

זיהוי ערוצי שידור מידע מקביליים בשיחות וידאו באמצעות למידת מכונה

אופיר יוסף

תקציר

תקיפת ערוצי תקשורת באמצעות התחזות היא מתודה בה נעשה שימוש כדי לעקוף מדיניות אבטחה ולאפשר שידור חשאי של מידע לנקודת האזנה נגישה או לחלופין לאפשר התפשטות של תוקף לרכיבים שונים ברשת.

מערכות תקשורת מבוססות טכנולוגיית VoIP (Voice over IP) או מערכות וידאו-אודיו חשופות לתקיפה במגוון שכבות הטכנולוגיה הנדרשות בכדי ליישם את הפונקציונאליות שלהן. בין שכבות אלו, בין היתר, ממומש פרוטוקול זמן-אמת או RTP (Real Time Protocol), פרוטוקול תקשורת זה עושה שימוש בפרוטוקולי תקשורת נוספים כגון TCP (Transmission Control Protocol) או UDP (User Datagram Protocol). התוקף יכול לעשות שימוש בערוצים אלו בכדי לפרוץ "חור" בהגנה על עמדות הקצה דרך מנגנון ההגנה שאותו מספק שירות ה-NAT (Network Address Translation), לאחר פריצה של חור בהגנה תתאפשר לתוקף גישה רשתית לעמדת הקצה ויצירה של ערוץ תקשורת מולו מנקודה אחרת ברשת, ערוץ זה יוכל לשמש למטרת זלג מידע או כערוץ התפשטות רשתית.

עבודה זו מציגה גישה חדשנית לתקיפה של מערכות VoIP, התקיפה מאפשרת מימוש של ערוצי זלג מידע והתפשטות תוקף במרחב רשתית של ארגון סגור או בין מרחבים רשתיים של ארגונים שונים העושים שימוש בתשתית ציבורית. התקיפה עושה שימוש בערוצי תקשורת חשאיים המבוססים על חיקוי של ערוץ ה-RTP המקורי. המתקפות המתוארות בעבודה זו מבוססות על יצירה של פריצה הגנתית באמצעות "התעלקות" על ערוץ UDP קיים וחוקי שנוצר ע"י אפליקציית Skype, המקימה ערוץ וידאו peer-to-peer. שיטות התקיפה שהודגמו במסגרת העבודה הצליחו להעביר קובץ טקסט קטן בין שני ארגונים שונים המוגנים ע"י NAT, ללא יצירה של הפרעה או פגיעה באיכות התקשורת בשיחה בצורה נראית לעין.

זיהוי מתקפה זו באחוז וודאות גבוהה היא משימה לא אפשרית באמצעות בחינה אנושית של נתוני התקשורת, כמו-כן במסגרת העבודה אנו מראים שמימוש אלגוריתמיקה קלאסית של למידת מכונה מאפשר זיהוי אפקטיבי של ערוצי תקשורת חשאיים אלו על בסיס נתונים סטטיסטיים שנדגמו מערוץ התקשורת.

הממצאים והתוצאות שהוצגו בתזה זו פורסמו במגזין Electronics והדגישו את חשיבותם וההשפעה של המחקר.

מספר מערכת: 9926933509905776