שליטה ובקרה גרעינית

chapter 13 – Nuclear Command and Control

צופית רונן

סמינר באבטחת מידע

פרופ' אור דונקלמן

מבנה -

- מה הקשר של שליטה ובקרה גרעינית?!
- שליטה משותפת – בעיה ופתרון
- יישומים שפותחו בזכות ההשקעה בשליטה ובקרה גרעינית -
  - קודי אימות
  - סכמות לבקרה משותפת
  - ערוצים סמויים (פירצת אבטחה)
- פתיחות או בטיחות?

מה הקשר של שליטה ובקרה גרעינית?!

- קיים חשש מהנזק שיגרם משימוש לא מורשה בנשק גרעיני או מהתפשטות הטכנולוגיה הגרעינית לגורמים לא רצויים
- החשש גורם למעצמות הגרעין להוציא סכומי כסף אדירים בשמירה על החומרים הגרעיניים וסביבת הפיתוח שלהם
- המדע התפתח רבות מנסיונות השליטה בנשק הגרעיני

modernukraine.eu

מה הקשר של שליטה ובקרה גרעינית?!

- בפרט, מגוון עצום של טכנולוגיות אבטחה נלמדו מתכנית הגרעין
  - הגילוי שסיסמאות הארוכות מ-12 ספרות לא שימושיות בשדה קרב
  - עטיפת התקנים בסיבים אופטיים, והגנה אפילו מפני תזוזה זעירה
  - זיהוי קשתית העין, המערכת המדויקת ביותר לזיהוי ביומטרי של יחידים
  - מומחיויות רבות בטכנולגיות חישה

בהמשך נברר לעומק כמה טכנולגיות אבטחה נוספות

מבנה -

מה הקשר של שליטה ובקרה גרעינית?!

שליטה משותפת – בעיה ופתרון

יישומים שפותחו בזכות ההשקעה בשליטה ובקרה גרעינית -

קודי אימות

סכמות לבקרה משותפת

ערוצים סמויים (פירצת אבטחה)

פתיחות או בטיחות?

שליטה משותפת

- מפתה לחשוב שאם פעולה משתבשת בהסתברות $\frac{1}{10}$ בשל טעות אנוש, אז אם ניתן ל-5 אנשים שונים לבדוק אותה נוריד את הסתברות השגיאה ל-$\frac{1}{100,000}$

- גם חיל האוויר האמריקאי חשב ככה
- הניסיון שלו עם בטיחות גרעינית לימד אותו אחרת

- באבטחה חשוב להכיר את החומר האנושי ולפי זה לתת פתרונות מתאימים

מה הבעיה בשליטה משותפת?

- כל אחד סומך על השני שיבצע את תפקידו, אך בעצמו מתרשל

- מה אפשר לעשות?
- איך ניתן לתכנן מערכות שלא יפלו מול דברים כאלו?

timmilburn.com

אישור, סביבה, כוונה

כדי שראש נפץ יתפוצץ, צריכים להתקיים שלושה תנאים:

- ✓ אישור/הרשאה – השימוש בנשק אושר על ידי הנשיא או בכירים אחרים המוסמכים לכך
- ✓ סביבה – הנשק "חש" בסביבה המתאימה לו
- ✓ כוונה – המפקד האחראי פקד באופן חד-משמעי על שימוש בנשק

שילוב של שלושת התנאים אמור להקטין באופן משמעותי שימוש לא רצוי בנשק

מבנה -

מה הקשר של שליטה ובקרה גרעינית?!

שליטה משותפת – בעיה ופתרון

יישומים שפותחו בזכות ההשקעה בשליטה ובקרה גרעינית -

- קודי אימות
- סכמות לבקרה משותפת
- ערוצים סמויים (פירצת אבטחה)
- פתיחות או בטיחות?

OTAC vs. OTP

one-time authentication codes (OTAC)

- העיסוק בשליטה ובקרה גרעינית הוביל לפיתוח של קודי אימות חד-פעמיים
- על הודעה שנשלחת מחושב קוד מוצפן ע"י מפתח. הקוד נקרא מאמת/תג ומצורף להודעה כדי לאמת את זהות השולח
- מכיוון שמשתמשים בכל מפתח רק פעם אחת, קודי האימות נותנים אבטחה ללא תנאי

OTAC vs. OTP

one-time pad (OTP)

- שיטת הצפנה, שבה המפתח באורך ההודעה המוצפנת, והוא נבחר באופן אקראי ומשמש להצפנה חד פעמית
- הוכח שOTP נותנת אבטחה מושלמת שאינה תלויה במשאבים וביכולות של התוקף
- כלומר, ההצפנה בלתי ניתנת לשבירה

- קיים הבדל בין OTAC לבין OTP

שימוש לא בטוח בקודי אימות - דוגמא

- המפתח מחולק לשניים - <הוראה שהקידוד שלה זוגי והוראה שהקידוד שלה אי זוגי , מספר סודי>
בקבלת ההודעה בודקים ששני חלקי המפתח ייושמו

- התחזות תצליח בהסתברות $\frac{1}{337}$, החלפה בהסתברות 1

- יש מגוון דרכים להשתמש בקודי אימות בצורה בטוחה – ביניהם MAC או שילוב של שימוש בצופן בלוקים

מבנה -

מה הקשר של שליטה ובקרה גרעינית?!

שליטה משותפת – בעיה ופתרון

יישומים שפותחו בזכות ההשקעה בשליטה ובקרה גרעינית -

קודי אימות

- סכמות לבקרה משותפת
- ערוצים סמויים (פירצת אבטחה)
- פתיחות או בטיחות?

סכמות לבקרה משותפת

- בשעת חרום צריך מערכת בקרה לגיבוי, שתופעל ע"י שילוב של כמה נושאי משרה או מפקדים בשטח, שביחד יפעילו את הנשק

- תקדים לכך היה בטילים בליסטיים ששוגרו מצוללות
- חלק מהצורך בטילים אלו היה לספק אפשרות של second-strike
- בנסיבות כאלו מפקד הצוללת לא יכול להשאר חסר יכולת לחמש את הנשק שלו אם הוא לא מקבל קוד מהנשיא

סכמות לבקרה משותפת - המשך

- לכן, שומרים תחמושת בשליטת קציני הספינה, עם הוראות מבעלי הסמכות באילו נסיבות להשתמש בכלי הנשק

- דרך פשוטה היא לתת לכל אחד מזוג קצינים חצי מפתח. חסרון - מפתח ארוך פי 2 כדי לשמור על אותה רמת אבטחה

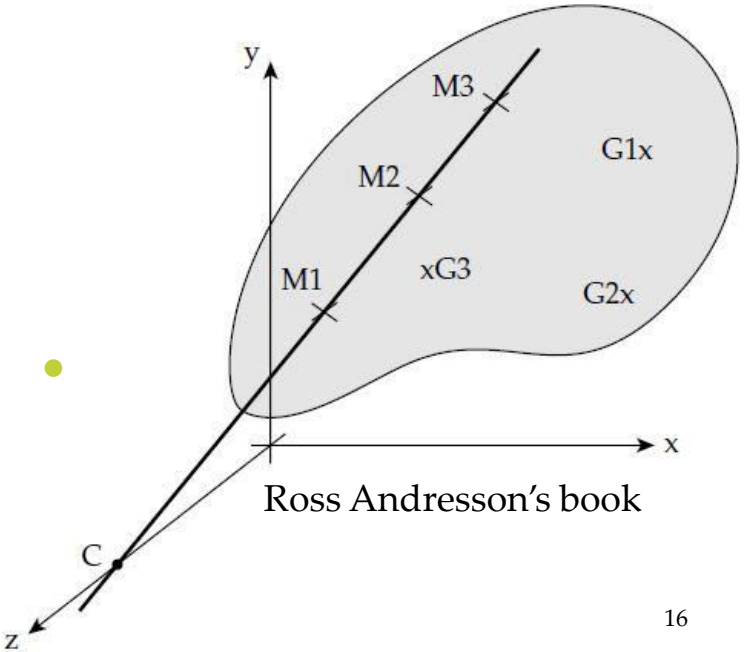
- גישה אחרת היא לתת לכל אחד מהזוג מספר, כאשר סכום המספרים הוא המפתח

סכמות לבקרה משותפת - המשך

- גישה כללית יותר נלקחת מתחום אחר של קריפטוגרפיה - סכמות לשיתוף סוד – ופותחה ע"י בלקלי ושמיר ב-1979

- ניתן להכליל את המבנה הפשוט של שלושת המימדים לגיאומטריה ב-n מימדים, או למבנים אלגבריים כלליים ולאו דווקא לקווים ומישורים

- באופן זה ניתן לאפשר קומבינציות מורכבות יותר כמו קישור בין נשקים ומפקדים ועוד



Ross Andresson's book

מבנה -

מה הקשר של שליטה ובקרה גרעינית?!

שליטה משותפת – בעיה ופתרון

יישומים שפותחו בזכות ההשקעה בשליטה ובקרה גרעינית -

קודי אימות

סכמות לבקרה משותפת

ערוצים סמויים (פירצת אבטחה)

פתיחות או בטיחות?

מה השתבש?!

- למרות הסכומים העצומים שהושקעו, מנגנוני בקרה ובטיחות גרעיניים סובלים מבעיות כמו כל מנגנון אחר

- דוגמא לכך היא התקפה (שכנראה התרחשה) והובילה לפיתוח של ענף חדש בקריפטוגרפיה המודרנית – מחקר של ערוצים סמויים, שרלוונטי לתחומים רבים

קצת היסטוריה...

- עסקת צמצום הנשק של ארה"ב וברית המועצות, נועדה לאמת את מספר הטילים הבליסטיים הבין-יבשתיים
- 100 טילים אמריקאים פוזרו אקראית ב- 1,000 ממגורות
- היה צורך שהרוסים ידעו שיש לכל היותר 100 טילים באזור הממגורות, בלי לדעת באילו ממגורות נעשה שימוש
- האמריקאים פיזרו אקראית במגורות חיישנים רוסיים שזיהו האם קיים טיל

הצצה לאלגוריתם חתימה דיגיטלי (DSA)

קבועי המערכת:

- p, מספר ראשוני
- q, מספר ראשוני שמחלק את p-1
  נסמן ב-N את מספר הסיביות של הייצוג הבינארי שלו
- g, יוצר של תת קבוצה של F_p^* מסדר q

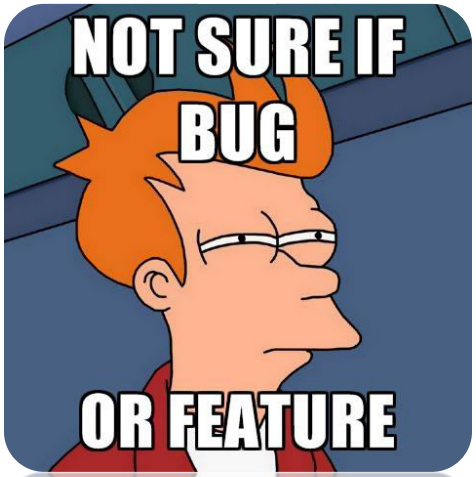
חתימה על הודעה M היא הזוג (r,s) כאשר

X מפתח פרטי, k מספר אקראי חד-פעמי, שניהם בטווח [1,q-1]

$$r = \left(g^k (\mathrm{mod}\ p)\right)(\mathrm{mod}\ q)\ ,\ s = \left(k^{-1}(z + xr)\right)(\mathrm{mod}\ q)$$

z הוא N הסיביות הנמוכות של H(M)

ערוצים סמויים – דוגמא לשימוש בDSA



- המיפוי מ-k ל-r הוא מקרי למדי
- אפשר להשתמש ביכולת זו כדי להכניס מידע על נגיף או על הרשעה פלילית לתוך דרכון או ת.ז דיגיטליים
- פתרון אפשרי - שימוש בסכמת חתימה דטרמיניסטית (כמו RSA), במקום בסכמה עם מפתחות אקראיים (כמו DSA)

מבנה -

מה הקשר של שליטה ובקרה גרעינית?!

שליטה משותפת – בעיה ופתרון

יישומים שפותחו בזכות ההשקעה בשליטה ובקרה גרעינית -

קודי אימות

סכמות לבקרה משותפת

ערוצים סמויים (פירצת אבטחה)

פתיחות או בטיחות?

פתיחות או בטיחות?

- בשנות ה30 פיסיקאים ממדינות רבות חלקו באופן חופשי את הרעיונות המדעיים שהובילו לפיתוח הפצצה הגרעינית
- לאחר שנחשף כי קבוצה המכונה "מרגלי האטום" העבירה לרוסים מסמכים סודיים הנוגעים לפרויקט הגרעין, היחס למדע הקשור לגרעין הלך לקיצוניות השנייה
- ארה"ב אימצה מדיניות לפיה כל ידע אטומי שהוא מוגדר כמסווג

פתיחות או בטיחות?

- דברים נרגעו מאז
- ככל שבדקו יותר את נושאי הביטחון, כמות מפתיעה של טכנולוגיה הותרה לפרסום
- החשיבות של ביקורת ציבורית על תכנון המערכות גברה על היתרון בכך שהיריב לא יכיר את פרטי המערכת שבשימוש
  - ניתן לראות זאת כגלגול מודרני של עקרון קרקהופס

פתיחות או בטיחות?

- דוגמא נוספת למתח זה התגלתה אחרי אירועי ה-11 בסמפטמבר
- מספר ממשלות חששו מהאפשרות שמחבלים ישתמשו בנשק ביולוגי, ולכן הטילו בקרות על מחקר והוראה בכמה תחומים של בילוגיה ורפואה
- לא נרצה שמדיניות זו תגרום לחוסר באנשי בריאות שיהיו מסוגלים להתמודד באיידס או בשפעת העופות

סיכום

- פעולות לשליטה בנשק גרעיני – מאבטחה פיזית של מתקני גרעין ועד בקרה על הסכמים בינלאומיים – תרמו תרומה עצומה לטכנולוגיית האבטחה

- ההחלטה להגן על נשקים וחומרים גרעיניים, כמעט בכל מחיר, גרמה לפיתוח רב של מתמטיקה ומדע

- סקרנו חלק מהיישומים שפותחו –

*קודי אימות *סכמות בקרה משותפת *ערוצים נסתרים

תודה על ההקשבה

שאלות?

Google images