? האם נעשה שימוש לא מורשה בנתונים האישיים של הלקוח?

ממדים של אבטחה בסחר אלקטרוני מנקודת המבט של הסוחר ושל הלקוח

ממד	מבט לקוח	מבט סוחר
זמינות	האם אני יכול לגלוש לאתר?	האם האתר מתפקד?



התמורה בין אבטחה וערכים אחרים

- אבטחה מול קלות שימוש
 - אבטחה עולה ← קלות שימוש יורדת
 - אבטחה עולה ← האתר הופך איטי יותר
- ביטחון הציבור מול חופש הפרט והרצון לאפשר אנונימיות
 - אבטחה: תועלת מול עלות



סיכוני אבטחה בסביבת הסחר האלקטרוני (1)

■ שלוש נקודות פגיעות:

■ לקוח

■ שרת

■ ערוץ התקשרות



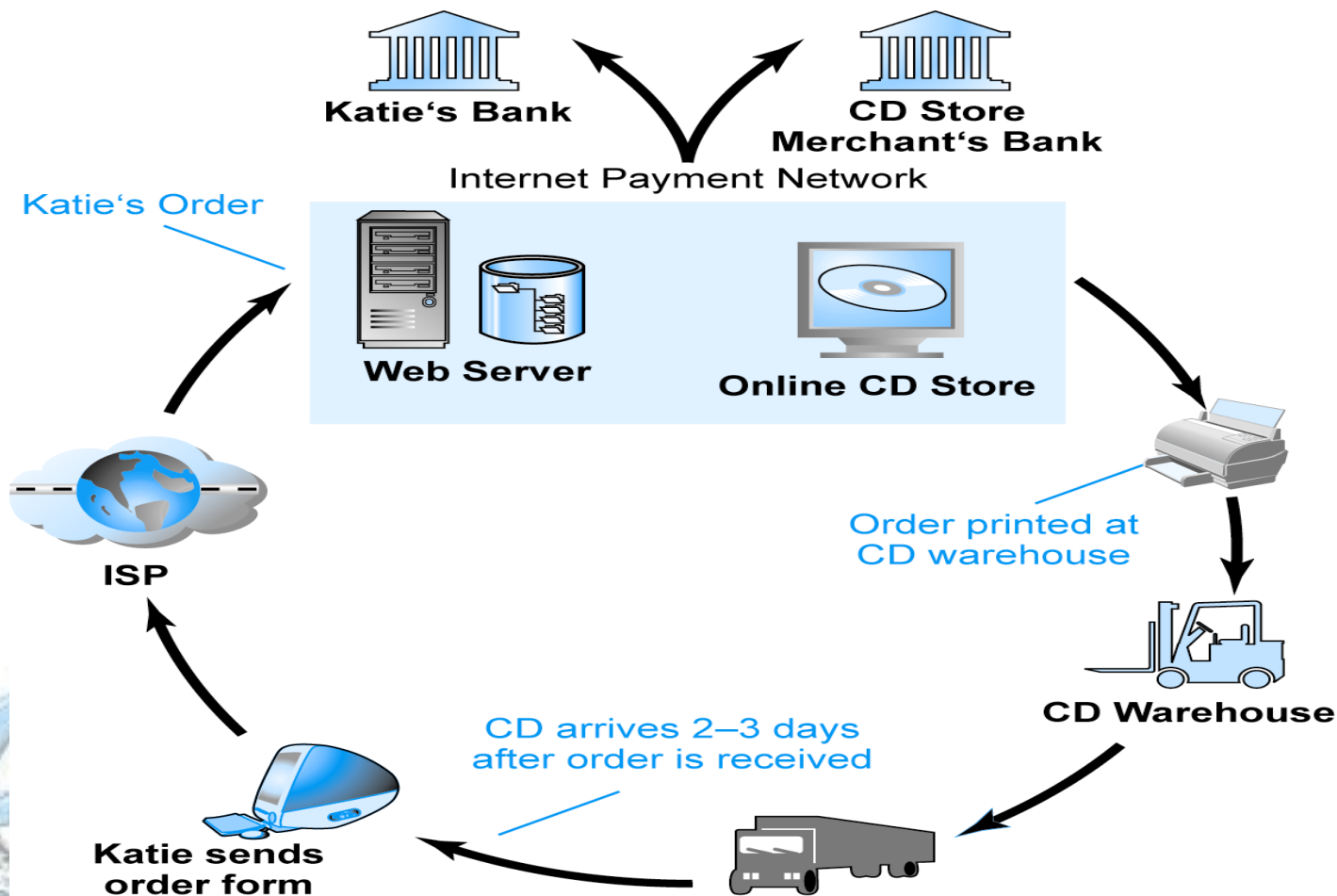
סיכוני אבטחה בסביבת הסחר האלקטרוני (2)

■ הסיכונים הנפוצים:

- קוד זדוני (Malicious code)
- Phishing
- Hacking and cybervandalism
- הונאות כרטיסי אשראי (Credit card fraud/theft)
- (Spoofing / pharming)
- Denial of service attacks
- האזנת סתר (Sniffing)
- עבודות פנימיות (Insider jobs)
- Poorly designed server and client software



תהליך טיפוס של עסקה בסחר אלקטרוני



SOURCE: Boncella, 2000.

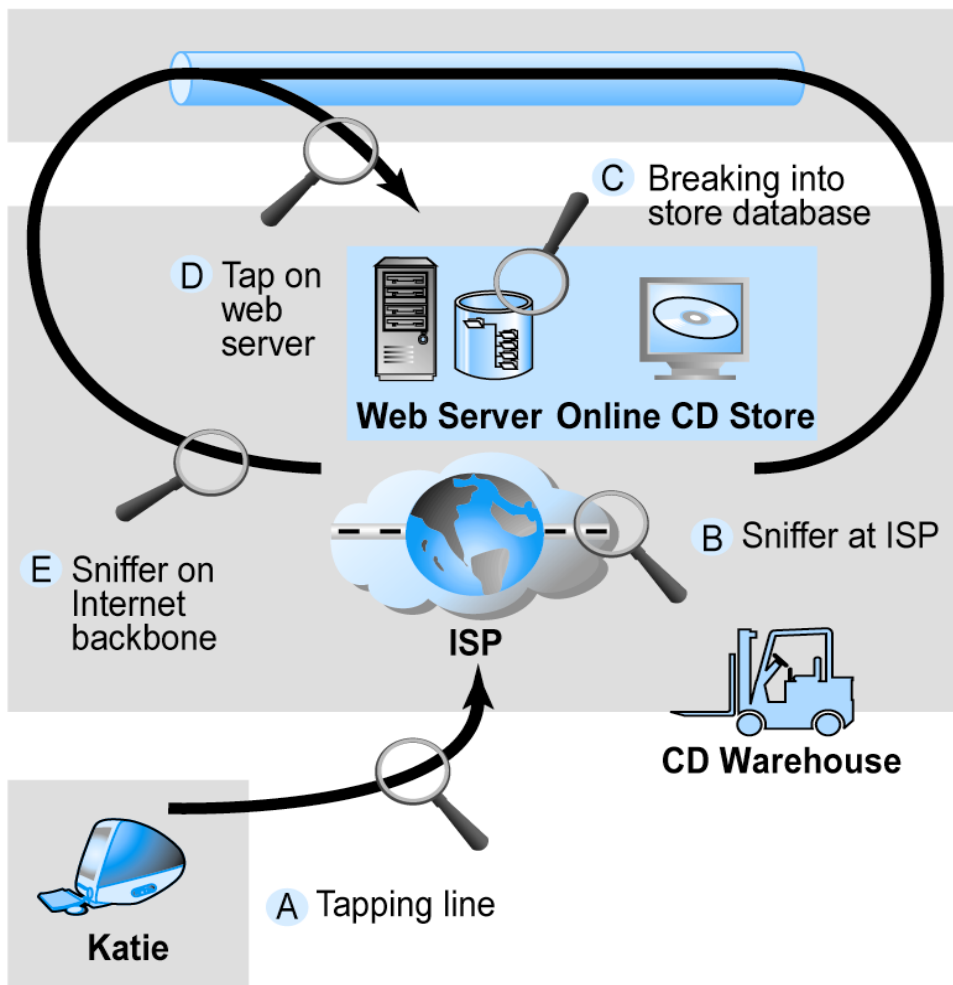
הנקודות הפגיעות בסביבת הסחר האלקטרוני

Security Risks

Internet communications

Servers

ISP
Merchant
Banks



Tapping and sniffing
Alteration of messages
Theft and fraud

DoS attack
Hacking
Malicious code attack
Theft and fraud
Line taps
Vandalism

Malicious code attack
Line taps
Physical loss of computer

Clients

Business
Home

Katie

SOURCE: Boncella, 2000.

מרצה: שי שקרוב

קוד זדוני (Malicious code)

- וירוסים: תוכנות מחשב המסוגלות להשתכפל ולהתפשט לתוכנות אחרות; יכולות להזיק או לא
- תולעים: מתוכננות לעבור ממחשב למחשב
- סוסים טרויאניים: נראים תמימים, ואז מפתיעים בפעולה הרסנית
- Bots: תוכנות המותקנות בחשאי על המחשב בעת שהוא מחובר לאינטרנט; מופעלות ע"י הוראה מרחוק של התוקף ומאפשרות לו לשלוט במחשב



Phishing

- כל ניסיון של צד שלישי להשיג מידע חסוי על מנת לזכות ברווח פיננסי
- הנפוץ ביותר: הודעת מייל
- גידול מהיר: שימוש באתרי מסחר אלקטרוני



Hacking and Cybervandalism

- האקר: אדם המנסה לפרוץ למערכות מידע אליהן אינו מורשה להכנס
- Cracker: האקר בעל כוונות פליליות
- Cybervandalism: הפרעה, הריסה או השחתה מכוונת של אתר אינטרנט
- סוגים של האקרים כוללים:
 - White hats
 - Black hats
 - Grey hats



הונאות כרטיסי אשראי (Credit card fraud/theft)

- הפחד שפרטי כרטיס האשראי ייגנבו מרחיק אנשים מעסקאות אלקטרוניות
- האקרים מנסים להגיע לקבצים המכילים פרטים אישיים של לקוחות ופרטי אשראי; עושים שימוש בפרטים כדי ליצור זהות בדויה
- אחד הפתרונות: מכניזם חדש לאישור זהות



Spoofing / pharming

■ Spoofing - התחזות למישהו שאינו קיים או למישהו אחר

■ pharming - יצירת אתר המתחזה לאתר אחר

■ מהווה איום על האותנטיות ועל השלמות של האתר



DoS and dDoS Attacks

- התקפת Denial of service (DoS): האקרים מציפים את האתר בתנועה סתמית במטרה לשבש את השימוש בו או להופכו בלתי זמין
- התקפת Distributed denial of service (dDoS): האקרים משתמשים במחשבים רבים כדי לתקוף רשת מנקודות רבות



סיכוני אבטחה נוספים

- האזנת סתר (Sniffing): תוכנות האזנה בסתר המצוטטות למידע העובר ברשת; מאפשרות להאקרים לגנוב מידע מכל מקום ברשת.
- עבודות פנימיות (Insider jobs): האיום הפיננסי הגדול מבין כלל האיומים
- עיצוב לקוי של תוכנות על השרתים או של הלקוחות.
- המורכבות של התוכנות מגדילה את נקודות התורפה שהאקרים יכולים לנצל



פתרונות טכנולוגיים

- הגנה על התקשורת באינטרנט (הצפנה / encryption)
- אבטחת ערוצי התקשורת (SSL, S-HTTP, VPNs)
- הגנה על הרשת (firewalls)
- הגנה על שרתים ולקוחות



כלים זמינים לאבטחת אתר

Encryption

Firewalls

Security Tools

Network Security Protocols

Security Management

Access Controls

Virtual Private Networks

Authentication

Tunneling

Proxy/Agent Systems

Intrusion Detection

Source: Laudon & Traver, 2006

מרצה: שי שקרוב

מסחר באינטרנט - נושא 12

22

הגנה על התקשורת באינטרנט: הצפנה (encryption)

- הצפנה: תהליך השינוי של נתונים רגילים לנתונים מקודדים, הניתנים לקריאה ע"י השולח והמקבל בלבד.

- המטרות:

- אבטחת מידע מאוחסן

- אבטחת העברת מידע

- מספק:

- שלמות המסר

- הכרה בעסקאות

- אותנטיות

- סודיות



הצפנה במפתח סימטרי (Symmetric or Secret key Encryption)

- השולח והמקבל משתמשים באותו מפתח דיגיטלי להצפנת מסר ולפענוח שלו.
- מחייב שימוש במפתח שונה לכל גוף איתו יוצרים תקשורת

- Data Encryption Standard (DES):
הסטנדרט הנפוץ ביותר במפתחות סימטריים;
עושה שימוש במפתח 56-bit

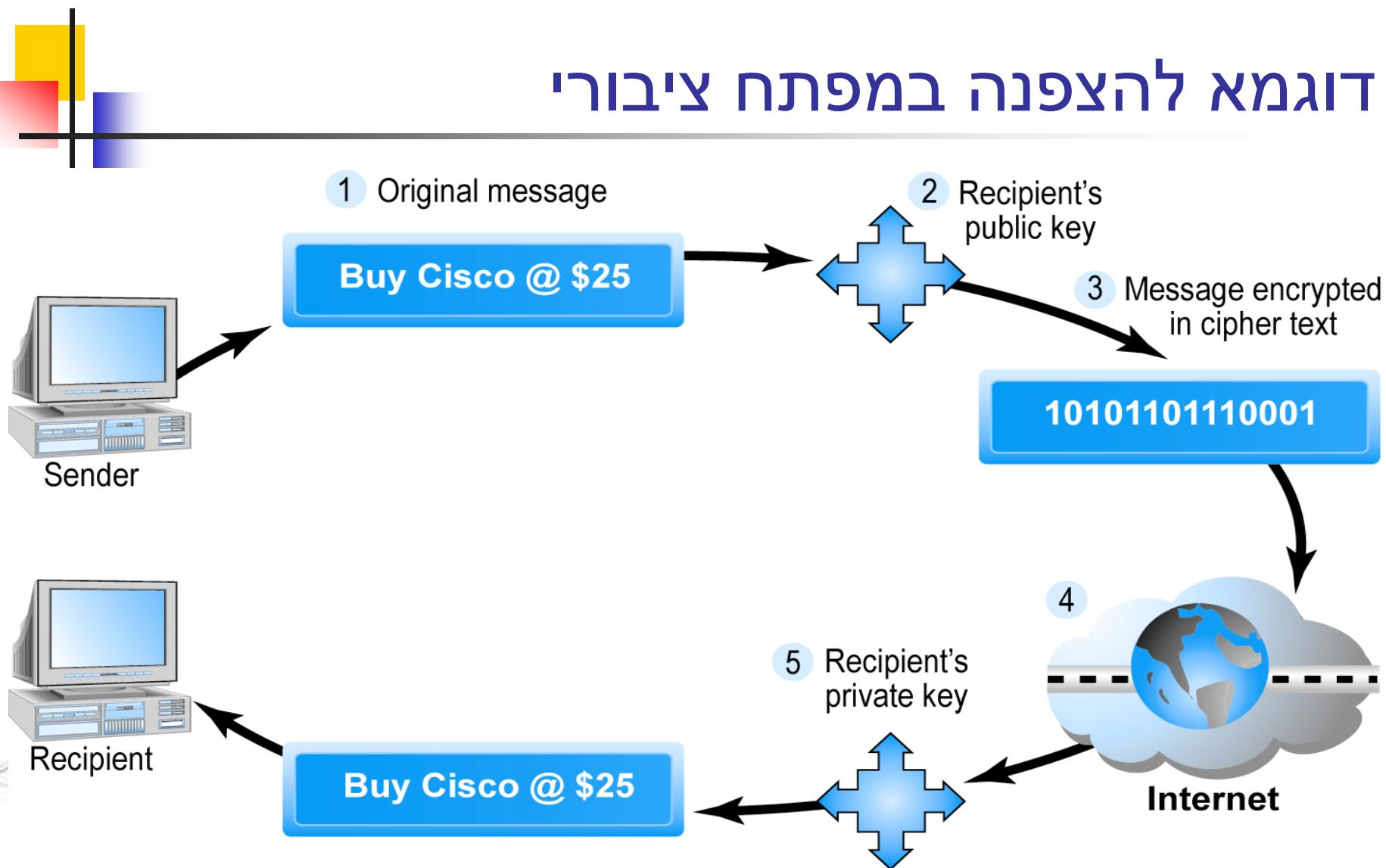
- מפתחות אחרים נעים בטווח של 128-2048 bit



הצפנה במפתח ציבורי (Public Key Encryption)

- המפתח הציבורי פותר את בעיית הצורך להחליף מפתחות בכל תקשורת חדשה.
- נעשה שימוש בשני מפתחות הקשורים מתימטית: הראשון ציבורי (חשוף לכלל) והשני פרטי (נשמר בסודיות ע"י בעליו)
- כדי להצפין ולפתוח מסרים יש להשתמש בשני המפתחות
- כאשר נעשה שימוש במפתח להצפנת מסר לא ניתן להשתמש בו לפתיחת אותו המסר.
- לדוגמא: השולח משתמש במפתח הציבורי של המקבל להצפנת מסר; המקבל עושה שימוש מפתח הפרטי שלו לפתיחת המסר.

דוגמא להצפנה במפתח ציבורי



Source: Laudon & Traver, 2006

הצפנה במפתח ציבורי תוך שימוש בחתימה דיגיטלית ו- Hash Digests

- מפתח ציבורי אינו מבטיח אותנטיות, שלמות והכרה בעסקאות

- הפתרון: לפני ההצפנה השולח מפעיל פונקציית Hash (אלגוריתם מתימטי) המייצר Hash Digests, המשמשות את המקבל לזיהוי של שלמות הנתונים.

- הצפנה כפולה עם המפתח הפרטי של השולח (חתימה דיגיטלית) מבטיחה אותנטיות והכרה בעסקאות.

- חסרונות:

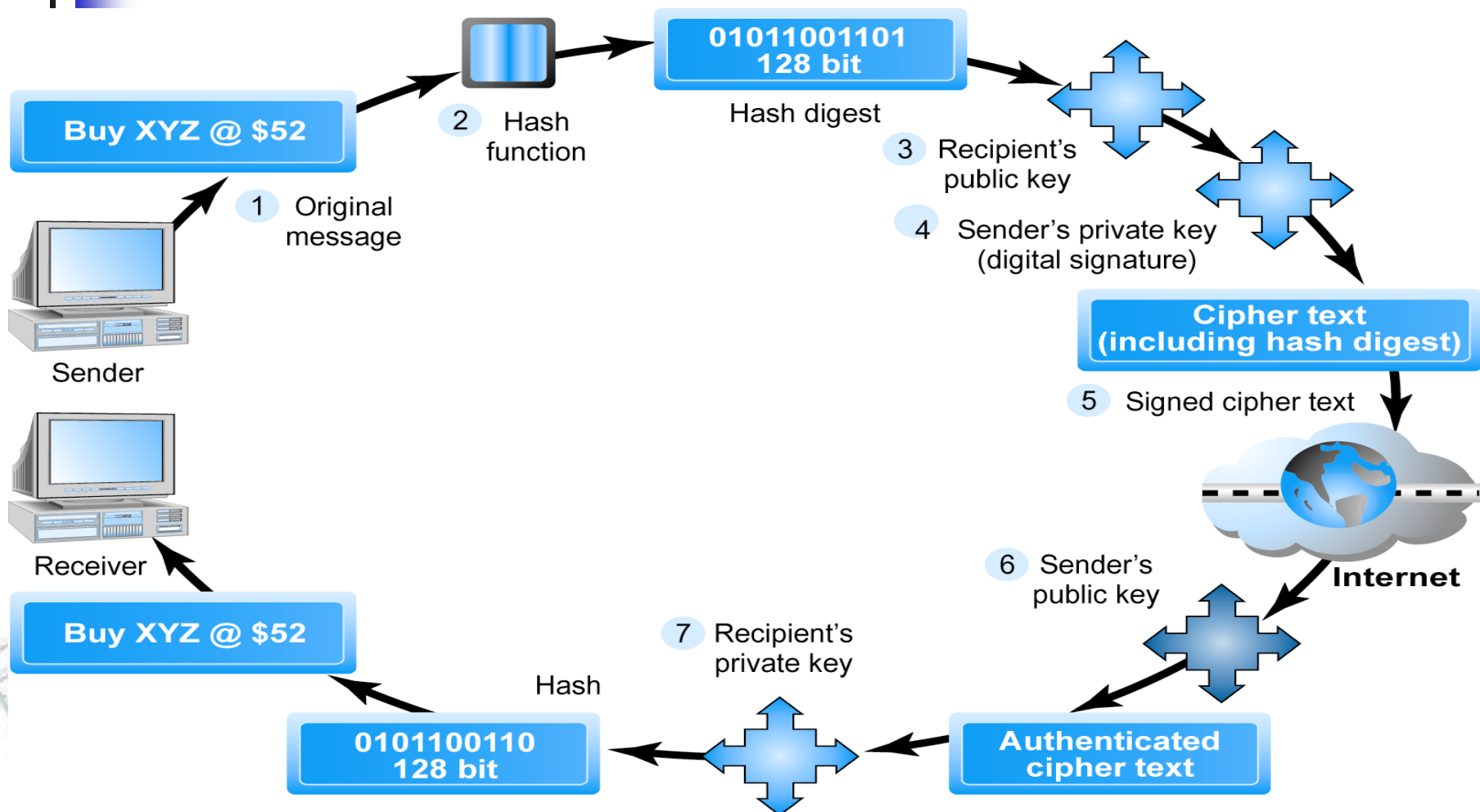
- תהליך המחשוב איטי

- מאט את העברת הנתונים

- זמן העיבוד גדל



דוגמא להצפנה במפתח ציבורי תוך שימוש בחתימה דיגיטלית



Source: Laudon & Traver, 2006

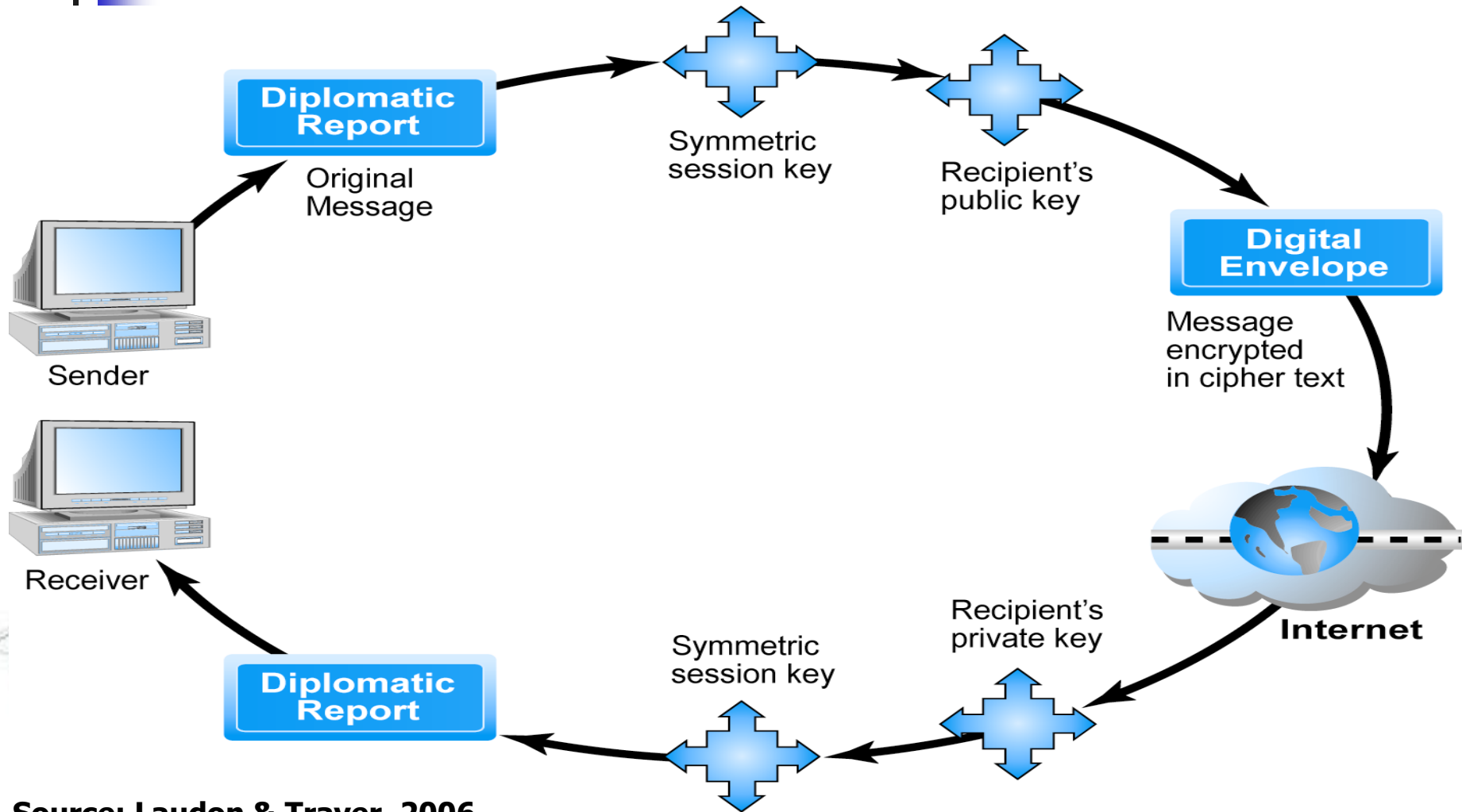
מרצה: שי שקרוב

הצפנה במפתח ציבורי תוך שימוש במעטפות דיגיטליות (Digital Envelopes)

- מתגבר על החולשות של השיטות הקודמות
- מצפינים את המסר בעזרת מפתח סימטרי; ואחר כך מצפינים את המפתח הסימטרי ושולחים אותו בעזרת הצפנה של מפתח ציבורי.



דוגמא להצפנה במפתח ציבורי תוך שימוש במעטפות דיגיטליות



Source: Laudon & Traver, 2006

מרצה: שי שקרוב

מסחר באינטרנט - נושא 12



תעודה דיגיטלית (Digital certificate)

■ תעודה דיגיטלית (Digital certificate) – מסמך דיגיטלי המכיל:

- שם האדם או הארגון

- המפתח הציבורי של האדם או הארגון

- מספר סידורי של התעודה

- תאריך תפוגה

- תאריך הנפקה

- חתימה דיגיטלית של הארגון שהנפיק את התעודה
(מוסד צד ג' מוכר - Certification Authority)

- פרטים מזהים נוספים

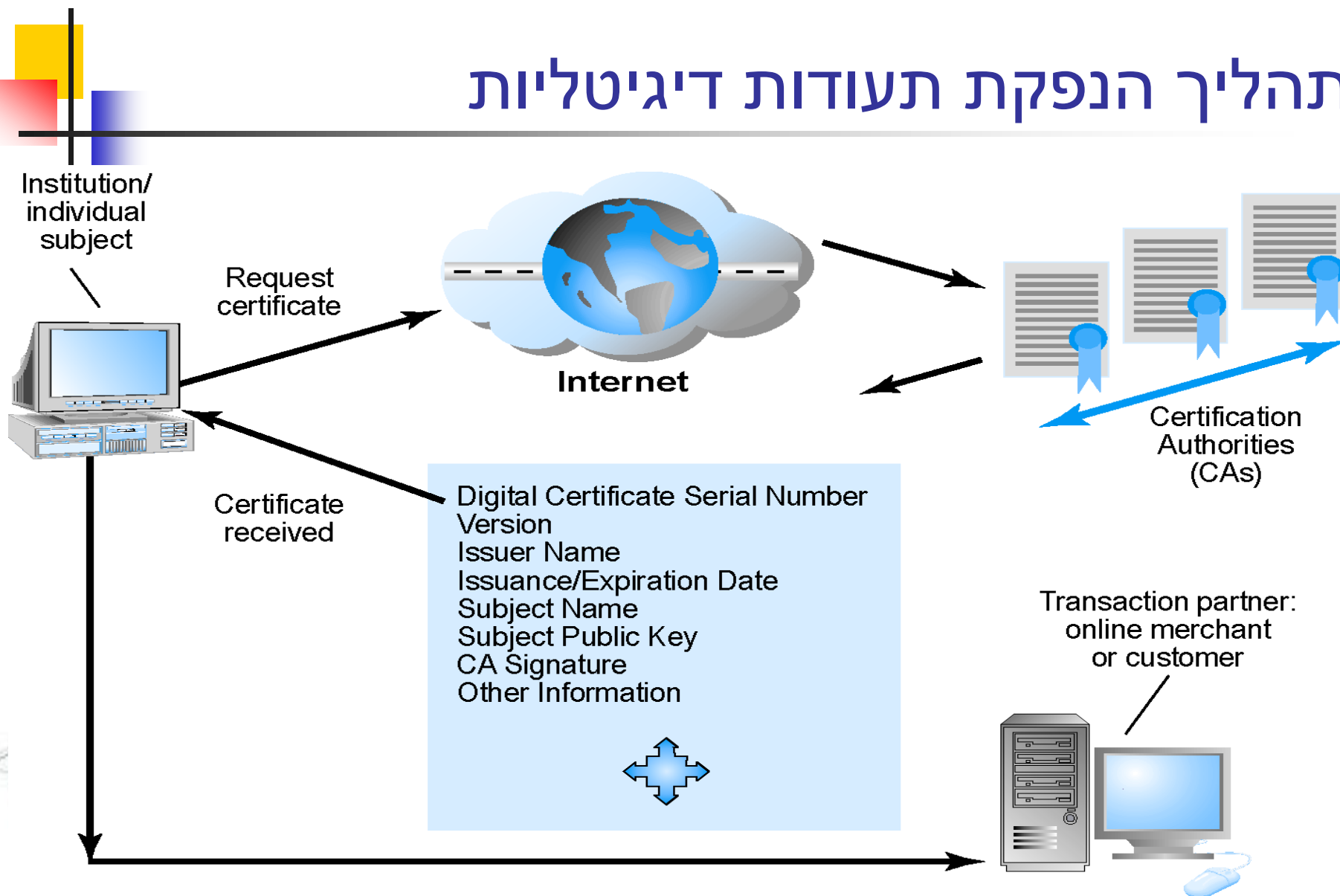
תשתית מפתח ציבורי

Public Key Infrastructure (PKI)

- מתייחס למוסדות המנפיקים תעודות דיגיטליות ולנהלים הכרוכים בהנפקתן המקובלים על כל הצדדים



תהליך הנפקת תעודות דיגיטליות



Source: Laudon & Traver, 2006

מרצה: שי שקרוב

מסחר באינטרנט - נושא 12

המגבלות של פתרונות ההצפנה

- PKI מתייחס בעיקר להגנה על מסרים במעבר
- PKI אינו אפקטיבי כנגד עבודות פנימיות
- הגנה על מפתחות פרטיים ע"י אנשים פרטיים נדירה: המשתמש אינו בהכרח הבעלים
- אין ביטחון שהמחשב של הסוחר המאמת את המסרים מאובטח
- אין רגולציה על הגופים המנפיקים את התעודות הדיגיטליות; הבחירה בהם אישית; תהליך מתן התעודות נתון לכשלים.

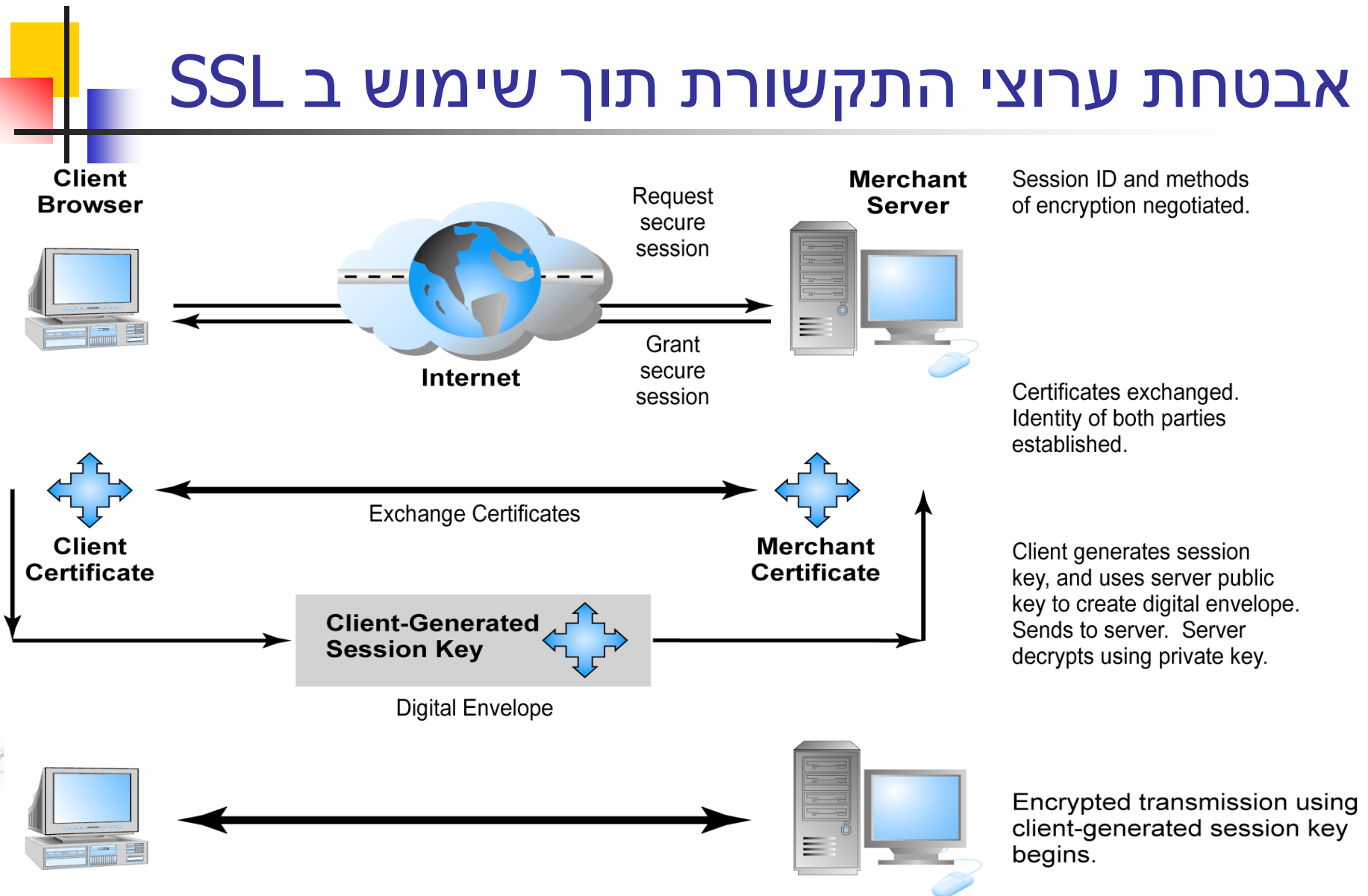
אבטחת ערוצי התקשורת (1)

■ (SSL) Secure Sockets Layer:

- הכי נפוץ (פרוטוקול HTTPS)
- משמש להקמת תקשורת מאובטחת – התקשורת בין שרת ללקוח בה גם ה-URL של המסמך המבוקש והתוכן שלו מוצפנים.



אבטחת ערוצי התקשורת תוך שימוש ב SSL



Source: Laudon & Traver, 2006

מרצה: שי שקרוב

מסחר באינטרנט - נושא 12

אבטחת ערוצי התקשורת (2)

■ S-HTTP

- פרוטוקול חליפי; מסוגל לעבוד בסביבת HTTP; מאפשר הצפנה, חתימה ואותנטיות; אוריינטציה של משלוח הודעה בודדת בבטחה.

■ רשתות פרטיות וירטואליות (Virtual Private Networks):

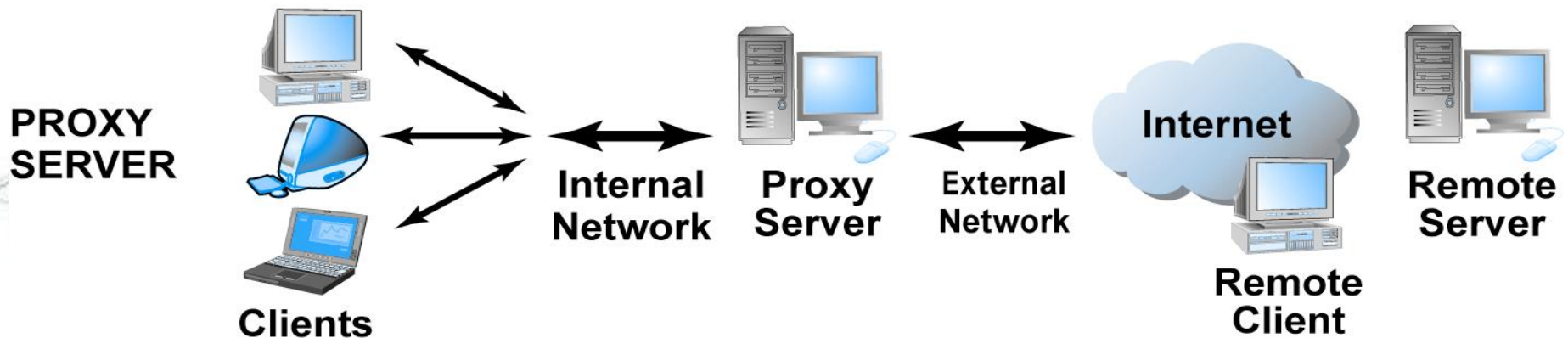
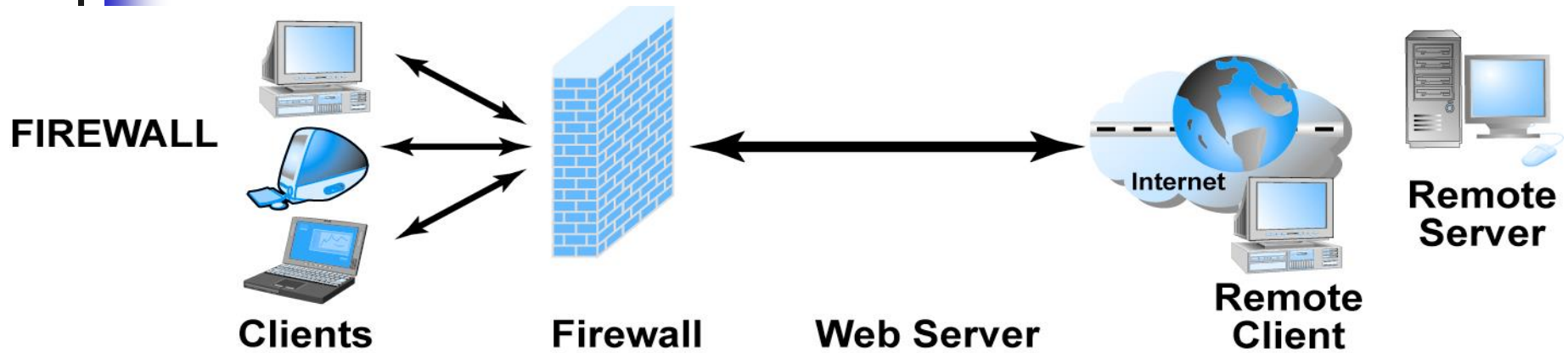
- מאפשרות למשתמש מרוחק להשתמש בבטחה ברשת פנימית באמצעות האינטרנט, תוך שימוש ב Point-to-Point Tunneling Protocol (PPTP)

הגנת רשתות: Firewalls and Proxy Servers

- חומת-אש: חומרה או תוכנה שחוסמת כניסת מידע לרשת הארגון על בסיס מדיניות האבטחה של הארגון.
- שרתי Proxy: שרתי תוכנה המטפלים בכל התקשורת הנכנסת אל הארגון והיוצאת ממנו דרך האינטרנט



הגנת רשתות: Firewalls and Proxy Servers



Source: Laudon & Traver, 2006

מרצה: שי שקרוב

הגנה על שרתים ולקוחות

- מערכות הפעלה: מנגנוני הרשאה
- תוכנות אנטי-וירוס: הדרך הקלה והזולה
לאבטחת שלמות המערכת

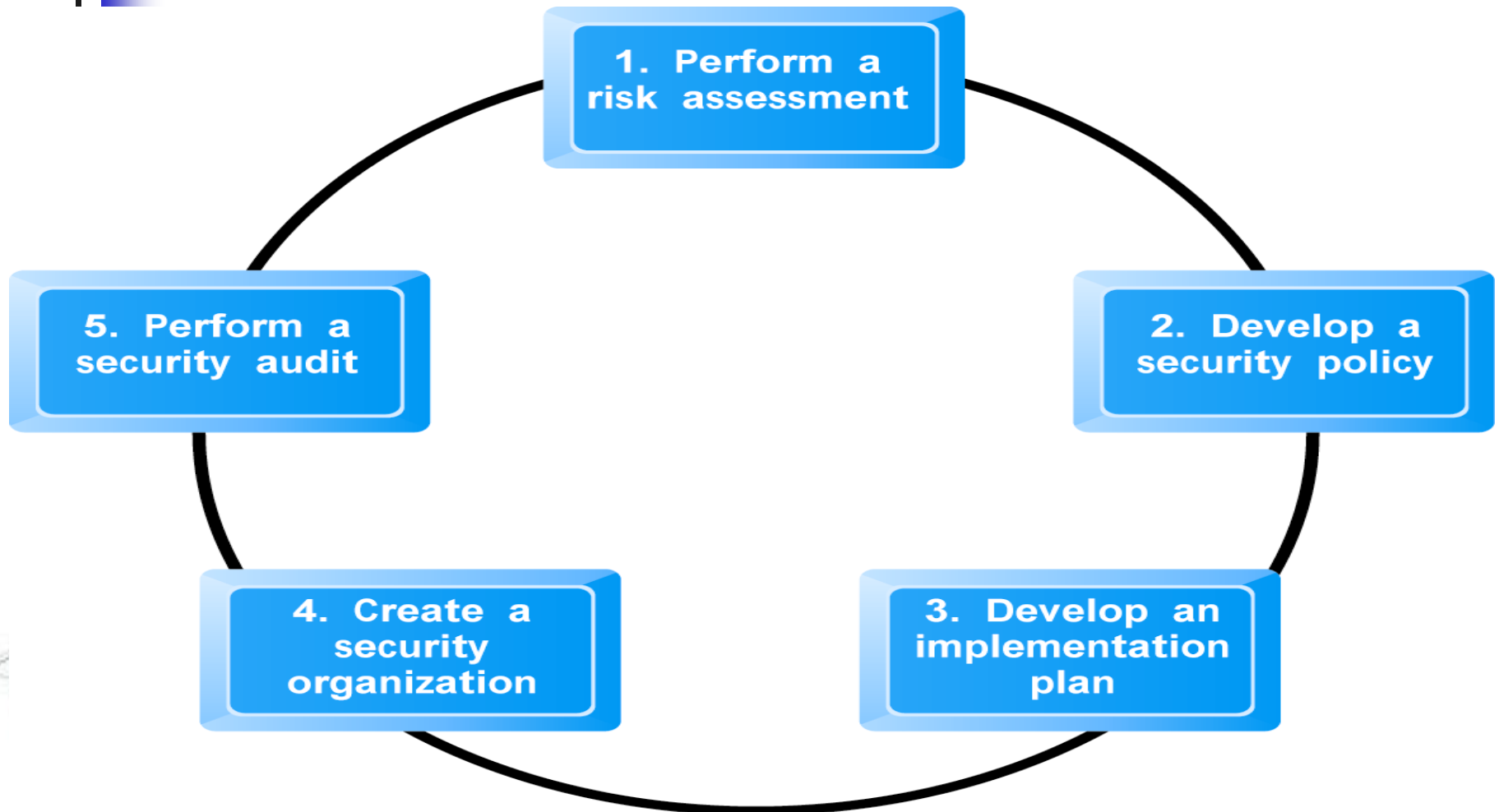


תכנית אבטחת מידע: צעדים ביצירת תכנית אבטחה

- ניתוח סיכונים: איתור סיכונים ונקודות חולשה
- פיתוח תכנית אבטחה: סט של הצהרות המתייחסות לסיכוני המידע ולסדרי העדיפויות; מזהות מטרות אבטחה, ומנגנונים להשגת היעדים
- פיתוח תכנית יישום: תכנית המפרטת את הצעדים הנדרשים להשגת המטרות
- יצירת ארגון מאובטח: מינוי אחראי אבטחה; כינוך והדרכה של המשתמשים; יצירת מודעת לחשיבות האבטחה בקרב המנהלים; ניהול בקרת גישה והרשאות
- בקרת אבטחה: על האבטחה בפועל ועל תהליכי האבטחה



תכנית אבטחת מידע: צעדים ביצירת תכנית אבטחה



Source: Laudon & Traver, 2006

מרצה: שי שקרוב

מסחר באינטרנט - נושא 12

להתראות!!!

