Banking And Bookkeeping

אוניברסיטת חיפה

סמינר אבטחת מידע 2014

ורוניקה משרי

מערכות בנקאיות

יש סוגים רבים של מערכות בנקאיות:

החל מהפשוטות ביותר שכולנו משתמשים בהן ביומיום, כמו מערכות של כספומטים וכרטיסי אשראי וכלה במערכות להעברת כספים ומערכות להנהלת חשבונות.

מערכות בנקאיות :
למה הן חשובות? למה מעניין לדון בהן?

- כמעט כל חברה כיום משתמשת במערכת הנהלת חשבונות. אלו מערכות קריטיות, שהצורך בהן היווה במשך שנים את עמוד התווך של תעשיית המחשבים.
- מערכות של העברת כספים בכל סכום שהוא היו אלה שהשיקו את "הקריפטוגרפיה המסחרית".
- הבנת תהליך העסקה הוא תנאי הכרחי להתמודדות רחבה יותר של בעיות המסחר וההונאה האלקטרונית (חברות רבות קרסו עקב בעיות בהנהלת חשבונות בסיסית).
- מערכות בנקאיות מספקות דוגמא נוספת לאבטחה רב שכבתית, אך מטרתן היא לאמת נתונים ולא סודיות.

נתמקד במספר מערכות מרכזיות:

- מערכות הנהלת חשבונות
- מערכות העברת כספים
- מערכות הכספומט
- כרטיסי אשראי
- טכנולוגיות מתקדמות יותר כמו כרטיסים חכמים ו- RFID

מקורות החשבונאות

- תחום הנהלת החשבונות החל במזרח התיכון בשנת 8500 לפנה"ס.
- אנשים החלו לייצר עודפי מזון וכתוצאה מזה לאחסן ולסחור בו. אז נוצר הצורך לעקוב מי לקח וכמה.
- תחילה, כל יחידת מזון הייתה מיוצגת כאסימון חמר ועליו חותמת של שומר המחסן.
- עם הזמן, כאשר המסחר התפתח, עסקים מסוימים היו גדולים מדי לניהול משפחה אחת.
- ככל שהכלכלה התפתחה, היה צורך לשכור מנהלים מבחוץ, מה שהקשה על הבעלים לפקח על הנעשה. מתוך זה התפתחה שיטת החשבונאות הכפולה.

שיטת החשבונאות הכפולה

שיטה זו מבוססת על רישום כל פעולה חשבונאית בשני ספרים נפרדים באופן שבו חשבון אחד מחויב וכנגדו חשבון אחר מזוכה. באופן זה תמיד נשמר איזון בין יתרות החובה לבין יתרות הזכות.

שיטה זו הפחיתה באופן משמעותי את אחוז ההונאות בעולם:

- מחייבת לפחות 2 משתפי פעולה על מנת לבצע מעשה מרמה.
- ישנן ביקורות אקראיות הבודקות כי אכן הספרים מאוזנים.

ועדיין, מקרי הונאות נפוצים בעולם...

תרמיות והונאות - קריסתה של חברת אנרון

- אנרון היא חברת אנרגיה אמריקאית שקריסתה ידועה כתרמית החשבונאית המתוכננת והמתוחכמת ביותר אי פעם.
- לאחר קריסתה בפשיטת רגל גדולה, התגלה כי החברה דיווחה במשך תקופה ארוכה על מאזנים שקריים.
- שערוריית אנרון הניעה את המחוקק האמריקאי לנסח חוקים שיגבירו את הפיקוח והבקרה הפנימיים של החברות בנוגע לדיווחים הכספיים. לדוגמא חוק סרבנס – אוקסלי.

הונאות באמצעות הטלגרף

הטלגרף הוא מכשיר להעברת מסרים למרחקים ארוכים באמצעות תשדורת של אותות אלקטרו-מגנטיים.

השימושים הראשוניים במכשיר זה היו צבאיים, אבל לאחר מלחמת נפוליון ממשלת צרפת פתחה את הרשת לשימוש מסחרי. ההתקפות לא איחרו לבוא:

- ב 1836 נתפסו שני בנקאים אשר במשך שנתיים שיחדו את המפעיל כדי שיעביר להם את תנועות שוק המניות בחשאי.
- הונאות נוספות התמקדו בהעברת אותות המשדרים תוצאות משחקים ומרוצי סוסים.

הבנקים היו בין הלקוחות הראשונים של הטלגרף והם החליטו שהם זקוקים למנגנוני אבטחה כדי למנוע שינויים בעסקאות ע"י גורמים זדוניים.

כיצד עובדות מערכות בנקאיות?

הבנקים היו בין הארגונים הראשונים שהשתמשו במחשבים. כבר בשנות ה-60 הם הציעו שירותי שכר אוטומטיים ותמכו בהעברת נתונים מחברה לחברה.

במערכת בנקאית טיפוסית יש מס' מבני נתונים:

- קובץ ראשי, המכיל את המאזן הנוכחי של כל לקוח.
- רשומות העוקבות אחר מזומן ונכסים בדרכם למערכת.
- יומנים שונים המחזיקים עסקאות שעברו דרך פקיד הבנק, הכספומט, הפקדת צ'קים וכדומה אשר לא הוכנסו עדיין לרשומות.
- מעקב המתעד אילו עובדים עשו מה ומתי.

בסוף כל יום תוכנת העיבוד שפועלת על מבני נתונים אלו תכלול הרצת לילה שמקבלת את כל התנועות ובמידה ומופר האיזון ישנה התראה מיידית על כך.

מודל האבטחה Clark- Wilson :
עקרון המודל

- המודל עוסק בעקרון של **שלמות מידע**.
- unconstrained data item – UDI
- constrained data item – CDI
- transformation procedures – TP
- integrity verification procedures – IVP
- "המשולש של קלרק-וילסון" – (משתמש, TP, CDI).

מודל האבטחה Clark- Wilson :
חוקי המודל

1) למערכת יהיו נהלים (IVP) עבור אימות שלמות ה- CDI.
2) יישום TP עבור CDI משמר את שלמותו.
3) CDI יכול להשתנות רק ע"י TP.
4) חברי צוות יכולים לאתחל TP מסוים על CDI מסוימים.
5) עקרון המשולש אוכף הפרדה לפי תפקיד.
6) TP מיוחדים שמופעלים על UDI יכולים לייצר CDI.
7) כל יישום TP חייב לגרום לבניה מחדש של מספיק מידע, כך שהוא ייכתב ל CDI מיוחד.
8) המערכת מאמתת חברי צוות שמנסים לגשת ל TP.
9) המערכת מאפשרת רק לחברי צוות מיוחדים כמו קציני ביטחון לבצע שינויים ברשימות הקשורות בהרשאות.

עיצוב הבקרה הפנימית

- **<u>עקרון השליטה הכפולה</u>** - שניים או יותר מחברי הצוות חייבים לפעול יחד כדי לאשר עסקה. למשל, במערכת פיקוד גרעינית.

- **<u>עקרון ההפרדה הפונקציונלית</u>** - שניים או יותר מחברי הצוות פועלים יחד על אותה עסקה בנקודות שונות עד שהעסקה מאושרת. למשל, עסקת רכש.

- ניתן לסכם עקרונות אלו כמודל של **מניעה – זיהוי – התאוששות**

עיצוב הבקרה הפנימית

- היבט חשוב בתהליך הבקרה הפנימית של מערכות בנקאיות הוא למזער את מס' ה SysAdmins – אנשים בעלי גישה מלאה למערכת כולה ובעלי יכולת לשנות אותה.
- הגישה הסטנדרטית כיום היא לשמור על צוות פיתוח נפרד לגמרי ממערכות הייצור. כך למשל, המערכת עצמה תורץ ע"י צוות ללא גישה לקומפיילרים או כלים אחרים שיאפשרו להם לשנות את הקוד.

מה השתבש?

סקרים רבים מוכיחים כי רוב ההונאות הגדולות בתחום התבצעו ע"י עובדים (מחציתם היו בחברה מעל 5 שנים וכשליש מהם מנהלים!).

להלן כמה דוגמאות:

- Paul Stubbs, פקיד שתפקידו היה לאפס סיסמאות בחברת HSBC, בעזרת חברת AT&T שינה את הסיסמא והעביר למעלה מ-20 מיליון דולר לחברות בחו"ל.
- ע"י שימוש ב"חשבון טעויות" של הבנק, פקידה בבנק דאגה לחייב חשבון זה ובמקביל העבירה אותו סכום לחשבון החבר שלה במשך כמעט כשנתיים. כך גנבה מאות אלפי דולרים.

מה השתבש?

- פקיד מאנגליה שם לב שהמערכת הבנקאית בבנק שעבד לא בדקה את כתובות הלקוחות. הוא מצא לקוחה עשירה, שינה את כתובתה לכתובת שלו, הנפיק כרטיס בשמה ואז שינה את הכתובת חזרה. באופן זה גנב כ- 8,600 פאונד מחשבונה.

ישנן כמובן הונאות בסדרי גודל גדולים בהרבה יותר:

- קריסתו של בנק ברינגס. זה היה הבנק המסחרי ה-1 בבריטניה. עובד בשם ניק ליסון הצטיין בבנק זה ונסע לנהל את הסניף בסינגפור, שם הוא הפסיד סכומי כסף עצומים והסתיר אותם בחשבון הטעויות שמספרו 88888. לבסוף, ברח מסינגפור והותיר אחריו חור של 1.3 מיליארד דולר במאזן הבנק ופתק בו כתב "אני מצטער".

מה השתבש?

- אתי אלון שמעלה בכספי הבנק למסחר בהיקפי ענק (254 מיליון ₪) וגרמה לקריסתו.
- בעיה מרכזית נוספת היא רואי החשבון. מצד אחד הם ממונים ע"י מנהלי החברה, ולכן לא יעלו על מרמה בידי מנהלים. בנוסף, היו מקרים בהם הציעו שירות זול רק כדי להכניס רגל לחברה ואז עשו את ה"מכה".

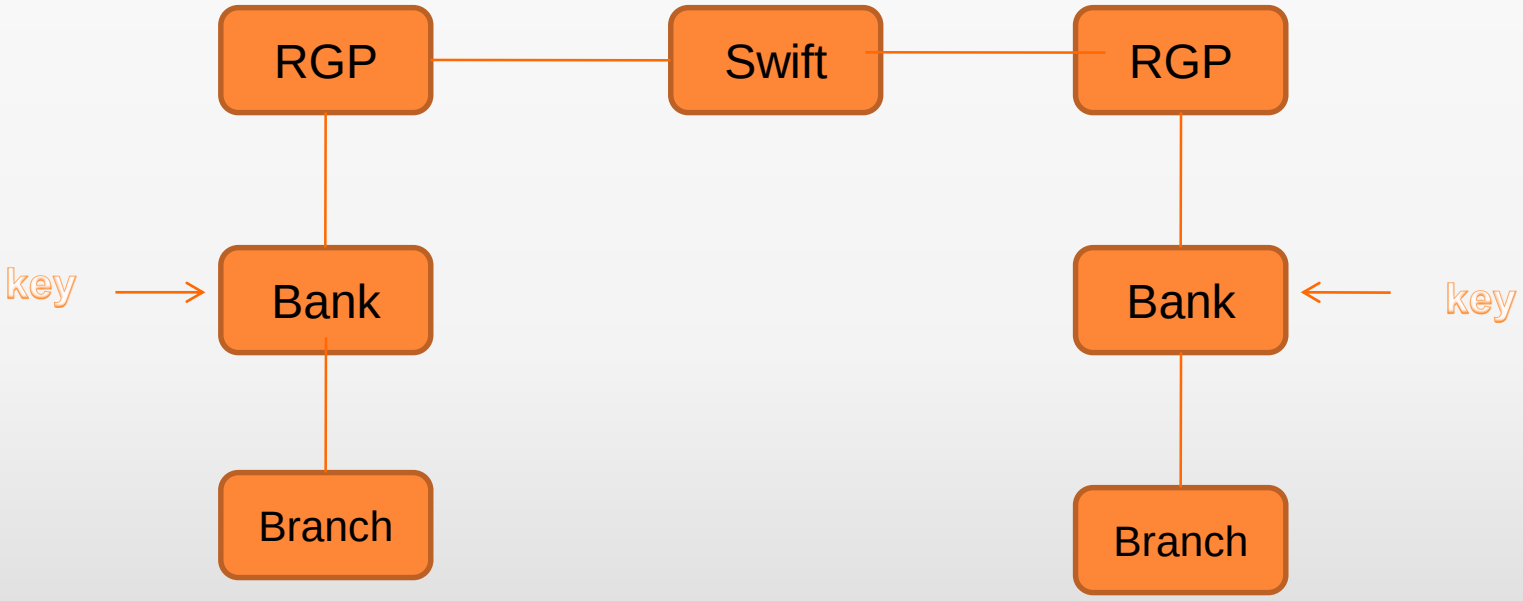
מהם הלקחים?

- לא תמיד ברור אילו עסקאות רגישות ואילו לא.
- כדאי להקשיב יותר ללקוחות שטענו כי רימו אותם.
- תמיד יהיו בני אדם שמאיישים עמדות מפתח.
- אין מערכות אבטחה שלא ניתנות לפריצה.
- אין דרך לנבא האם הצוות טוב או לא.
- לא מספיק לבדוק שהספרים החשבונאיים מאוזנים, צריך לבדוק שזה תואם למציאות.

SWIFT - The Society for Worldwide International Financial Telecommunications

- הוקמה ב 1970 וסיפקה אמצעי בטוח ויעיל יותר לשליחת הוראות תשלום בין חברי הבנק ובין הבנקים.
- הרעיון היה העברת הודעות ע"י קוד אימות – MAC בבנק השולח ובדיקתו בבנק המקבל.
- הבנקים בכל מדינה שלחו את המסרים שלהם למעבד אזורי RGP והוא העביר ל - SWIFT.
- ה- RGP היה מנוהל בד"כ ע"י חברה חיצונית.

SWIFT - The Society for Worldwide International Financial Telecommunications



איכות האבטחה אם כך תלויה בהצפנת ההתקנים בבנקים וצמתי ה - RGP.

מה השתבש?

- SWIFT רץ במשך כ- 20 שנה ללא דיווחי הונאות.
- המתקפות העיקריות במערכות מסוג זה לא עירבו את המנגנונים עצמם.
- הדוגמא הקלאסית היא בהנפקת כתבי ערבות:

פעולה זו יכולה להיות מוגדרת כהודעת SWIFT ואם ערבות מזויפת מתקבלת כאמיתית יכול התוקף לקחת את הזמן שלו, ללוות כסף מבנק נותן ההלוואה ורק אז להעלם.

ATM

- המצאת הכספומט הייתה בין החידושים הטכנולוגיים המשפיעים ביותר של המאה ה-20.
- הומצא בשנת 1938 ע"י Luther Simjian .
- תחילה לא ראו בכספומט שימוש ורק אחרי כמה שנים חזר הכספומט לרחובות.

ATM

Account number PAN: 8807012345691715

PIN key KP: FEFEFEFEFEFE

Result of DES {PAN} : A2CE126C69AEC

N decimalize: 0224126269042823

Natural PIN : 0224

Offset: 6565

Customer PIN: 6789

בשיטה זו, הכרטיס מכיל את מס' החשבון העיקרי של הלקוח ומפתח סודי העובר תהליך של עריכה בשיטה העשרונית ואז קיצוץ וכן נוצר ה PIN "הטבעי". ניתן להוסיף 4 ספרות של offset והתוצאה תהיה קוד ה PIN של הלקוח.

כיצד מיושם עקרון הבקרה הכפולה בכספומטים?

- הנפקה ופעולות הקשורות למפתח PIN נעשות ע"י חומרה ואף פעם אינן זמינות לחברי הצוות של הבנק.
- הכרטיס וקוד ה PIN מודפסים במכונות נפרדות.
- המפתח הראשי עבור כל מכשיר כספומט מסופק לבנק ע"י שני גורמים נפרדים.

מה השתבש : איומים מבפנים

- Andrew Stone מבריטניה שינה את מס' החשבון שלו לזה של אשתו וגילה שהוא יכול למשוך כסף באמצעות הקוד שלו. זה קרה משום שהבנק שלו כתב אלגוריתם הצפנה לכרטיס מבלי לקשר אותו למס' החשבון.
- הונאות ע"י עובדי הבנק עצמו (דוגמת הטכנאי הסקוטי שהתקין מחשב בתוך הכספומט וכך קיבל נתונים של לקוחות רבים).
- בנק קטן הנפיק בטעות לכל לקוחותיו את אותו קוד ה PIN.
- שיטות אימות לא טובות של בנקים (למשל מפתחות PIN בצורה של 4455).
- לקוחות רמאים שנכנסים לבנק וטוענים כי שכחו את הקוד שלהם.

מה השתבש : איומים מבחוץ

- כספומטים מזויפים - היו גניבות בתהליך השליחה עצמו.
- השיטה השנייה של Andrew Stone הייתה פשוט לעמוד מאחורי לקוח ולתצפת על הכנסת קוד ה- PIN, ולאחר מכן לאסוף את הפתקית (שבה בד"כ היה מצוין מס' החשבון במלואו).
- שימוש במצלמות וידאו עם חיישני תנועה.

אז, מי אשם?

הבנק? הלקוח?

סיפורו של John Munden : שוטר מקומי שחזר מחופשה וגילה שחשבון הבנק שלו ריק. הוא התלונן לבנק שלו והבנק טען כי הוא מנסה להשיג כסף במרמה. במהלך המשפט הבנק טען כי מערכת הכספומט שלהם לא יכולה בשום אופן לסבול מבאגים. השוטר הורשע ופוטר ממקום עבודתו.

כרטיסי אשראי

- כרטיס האשראי הומצא בשנות ה-50. תחילה הבנקים לא ראו רווח עסקי מכרטיסים אלו. בבריטניה לקח כמעט 20 שנה עד שהבנקים הבינו שזה עסק משתלם.
- במקרה של הונאה בכרטיס אשראי, עיקר הנזק מוסב לחנות בה בוצעו הרכישות ולחברת האשראי, ואילו בעל הכרטיס נושא בנזק קטן יחסית (אם בכלל).
- כל עסקה שסכומה גבוה מסכום שנקבע עוברת לאימות מול הבנק וחברת האשראי.
- הבעיה היא שתהליך האימות משתנה מבנק לבנק :

האחד ישלח SMS לאימות והשני יבקש להכניס את הקוד הסודי של כרטיס האשראי ובכך יהפוך את הלקוח למטרה.

זיוף כרטיסי אשראי

- "מפעילי העסקים העקומים".
- מסופים מזויפים, מכשירי ציתות ששימשו להאזנת

נתוני כרטיס האשראי וכדומה.

שני חשודים בהונאות נתפסו עם 17 כרטיסי אשראי

החשודים: תושב קדית ים בן 35 ותושב טירת כרמל בן 40. בנוסף נעצר צעיר מקדית שמואל שברשותו נתפס "קורא שפתיים" של כרטיסי אשראי

תושב קדית ים (35) ותושב טירת כרמל (40) נעצרו ביום רביעי שעבר לאחר שברשותם נתפסו כרטיסי אשראי החשודים כגנובים או מזויפים.

במהלך חיפוש שביצעו שוטרים מתחנת זבולון במחסן בבית הוריו של אחד החשודים, שבו שהו חשודים, נתפסו 17 כרטיסי אשראי וכן מכשיר לקיורד כרטיסי אשראי ("קורא שפתיים"). ביום חמישי הובאו השניים, המיוצגים על ידי עו"ד מיקי זילברשמיד ועו"ד יוגב אוזלאי, להארכת מעצר בפני סגן נשיא בית משפט השלום בקריות השופט איתן מגן. בדיון ציין נציג המשטרה רס"מ שמעון תורג'מן כי הצוותים הגיעו להסכמה, שמעצרם של החשודים יוארך בשלושה ימים ולאחר מכן ישוחררו בתנאים המשטרה. השופט קיבל את עמדת הצדדים.

עוד באותו היום נעצר תושב קריית שמואל (25), לאחר שבמהלך פשיטה בביתו נתפס קורא שפתיים של כרטיסי אשראי, מכשיר קשר, סורק תדרים וכוונן מחשב שעל פי החשד משמשים לזיוף, הפצה והרווחה בכרטיסי אשראי. עוד באותו יום הובא החשוד להארכת מעצר בפני השופט מגן. נציג המשטרה רס"מ תורג'מן ביקש להאריך את מעצרו בחמישה ימים והסביר: "היה דבר העיקרי שנתפס הוא המכשיר שבעזרתו מזייפים כרטיסי אשראי. ברצוננו לברוק את תוכן המחשב ולברוק כיצד השיג את המכשיר שבעזרתו הוא מזייף את הכרטיסים".

בשיתוף עם ויזה. סרדל

סניגורו של החשוד עו"ד אודן ביטון אמר בדיון כי מהומר הראיות לא עולה חשד סביר לכך שהחשוד ביצע את החשדות המיוחסים לו ויש לשחררו ממעצר. השופט מגן ציין בהחלטתו כי החשוד שמר על זכות השתיקה ולכן, אם הדבר מכיר על עברתם של השוטרים ויש צורך לאפשר להם לבצע את החקירה ללא הפרעה, אל לו להתלונן. "את מעמדו כברוקאי לא רכש החשוד עקב שוטטות על גלי האתר או במהלך גלישה באינטרנט. כשהוא הופך פתאום חובב אלקטרוניקה ומסרב לגלות מניין החפצים ולמה נועדו, הרבר אומר דרשני", עקץ השופט. הוא ציין כי יש יסוד מוצק לחשד, וכי שיתרורו של החשוד עלול לחבל בחקירה. מעצרו הוארך בחמישה ימים.

קצין מודיעין בילוש תחנת זבולון רס"ק אילן סרדל אמר השבוע כי השוטרים עסקו בפרשת כרטיסי האשראי יותר מחודש: "עברנו על הנושא בשיתוף עם חברת ויזה כאל. נעדכו מעקבים, תצפיות וצילומים של תרמיות בשווי מאות אלפי שקלים.

"לאחר כחודש של מעקבים ברצו מעצרים ונתפסו 'שפתיים', מכונה לזיוף כרטיסים ברמה מאוד גבוהה ומחשב הכולל שפתיים לשיכפול כרטיסי אשראי של כל החברות".

מורן כץ

המשטרה חשפה הונאה במוסך במישור אדומים:

גיהצו כרטיסי אשראי של לקוחות

בעקבות תלונות של מספר תושבים על חיובים חריגים בכרטיס האשראי, פתחה משטרת מעלה אדומים בחקירה סמויה שהעלתה חשד חמור להונאת אשראי על ידי אחד המוסכים במישור אדומים. דובר המשטרה: "אם גיליתם חיוב חריג ולא מוכר, אנא הגיעו לתחנת המשטרה למשרד החקירות"

חשד להונאה במוסך מוכר במישור אדומים. בעקבות מספר תלונות שהתקבלו על ידי תושבים שאיתרו חיובים גבוהים וחריגים בחיוב האשראי שלהם, פתחה משטרת מעלה אדומים בחקירה סמויה אשר ממנה עלה חשד כי אחד המוסכים במישור אדומים, אשר שמו נאסר לפרסום, בו טיפלו כל המתלוננים ברכבם, הונה את לקוחותיו על ידי שימוש בכרטיסי האשראי, אותם סלק לטובת תשלום עבור טיפול שהעניק להם.

על פי חקירת המשטרה עולה כי בכרטיסי האשראי נערכו "קניות" של חלקי רכב, אביזרי רכב ועוד. לדברי המשטרה, השיטה בה נהג בעל העסק אשר נחקר בתחנה היא העתקת מספר כרטיס האשראי.

לידי עיתון "זמן מעלה" הגיעו ידיעות כי החשדות מתרכזים באחד העובדים במוסך אשר ביצע על פי החשד חלק מהקניות. בשיחה עם "זמן מעלה" סיפר אחד הלקוחות שביקש להישאר בעילום שם, כי בחיוב שהגיע עם תחילת החודש הוא שם לב לחיובים חריגים בסך 15 אלף שקלים עבור קניית מוצרי ניקיון תעשייתיים. לאחר בירור קצר וחקירה עצמאית, הבין שאחד הפועלים במוסך הוא החשוד בהונאה, ולכן מיהר להגיש תלונה במשטרה וכן מול חברת כרטיסי האשראי, ממנה הוא דורש את החזרת הסכומים לחשבונו באופן מיידי.

דובר תחנת מעלה אדומים, רפ"ק דודי אבוחצירא, פנה לתושבים בבקשה לבחון את חיובי האשראי שלהם, "אנו פונים לתושבי מעלה אדומים אשר נעשו חיובים חריגים ולא מוכרים בכרטיסי האשראי שלהם, להגיע לתחנת מעלה אדומים למשרד החקירות".

אריק בן שמעון

נתונים כמותיים

- חברות האשראי מקדישות מאמצים רבים לאיתור מהיר של מעשי מרמה, אך הן אינן מפרסמות נתונים על היקף הנזק הנגרם להן (לדוגמא חברת ויזה שפרסמה ביום אחד גם ירידה וגם עליה בשיעור ההונאות).
- ב–1990 0.15% מסך העסקאות הבינלאומיות באמצעות ויזה ומאסטרקארד היו מדווחות כעסקאות במרמה.
- ניתן לראות הבדלים לאומיים: בארה"ב האחוז עמד על 1%, באנגליה על 0.2% ובצרפת וספרד מתחת ל 0.1%
- צרפת למשל כבר בסוף שנות ה-80 השתמשה בטכנולוגיה חדשנית – כרטיסים עם שבב מה שגרם לירידה חדה באחוזים.

הונאות אונליין

- מ-1995 נוצרה חרדה גדולה כי השימוש בכרטיסי אשראי באינטרנט יוביל להמון מעשי מרמה.
- האיום הממשי היה כפול – ראשית, צמיחת הפישינג, כאשר הגורם למתקפות מסוג זה הוא הגורם הפסיכולוגי, האנושי ולא הטכנולוגי.

  שנית, רוב מס' האשראי שהגיעו לידיים הלא נכונות הגיעו כתוצאה מחבלה במחשבי בעלי העסקים. כך למשל, משנת 2000 ויזה הכריחה את כל בעלי החנויות להתקין firewall.

הונאות אונליין

- רוב העסקאות הן בינלאומיות ואימות כתובת בחו"ל בעייתית במקרה כזה.
- הונאות מסוג "סיור חינם" והכנסת מס' כרטיס אשראי כדרך להזדהות.
- מנגנון ההחזר הכספי לקונה. כך למשל קרסו הרבה אתרים קטנים שהתקשו לעמוד בעמלות הבנקים על החזר כספי (boo.com).
- עובדה זו גרמה לסוחרים להיזהר מעסקאות מוזרות כמו למשל קניית 4 שעונים, הזמנות ממדינות מפוקפקות, בקשות למשלוח זריז וכו'.

הכרטיס החכם

הכרטיס החכם

- הכרטיסים החכמים נכנסו לשימוש עוד באמצע שנות ה-80. תחילה שווקו כתרומתה של צרפת להתפתחות עידן המידע. בשאר העולם התפשטות הכרטיסים הייתה איטית יותר.
- הכרטיס החכם מכיל בתוכו גם מעגל משולב (שבב), המסוגל לתקשר עם מערכות שמחוץ לו, לרוב בכפוף למנגנוני אבטחה שונים.
- בשנות ה-90 התחילה באירופה פעילות של שימוש בכרטיסים חכמים כמנגנון ארנק אלקטרוני. משנת 1992 התאגדו חברות Europay MasterCard ו - Visa לאיגוד EMV ליישום שימושי ארנק אלקטרוני, ופיתחו מערכת תקנית לנושא.

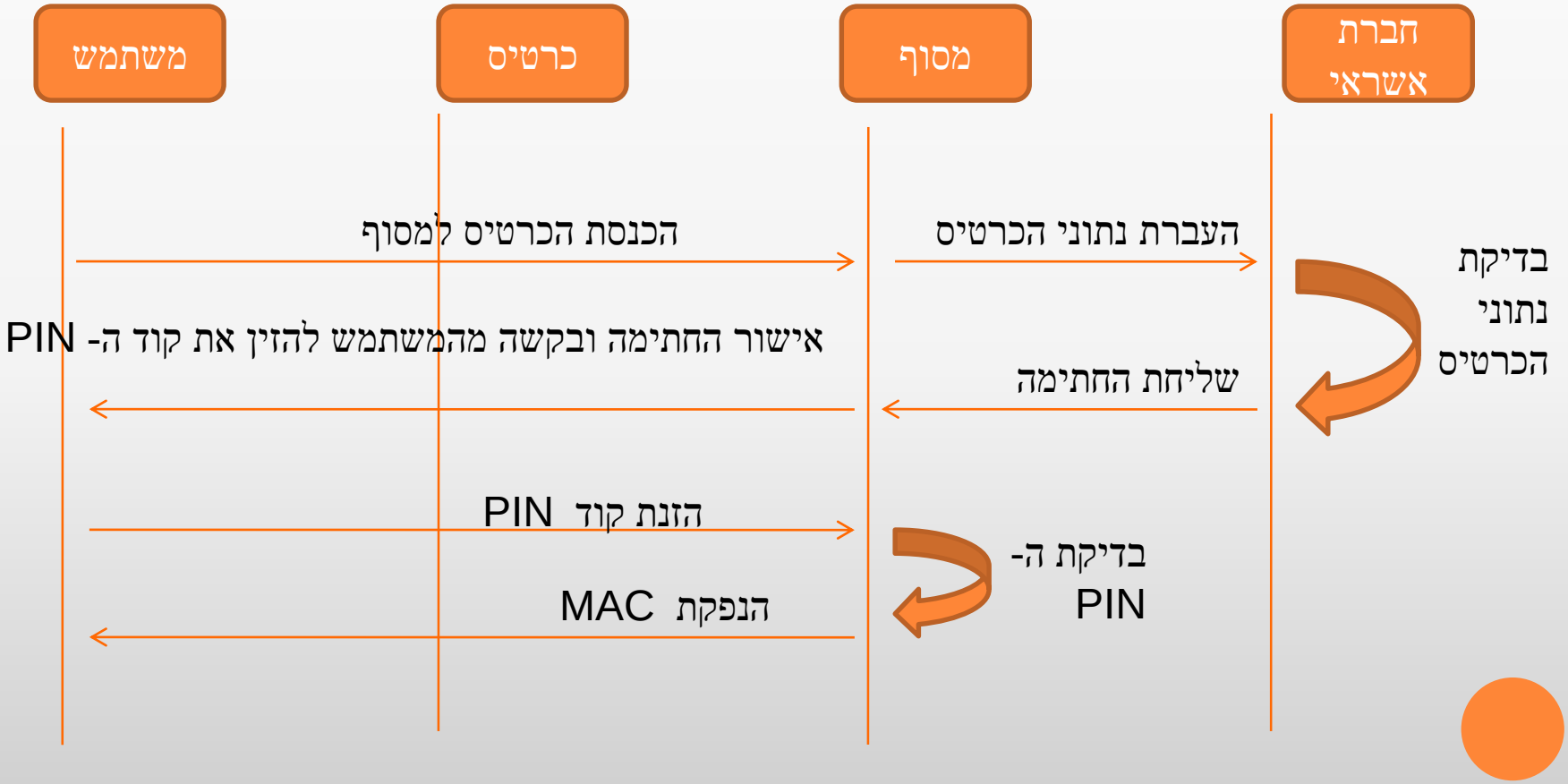
תקן ה- EMV : כיצד זה עובד?

כל כרטיס מכיל צ'יפ עם היכולת לאמת את קוד ה-PIN.

הכרטיסים מגיעים ב- 2 סוגים:

- בעלי עלות נמוכה – עושים הצפנה סימטרית בלבד (שיטה שבה מפתח הפענוח זהה למפתח ההצפנה), משתמשים בפרוטוקול SDA.
- בעלי עלות גבוהה – כרטיסים המייצרים חתימות דיגיטליות המיושמים בד"כ באמצעות הצפנה א-סימטרית (שיטה שבה מפתח ההצפנה שונה ממפתח הפענוח), משתמשים בפרוטוקולים DDA ו-CDA.

פרוטוקול SDA



פרוטוקול SDA

- זהו פרוטוקול ברירת המחדל של EMV.
- MAC- מכיל מס' מזהה הסוחר, סכום, מס' סידורי וכו'.
- המפתח המשמש לחישוב ה- MAC משותף בין הכרטיס והבנק המנפיק, ולכן בעצם האימות מתבצע רק ע"י הבנק.

פרוטוקול SDA

מעשי המרמה לא איחרו לבוא:

- ביקור "תחזוקה" של נוכלים.
- פגם בהתקן עצמו.
- אופן אימות הנתונים.

פרוטוקול DDA

- זהו פרוטוקול EMV מורכב יותר. השימוש העיקרי בו נעשה בגרמניה.
- השינוי מ-SDA הוא בכך שהכרטיסים מסוגלים לעשות הצפנה ע"י מפתח ציבורי. כלומר, לכל לקוח יש זוג מפתחות, פרטי וציבורי, כאשר הציבורי גלוי על גבי הכרטיס.
- ההתאמה הנה חד-חד-ערכית (לכל מפתח פומבי קיים אך ורק מפתח פרטי יחיד המתאים לו).
- פרוטוקול זה מוגן יותר אך יקר יותר מ SDA.

RFID

- חסידים של EMV קיוו כי תקן זה יהיה עולמי אולם מדינות כמו ארה"ב לא השתכנעו והעדיפו לחכות לשיטה שנקראת RFID.
- זוהי טכנולוגיה של תיוג אלקטרוני באמצעות גלי רדיו והיא מבוססת על התקנים קטנים המוצמדים לעצם אותו מעוניינים לזהות.
- שיטה זו הייתה מציאות במשך כמה שנים במס' מערכות תחבורה ביפן.

RFID

באמצעות טכנולוגית RFID פותחה טכנולוגית NFC – תקשורת טווח אפס המאפשרת למשל תשלום באמצעות הטלפון הנייד.

THE END