הצעה לפרויקט באבטחת מידע 236349
פרויקט בסביבות מחשוב אמינות

מנחה: אסף רוזנבאום sassafro@cs

1 רקע

בשל האיום הגובר למערכות מחשב ורמת הסיכון הנובעת מתקיפתן הצורך להגנה על מערכות אלה הולך וגובר. אחד מהפתרונות ההגנה הקיימים כיום הינו סביבת מחשוב אמינה (trusted execution environment או בקיצור TEE), שהיא סביבת חישוב נפרדת המוקדשת לפעולות קריטיות מבחינת אבטחה. מרכיב חשוב ביכולות של סביבה כזו הינו remote attestation, היכולת להוכיח לגורם חיצוני את מצב הסביבה על מנת לבנות אמון בין הצדדים.

1.1 Remote Attestation

על מנת לבצע remote attestation מבצעת סביבת המחשוב האמינה סדרה של מדידות הכוללות, בין השאר, גרסאות אבטחה של אלמנטי חומרה ותוכנה המרכיבים את הסביבה, הגדרות של הסביבה, מדידות של הקוד שנטען להרצה ועוד. המדידות מוגנות קריפטוגרפית על מנת למנוע מתוקף לזייף מדידות ונשלחות אל הגורם אשר איתו מעוניינים ליצור ערוץ תקשורת מאובטח.

פרוטוקול remote attestation מגדיר את האופן בו מתבצע התהליך, החל מיצירת הקשר מול הגורם החיצוני, עבור אל בניית ה–attestaion עצמה, כלומר מה יש למדוד ובאיזה אופן ועד לסיום מוצלח של הקמת ערוץ מאובטח.

1.2 TrustZone

מעבדי ARM מאפשרים ליצור TEE בעזרת הרחבה יעודית הנקראת TrustZone. ההרחבה מחלקת את המעבד לשני מעבדים וירטואלים, כאשר אחד מוגדר כ"מאובטח" והשני כ"רגיל", בעזרת ביט בקרה מיוחד הקבוע באיזה מצב נמצא כרגע המעבד. המצב המאובטח של המעבד משמש למימוש ה–TEE. ל–TEE מבוסס TrustZone מערכת הפעלה משלו בדרך כלל מבוססת מיקרו–קרנל (אשר רצה לצד מערכת ההפעלה של סביבות החישוב העיקרית), ומעליה רצים השירותים שמספקת ה–TEE לסביבת החישוב העיקרית.

2 מטרת הפרויקט

בפרויקט זה נתכנן ונממש שירות remote attestation עבור סביבת מחשוב אמינה מבוססת trustzone המפותחת במעבדה לאבטחת מידע. יעדי הפרויקט הם:

- הגדרת מודל האיום.

- תכנון פרוטוקול ל–remote attestation. התכנון יכול להתבסס כל פרוטוקלים קיימים או להיות מקורי לגמרי.
- ניתוח ההגנות שמספק הפרוטוקול אל מול מודל האיום.
- מימוש הפרוטוקול כאפליקציה על סימולציה של מערכת ההפעלה Genode המשמשת כמערכת ההפעלה של סביבת המחשוב האמינה.
- אינטגרציה מול סביבת המחשוב האמינה.

3 דרישות קדם

- הגנה במערכות מתוכנתות / אבטחת מחשבים.
- ידע ב–c++.
- יתרון (לא חובה): ידע רלבנטי בקריפטוגרפיה.

References

[1] George Coker, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O'Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen. Principles of remote attestation. http://web.cs.wpi.edu/~guttman/pubs/good_attest.pdf.

[2] Norman Feske. Genode foundations. http://genode.org/documentation/genode-foundations-17-05.pdf.

[3] Trusted Computing Group. Trusted platform module (tpm) specifications. https://trustedcomputinggroup.org/tpm-main-specification.

[4] ARM Ltd. Building a secure system using trustzone technology. http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf.

[5] Amit Vasudevan, Emmanuel Owusu, Zongwei Zhou, James Newsome, and Jonathan M McCune. Trustworthy execution on mobile devices: What security properties can my mobile platform give me? https://users.ece.cmu.edu/~jmmccune/papers/VaOwZhNeMc2012.pdf.