ממ"ן 16(פרויקט) במבוא לאבטחת המרחב המקוון

כללי: לתכנן ולממש העברת הודעות מוצפנות מקצה לקצה(E2EE - END TO END ENCRYPTION, בדומה ל וטסאפ). **הפתרון צריך לעמוד גם במתקפת MITM בכל המרכיבים והשלבים.**
למרות שקיימים פרוטוקולים שימושיים(כמו SIGNAL למשל), המטרה היא לתכנן פרוטוקול משלכם **המתבסס על ההנחות בהמשך** שיעמוד בדרישות ולהשתמש מעשית בתכני הקורס השונים.

מבחינת הלמידה, הדרך הטובה ביותר היא לתכנן לבד מ 0 ולוודה שהפרוטוקול עומד בכל הדרישות.
אחרי זה ניתן להשוות עם פרוטוקולים קיימים כדי לבדוק שאכן הוא עומד בכל הדרישות **כשלוקחים בחשבון את ההנחות הקיימות בפרויקט. אין לממש דברים מיותרים(מבחינת אבטחה).**
ניתן להיעזר בקובץ קישורים במידת הצורך גם בשלב התכנון וגם בשלב המימוש. הימנעו מ"העתק-הדבק".

חלק 1 תכנון(55 נק'):

תכננו ותארו בצורה **מפורטת וברורה** את פרוטוקול העברת הודעות E2EE עם אישורים על קבלתן דרך השרת עם אפשרות שליחת הודעה ללקוח לא מחובר כעת וקבלתה אחרי ההתחברות.
הפרוטוקול צריך לעמוד בדישות סודיות CONFIDENTIALITY ושלימות INTEGRITY כולל מקוריות AUTHENTICATION בכל המידע עם עמידות נגד התקפות MITM **בכל השלבים.**

התייחסו לנקודות הבאות, הסבירו בקצרה את הבחירה שלכם ואיך היא משיגה את המטרה:

א. שיטת ההצפנה(סימטרית או א-סימטרית) ואופן יצירת מפתח/ות.
ב. תהליך הרישום הראשוני.
ג. אופן יצירת והחלפת מפתח/ות, מקום שמירתם(שרת/לקוח) ובטיחות החלפתם.
ד. אופן השגת השלמות במובן הרחב(מקור ותוכן ההודעה), פרטו את השיטה ואת דרך יישומה.
ה. מהלך שליחת ההודעה והאישור על קבלתה.
ו. תארו בצורה מפורטת את מבנה(שדות) ההודעה(אם צריך תוכן השדות הנוספות על המידע ואופן/שיטה יצירת השדות האלה).
ז. תארו בצורה מפורטת את מבנה הנתונים בשרת(מה ואיך נשמר).

הנחות:

א. ההנחות הסטנדרטיות(הצפנה סטנדרטית לא פריצה למשל). תבחרו מפתח באורך המתאים למטרות
ב. ההודעות הן קצרות.
ג. בין השרת לכל לקוח קיים ערוץ בטוח המאפשר שליחה חד פעמית של קוד סודי **בן 6 ספרות**(כמו בווטסאפ ברישום). התייחסו לאורח החיים של הקוד. התייחסו לאפשרות שימוש ב(**KDF**) **key derivation function** (מתאימה/באיזו מידה/לא מתאימה). עיינו בקישורים.
ד. המפתח הציבורי של השרת קבוע ומובנה בתוך אפליקציית לקוח.
ה. בשביל פשטות הפתרון, השרת מיועד ללא יותר מ 10 לקוחות(גודל מבנה הנתונים).

הערות כלליות:

א. כשבוחרים בשיטה מסוימת, הגדירו אותה במדויק, למשל הצפנה סימטרית CBC-256 , HASH SHA-256 וכדו'.
ב. אין לבצע פעולות מיותרות, כמו למשל הצפת מה שלא דורש הצפנה או אימות מה שלא דורש אימות.
ג. המימוש צריך להיות סביר ונוח לשימוש, למשל אין לדרוש הזנת קוד אימות בשליחת כל הודעה ואין להשתמש בערוץ בטוח להעברת ההודעות, **אלא רק לצורך אימות בשלב אתחול(רישום)**.
ד. השרת צריך לתמוך ב Multi-Threading כמימוש ריבוי לקוחות, הלקוח לא חייב, לבחירתכם.
ה. אם מתקשים בתכנון/מימוש חלק מסוים, ציינו את זה בהגשה. מודעות לחיסרון ללא מימוש עדיפה על העדר הבנה.
ו. ציינו את המגבלות/חסרונות(למקרים רגילים, לא למקרי קצה) של הפתרון אם יש.

חלק 2 מימוש מעשי בקוד(40 נק'):

ממשו את התכנון מסע' א' ב CLI (**עדיף וכדאי בפייתון,** כל אפשרות אחרת בתיאום עם המנחה). הקוד צריך לעבוד תקין בבדיקה עם ברירת מחדל של הסביבה הסטנדרטית.

- כל לקוח מזוהה ע"י "מספר הטלפון" שלו- רצף מספרים באורך שתבחרו. הוא יכול להיות מובנה באפליקציה(אם כן בשביל ההדגמה צריך כמה גרסאות), מתקבל מהקלט בזמן הפעלת הלקוח או להתקבל כמספר אקראי מתוך הרשימה המובנית בלקוח או בקובץ. אין צורך "להמיר" את "מס' הטלפון" לשם לקוח.
- אפשר להשתמש בכל הפונקציות הסטנדרטיות ולייבא מודולים סטנדרטיים, אסור לייבא מודולים מיוחדים שמישהו אחר פיתח.
- ממשו פונקציה SendBySecureChannel(...) לשליחת קוד אימות בדרך רגילה(שליחה סתמית), אך הניחו שהיא בטוחה.
- הדפיסו את ההודעות אחרי קבלתן ואת הודעת קבלת האישור.
- הדפיסו את התוצאות של ביצוע כל פעולות האבטחה(יצירת המפתח, קבלת המפתח, יצירת אמצעי אימות, הודעה סופית שכוללת הכל).
- הפרויקט לא בתקשורת, לכן בשביל להקל, אפשר לממש בצורה מינימליסטית, לדוגמא: שליחת וקבלת הודעה/אישור לא יתרחשו באותו זמן, לא צריך לטפל בתקלות, כמו שרת לא פעיל.
- אפשר להניח הנחות נוספות ולבחור צורות נוחות כל עוד הן לא מצמצמות את משימות האבטחה. **את כולם צריך לפרט בהגשה**.

לדוגמא: כמה הודעות לשמור בשרת כשלקוח יעד לא מחובר? אפשר לצמצם ל 2 . מה לעשות אם שולחים יותר? שום דבר, פשוט לא לשלוח בהדגמת הרצה ולהניח שלא שולחים יותר.

- מימוש חלקי יזכה בניקוד חלקי, אך צריך לציין מה מומש ומה לא.
- הקליטו סרטון הסבר קצר עם הדגמת ההרצה והתייחסות לנקודות עיקריות. עם הסרטון גדול מדי(יותר מ 300MB)בשביל תיבת ההגשה, תעלו אותו לדרייב וצירפו את הקישור.

חלק 3 שאלה (5 נק'):

האם ניתן להבטיח זמינות AVAILABILITY ?
הסבירו איך ניתן או למה לא ניתן.

אופן הגשה:

החלק העיוני עדיף מוקלד ב WORD או PDF . במקרה הצורך בכתב ברור וקריא.
בזוגות, הגשה אחת עם ציון פרטי 2 המגישים.
מניסיון עדיף מאותו מנחה, אחרת יש עיקובים וטעויות בהזנת הציונים.

תאריך הגשה אחרון:

01/01/2025 23:59 . לא יינתנו דחיות חוץ מהמקרים החריגים ביותר.

מדיניות האיחורים:

על כל יום איחור הציון יורד ב 2 נק', 10 נק' לכל שבוע שלם של איחור.
כתוצאה מאיחור, הציון לא יורד מתחת ל 60.

בהצלחה!