30/01/2019

קול קורא להגשת הצעות מחקר בתחום הסייבר ואבטחת מידע
לשנת תשע״ט

מרכז המחקר לאבטחת סייבר ע״ש הירושי פוג׳יוארה הוא גוף משותף לטכניון ולמטה הסייבר הלאומי במשרד ראש הממשלה, המיועד לקדם מחקר (ופעילות אחרת) במגוון התחומים הטכנולוגיים, ההנדסיים והמדעיים של סייבר ואבטחת מידע. במסגרת קול קורא זה יוענקו מענקי מחקר בתחומים אלה.

א. <u>תנאי המענק</u>

המרכז יעניק מספר מענקי מחקר בהיקפים שונים. עד 80,000 ₪ למחקר מקדים למשך שנה. עד 200,000 ₪ לשנה למחקרים עם חוקר יחיד ועד 500,000 ₪ לשנה למחקרים של קבוצות חוקרים. (הוועדה המדעית וועדת ההיגוי יוכלו לאשר תקציב חריג במקרים שזה יתבקש).

משך המחקר יהיה שנה, שנתיים או לכל היותר שלוש שנים.

מספר המענקים והיקפיהם ייקבעו על ידי הנהלת המרכז בהמלצת הועדה המדעית. בקול הקורא הנוכחי צפוי שיאושרו מחקרים בהיקף כולל של עד 4 מיליון ₪.

מענק המחקר יכול לכלול מימון מלגות לסטודנטים לתארים מתקדמים ובתר דוקטורנטים (עד 100% מהמענק), חוקרים בצוות מחקר (עד 40% מותנה באישור פרטני מראש), כוח אדם טכני (עד 40%), נסיעות לכנסים (עד 10%), רכש ציוד וכוח חישוב (עד 10%), ושונות (עד 5%). ניתן יהיה לבקש שינויים באחוזים הללו באישור ראש המרכז וועדות המרכז.

המענק לא יכלול מימון שכר או תוספות שכר לחברי סגל.

ב. <u>זכאות להשתתפות</u>

המענקים מיועדים לחוקרים או לקבוצות חוקרים חברי מרכז המחקר לאבטחת סייבר בטכניון, זאת למטרת עריכת מחקרים חדשניים בנושאי אבטחת סייבר.

חוקרים יכולים להגיש בקול קורא זה גם הצעות מחקר שכבר עברו שיפוט חיצוני אחר בכדי להרחיב את היקף המחקר. שימו לב שחברי מרכז ששותפים במחקר שזכה במימון ממרכז סייבר באוניברסיטה אחרת בארץ (ללא מימון לחלק הטכניוני) יכולים לבקש לקבל מימון של החלק הטכניוני במסגרת קול קורא זה (במקרה כזה נא לציין באיזה מרכז סייבר זכתה ההצעה בעבר).

חבר סגל בטכניון שאינו חבר מרכז יכול להגיש הצעת מחקר לקול קורא זה בצירוף בקשת הצטרפות כחבר מרכז.

ההצעה יכולה גם לכלול שותפים מחוץ למרכז המחקר, אך תקצוב יתקבל לחברי המרכז מהטכניון בלבד.

ג. <u>הגשת ההצעות</u>

הצעת מחקר שתוגש תכלול את הפרקים הבאים:

1. נושא ההצעה ושמות המגישים.
2. תקציר מנהלים (עד עמוד).

3. תיאור המחקר המוצע, הרקע המדעי ומצב הידע העכשווי (עד 5 עמודים).
4. פירוט המטרות והקשר שלהן לנושאי אבטחת סייבר, תוך הדגשת החדשנות (עד עמוד).
5. פירוט אפשרויות יישום ושת"פ אפשרי עם גופים נוספים.
6. פירוט תקציבי (לפי שנים, בטבלה, על פי ההוצאות המותרות הרשומות לעיל) והצדקת תקציב (עד עמוד). אין צורך לציין תקורות בפירוט התקציבי. במקרה של הצעה הכוללת כמה חוקרים ראשיים, נא לפרט לכל אחד בנפרד + סיכום התקציב הכולל.
7. פירוט תקציבי מחקר קיימים בנושא, בנושאים משלימים או בנושאים קשורים, יחד עם הבהרה באשר לחלקי הצעת המחקר הזוכים למימון מגורם אחר, או באם ההצעה כבר עברה שיפוט על ידי וועדת מענקים אחרת והעתק דווחי השפוט. כמו כן, פירוט הגשות מקבילות לגורמי חוץ.
8. קורות חיים של המציעים (אפשר מקוצרים בשני עמודים כ"א): מידע המתייחס לחמש השנים האחרונות לפחות (מאמרים, כינוסים, סטודנטים משתלמים, הצעות מחקר שזכו במימון חוץ וכיו"ב).
9. אבסטרקט לפרסומי המרכז (כ-8-10 שורות).
10. בקשת הצטרפות למרכז (במקרה של מגישים שעדיין אינם חברי מרכז).
11. שתי הצעות לשופטים מתוכם לפחות אחד מחו"ל.

הצעת המחקר תוגש **באנגלית** בקובץ PDF אחד, כאשר סעיפים 1-7 מוגבלים יחד ב-10 עמודים. ההגשה תתבצע בדואר אלקטרוני לכתובת cyber@technion.ac.il.

תאריך אחרון להגשה: 17.02.2019.

ד. <u>שיפוט ההצעות</u>

הצעות המחקר תועברנה לשיפוט על ידי ועדת שיפוט שתכלול את הוועדה המדעית של המרכז, ושתיעזר בשופטים חיצוניים. הועדה תבדוק את הצעות המחקר שהוגשו ותחליט על פי שיקול דעתה על הזוכים במענקים ועל ההיקף התקציבי. החלטות הועדה יאושרו על ידי ועדת ההיגוי ותהיינה סופיות. בין השיקולים העיקריים של הוועדה יהיו רלוונטיות לאבטחת סייבר, חדשנות ורמה מדעית/טכנולוגית, ניסיונם של המציעים בתחום המוצע ויכולת המציעים לקיים את המחקר המוצע.

ה. <u>קניין רוחני</u>

הבעלות בתוצרי המחקר תהיה של מוסד הטכניון למחקר ופיתוח בע"מ. תוצרי המחקר כפופים לזכות שימוש של המדינה לצרכים לאומיים ולתשלום של 5% תמלוגים למדינה במקרה של מסחורם.

ו. <u>דיווח</u>

על הזוכים במענקים להגיש להנהלת המרכז דו"ח מדעי שנתי על התקדמות המחקר, ודו"ח מדעי מסכם בסיום המחקר (עד 10 בדצמבר בכל שנה). בסוף כל שנת מחקר יוגש גם דו"ח כספי. הפרסומים והדו"חות המדעיים יכללו הבעת תודה לממנים (ובפרט למערך הסייבר הלאומי ולמרכז).[1] במידה שיתבקשו, על החוקרים להציג את הצעת המחקר ואת תוצרי מחקרם במהלך הכנס שנתי של המרכז.

[1] למשל על פי הניסוח
"This research was partially supported by the Technion Hiroshi Fujiwara cyber security research center and the Israel cyber directorate."