חוקרים מהטכניון ומאוניברסיטת תל אביב הצליחו להשתלט על אחד הבקרים התעשייתיים המאובטחים בעולם

במסגרת הדגמת התקיפה הצליחו החוקרים לכבות ולהדליק את הבקר, לטעון לתוכו לוגיקות בקרה שונות כרצונם ולשנות את קוד ההפעלה ואת קוד המקור. יתר על כן, הם הצליחו ליצור מצב שבו המהנדסים המפעילים את הבקר לא יזהו את "ההתערבות העוינת" שלהם.
<u>הדגמת התקיפה על בקר Simatic S7 של סימנס תוצג היום בכנס ההאקינג היוקרתי Black Hat</u>

חוקרים ממרכזי הסייבר בטכניון ובאוניברסיטת תל אביב בשיתוף מערך הסייבר הלאומי הצליחו להשתלט על בקר של חברת סימנס, הנחשב לאחד הבקרים המאובטחים בעולם. החוקרים יציגו את הדגמת התקיפה בכנס ההאקינג היוקרתי Black Hat שיתקיים השבוע בלאס וגאס. גירסה של המאמר נשלחה לחברת סימנס כדי שתוכל לתקן עד אז את החולשות שנמצאו.

את המתקפה הובילו ראש מרכז המחקר לאבטחת סייבר ע"ש הירושי פוג'יווארה בטכניון **פרופ' אלי ביהם וד"ר שרה ביתן מהפקולטה למדעי המחשב בטכניון יחד עם פרופ' אבישי וול מביה"ס להנדסת חשמל באוניברסיטת תל אביב**, בשיתוף הסטודנטים אביעד כרמל, אלון דנקנר ואוריאל מלין. במסגרת המתקפה ניתחו החוקרים וזיהו את רכיבי הצופן בפרוטוקול הקנייני של סימנס, ועל בסיס הניתוח יצרו תחנה הנדסית מזוייפת, חליפית לתחנה ההנדסית הרשמית של סימנס. התחנה ההנדסית המזוייפת מסוגלת לפקוד על הבקר לפי רצון התוקף. הם הצליחו לכבות ולהדליק את הבקר, לטעון לתוכו לוגיקות בקרה כרצונם ולשנות את קוד ההפעלה ואת קוד המקור. יתר על כן, הם הצליחו ליצור מצב שבו המהנדס המפעיל את הבקר לא יזהה את "ההתערבות העוינת" שלהם.

המחקר שהוביל למתקפה התמקד בסדרת ב-Simatic S7 של סימנס – סדרה של בקרים הניתנים לתכנות (PLC). בקרי PLC משמשים כיום בספקטרום רחב מאוד של יישומים ובהם תשתיות קריטיות דוגמת תחנות חשמל, משאבות מים, בקרת מבנים, פסי ייצור, מערכות תאורה, כלי רכב, כלי טיס, השקיה אוטומטית, ובתים חכמים. מטרתם הכללית: בקרת-תהליכים אוטומטית המגיבה באופן אופטימלי לתנאי הסביבה ולשינויים בהם הבקרים מקבלים את ההוראות ממחשב ומפעילים על פיהן את ציוד הקצה הרלוונטי למפעיל: חיישנים, מנועים, רמזורים ועוד.

הדורות החדשים במשפחת Simatic S7 נחשבים בטוחים ומוגנים יותר מקודמיהם, בעיקר בשל השיפורים באיכות ההצפנה. לכן מתקפות עליהם מהוות אתגר מורכב המצריך ידע נרחב בתחומים ושונים.
מאחר שסימנס אינה מפרסמת את פרוטוקול הפעולה של הבקרים, שחזרו החוקרים את הפרוטוקול מתוך ניתוח הבקר (reverse-engineering).

לדברי פרופ' וול, חלק זה של "עבודת בילוש" דרש חודשי עבודה רבים.
בתום שחזור הפרוטוקול ניגשו החוקרים למיפוי מערכות האבטחה וההצפנה של הבקר ולאיתור חולשות במערכות אלה. ואכן, הם הצליחו לקבוע מפתחות משותפים עם הבקר ובאמצעותם להתחזות לתחנה הנדסית לגיטימית מנקודת המבט של הבקר.

כל זה אפשר להם לטעון על הבקר תוכנה זדונית למרות האבטחה הקריפטוגרפית הגלומה במערכות. לדברי פרופ' ביהם, "זה היה אתגר מורכב בגלל השיפורים שסימנס הכניסה בגירסאות החדשות יותר של בקרי SIMATIC. ההצלחה שלנו קשורה בניסיון הרב שלנו בחקר בקרים ואבטחתם ובשילוב של הידע המעמיק שלנו בכמה תחומים – הבנת מערכות, יכולות reverse engineering, ניתוח פרוטוקולי תקשורת, וניתוח קריפטוגרפי."

דר' ביתן ציינה שהמתקפה מדגישה את הצורך בהשקעה של יצרנים ולקוחות כאחד באבטחת מערכות בקרה תעשייתיות. לדבריה, המתקפה מראה שאבטחת מערכות בקרה תעשייתיות היא משימה קשה ומאתגרת יותר מאבטחת מערכות מידע.

<u>אוריאל מלין וד"ר שרה ביתן יציגו את המחקר היום בכנס ההאקינג היוקרתי Black Hat שיתקיים בלאס וגאס. ההרצאה תתקיים היום, יום חמישי, 8 באוגוסט, בשעות 11:00-11:50 (שעון ארה"ב)</u>

לתמונות לחצו כאן
כיתוב:
1. פרופ' אלי ביהם, הפקולטה למדעי המחשב בטכניון
2. פרופ' אבישי וול, ביה"ס להנדסת חשמל באוניברסיטת תל אביב
3. ד"ר שרה ביתן, הפקולטה למדעי המחשב בטכניון
4. אוריאל מלין, ביה"ס להנדסת חשמל באוניברסיטת תל אביב
5. תמונת הבקר מדגם Plc-s7-1500 של סימנס

לפרטים נוספים: דורון שחם, דוברת הטכניון – 050-3109088
אורנה כהן, דוברת אוניברסיטת תל-אביב 054-7888437