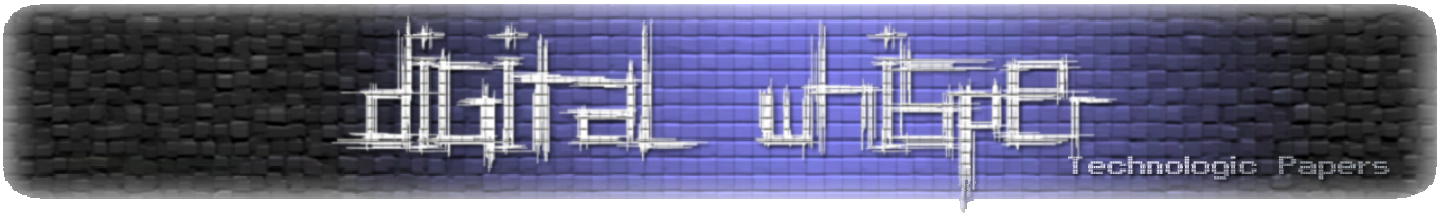

אבטחת SIP עם Asterisk

מאת עידו קנר

אבטחת מידע מעלה אצל לא מעט אנשים מחשבות אודות Buffer Overflow, Format String, XSS, SQL Injection ובעיות רבות הנוגעות למחשב ובעיקר לתוכנה, אך אבטחת המידע המודרנית של ימנו לא החלה עם הופעת המחשב האישי, אלא עם הגעת המכשור הטלפוני למרבית הבתים, שלא לדבר על הטכנולוגיה הסלולרית. חיובי חברות הטלפוניה עבור השימוש במכשירי הטלפון השונים הובילו אנשים לחיפוש ולייצור מערכות המזייפות את אמצעי התשלום (billing) ועוזרות להימנע מתשלום, או סתם להתלבש על שיחה קיימת (man in the middle) וניצולה לצורכי התוקף. התקפות אלו בוצעו על ידי קופסאות כחולות, שחורות ואדומות. בימים ההם פעלו אנשים כדוגמת Captain Crunch אשר התפרסם כחוקר אבטחת מידע, וייצר את הקופסה הכחולה הראשונה. עם מעבר עולם הטלפוניה לתקשורת דיגיטלית באופן כמעט מוחלט, הקופסאות הצבעוניות נמוגו מהעולם כמעט לגמרי, אך אנשים כדוגמת הקפטן עדיין מספקים לנו השראה בעולם אבטחת המידע, וכל חוקר אבטחת מידע (או סתם חובב) המכבד את עצמו מכיר אותו ואחרים מאותה התקופה.

במאמר זה אדון במרכזיית הטלפוניה Asterisk, מרכזיית תוכנה המשוחררת כקוד פתוח. המרכזייה עצמה שינתה את פני הטלפוניה בעולם בכלל ובישראל בפרט אך לדעתי נושא אבטחת המידע בתחום הטלפוניה אינו מקבל חשיפה ראויה.

מה היא מרכזיה ומה זו טלפוניה?

טלפוניה היא תחום רחב, עוד הרבה לפני שהמילה VoIP נכנסה לתמונה, לכן חשוב להבין ולהכיר כמה מונחים בתחום. טלפוניה היא תת נושא בתוך נושא הנקרא טלקומיוניקציה -היכולת לבצע תקשורת בצורה מרוחקת תוך שימוש באותות (signaling) שונים. אותות מוכרים הם: תופים, סימני עשן, סימני דגלים, מורס ועוד.

בהכללה גסה זהו כלי או מכשיר המאפשר להעביר קול בצורה מרוחקת באמצעות אותות וסימנים מוסכמים. כיום אלו סימנים שהם בעיקר דיגיטליים, כאשר בחומרה כדוגמת ISDN אנחנו נעביר את המידע של האותות על ערוץ המיועד לכך הנקרא d-channel בעוד שהמידע הקולי ו/או וויזואלי יעבור תחת ערוצי הקול ו/או הווידאו -b-channel. השימוש של ISDN נעשה על ידי "פרוטוקולים" המתארים את ספקי הטלפוניה, כאשר יש פרוטוקול בשם E1 (בארץ ובאירופה, T1 ארה"ב ו-J1 במזרח הרחוק).

מונח חשוב נוסף הוא מרכזייה, אשר כשמה כן היא: מכשיר המרכז אליה דבר מה. כאשר מדברים על מרכזיית טלפון, מתכוונים לכלי אשר מרכז בתוכו את כל התקשורת הקשורה לטלפוניה ומחליט על ניתובה ליעד. בהקשר של Asterisk מדובר במרכזייה פרטית לעסק או ארגון (בניגוד למרכזייה של ספק טלפוניה. מרכזיית טלפון כזו נקראת Private Branch Exchange או PBX בקיצור.

צורת טלפוניה נפוצה כיום נקראת Voice Over IP או VoIP בקיצור. כמו כן קיים מונח מקביל בשם VoB או VOBB אשר מדבר על Voice Over Broadband או Video Over Broadband המאפשרים בעצם לתקשר בקול ובווידאו דרך רשת האינטרנט בפס רחב. 2 אמצעים אלו, שהם למעשה אותו הדבר ממומשים דרך תוכנה ודורשים תקשורת בפרוטוקולים שונים המבוססים בדרך כלל על udp.

Asterisk על קצה המזלג:

Asterisk הנה מרכזיית טלפוניה פרטית לעסק המשוחררת בקוד פתוח ונוצרה על ידי אדם בשם מארק ספנסר מחברת Digium שבבעלותו. Asterisk רצה בתור שרת במערכות ההפעלה לינוקס ויוניקס בעיקר, אך ניתנת להרצה כיום גם תחת MS Windows.

המרכזייה תומכת ב:

- טלפוניה פשוטה (POTS) או תקשורת עם מרכזיות ציבוריות, שבארצנו נקראת גם קו בזק
- תמיכה בתקשורת PRI ו-BRI
- תקשורת VoIP הכוללת בתוכה גם תמיכה בווידאו, בפרו\טוקולים שונים כדוגמת SIP, IAX2, H232, Jabber, Skype ואחרים
- מיפוי מפר מול אדם בין מערכות כדוגמת DUNDI ו-ENUM עבוד ניוד מספרים
- תמיכה בתוספים שונים כולל צד שלישי

את המרכזיה ניתן לתכנת באופן מלא בין אם עבור שיחה נכנסת, שיחה יוצאת, שיחה בתוך המרכזיה או מעקב אחר משתמשים שונים במערכת. המרכזיה עצמה, כאמור, היא שרת תוכנה לכל דבר ועניין אשר מאזין לפרוטוקולי VoIP, מספקת API שחלקו תחת תקשורת TCP לתכנות והאזנה למרכזייה עצמה כדוגמת FastAGI אשר מתממשקת לשפת תכנות חיצונית באמצעות TCP או Manager אשר מספק יכולות לדעת ולשלוט מה קורה במרכזייה עצמה, על ידי שימוש בכמה פרוטוקולים כדוגמת HTTP, פרוטוקול פנימי שלו, ועוד כמה צורות עבודה כדוגמת צינורות (pipe) לקלט ופלט. בנוסף המרכזייה יודעת לדבר עם מסדי נתונים שונים כדוגמת MySQL, SQLite, ODBC ו-Berkly DB.

Asterisk תלויה במודולי קרנל אשר מאפשרים לשרת לדבר עם כרטיסי טלפוניה שונים כדוגמת ISDN, כרטיסי טלפוניה פשוטה, כרטיסים שאליהם מתחברים הטלפונים עצמם, או חומרה נלווית המתחברת

בדרך כלל דרך USB אל השרתים. ניתן להבין כי אבטחת Asterisk כוללת הרבה מאוד אלמנטים וגישות. בנוסף לכך כל בעיה רגילה שיכולה להיות לשרת, אפשרית ואף לפעמים מתרחשת במרכזיה עצמה. היתרון העיקרי של Asterisk נעוץ בכך שהמרכזיה משוחררת בקוד פתוח ולכן ההתנהלות בבעיות האבטחה מתבצע בד"כ בצורת Full Disclosure בעת שחרור התיקון.

אבטחת המידע ב-Asterisk

בטלפוניה קיימות כיום מספר בעיות מרכזיות הנוגעות לתחום אבטחת מידע:

- גניבת שיחות על ידי שירות "עקוב אחרי"-לאחר חיוג ליעד מופעל קוד המפנה את הקו להיות קו שממנו יבוצעו שיחות יוצאות ומאפשר גניבת שיחות.
- השתלטות על שרתי VoIP-שרתים שאינם מאובטחים כהלכה נפרצים וכך התוקפים יכולים להוציא שיחות ללא עלות מצדם.
- התחזות-האדם שמעבר לקו מאמץ זהות שאינה שלו, בארץ לא ניתן לעשות שזאת למעט בשיחות שאינן מזוהות אלא אם מדובר ב-VoIP נקי. סוג זה של הונאה מאפשר לתוקפים להזדהות כבנקאים בבנק שלכם או כבעלי סמכות כלשהי ולקבל מידע שהוא פרטי.
- האזנות והקלטות שאינן חוקיות, בהן נוכחות המבצע אינה מורגשת (על ידי תפיסה של קו VoIP או גישה פיזית לאחד מצדי השיחה)
- חייגני מלחמה-צורת התקשרות אוטומטית לרוב שמטרידה אנשים ומסייעת בגניבת מידע, התקפות אלו דומות להתקפות עקוב אחריי אך ללא מענה אנושי. צורה זו נפוצה להפצת ספאם טלפוני.
- שידור מידע על Early media (חוסר יכולת לגבות כסף על השיחה). הגופים היחידים בארץ שמורשים לשדר ב-Early Media (המוכרים לי) הם ספקי הטלפוניה שמשמיעים מוזיקה מעל צליל החיוג, או שירות 144 אשר מתבצע מעל מהלך זה.

עוד מידע בנושא אפשר למצוא ב-Wikipedia במאמר בנושא אבטחת טלפוניה.

אבטחת VoIP

לא ניתן להתייחס באופן כללי ל-VoIP כאשר מדובר באבטחת מידע, היות וכל פרוטוקול וצורת עבודה דורשים התייחסות שונה לגמרי מהאנשים האמונים על התשתיות ואבטחת המידע. בעוד שחשוב להבין כי ישנם פרוטוקולים רבים (חלקם בשימוש נרחב יותר מאחרים וחלקם פחות) יש לזכור כי אי אפשר להתייחס במאמר אחד לכולם, לכן נסתפק לעת עתה בפרוטוקול בשם SIP הנפוץ מאוד בעולם התקשורת.

היכרות עם SIP

ראשי התיבות SIP הינם Session Initiation Protocol, שם המרמז בעצם על פעולת הפרוטוקול: יצירת סשן המאפשר לנהל תקשורת בין צדדים שונים. הכוונה ביצירת סשן מזכירה לנו מאוד את פעולת ה-SYN בתקשורת TCP, שבסופו של דבר אחראית על תקשורת בין הצדדים להעברת פקטות ה-TPC. רבים מתייחסים, שלא בצדק, אל SIP כאל מנהרה. בתוך SIP לא עובר מידע נוסף, כדוגמת מנהרת SSL, הפרוטוקול אחראי רק על יצירת הקשר ודואג שהמידע יגיע מנקודת ההתחלה לנקודת הסיום. אפשר להגדיר את SIP כגשר יותר מאשר מנהרה. פרוטוקול ה-SIP נחשב לאחד הפרוטוקולים המסובכים ביותר שיש ומכיל מספר RFC שמוסיפים אחד לשני עוד מידע והסברים. לפי אחד מאותם RFC, פרוטוקול התקשורת ש-SIP יכול להשתמש בו הוא UDP אבל גם ניתן לממש אותו מעל TCP (פחות נפוץ תאורטית). לאחר ש-SIP נמתח מנקודת התחלה לסיום, מתחילים פרוטוקולים אחרים להכנס לשימוש. הפרוטוקול המוכר כמעט לכל אדם המשתמש ב-SIP הוא ה-RTP, שתפקידו להעביר את שיטות הקול והווידאו (codec) של השיחה עצמה. בנוסף ישנו פרוטוקול חשוב בשם SDP שתפקידו לתאם את סוג המדיה שתעבור בין הצד המבקש ליעד הסופי. בנוסף לפרוטוקולים אלו, ישנם עוד פרוטוקולים שונים אשר עוברים, חלקם אינם נדרשים, אך מוסיפים תכונות כדוגמת MSRP אשר מספק יכולת משלוח טקסט ולגרום ל-SIP לשמש גם כסוג של פרוטוקול Instat Messages.

אופן השימוש ב-SIP

השימוש ב SIP יכול להתבצע ב-3 צורות עיקריות:

1. שרת אל לקוחות
2. שרת אל שרת
3. קישור מחשב לרשת טלפוניה אחרת, קווית לרוב

כאשר מדובר על **שרת מול לקוחות**, הכוונה היא שיש שרת המדבר ב-SIP ויש לקוחות שונים (טלפונים שהם חומרה -> hard phone, טלפונים שהם תוכנה -> soft phone ו-Instant Messages).

בשרת אל שרת, אנחנו משתמשים ב-SIP כ-Proxy בין נקודות, אשר בעצם עוזר להעביר שיחות משרת אחד למשנהו. פעולה זו נקראת SIP Proxy ניתן למצוא על זה מידע ב-RFC מספר 3261. בקישור לרשת טלפוניה אחרת ניתקל בשם SIP Trunk, בו אנחנו מדברים ב-SIP בצד הלקוח ומתחברים לשרת, שהיציאה שלו היא בדרך כלל לתקשורת קווית.

בעיות הקיימות עם SIP

ל-SIP יש מספר בעיות מורכבות שיש לתת עליהן את הדעת לפני שניתן בכלל לדון בהגנה על הפרוטוקולים השונים.

- הבעיה הראשונה והחשובה ביותר היא בכך שהפרוטוקול דורש טווח של 10,000 פורטים פתוחים. בעוד ש-SIP עצמו דורש רק פורט אחד, 5060, שאר הפרוטוקולים דורשים את הטווח העצום הזה של הפורטים. זה לא הכל, היות ופרוטוקולים כדוגמת RTP ו-SDP בוחרים בצורה רנדומלית פורט אחד מתוך הטווח, אי אפשר לדעת מה יבחר מראש. בנוסף, Asterisk למשל, אינו מאפשר להגביל את הטווח הזה, למרות שיש מספר שרתים ולקוחות המאפשרים להגבילו.

בעיית הפורטים יוצרת מצב בו מאוד לא פשוט לעבוד עם NAT ובד"כ במקרה של מחסור בכלי הגנה שיודעים לעבוד עם SIP יש לבטל צורות הגנה כלליות כדי לאפשר את הטווח.

- הואיל ומדובר בפרוטוקול טקסט נקי ונדרשת הזדהות, הסמאות גלויות לכל, גם אם משתמשים ב-Digest להצפנתן.
- בטלפוניה בכלל וב-SIP בפרט יש רגישות יתר להתקפת man in the middle. במקרה של SIP קל מאוד לגנוב מאחד הצדדים את התקשורת, להאזין לשיחה או סתם לזהות את הצדדים המעורבים בה. כל מה שצריך זה לשתול עוד שורה בתחילת השיחה של Contact בשביל לשנות את הכתובת לכתובת החדשה והתקשורת הועברה לכתובת אחרת.
- SIP מאוד פגיע להתקפות DoS בכל נקודה ברשת, ואפילו שינוי ברוחב הפס לרעת ה-SIP יכולים להיחשב ככזו.
- ניתן להתערב ל-SIP באלגוריתמים, בפרוטוקולים והראשים השונים, דבר שיכול לגרור לבעיות אבטחה שלא תמיד ניתנות לחיזוי מראש.

עבודה בטוחה עם SIP

כדי להעביר בצורה בטוחה את כל הפורטים השונים, ניתן כאמור להשתמש בציוד היודע לעבוד עם SIP, אך מדובר בדרך כלל בציוד יקר מאוד. לכן ניתן לעבוד עם מנהרה בשם stun המאפשרת להעביר את כל פרוטוקולי התקשורת כדוגמת RTP ו-SDP תחת אותה מנהרה. המנהרה עובדת ב-UDP ומאפשרת לעבור NAT. קל יותר לאפשר פורט בודד מאשר טווח של 10,000 פורטים.

בנוסף, יש לזכור שיש בעולם גם את IPv6, אשר תאורטית מעלים את הצורך ב-NAT היות ואין הבדל בין כתובות פנימיות וחיצוניות, דבר שמשנה את כל הגישה לכמות הפורטים שצריך להעביר "פרטית" לרשת "חיצונית".

בעבר היה שימוש בשיטת הזיהוי של PGP בה לכל צד יש מפתח ציבורי ומפתח פרטי ובהתאם למפתח הציבורי של הצד השני כפול המפתח הפרטי של הצד המדבר היה זיהוי חד ערכי בין כל צד- דבר שניסה למנוע Man in the middle, אך שיטה זו נגנזה מחוסר הגדרה ברור בתקן.

RTP ו-פרוטוקול בשם RTCP (עוד פרוטוקול בשימוש SIP) מכילים הגנות שונות:

- פרוטוקול בשם ZRTP שנועד לבצע את אימות התעודות במצב ה-RTP ובכך כאמור לעזור במניעת Man In the Middle.
- יש פרוטוקול הצפנה בשם SRTP שביחד עם אחיו SRTCP מאפשרים לקודד תקשורת קולית וויזואלית.

שיטות הגנה אלו דורשות ששני הצדדים יתמכו בשיטות העבודה האלו, לצערי ישנם לא מעט לקוחות SIP אשר אינם תומכים בהן.

כאשר מדובר בארגון מסודר ישנן הגנות נוספות

הגנות ברשת מקומית: ברשת הפנימית בארגון מומלץ בראש ובראשונה ליצור באמצעות VLAN רשת המיועדת לתחום ה-SIP ושום דבר אחר אינו מאושר להשתמש בה. היתרון של VLAN הוא בכך שהוא לוקח רשת ומחלק אותה בצורה ווירטואלית לרשת חדשה, פעולה שמפרידה בעצם את התקשורת בין הרשת במשרד המיועדת למידע כללי לבין רשת המיועדת רק ל-SIP. פעולה זו גם מאפשרת ליצור מסננים שונים עבור פעולות שונות כדוגמת Quality Of Service (מוכר בשם QoS) אשר יכול לספק תעדוף בתקשורת עבור תעבורת SIP. ניתן לאפשר רק לכתובות IP עם כתובות MAC ספציפיות. באותה רשת תקשורת הווירטואלית יתחברו רק הלקוחות SIP בעוד שכל סוג תעבורה אחר לא יחובר אליו.

כל הזדהות תתבצע באמצעות Message Digest אשר מצפין סמאות (אבל עדיין מאפשר הזדהות עם ההצפנה עצמה גם למי שרק "מאזין" לתקשורת) בצורה שאי אפשר לשחזר, ובנוסף גם ההזדהות יכולה להיות מבוססת כתובת IP ספציפית וכך כל ניסיון ניתוב מחודש של בקשת SIP לא תעבור הלאה גם אם מדובר בלקוח בתוך הרשת הייעודית.

במידה ובארגונים שונים יש גם כמה אתרים שונים שאינם יכולים להתחבר ל-VLAN אחד בצורה מאובטחת, ניתן לעבוד עם VPN מאובטח, אשר משם אפשר להכניס את 2 הרשתות לתוך VLAN בצורה מאובטחת יותר.

הגנות ברשת האינטרנט: במידה ואי אפשר לדבר ב-VPN מאובטח, יש להבטיח שרק כתובות IP מוגדרות יוכלו לדבר עם שרת ה-SIP, בנוסף להצפנות שהוזכרו למעלה. כמו כן, אפשר להגדיר לשרתים שונים (בד"כ באמצעות כלים כמו OpenSips להתעלם מבקשות Contact אשר מבקשות שכל מענה יתבצע בכתובת שונה.

כמו בכל שרת, החשיפה לאינטרנט צריכה להיות מינימלית ביותר, ומוגבלת לחיונית ביותר. כמו כן, צריך לזכור להוריד הרשאות למינימום ההכרחי לכל תהליך שרץ, כך שגם אם יש בעיית אבטחה, סביר להניח שהיא לא תספק אפשרות להסלמת הרשאות.

סיכום

עולם הטלפוניה גרם לכך שעידן המידע המודרני היה צריך לתת מענה לאבטחת מידע הרבה לפני התפתחות המחשוב האישי ונגישות המידע שקיימת כיום. הכרנו בעולם הטלפוניה את מרכזיית Asterisk המשוחררת בקוד פתוח ומספקת תמיכה בהרבה מאוד יכולות. באמצעות Asterisk גילינו כי עולם הטלפוניה מכיל המון תתי נושאים על גבי תתי נושאים, וכל אחד מהם מהווה בעיית אבטחת מידע משל עצמה שצריך לתת עליה את הדעת.

תחום ה-VoIP הוא מאוד כללי וצריך לרדת לרמת הפרוטוקולים שבשימוש על מנת לדעת איך לאבטח את הנושא. ראינו כי פרוטוקול ה-SIP מורכב מאוד ודורש התייחסות נקודתית, והבנו חלק קטן מהבעיות שקיימות בשבילו.

כדי לדעת עוד על אבטחת פרוטוקול SIP מומלץ מאוד לקרוא את ה-RFC המטפל בנושא ולהבין שגם הוא לא מספיק בשביל לספק את מלוא ההגנה הנדרשת. הכי חשוב לזכור כי באבטחת מידע, הצרכים הם אלו שמכתיבים את צורת ההגנות ולכן לא באמת ניתן לכתוב מאמר שיכסה את כל האפשרויות לאבטחת פרוטוקולים כדוגמת SIP.