

# השימוש במכשיר טלפון בתור אמצעי לזיהוי לקוח במערכת הפיננסית

Recognition by DTMF and another  
modern phone bridge

מאת: אמיתי דן-חוקר אבטחת מידע

# קצת היסטוריה

- מהו פריקינג.
- פריצות פריקינג ( Phreaking ) בעבר.
- מבנקאי אישי לבנקאי טלפוני.
- למה בכלל צריך ללמוד היסטוריה כשבאים להגן על מערכת?

# שיטות הזדהות טלפוניות

- הקשת תעודת זהות וסיסמא- זיהוי בעזרת DTMF .
- זיהוי קולי.
- DTMF signal in voip software .

# מה עושים עם DTMF

- DTMF- Dual-Tone Multi-Frequency
- שליחת צלילים בעלי ערך מספרי.
- פענוח הצלילים מאפשר גישה לחשבונות הבנק דרך בנקאי טלפוני.
- הגנה על הלקוח והבנק לעומת העבר שבו הבנקאי האישי ענה לטלפון ישיר וביצע לעתים פעולות ללא זיהוי מלא (תוך הכרות אישית עם הלקוח).
- חיסכון בביצוע פעולות.
- חיסכון בעמידה בתורים.
- בנקאי זמין גם לאחר שעות העבודה.

# DTMF-חולשות

- בסניפי בנק רבים הוטמעו טלפונים לשימוש הלקוחות.
- כסטנדרט קיימים בטלפונים כפתורי חיוג חוזר.
- הלחיצה משמיעה את צלילי ההקשות האחרונות.
- צליל שווה מספר.
- מספר שווה חשבון (בנק).
- כספת עם מפתח בכניסה.

# הדגמות

- הדגמת ווידאו של פענוח DTMF בעזרת תוכנת פענוח בשם DTMFdec .
- המחשת מכשיר טלפון פיזי.

# דרכי תקיפה

- DTMF decoding by Iphone and another smartphones .
- תוכנות DTMF decoding במחשבים.
- מכשירים ייעודיים לפענוח- Portable DTMF .decoders
- שידור אותות DTMF משפופרות טלפון שהוחלפה במכשיר טלפון בבנק. (שידורי משדר מקלט, GSM, WIFI, . .)

# תקיפות נוספות

- פענוח אותות DTMF ממכשירי טלפון ביתיים.
- פענוח האותות של תוכנות voip לא מוצפנות דרך ה data).
- פענוח של תוכנות voip מוצפנות דרך האזנה לצליל DTMF מלאכותי במחשב עצמו.
- פענוח אותות DTMF ממכשיר סלולרי דרך סוס טרויאני שיודע להתמקד במספרי הבנקים.

# שיטות הגנה

הטענה שלי היא שניתן להמשיך להשתמש במערכות אלו לאחר ארגון מחדש של תפיסות האבטחה בנושא.

- הקשחת מכשירי הטלפון באופן מלא.
- Multi-factor authentication
- זיהוי בעזרת שאלות הזדהות אישיות, sms.
- שיתוק כפתורי החיוג החוזר באופן מיידי.
- מחולל סמאות דינאמי (חומרתי/תוכנתי) כמו שקיים בPayPal ובאוניברסיטאות רבות.

# שיטת הגנה-המשך

- פיתוח של מכשירי טלפון קוויים אלחוטיים עם הצפנה בין עמדת ההטענה לטלפון עצמו.
- הבנה תפיסתית שלצורך הגנה על כשלים שיטתיים צריך לפתח שיטות הגנה פיזיות של מכשירים טכנולוגיים.
- הסקת מסקנות שתמנע הטמעה מהירה של דרכי התייעלות ללא הבנה שהטמעה מהירה מידי של מכשיר פיזי תביא לכאב ראש לוגיסטי בזמן התיקון.

# The flash button

- כפתור ה Flash כמפתח למרכזייה.
- SE and data gathering .
- פרטי הזדהות של בנקאי.
- מהתחזות ללקוח בפרצת DTMF להרשאות בנקאי.
- טלפונים ציבוריים עם חיוג למספר מוזן מראש קיימים גם בקופות חולים.
- שיחות חינם.

# הסקת מסקנות מהמחקר

- חובת ההגנה היא של הבנק אך לא פחות מכך של הלקוח.
- צורך בשילוב של ידע בהגנת המידע הדיגיטלי ושל אבטחה פיזית של חומרות ומתחמים.
- מניעה של פגיעה של תוכנות בחומרות, ועצירת כשלי תוכנות שחומרות תוקפות אותם.
- במאה ה 21 איש אבטחת מידע, וקב"ט פיזי צריכים להיות בעלי ידע רב תחומי.
- כשיש כשל שיטתי במוצר כדאי לחפש כשל נוסף.

# דעה אישית

- יש צורך בשינוי תפיסתי ביחס להתרעות על בעיות אבטחה.
- פתיחת מחלקות פיתוח מוצרים פיננסיים בהשפעת לקוחות.
- הבנה שיש בעיות.
- שיתוף הציבור המקצועי והלקוחות בבניית מוצרים פיננסיים.

# תחרות X-Bank

- תחרות פיתוח מוצרים פיננסיים.
- הבנקים ירוויחו מוצרים, שיכניסו כסף נוסף.
- הלקוחות ישפיעו על הבנק ויזדהו עם המותג.
- מי שייצור בתחרות מוצר פיננסי חדש יתוגמל ע"י הבנק בעבודה כסף או פטור מעמלות.
- יוצרו רעיונות חדשים להגנה על עמדות פיזיות לשירות עצמי (Self service machine, ATM's).
- הכורח הוא אבי ההמצאה כך שתקיפת חומרה תביא ליצירת פתרונות.

# תחרות ה X-bank המשך

- תחרויות מוגבלות זמן, אירועי תקיפת מערכות בנקים.
- האם האקרים יכולים ליצור?
- מה משמעות המילה האקר?
- האם ניסיתם להמציא פטנטים פיזיים?
- לאחר דיווח על בעיות אבטחת מידע האם נתתם פתרונות?
- יש שאלות?

אמיתי דן [popshark1@gmail.com](mailto:popshark1@gmail.com)