10 דצמבר, 2016

מדריך להנדסת מערכות מכוונת חסינות

מאמר לכנס אינקוזי 2017

אבי הראל, ד"ר אביגדור זוננשיין

מאמר זה מציג את המדריך להנדסת מערכות מכוונת חסינות (קישור למדריך). מדריך זה מהווה הרחבה של המדריך לאבטחת חסינות, אשר פורסם לראשונה בכנס אינקוזי (Zonnenshain and Harel, 2015). מאמר זה מציג את התוספות והשינויים ביחס למדריך המקורי, אשר מאפשרים להציע אותו כבסיס להנדסת מערכות מכוונת חסינות.

שינויים מבניים

המדריך המקורי היה מורכב ומסורבל, ולפיכך קשה ליישום. המדריך כלל תיאור של אופני כשל רבים, שהוצגו על פי מודל של חסינות מערכת וכן הנחיות והמלצות למניעת אופני הכשל הללו. מהנדס המערכת שביקש ליישם את ההנחיות וההמלצות שבמדריך נדרש למפות אותן כך שישתלבו בנוהלי הפיתוח המקובלים, ובשיטות התכן המקובלות. מיפוי זה אילץ את המשתמשים במדריך להשקיע זמן רב בלימוד ובארגון המידע, והתאמתו על פי שלבי הפיתוח. המדריך החדש כולל שינויים מבניים שמאפשרים למשתמש בו למצוא בקלות את הסעיפים במדריך המתאימים לשלב בתהליך הפיתוח.

תיאוריה לחוד ופרקטיקה לחוד

חלק נכבד מהקושי בשימוש במדריך נבע מכך שההנחיות וההמלצות אורגנו על בסיס מודל החסינות. מודל זה הוא תיאורטי, ויתרונו בכך שהוא מאפשר בחינה של אופני הכשל, והערכת תכונות של אלמנטים המאפשרים אבטחת חסינות. הבעיה בהתבססות על מודל כזה היא חוסר הנוחות בפרקטיקה של הנדסת מערכות. במדריך החדש קיימת הפרדה בין החלק התיאורטי (קישור למדריך) לבין החלק הפרקטי (קישור למדריך), באופן שמאפשר התמצאות נוחה, תוך שימוש במונחים המוכרים בהנדסת מערכות.

הפרדה בין התיאוריה לפרקטיקה מאפשרת למשתמש במדריך להתכונן לקראת שלב הישום. בשלב הראשון הוא יכול ללמוד את עקרונות החסינות על ידי עיון בפרק התיאוריה. בשלב הישום, ההנחיות וההמלצות מאורגנות במונחים המוכרים של תכן תהליכים, ארכיטקטורה, מודולים, תקשורת, אירועים, מצבים וכיו"ב.

ארגון ההנחיות וההמלצות

גורם קושי נוסף בישום המדריך המקורי הוא ההשפעות ההדדיות בין ההנחיות וההמלצות, ובמיוחד אלה שלכאורה סותרות זו את זו. המהנדס שמבקש ליישם המלצה מסויימת נדרש לבדוק את ההשפעה של ישום שלה על הנחיות והמלצות אחרות, שנמצאות באזורים אחרים של המדריך, לצורך בקרת התכן.

במדריך החדש, ההנחיות וההמלצות מאורגנות כך שניתן להגיע אליהן בשתי דרכים: דרך הארכיטקטורה ודרך שכבות ההגנה. הגישה דרך הארכיטקטורה מתאימה היטב לשלב תכן המערכת, כאשר המשתמש במדריך מתכנן את המודולים של אבטחת חסינות על פי ההיררכיה שמוצגת במדריך. הגישה דרך שכבות ההגנה מתאימה היטב לשלב של בקרת התכן, כאשר המבקר עובר על שכבות ההגנה השונות ומוודא שהתכן כולל פתרון ברמות השונות.

הארכיטקטורה המומלצת

המדריך המקורי כלל תיאור של ארכיטקטורה שמאפשרת מימוש של עקרון ההנחיה העצמית, על בסיס הרעיון של STAMP (קישור למדריך). במדריך החדש, הארכיטקטורה עברה עיבוד נוסף (קישור למדריך), והיא כולל פירוט של המודולים שמאפשרים אבטחת סינות (קישור למדריך):

- ממשקי תפעול יעודיים, המאפשרים התאמת סגנונות אינטראקציה למצב התפעול (קישור למדריך)
- מודולים שמאפשרים הגדרת בסיסי ידע, המיישמים את חוקי התפעול
- מודולים שמאפשרים ניתוח פעילות המערכת בהשוואה לתרחיש ולחוקי התפעול
- מודולים שמאפשרים תיקון מהיר של המצב, בטרם הוא מתפתח לאיום (קישור למדריך)
- מודול בקרת מכונה שמאפשר ניתוב הבקרה בין המכונה למפעילים, וכן הדמיית איומים לצורך בדיקות.

שכבות ההגנה

המדריך החדש כולל הגדרה של שכבות הגנה (קישור למדריך) כדלקמן:

- מניעת טריגרים
- מניעת התפתחות הטריגר לאיום
- תכן ההתאוששות מאיום
- מניעת הסלמה
- תכן ההחלצות ממצבי חירום
- בדיקות פרואקטיביות
- תכן המידע לתחקירים

פרק למתחילים

במדריך החדש נוסף פרק למתחילים, הכולל הכוונה למימוש ארכיטקטורה בסיסית, שהיא גירסא מנוונת של הארכיטקטורה המומלצת, שמאפשרת איתור מצבים בלתי צפויים, וכן ייזום בדיקות של מצבים כאלו (קישור למדריך). הפרק כולל הנחיות לפיתוח הדרגתי של חוקי התפעול, על בסיס נסיון שמתקבל במהלך התפעול (קישור למדריך).

מטריצת הבקרה

המדריך המקורי כלל הצגה של דילמת האוטומציה, דילמה זו מתייחסת אל המצבים בהם יש יתרון לאוטומציה על פני בקרת מפעיל, ואל המצבים בהם הסיכונים של האוטומציה עלולים לעלות על התועלת שבה (קישור למדריך). המדריך כלל אבחנה בין אוטומציה לפעילות שוטפת לבין אוטומציה במצבים חריגים. המדריך המקורי כלל איזכור של בעיות הקשורות בכשירות המפעילים. כמו כן המדריך ציין שהפתרון קשור אל זמן החסד, דהיינו, מרווח הזמן בו המפעיל יכול לפעול לתיקון המצב מבלי להסתכן. המדרך המקורי לא כלל הנחיות או המלצות למדידה של כשירות המפעילים ושל זמן החסד, וישומם לפתרון דילמת האוטומציה.

המדריך החדש כולל הצעה לפתרון דילמת האוטומציה בעזרת מטריצת הבקרה, המבוססת על מדידות לגבי מצב הכשירות של המפעיל ולגבי זמן החסד (קישור למדריך). המדריך כולל הצעה לחישוב זמן החסד על בסיס שיערוך מגמות, והגדרה של הזמן הקריטי, חסמי אזהרה וחסמי בטיחות.

הגנה בפני סיכונים משניים

המדריך המקורי הציג את דילמת התועלת של עזרי חסינות, בהשוואה לסיכונים שקשורים בישומם, כולל דוגמאות מהתחום של התרעות בנהיגה. כמו כן, המדריך הציג בעיות הקשורות ביצירת תלות של המפעיל בעזרי הבטיחות (כגון, "התמכרות לאוטומציה").

המדריך החדש כולל הגדרה של שכבת הגנה ספציפית לסיכונים משניים, שמאפשרת התייחסות סיסטמתית לסיכונים המשניים, וכן תהליך של פיתוח שכבות ההגנה (קישור למדריך).

אישור החסינות

המדריך המקורי הציע דרך לחישוב האמינות ברמת המערכת על בסיס אמינות הרכיבים. המדריך החדש כולל הגדרה של מדד חסינות, על בסיס השיעור של מצבים בלתי צפויים. המדריך כולל הצעה להגדרת יעד חסינות ברמת הארגון, על בסיס רמת הסיכון למפעילים ולציבור. המדריך מציע דרך לשערוך חסינות המערכת על בסיס מדדי האמינות של הרכיבים, וכן תהליך של אישור החסינות על ידי קריטריון המבוסס על השוואת הערך המשוערך עם הערך שהוגדר כיעד החסינות.

שילוב אבטחת החסינות בהנדסת מערכות

המדריך החדש כולל פרק שעוסק בשילוב בין הדיסציפלינות ההנדסיות השונות, וכן הצבעה על פעילויות הקשורות להנדסת חסינות בשלבים השונים של תהליך פיתוח המערכת (קישור למדריך).

מקורות

Zonnenshain, A. and Harel, A., 2015, "A practical guide to assuring the system resilience to operational errors". INCOSE Annual International Symposium, Seattle. http://avi.har-el.com/eng/Articles/Seattle-v3.pdf