ELECTRONIC AND INFORMATION WARFARE

(לוחמה אלקטרונית ולוחמת מידע)

פרק 19

מארגן הסמינר:
פרופ׳ אור דונקלמן

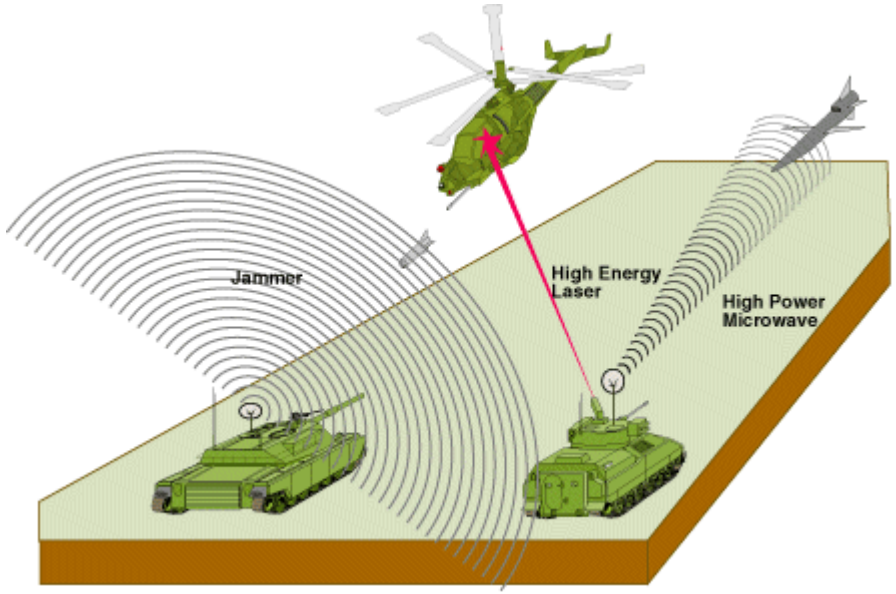
מרצה : אנטון

מבוא

- במשך זמן רב, לוחמה אלקטרונית ואבטחת מחשבים היו תחומים נפרדים.
- בזמן האחרון, ניתן להבחין בשילובם של שתי התחומים אל תוך תחום אחד, "לוחמת מידע".
- מדוע מהנדסי אבטחה צריכים ללמוד בכלל על לוחמה אלקטרונית?

מבוא – סקירה של לוחמה אלקטרונית

- אז מה זה "לוחמה אלקטרונית" ?



מבוא – סקירה של לוחמה אלקטרונית

עדיפויות לוחמה אלקטרונית	עדיפויות אבטחת מחשבים
1. denial of service	1. סודיות המידע
2. הונאה	2. שלמות המידע
3. ניצול המידע	3. זמינות המידע

מערכות תקשורת

- חשיבותן של מערכות תקשורת:
המפקד צריך להעביר מידע חיוני לחיילים שלו שנמצאים בשטח הקרב.

- עד 1915 תקשורת התנהלה באופן פיזי, לאחר מכן התחילו להשתמש בטלגרף, טלפון ובימנו ישנם מגוון רחב של אמצעים דרכם ניתן להעביר מגוון רחב של מידע(קול, תמונה, וכו׳)

מערכות תקשורת – סיכונים אפשריים

- סודיות ושלמות המידע.
- סודיות המיקום.
- שיבוש התקשורת.
- ניתוק פיזי של התקשורת.

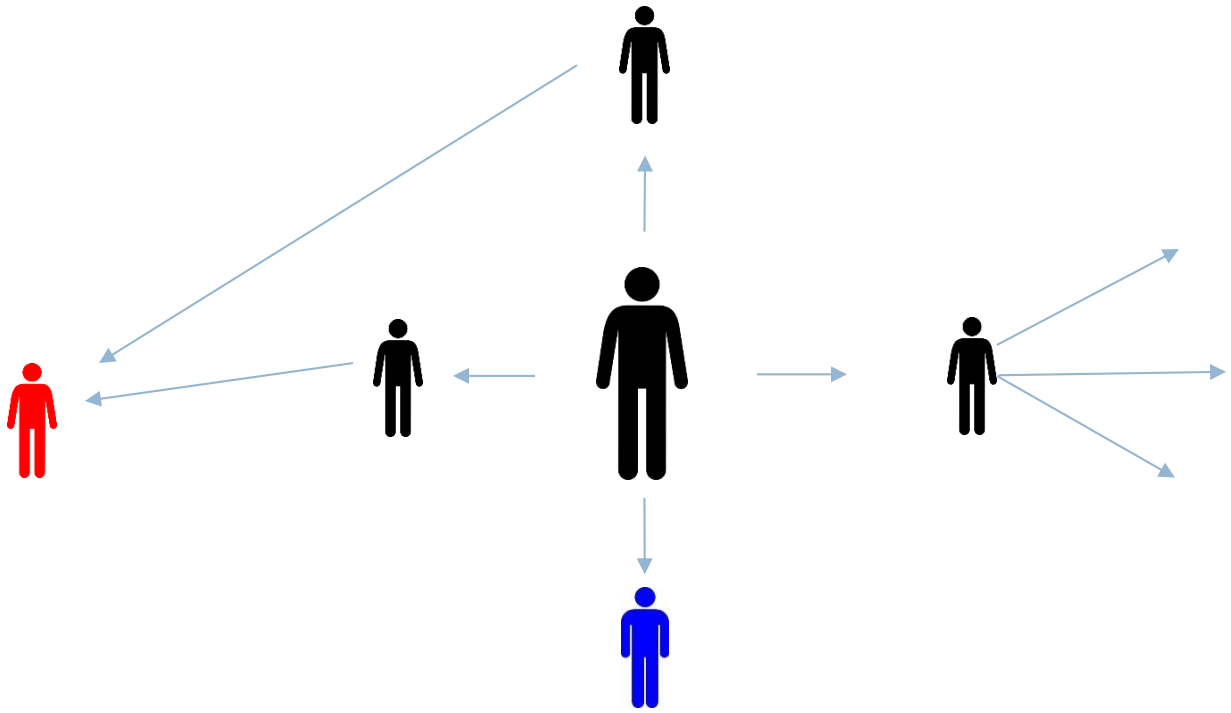
מערכות תקשורת – סיכונים אפשריים

- מכל אוסף הדוגמאות הקודמות, ניתן לראות שיש סיבות רבות להגן וגם לתקוף את המערכת האלו.
- לפעמים צריך גם לחשוב מחוץ לקופסא.

מערכות תקשורת – מיפוי הרשת

- טרם תקיפה של מערכות תקשורת, אנחנו צריכים למפות את רשת התקשורת של האויב.
- ניתוח המידע ומיפוי הרשת בהקשר של מערכות תקשורת.
- מענה לצורך זה ניתן ע"י תחום "מודיעין אותות" (Signals Intelligence).
- דוגמא לניתוח מידע: "כדור השלג".

מערכות תקשורת – מיפוי הרשת –"כדור השלג"



יש לזכור שזה לא תמיד כך פשוט

מערכות תקשורת – התקפות

נדבר על עקרונות ופחות על פרטים טכניים.

- התקפות קריפטוגרפיות.
- ההתקפות גניבת "Key Material".
- "הונאות" ושיבושים.
- ניתוק פיזי של כבלי / תחנות התקשורת.

מערכות תקשורת – הגנות

- שימוש בקריפטוגרפיה.
- סיבים אופטיים.
- לייזר אינפרה אדום.
- FREQUENCE HOPPING.

- על כל הגנה יש התקפה חדשה וכך זה מתגלגל, בדומה לתחום של אבטחת מחשבים.

לוחמת מידע

- כיום , לא באמת נדרש לשגר טיל כדי לגרום נזק לאויב. אפשר:
  - להפיל את הבורסה ולפגוע בכלכלה.
  - להפיל את מערכות החשמל.
  - להפיל את מערכות המים.
  - להפיל חברות ממשלתיות.
- כל אלו יגרמו נזק משמעותי, ומכך יש לנו זירת קרב חדשה שמתפתחת.

לוחמת מידע

- הגדרה מקובלת של לוחמת מידע:
  "לוחמת מידע היא השימוש ההתקפי או הגנתי, במידע ומערכות מידע, על מנת למנוע, לנצל, להשחית או להרוס מידע, תהליך עיבוד המידע, מערכות מבוססות מידע ומערכות תקשורת מבוססות מחשב. מטרת פעולות אלה היא להשיג יתרון על יריב צבאי או עסקי."
  דר' איוון גולדברג (ראש המכון ללימודים מתקדמים של מלחמת מידע (IASIW)

לוחמת מידע – דוגמאות

- 1982 – פיצוץ צינור הגז הסובייטי.
- 1990 – מלחמת המפרץ.
- 2007 – ההתקפה של רוסיה על אסטוניה.
- 2007 – התקפת הכור הסורי.
- 2010 – STUXNET.
- 2014 – ההתקפה של צפ׳ קוריאה על חברת סוני.

לוחמת מידע – עקרונות מלוחמה אלקטרונית

- ישנם עקרונות משותפים ללוחמה אלקטרונית ולוחמת מידע. ניתן מספר דוגמאות:
  - מתודולוגיות דומות.
  - false accept and false reject rate.
  - העניין הכלכלי.
  - לא נרצה לחשוף את יכולתנו.

לוחמת מידע – עקרונות מלוחמה אלקטרונית

- עם זאת , יש גם הבדלים:
  - סקריפט קידיס.
  - מרחבה הלחימה שונה.

סיכום

- התחום של לוחמת מידע הולך ומתפתח עם הגידול בשימוש בטכנולוגיות האינטרנט והמחשבים, לכן חשוב לנו להתכונן לבעיות הרבות שיכולות לצוץ ברמה המדינית.

- אנחנו מנסים ללמוד מה השתנה מהמעבר מהשטח לאינטרנט , לכן כדאי מאד למהנדסי האבטחה להבין טוב את התחום של לוחמה אלקטרונית כי מסתבר שיש הרבה עקרונות משותפים.