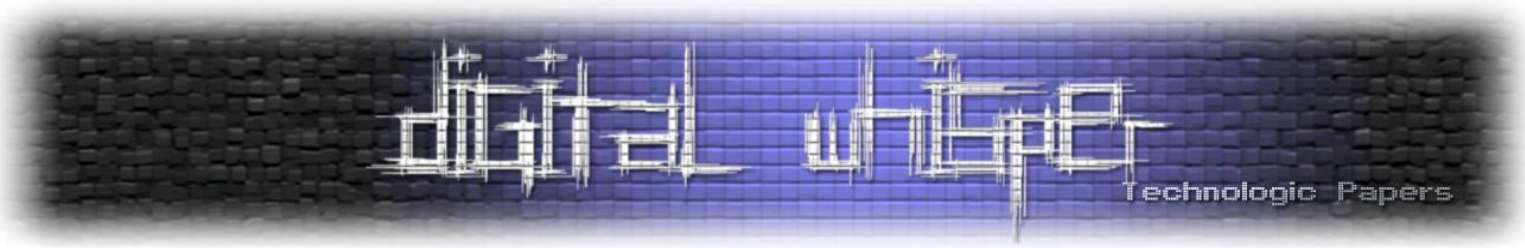


משפחת פרוטוקולי IPSec

מאת סולימני יגאל

משפחת הפרוטוקולים IPSEC אחראית על אבטחת התקשורת העוברת בין ציוד ברשת, מאמר זה יתמקד במכלול השירותים המסופקים בה. נבין מהו פרוטוקול להחלפת וניהול מפתחות מוצפנים, נכיר את מבנה הפרוטוקולים המרכיבים אותה ונסביר על אופן הגנתה מפני המתקפות השונות.

מדוע עלינו לאבטח את הרשת?

ישנן מספר רב של מתקפות המאיימות על הרשת הפנים אירגונית שלנו. ישנן מתקפות המגיעות מתוך הרשת (תוקף פנימי- יכול להיות עובד אירגון המנסה לקבל גישה למחשבו של עובד אחר לדוגמא) וישנן מתקפות המגיעות מחוץ לרשת. מספר רב של מתקפות נובע מחוסרים במנגנוני האבטחה הקיימים בפרוטוקולים אשר נמצאים בשימוש ברשת הפנימית. לדוגמא, מתקפת Arp Poisoning הופכת לכמעט לא רלוונטית כאשר המידע העובר ברשת מוצפן, ומתקפת Replay Attack אינה יכולה להתבצע על מערכות אשר עושות שימוש במנגנוני Timestamp. אלו רק דוגמאות אחדות למתקפות המאיימות על הרשת שלנו שאנו יכולים למנוע בעזרת השימוש בתקשורת מאובטחת. ולכך נועדה משפחת ה-IPSEC.

Internet Protocol Security (IPSec)

משפחת IPSEC מספקת שרותי אבטחה בשכבת ה-IP, היא מגדירה את האלגוריתם לשימוש המערכת, ומשתמשת ב-"מפתח" מוצפן כדי לספק תקשורת מאובטחת בין מחשבים או רשתות. הפרוטוקול יכול להתנהל בין זוג hosts, זוג secure gateways או בין host ו-secure gateway.

מכלול שרותי האבטחה ש-IPSEC מספק כוללים:

- בקרת גישה, הגבלת גישה לקבצים או מערכת.
- אימות נתונים במוצא.
- דחייה של מנות.
- שליחה חוזרת של מנות פגומות או לא רציפות שהתקבלו עקב בעיה או רעשים בקו.
- הצפנה.

כיוון ששרותים אלו ניתנים בשכבת ה-IP, פרוטוקולים בשכבות גבוהות יותר יכולים להיעזר בשרותים הללו. פרוטוקולים לדוגמא: TCP, UDP, ICMP, BGP וכו'.

יכולות אלו מאופשרות על ידי 2 פרוטוקולי אבטחת תעבורה הקיימים במשפחה זו: Authentication Header (AH) ו-Encapsulation Security Payload (ESP), ובאמצעות מפתחות מוצפנים ופרוצדורות ניהול.

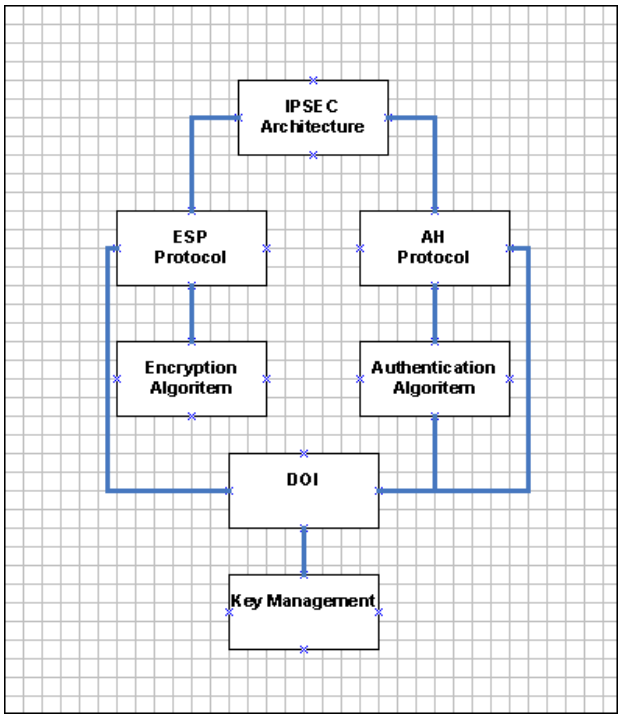
מכלול פרוטוקולי IPSec ואופן הגדרתם מתבצע על פי דרישת המערכת, המשתמשים או מנהלי האתר. מכלול הפרוטוקולים הסטנדרטי מתאים לכלל המשתמשים ברשת, אולם השימוש בפרוטוקולים אלו בתוספת IPSEC מאפשר את אבטחת התעבורה ברמה גבוהה ביותר.

פרוטוקולים להחלפת מפתחות

המטרה של פרוטוקולים להחלפת מתפחות היא הסכמה על מפתח משותף לשני המשתתפים. פרוטוקול כזה צריך לקיים את התכונות הבאות:

- **Authenticity**- אימות הזהות של המשתתף השני (מניעת התקפות Man in the Middle).
- **Secrecy**- רק שני המשתתפים המקוריים יודעים את המפתח הסודי המשותף.

מבנה הפרוטוקול:



IP Authentication Header (AH)

ה-AH הוא פרוטוקול מרכזי ב-IPSEC, אחראי על רציפות התקשורת, אימות הנתונים בתעבורת הרשת ומספק הגנה מתעבורה חוזרת (שידורים חוזרים שלא זקוקים להם), ניתן להגדיר את הפרוטוקול כפרוטוקול הראשי בשילוב עם IP Encapsulating Security Payload (ESP) שעליו נרחיב בהמשך.

פרוטוקול AH ניתן לשימוש בין תחנות ברשת, בין secure gateways. בגדול, הפרוטוקול AH מעניק את אותן יכולות האבטחה כמו ESP מלבד ההצפנה.

כשמשתמשים ב-IPv6 ה-"Authentication Header" מופיע בין "IPv6 Hop-by-Hop Header" לבין "IPv6 Destination Options", אך כשמשתמשים ב-IPv4 ה-"Authentication Head" מופיע ישירות אחרי ה-"IPv4 header" הראשי.

מבנה חבילה בפרוטוקול:

8 bits	16 bits	32 bits
Next Header	Payload Length	Reserved
Security parameters index (SPI)		
Sequence Number Field		
Authentication data (variable)		

- "Next header"- מגדיר את סוג השדה שלאחר ה-"Authentication Header".
- "Payload Length"- מציין את אורך ה-AH ב-32Bit.
- "SPI"- שדה מספרי בגודל- 32 Bit שבשקלול עם כתובת ה-IP של היעד וה-AH מגדיר את קוד ההתקשרות, ליתר דיוק את קוד השיחה. יכולות להיות מספר שיחות מאובטחות, השקלול הזה מגדיר מעין מספר סידורי של ההתקשרות.
- "Sequence Number"- מונה מסגרות- שדה שמכיל מספר רץ.
- "Authentication Data"- שדה ביקורת Integrity Check Value (ICV) הוא קוד לזיהוי שגיאות שמעניק את האפשרות לזהות את השגיאות ואפילו לתקנן, שדה זה הוא חשוב ביותר ומורכב מאוד לזיהוי שגיאות במידע, הוא מופעל כפונקציית בדיקה על המסגרת, 2 הצדדים מחליטים על פונקציה מסוימת מראש, ומצרפים חלק נוסף להודעה, שהיא בעצם התוצאה של הפונקציה שהופעלה על המסגרת , הצד המקבל צריך להפעיל את הפונקציה שהוסכמה מראש על ההודעה ולוודא שמתקבלת תוצאה זהה לחלק שצורף להודעה, אם היא לא זהה, המקבל מבין שנקלטה הודעה עם שגיאות ומבקשת שליחה מחדש.

IP Encapsulating Security Payload (ESP)

ה-ESP הוא פרוטוקול מרכזי בארכיטקטורת IPSec. הפרוטוקול מעניק שרותי אבטחה ב-IPv4 וב-IPv6, שירותי האבטחה כוללים הצפנה ושליחה רציפה ללא שגיאות (במקרה של שגיאה תתבצע שליחה חוזרת). המידע המוצפן מועבר בשדה Payload data.

פרוטוקול ESP מזוהה ע"י המספר 50, מספר זה ניתן לפרוטוקול על ידי IANA (Internet Assigned Numbers Authority) שהיא הרשות שהיתה אחראית על המדיניות של הקצאות מספרים לפרוטוקולים, לפורטים או למספרי IP, הרשות שאחראית על הנושא כיום היא ICANN (Internet Corporation of Assigned Names and Numbers)

מבנה חבילה בפרוטוקול:

16 bits	24 bits	32 bits
Security association identifier (SAID)		
Sequence Number		
Payload data (variable length)		
Padding (0-255 bytes)		
	Pad Length	Next Header
Authentication Data (variable)		

- "Security association identifier"- מספר הזיהוי של הפרוטוקול, כדי שהתחנה הקולטת תדע כיצד לפעול עם הקלט של המסגרת.
- "Payload Data"- שדה באורך משתנה המכיל את המידע.
- "Padding C"- שדה המכיל ריפוד עבור ההצפנה, 2 הצדדים מסכימים על גודל מסויים של סך ה-bytes במידע, את השאר מרפדים באפסים ואז מצפינים, לדוגמא: הסכמה על שדה בגודל 10bytes, אם נכנסים למסגרת רק 97 bytes, אזי מרפדים ב-3 אפסים ואז מצפינים. מנגנון זה מגביר את האבטחה על תעבורת המידע.
- "Pad length"- מציין את מספר ה-bytes בשדה הבא.
- "Next header"- מגדיר את סוג המידע שמכיל שדה ה-Payload Data.

Internet Security Association and Key Management Protocol (ISAKMP)

פרוטוקול מרכזי בארכיטקטורת IPSec, נוצר על ידי ה-NSA, מגדיר את התהליכים ואת עיצוב המסגרות, מעניק ערוץ מאומת ומאובטח המשמש להסכמה על מפתחות ומנהל את החלפת המפתחות המוצפנים.

פרוטוקול זה מכיל שני שלבים עיקריים:
שני הצדדים יוצרים ערוץ מוגן ומסכימים על נהלי השליחה, בשלב זה נוצר ה-SA בינהם.
יש קישור מאובטח בין שני הצדדים ומידע נשלח בהתאם לנהלים שנקבעו בשלב א.

מבנה חבילה בפרוטוקול:

8 bits	12 bits	16 bits	24 bits	32 bits
Initiator Cookie				
Responder Cookie				
Next Payload	MjVer	MnVer	Exchange Type	Flags
Message ID				
Length				

- "Initiator Cookie"- המחרוזת שעל השולח לשלוח כדי להזדהות בפני הצד המקבל.
- "Responder Cookie"- המחרוזת שנשלחת כדי לאשר הקמת או מחיקת SA.
- "Next Payload"- סוג השדה הבא בהודעה.
- "MjVer"- הגרסה הראשית של פרוטוקול ISAKMP שבשימוש כרגע.
- "MnVer"- הגרסה המשנית של פרוטוקול ISAKMP שבשימוש כרגע.
- "Exchange Type"- סוג החילוף שמתבצע כרגע.
- "Flags"- אפשרויות שונות שנקבעות לחילופי ISAKMP.
- "Message ID"- קוד הזיהוי למצב הפרוטוקול במהלך המעבר בין השלב הראשון לשני .
- "Length"- אורך ההודעה.

Internet Key Exchange (IKE)

ה-IKE הוא פרוטוקול לבניית וניהול IPSEC SA האחראי על החלפת המפתחות בין שני מחשבים שמשתמשים ב-IPSEC, פרוטוקול זה ממומש כאפליקציה העובדת מעל UDP בפורט 500.

ה-IKE משלב בתוכו שני פרוטוקולים ISAKMP ו-OAKLEY (פרוטוקול להסכמה על מפתחות ועל תכונות ה-IPSEC SA).

כאשר מחשב ברשת מבקש חיבור מאובטח, IKE מופעל על חבילות המידע רק בשלב הראשוני, כלומר לפני שהוסכם על SA ועד שיוסכם על SA.

ה-IKE מורכב משתי פאזות, הפאזה הראשונה מייצרת ערוץ מאובטח כדי להגן על הפאזה השנייה, במהלך הפאזה הראשונה, הצדדים מסכימים על ה-ISAKMP שיגן על הפאזה השנייה, על שיטות האימות והמפתחות, הכנת keying material סודי משותף לשני הצדדים-ורק להם שממנו יגזרו מפתחות ל-ISAKMP SA. הפאזה השנייה בונה את ה-SA עבור IPSEC.

יתרונות ה-IKE

- סודיות ואימות.
- חסינות לשידור חוזר.
- הגנה על זהות המשתתפים בשיחה.
- פרוטוקול פשוט לאנליזה ושימוש.
- עמיד בתקפות שונות (התחזות, Man in the middle, Denial of service).

חסרון ה-IKE

- מבצע חישובים יקרים (מפתח DH למשל, הוא חישוב יקר שדורש העלאות רבות בחזקה מודולו מספר ראשוני, דבר האורך זמן רב.)

הגנה מפני מתקפות שונות

השימוש במשפחת ה-IPSec מונע מהרשת שלנו להיות חשופה למספר גדול של מתקפות, בחלק זה של המאמר נסקור אותן ונסביר כיצד הדבר מתבצע.

הגנה מפני Denial of service Attack

התקפה זו מתבצעת על ידי תוקף שמבצע בדרך כלל IP spoofing, התוקף בעצם מציף את הקורבן בבקשות IKE ומכריח אותו לבצע חישובים יקרים, כדי למנוע את החישובים היקרים האלו, בזמן קבלת המידע יש צורך לוודא שהצד השולח נמצא בכתובת ה-IP שמופיעה ב-IP header .

הבעיה: התוקף יוזם הפעלות רבות של ה-IKE מול הנתקף בפרק זמן קצר, שמכריחות את הנתקף לבצע חישובים כבדים ויקרים, לאחר זמן מסוים הנתקף לא יוכל להפעיל IKE עם משתמשים אחרים והתוקף לא מבצע כלל את חישובי ה-DH.

בדרך כלל בהתקפות DoS בכל הפעלה של IKE התוקף ישתמש בכתובת מקור אחרת (IP Spoofing)

בדרך זו התוקף אינו חושף את עצמו, כיוון שהוא לא משתמש בכתובת ה IP שלו, לכן הנתקף אינו יכול להגן על עצמו על ידי הגבלת מספר ההתקשרויות המותרות בו זמנית מכתובת IP מסוימת.

הפתרון: שימוש מחרוזות Cookies.

כל משתמש בפרוטוקול שולח מחרוזת אקראית (Cookie) לצד השני, שנדרש להשיב את המחרוזת שקיבל כדי להוכיח שהוא אכן מקיים מהלך שיחה רציף, החישובים הכבדים והיקרים יתבצעו רק לאחר קבלת המחרוזת המקורית.

כך, נוכל לדעת **לפני שנבצע את החישובים היקרים** האם בקשות ה-IKE אכן רלוונטיות או לא.

הגנה מפני מתקפות MITM Attack כדוגמת Arp Poisoning

התקפה זו מתבצעת ע"י תוקף שהצליח לנווט את המידע היוצא מתחנה אחת לתחנה שניה- דרכו (לדוגמא- למידת טבלאות ה- Arp ועידכון ה-Physical Address של ה-Destination ל- Physical Address שלו עצמו), וכך יוכל לדלות מידע (כגון שמות משתמשים וסיסמהות) או לערוך מידע וכד'.

הבעיה: התוקף לומד את טבלאות ה-Arp ברשת, מעדכן אותם בפרטיו לתחנות ספציפיות וגורם למידע שנשלח מהן לעבור דרכו וכך יוכל לראות את תוכן חבילות המידע העוברות בתקשורת.

הפתרון: שימוש בהצפנה.

המידע העובר ברשת מוצפן בעזרת מנגנוני הצפנה מבוססי מפתח, במידה ותוקף יבצע מתקפת MITM בכדי לעיין במידע- התוקף לא יוכל לעשות עם המידע כלום מפני שהוא מוצפן.

הגנה מפני Replay Attack

התקפה זו מתבצעת ע"י תוקף המאזין לקשורת ברשת, ומתחקה לאחד המשתתפים בשיחה על-ידי שידור חוזר של המסגרות שלו, בכוונה שהצד השני יעביר את השידור אליו.

הבעיה:

התוקף מבצע מתקפת MITM לתחנות ברשת ומאזין לתקשורת ביניהם, במטרה לשלוף מסגרת מידע רלוונטית לזהותו של אחד הצדדים בשיחה במטרה לשלוח אותה לצד השני עם פרטיו בכוונה שהצד השני יעביר את השידור אליו.

הפתרון: שימוש במנגנון Timestamp.

כאשר כל צד משתמש במנגנון Timestamp בכדי לאמת את "טריות" המסגרת. יש לציין כי חתימת הזמן מוצפנת ביחד חבילת המידע כך שלא יהיה ניתן לזייפה. כך כל מסגרת שמתקבלת נבדקת ואם היא לא "טרייה" , אזי יש נסיון פריצה לרשת . חשוב לסנכרן בין כל הציוד ברשת , כדי שהשעון יהיה זהה.

סיכום

במאמר זה הצגנו את מבנה פרוטוקולי האבטחה והפרוטוקולים לניהול והחלפת מפתחות היוצרים את משפחת ה-IPSec, הבנו את חשיבות השימוש בתעבורה מוצפנת ברשת שלנו וסקרנו מספר מתקפות ואת אופן מניעתן בעזרת שימוש בפרוטוקולים אלו.