פרויקט גמר

**מניעת התקפות מסוג פישינג במערכות הצבעה אינטרנטיות באמצעות אלגוריתם קריפטוגרפיה ויזואלית (Visual Cryptography)**

יובל ממן 326284320, יונתן כהן 214667966, גור סיני 326531985.

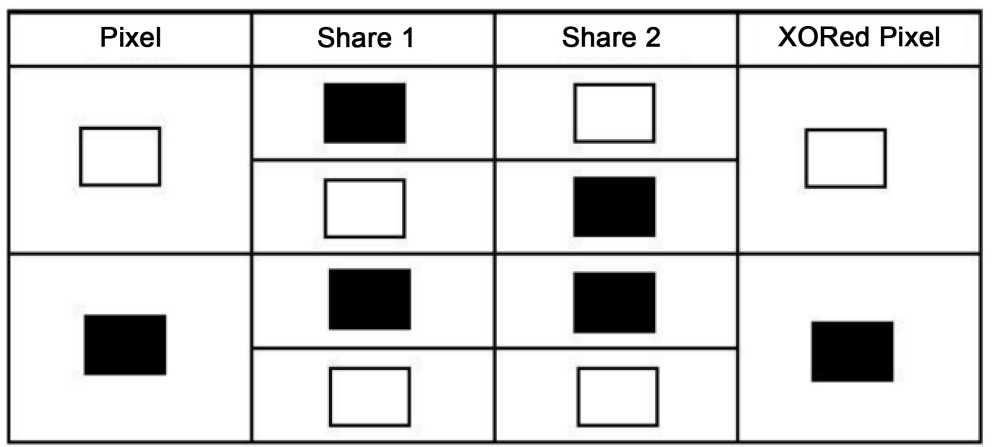
המדריך – ד"ר גרשון קגן

1. אלגוריתם VC (Visual Cryptography)

אלגוריתם הצפנה VC מבוסס XOR (בו נשתמש בפרויקט זה) זה מקבל כקלט תמונה בינארית ומחזיר שני תמונות הנקראות Share 1 ו- Share 2. כאשר מבצעים פעולת bitwise-XOR על שתי התמונות, מקבלים את התמונה המקורית.

האלגוריתם עובד בצורה הבאה:

\*קיימת הנחה שפיקסל לבן שווה ל-0 ופיקסל שחור שווה ל-1.



תמונה 1

כל פיקסל בתמונה המקורית מתורגם לזוג פיקסלים, אחד יהיה שייך ל-Share 1 והשני ל-Share 2.

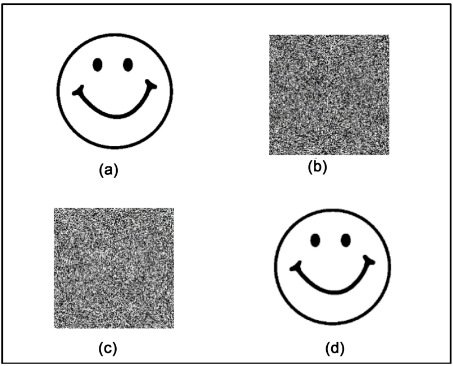
פיקסל לבן במיקום :

יבחרו אחת משתי האפשרויות הבאות באקראיות לכל פיקסל:

1. Share 1 יקבל פיקסל לבן ו-Share 2 יקבל פיקסל שחור.
2. Share 1 יקבל פיקסל שחור ו-Share 2 יקבל פיקסל לבן.

כך, ה-XOR של שני הפיקסלים יצור בחזרה פיקסל לבן.

בדומה לכך, פיקסל שחור ייווצר בהתאם לערכים בתמונה 1.

להלן דוגמה:

תמונה 2

1. – התמונה המקורית
2. – Share 1
3. – Share 2
4. – XOR של Share 1 ו- Share 2

2. שימוש באלגוריתם VC למניעת מתקפות פישינג

מתקפות פישינג – ניסיון להתחזות לגוף מהימן על מנת להשיג נתונים רגישים.

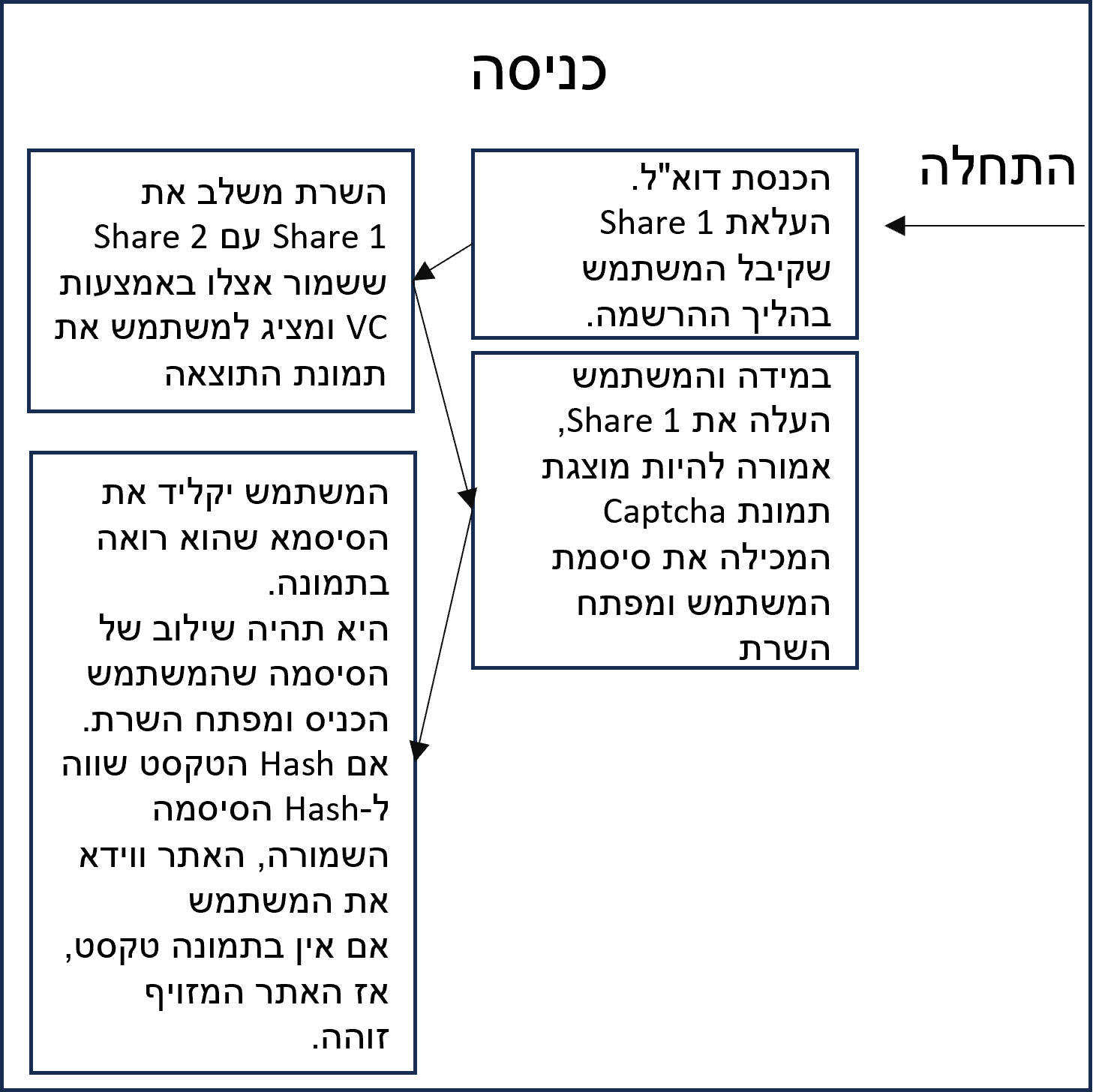
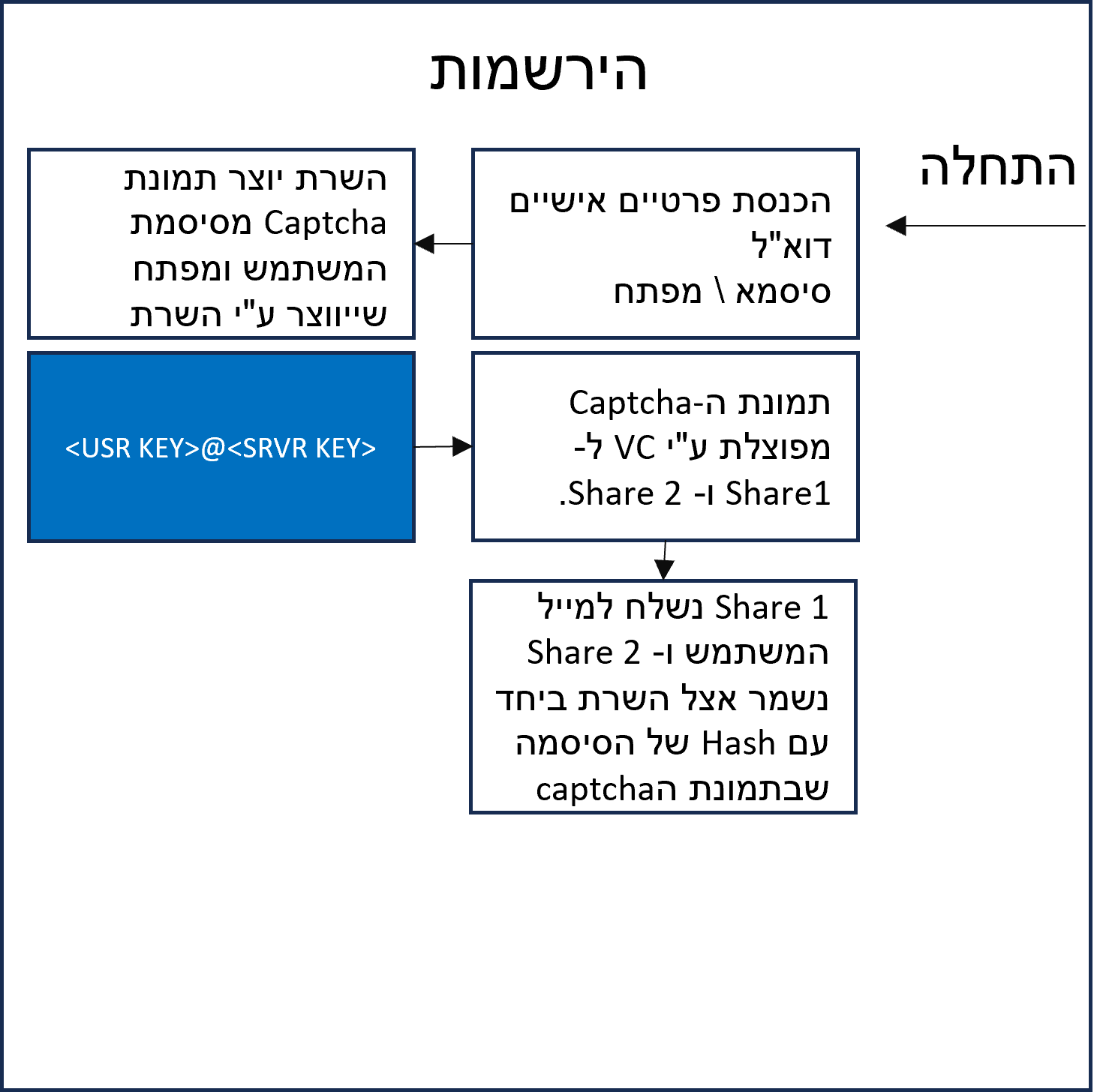
מתקפות פישינג יבואו אצלנו לידי ביטוי בכמה דרכים עיקריות.

1. התחזות לאתר שלנו (אתר מזויף). עם בעיה זו, אין לנו דרך להתמודד שכן אם אדם מבצע את כל הפעולות באתר מתחזה, לנו אין דרך לדעת על כך.

אנו כן נספק למשתמש דרך לראות שהאתר שלנו הוא אכן האתר שאליו נרשם. פירוט יהיה בהמשך.

1. התחזות של אדם זדוני לאדם תמים.

כעת נציג את מבנה האתר ולאחר מכן נציג כיצד הוא פותר את שני הבעיות הללו.



\*מפתח השרת הכרחי, שכן הוא מה שגורם להבדלה בין כניסה עם סיסמה רגילה לכניסה עם VC. בלעדיו, לא משנה איזה תמונה תוחזר מהשרת, המשתמש יוכל להכניס את סיסמתו ולהיכנס!

1. במידה והאתר אליו המשתמש מנסה להתחבר הוא **זדוני**, בעת ההתחברות האתר לא יוכל להחזיר את תמונת ה-Captcha המקורית, ולכן המשתמש יזהה את האתר כמזויף.
2. בשביל להתחבר לחשבון המשתמש, יש לקבל גישה לShare המשתמש כדי לקבל את הסיסמא המלאה לחשבון. אך ורק באמצעותה ניתן להיכנס לחשבון.

עיצוב מסד הנתונים הטבלאי:

**מקרא:**

מפתח ראשי, מפתח זר, שדה רגיל

**משתמשים:**

מייל משתמש, שם פרטי, שם משפחה, כתובת Share 2, Hash סיסמת המשתמש, Hash קוד השרת שמופיע בתמונת ה-Captcha, שאלת הביטחון של המשתמש.

**סקר:**

מ.ז. סקר, שם הצבעה, תאריך התחלה, תאריך סיום, מייל בעלים (משתמשים).

**משתמש בסקר:**

מ.ז. סקר, מייל משתמש, האם הצביע או לא.

\*\*\* הסיבה שמייל המשתמש אינו מפתח זר לטבלת המשתמשים היא כי כתובת מייל שהוזמנה לסקר לא בהכרח משתמש! עליו להירשם ורק אז יוכל להיכנס לדף ההצבעות.

**מועמד בסקר:**

מ.ז. מועמד, מ.ז. סקר, שם, תיאור, כתובת לתמונה