האם קוד פתוח פחות בטוח?

מאת אורי עידן

הקוד הפתוח תופס תאוצה וכיום די קשה לדמיין את עולם האינטרנט , ובכלל את עולם התוכנה, ללא קוד פתוח. הקוד הפתוח מהווה איום לא קטן על המודל העסקי המיושן של מכירת רשיונות שימוש, אך חשוב מאוד לציין כי על אף המודל העסקי הלא הגיוני של הקוד הסגור, חברות רבות ואנשים רבים עדיין תומכים במודל זה. אותם תומכים מחפשים כל דרך להכפיש את שמו של הקוד הפתוח.

הסברים נוספים על חוסר ההיגיון במודל הקוד הסגור ניתן למצוא בבלוג הישן שלי:
http://www.oriidan.info/article/thoughts

(מומלץ לשים לב בעיקר למאמר השביעי), במאמר זה לא נרחיב על כך.

יש החושבים שקוד פתוח פחות בטוח , מאחר וכל אחד יכול לראות כיצד כתובה התוכנה , וכך קראקרים יכולים לבנות תכנות פריצה או לכתוב וירוסים ביתר קלות. אך לעומת זאת, המציאות שלנו מוכיחה בדיוק להפך, יישומי קוד פתוח פחות פריצים מיישומי קוד סגור. למתנגדי הקוד הפתוח יש נימוק גם לזה - הקוד הפתוח נפוץ פחות ולכן פחות מנסים לפרוץ אותו . (אישית, אני מעדיף להשתמש במונח "קראקר" לאדם המנסה לפרוץ ולהזיק. המונח האקר שמשום מה הפך למקובל בעיתונות בעצם מדבר על אדם שאוהב משהו ולא בהכרח אדם רע המנסה לפרוץ . גם אני -במובן מסוים- האקר, אם כי מעולם לא ניסיתי לפרוץ למערכת כלשהיא).

במאמר זה אני אנסה לתקוף את שתי הדעות הללו ולהסביר מדוע , למרות שלכאורה ניתן לנתח את קוד המקור על מנת לפרוץ את אותם היישומים המופצים כקוד פתוח, במציאות יישומים אלה נפרצים פחות. כמו כן אוכיח שהמיתוס שקוד פתוח אינו נפרץ מאחר שהוא נפוץ פחות, לחלוטין אינו נכון. מאחר שנושאי אבטחת מידע ובטיחות יישומי תוכנה הפכו להיות נושאים חיוניים מאוד ובעלי חשיבות עליונה, מן הסתם שנושא זה יהיה במרכז הדיון, ומשום כך, מתנגדי הקוד הפתוח הפיצו כל מיני מיתוסים לגבי בטיחותם של יישומי קוד פתוח. במאמר זה אנסה גם להתמודד עם חלק ממיתוסים אלו.

אקדים ואומר כי איני איש אבטחת מידע , אך יחד עם זאת יש לי ניסיון של למעלה מעשרים וחמש שנה בתכנות, והיכרות של כעשרים שנה עם עולם האינטרנט- כך שיש לי פרספקטיבה די נרחבת על כל עולם המחשבים והאינטרנט. אני מסתמך על הניסיון שלי , ועל מספר מאמרים בנושא , שחלקם די ישנים, אבל לדעתי עדיין רלוונטיים. המאמר העיקרי הופיע ב-theregister:

http://www.theregister.co.uk/2004/10/22/security_report_windows_vs_linux

לדעתי, מרבית המיתוסים על קוד פתוח הופצו על ידי מתנגדי הקוד הפתוח היות ולרוב העובדות מוכיחות את ההיפך. ניתן מספר דוגמאות: ניסו לבדוק מה הזמן הממוצע שלוקח למכונת חלונות המחוברת לרשת

להדבק בוירוס או נוזקה כלשהיא. התוצאה הייתה בערך 16 דקות, לי זה נראה קצת נמוך מדי, אבל גם אם הזמן היה גדול יותר, עדיין היה מדובר בנתון מפחיד.

למערכת חלונות יש משום מה קבוצה גדולה של תומכים שמוכנים להישבע שהיא המערכת הטובה ביותר והבטוחה ביותר. הנימוק שלהם לגבי הזמן הקצר שלוקח למכונת חלונות להפרץ הוא בדרך כלל המיתוס השני- שלינוקס, או מערכות הפעלה אחרות (שאגב, רובן מבוססות על יוניקס, בצורה זו או אחרת) אינן נפוצות ולכן אין לאנשים אינטרס לפרוץ אותן. אמירה שכזו נובעת מהסתכלות צרה על עולם המחשוב ומיד אסביר מדוע. זה נכון שבתחום המחשבים השולחניים, מערכות ההפעלה ממשפחת "Windows" תופסת נתח של בערך 90% מהשוק, אבל האם המחשבים השולחניים הם כל המחשבים בעולם?

היום מחשב נמצא כמעט ב כל מקום, אפילו בתוך הראוטר יש לכם מחשב שבמקרים רבים מריץ לינוקס. גם טלפונים סלולריים כיום הם בעצם מחשב, ויותר ויותר מהם מריצים הפצה כלשהיא של לינוקס, או במקרה של iPhone, שאמנם מריץ מערכת קניינית לחלוטין עם רשיון שימוש דרקוני, אך אסור לשכוח כי מדובר במערכת המבוססת על מערכת ה-BSD שהוא יוניקס חופשי. כך יוצא, שבעצם רב האנשים בעולם משתמשים בצורה זו או אחרת בלינוקס או במערכת הפעלה אחרת המבוססת קוד פתוח. אז האם לינוקס או מערכות קוד פתוח לא נפוצות?

כל זה, עוד מבלי שהזכרנו בכלל את שרתי האינטרנט. כיום, לפי NetCraft, מרבית השרתים מריצים גרסה זו או אחרת של יוניקס או לינוקס, כאשר גם מערכות היוניקס המקובלות הן בעצם גרסה כדוגמת FreeBSD. מבחינת שרתי ווב, למעלה מחמישים אחוז מהשרתים מריצים אפאצ'י - כמובן שרת בקוד פתוח. אני מניח שרבים יסכימו איתי שיש יותר אינטרס לפרוץ לשרת מאשר למחשב שולחני.

לאחר שהבנו שמערכות קוד פתוח לא רק שנפוצות כנראה יותר מאשר חלונות, אלא שיש את האינטרס הגדול ביותר לפרוץ אותן, נעבור למיתוס הראשון- קל יותר לפרוץ למערכות קוד פתוח מאחר והקוד גלוי. בניגוד למיתוס השגוי שאין אינטרס לפרוץ למערכות קוד פתוח, כאן יש הגיון כלשהו.

נתחיל קודם כל מהעובדות בשטח- שוב אפאצ'י, כידוע שרת האינטרנט הנפוץ בעולם, וגם תוכנת קוד פתוח. יחד עם זאת, אפאצ'י נחשב לשרת האינטרנט הבטוח ביותר. כאן אפשר לקחת כדוגמה גם את דפדפן האינטרנט: "אינטרנט אקספלורר" על גרסאותיו השונות לעומת דפדפן פיירפוקס. אקספלורר כידוע הוא קוד סגור, ופיירפוקס קוד פתוח, אך יחד עם זאת פיירפוקס נחשב לבטוח יותר.

אז כיצד נסביר כי למרות שלכאורה במיתוס זה כן יש הגיון מסויים עדיין המציאות הפוכה? לפי דעתי, יש שגיאה בסיסית במיתוס. נכון שהקוד פתוח ונכון, שאפשר למצוא את הדרך אל המערכת מעיון בקוד, אבל אם אפשר למצוא את הדרך לפרוץ - אפשר גם למצוא את הדרך להגן! כמו בכל דבר, אפשר להסתכל על חצי הכוס הריקה (למצוא את הפרצות) או להסתכל על חצי הכוס המלאה (לתקן את הפרצות).

כאשר מדברים על מערכות הפעלה, ולא רק על תוכנות ספציפיות, שוב נוכל למצוא שלינוקס בטוחה יותר מחלונות, ושוב בניגוד להגיון שאומר שבלינוקס הכל פתוח ולכן יהיה קל יותר לפורצים למצוא דרך. כאן ניתן למצוא התעלמות מעובדה נוספת ומעניינת- מגוון התוכנות לביצוע כל משימה בלינוקס גדול בהרבה. אם ב-Windows מקובל שלרוב משתמשים בדפדפן אחד ובתוכנת ניהול דוא"ל אחת (לשמחתנו הרבה

מגמה זו משתנה בשנים האחרונות), בעולם הלינוקס המצב שונה לחלוטין ברב המקרים. ישנם מספר דפדפנים מקובלים ומספר לקוחות דואר, כאשר כל משתמש יכול לבחור במה הוא מעדיף להשתמש. אותו הדבר נוגע גם לשולחנות העבודה, יש מספר תוכנות שולחן עבודה שניתן לבחור מביניהן , כך שהמגוון הגדול ללא ספק מקשה על הפריצה.

העובדה שיותר אנשים רואים את הקוד אומרת גם שיותר אנשים יכולים לשנות ולתקן אותו, וזו הסיבה שקצב השינויים והגרסאות החדשות בקוד פתוח גדול בהרבה מקצב השינויים של תוכנת קוד סגור. כאשר קצב שחרור הגרסאות מהיר יותר , גם הפורצים צריכים לעמוד בקצב , וזה לא קל בכלל . במקרים רבים קורה שמופיעה ברשת הודעה על פרצת אבטחה בתוכנה ועוד לפני שמופץ קובץ העושה שימוש בפרצה זו, מופיע תיקון לפרצת האבטחה.

עוד נקודה שרבים די נוטים לשכוח היא שאמנם הקוד פתוח, אך להבין את הקוד של תוכנות מורכבות כמו דפדפן פיירפוקס, שרת אפאצ'י או כל תוכנה אחרת זו משימה לא קלה בכלל. לצורך העניין, יתכן ויותר קל להשתמש בשיטות הפריצה המקובלות בתוכנות הקוד הסגור. אם תוקף שלא מכיר את הקוד ילך ויחפש משהו בקוד, כנראה שייקח לו יותר זמן ממה שייקח למי שכן מכיר את הקוד לתקן את פרצות האבטחה הקיימות.

לאחר שסקרנו מדוע שתי הטענות העיקריות אינן נכונות ננסה עתה להבין מדוע קוד סגור פחות בטוח . בקוד סגור, מעט מאד אנשים יראו את הקוד כך שיותר קל להסתיר בעיות ("security by obscurity"). לעומת זאת, תוכנות קוד פתוח, נכתבות על ידי מתכנתים אשר מוכנים לחשוף את הקוד שלהם לעין כל , ומאחר שהם אכן מוכנים לחשוף את כל "קלפיהם" על השולחן, סביר להניח כי הם ינסו לכתוב את הקוד הטוב ביותר שיוכלו.

נקודה חשובה נוספת נוגעת לגבי מי שבעצם יכול לתקן בעיות בקוד סגור- במידה וקיימת בעיה ישנם מעט מאד מתכנתים שיוכלו לתקן אותה, ולפעמים אפילו רק אחד. בתוכנות קוד פתוח, המספר הפוטנציאלי של מתכנתים הוא בעצם אינסופי, בניגוד למספר הדי מוגבל של הקוד הסגור. כאשר מתגלה באג בתוכנת קוד סגור כלשהיא, סביר להניח כי מי שכתב אותה עסוק כרגע בכתיבת הגרסה הבאה או בכתיבת תוכנה אחרת, כך שאם הוא יתפנה לתיקון הבאג , משמעות הדבר עיכוב בתוכנה אחרת שמהווה את ההכנסות העתידיות של אותה חברה... נתונים אלו מרמזים על כך שלחברת תוכנה קניינית כנראה שלא כל כך יהיה אינטרס לתקן באגים.

מדוע בקוד פתוח זה לא יקרה? כי לא רק אדם אחד יכול לתקן את הבעיות אלא הרבה יותר, כך שגם אם המתכנת המקורי עסוק בכתיבת הגרסה הבאה, עדיין יש מתכנתים אחרים, גם מחוץ לחברה שיוכלו לתקן את הבאג.

על המחבר

אורי עידן הוא סופר ויועץ תוכנה חופשית. עוסק בתכנות למעלה מעשרים וחמש שנה. כיום מתפרנס מתוכנה חופשית בלבד. בנוסף לכך, נותן הרצאות בנושא תוכנה חופשית והפילוסופיה מאחורי התוכנה החופשית.