אבטחת מחשבים ורשתות

203.4448

סמסטר חורף תשע"ב (2011)

הרצאה 1 - מבוא

שקפי הקורס נכתבו על ידי אלי ביהם, שרה ביתן, אור דונקלמן, יוליה צ'וז'וי ואריק פרידמן

סגל

מרצה:

אור דונקלמן

דוא"ל: orrd@cs

טל. 8447

שעת קבלה: יום א' 15:00-16:00

בודק תרגילים:

תומר אשור

דוא"ל:
tashur01@campus.haifa.ac.il

שעת קבלה: יום ב' 9:45-11:45

אבטחת מחשבים ורשתות

אתר הקורס:

http://www.cs.haifa.ac.il/~orrd/Security

רשימת תפוצה:

כל הודעות הקורס יופצו דרך רשימת תפוצה.

לאחר סיום מועד ההרשמה לקורס, ישלח אימייל לכל הסטודנטים הרשומים. סטודנט שלא יקבל את האימייל, צריך לשלוח אימייל ל-orrd@cs.

יש לעקוב אחרי ההודעות הנשלחות ברשימת התפוצה ומופיעות באתר הקורס.

אבטחת מחשבים ורשתות

מועדי המבחן:

מועד א – 5.2.2012 (יום א')

מועד ב – 6.3.2012 (יום ג')

ציון:

- 70% מבחן.
- 30% תרגילי בית (ממוצע תרגילי הבית מהווה מגן).

אם הציון במבחן נמוך מ-46, תרגילי הבית אינם מגנים:

ציון המבחן יהיה הציון הסופי.

תרגילי בית

ינתנו 5 תרגילי בית.

כל תרגיל בית מהווה מגן של 6% בנפרד.

הגשה בבודדים או בזוגות.

הגשה באיחור רק באישור של 24 שעות מראש מאור.

העתקות יטופלו בחומרה!

מותר, ואף רצוי לעבוד בקבוצות. עם זאת, **אסור** להעתיק.

נושאי הקורס

מבוא:

- מהי מערכת מחשב
- סוגי איומים על מערכות מחשבים
- מדיניות הגנה
- הגנה פיסית

מושגי יסוד בקריפטולוגיה:

- צפנים – צפני מפתח משותף וצפני מפתח פומבי
- פונקציות תמצות קריפטוגרפיות ושימושיהן
- אימות (MAC, חתימות דיגיטליות)
- ניהול מפתחות ו-Public Key Infrastructure
  - X.509,Trust Models, PGP

נושאי הקורס (המשך)

היבטי אבטחה במערכות הפעלה מודרניות:

- בקרת גישה
- כתיבת קוד בטוח
- הצפנת קבצים והתקני אחסון
- וירוסים, תולעים, סוסים טרויאנים

בקרת כניסה:

- אימות זהות של משתמש אנושי
- סיסמאות חד-פעמיות
- פרוטוקולי אתגר-מענה (Challenge-Response)
- EKE
- Kerberos

נושאי הקורס (המשך)

הגנה על רשתות מחשבים:

- מהי רשת מחשבים
- מבוא: מודל השכבות, TCP/IP
- שילוב הגנות במודל השכבות – אפשרויות ושיקולים
- Firewalls
- פרוטוקולים לאבטחת מידע:
  - IPSec
  - SSL/TLS
- פרוטוקולים להחלפת מפתחות (IKE)
- בטיחות אלחוטית:
  - WEP, 802.11, 802.1X WPA, EAP

ספרי לימוד

- Cheswick, Bellovin & Rubin, *Firewall and Internet Security,* 1st edition 1994. (Second edition exists: Addison Wesley, 2003)
- Kaufman, Perlman & Speciner, *Network Security, Private Communication in a Public World*. 2nd edition Prentice Hall, 2002 (1st edition 1995).
- Stallings & Brown, *Computer Security :Principles and Practice*. Pearson/ Prentice Hall, 2008

מטרות הקורס

- הכרת סוגי האיומים על מערכות מחשב
- הכרת גישות להגנה על משאבי מחשוב
- הכרת מנגנונים להגנה והתמודדות
- הקניית היכולת לגבש ולממש מדיניות הגנה (Security Policy)
- הצגת התפתחויות בתחום אבטחת המידע והמחשבים
- הכרת דרך החשיבה באבטחת מידע (Security mindset)

מה אין בקורס?

- לימוד מערכות הפעלה
- לימוד רשתות מחשבים ותקשורת
- לימוד קריפטוגרפיה

עם זאת, כדי לבנות ולהשתמש במנגנוני הגנה שונים יש צורך (ואפילו חשוב) להכיר את הנושאים לעיל.

- לא נלמד בקורס כיצד לתקוף מערכות מחשבים. כן נראה דוגמאות של התקפות שהיו, על מנת ללמוד ממה יש להזהר וכיצד ניתן למנוע התקפות מסוגים שונים.

ולעניינים...

מהי מערכת מחשב?

כל רכיב אלקטרוני המכיל מעבד או שערים לוגיים מהווה מערכת מחשב.

לדוגמה:

- מחשב ביתי (PC)
- רשת המחשבים של האוניברסיטה
- מכשיר כספומט
- טלפון נייד
- ממיר של חברת כבלים
- כרטיס חכם של רכבת, טלפון, ועוד
- מכונית
- ועוד ...

שלבי בניית מערכת הגנה

- זיהוי האיומים הפוטנציאליים
- ניתוח סיכונים הנובעים מהאיומים
- גיבוש מדיניות הגנה (שקובעת על מה רוצים להגן וכיצד)
- מימוש מדיניות ההגנה בעזרת מנגנוני הגנה

- בסופו של דבר שם המשחק הוא כסף. אם מה שאנו מעוניינים להגן עליו שווה מיליון דולר, אף אדם שפוי לא ישקיע שני מיליון דולר בהגנה עליו.

סוגי האיומים – איומים על נתונים

פגיעה ב:

סודיות (secrecy), פרטיות (privacy): קריאה/פרסום נתונים סודיים

שלמות (integrity): שינוי תוכן הנתונים ע"י אנשים לא מורשים

זמינות (availability): פגיעה בנגישות הנתונים

ניתן לפגוע בנתונים בזמן שהם נשלחים ברשת (data in transit), או כאשר הם שמורים במערכת (data at rest).

כדאי לזכור כי לפעמים בעל המערכת הוא המאיים על הנתונים (נראה בהמשך).

סוגי האיומים – איומים על משאבים

פגיעה בזמינות, או שימוש לא חוקי במשאבים (שגורם לפגיעה בזמינות עבור המשתמשים החוקיים):

- פגיעה במעבד והחומרה שמסביבו
- התוכנה
- קווי תקשורת
- יחידות היקפיות: דיסקים וכו'
- גניבת שיחות

מדוע להתקיף?

פירצה פשוטה באתר של מופז
חשפה פרטי רבבות מתפקדים
פרטים אישיים של כ־ 30 אלף מתפקדי קדימה נחשפו עקב פירצת אבטחה פשוטה. בעקבות פניית כלכליסט נחסמה הפירצה
עידו קינן
11.08.08, 06:58
http://www.calcalist.co.il/internet/articles/0%2C7340%2CL-3102144%2C00.html

August 11th, 2008
Coordinated Russia vs Georgia cyber attack in progress
Posted by Dancho Danchev @ 4:23 pm
http://blogs.zdnet.com/security/?p=1670&tag=nl.e539

ניסיון לגניבת פרטים של לקוחות בנק אוצר החייל
נוכלים מתחזים ל"בנק הפועלים" ובנק אוצר החייל, ומנסים לגנוב פרטים של לקוחות להתחברות לחשבון באמצעות הונאה, על ידי הקמת אתר מזוייף לבנק
אהוד קינן
פורסם: 24.08.08, 11:19
http://www.ynet.co.il/articles/0,7340,L-3586719,00.html

- פגיעה במוניטין של המותקף
- השגת מוניטין לתוקף
- גניבת כסף
- פגיעה ביריב (מחיקת מאגר הנתונים שלו)
- האקטיביזם
- ריגול עסקי
- לוחמה ממוחשבת (cyber warefare)
- כסף, כבר אמרנו?

כיצד מתקיפים?

איך מתקיפים:

- התקפה פסיבית (למשל ציתות)
- התקפה אקטיבית (למשל שינוי תוכן הודעה שנשלחת ברשת, פריצה למחשב)

תכנון ההתקפה:

- התקפה לא מכוונת (באגים, שכחתי את הסיסמה...)
- ניצול feature
- Social Engineering
- איום מתוכנן
- איום טבעי (אסונות טבע)
- תולעים (worms) – התפשטות מהירה (אפקט כדור השלג)

את מי/מה מתקיפים?

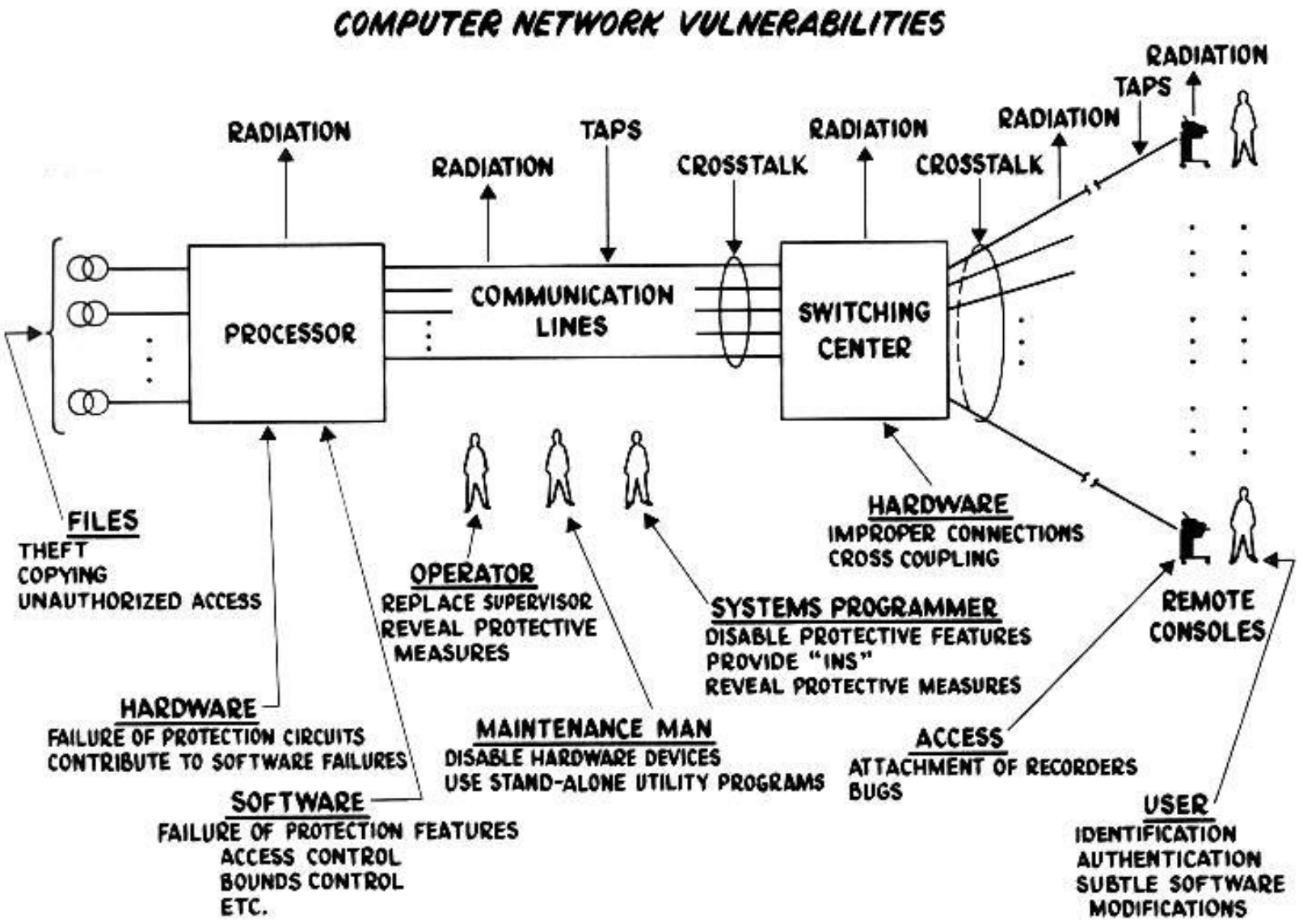
יעד ההתקפה

- נקודתי (שרת מסוים, מאגר נתונים מסוים)
- מערכת מחשוב שלמה (רשת האוניברסיטה)
- כל מערכות המחשב המחוברות לרשת

דוגמאות

- העברת חלקי אגורות לחשבונו של עובד הבנק
- גניבת סרטי גיבוי ומחיקת דיסקים ע"י עובד החברה
- ברכה לחג המולד – סוס טרויאני ב-PostScript
- וירוסים ב- Mail attachments, לדוגמא I Love you
- תשלומים בעזרת כרטיסי אשראי בטלפון (ב-Internet)
- סוס טרויאני - Windows NT registration
- שינוי דף הבית של ה-C.I.A
- Internet Worm, MSBlaster, SQL Slammer,NACHI, Nimda, MyDoom
- פרסום הדיסק של יזהר אשדות בסוף שנות ה-90
- התקפת ה-DDoS על CNN, Yahoo, Amazon ועוד

איומים על מערכות מחשב



הכר את האויב - התוקפים ("האקרים")

- צוותי מחקר במוסדות אקדמאיים
  - מטרה: אנליזה של מערכות
  - (לדוגמא http://www.isaac.cs.berkeley.edu)
- White hats
  - מועסקים ע"י חברות למטרות בדיקת מערכות
  - פועלים עצמאית לזיהוי חולשות במערכות ומדווחים עליהם לחברות
- Gray hats
  - פועלים עצמאית, לעיתים מדווחים, ולעיתים לא
- Black hats
  - זדוניים, לא חוקיים
  - מוטיבציה – כלכלית או פוליטית
- חובבים
  - Script Kiddies
  - משתמשים בקוד וכלים שנכתבו ע"י אחרים
  - לרוב משאירים עקבות

האבולוציה של התוקפים – script kiddies

Chen Ing Hau, Taiwan

Author of CIH virus (AKA Chernobyl), 1999 (written at the age of 24)

Joseph McElroy, UK

Broke into top secret research lab in 2002 (at the age of 16)

Jeffrey Lee Parson, USA

Auther of Variant B of the Blaster worm in 2003 (at the age of 18)

Sven Jaschan, Germany

Author of Netsky and Sasser in 2004 (at the age of 16)

האבולוציה של התוקפים – hacking for profit

Jeremy Jayens, USA

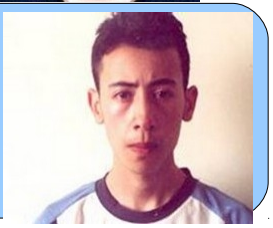
Spammer (earned estimated 24 M$, sentenced for 9 years)

Jeanson James Ancheta, USA

Botnet operator, adware, DDoS, spam, arrested in 2005

Farid Essebar, Morocco

Author of Zotob worm in 2005 (at the age of 18) to facilitate credit card forgeries

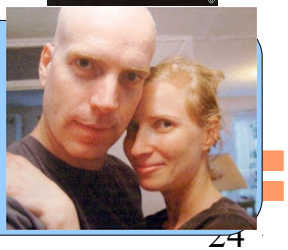


Maria Zarubina, Russia

Wanted for DdoS extortion (2004 and later)

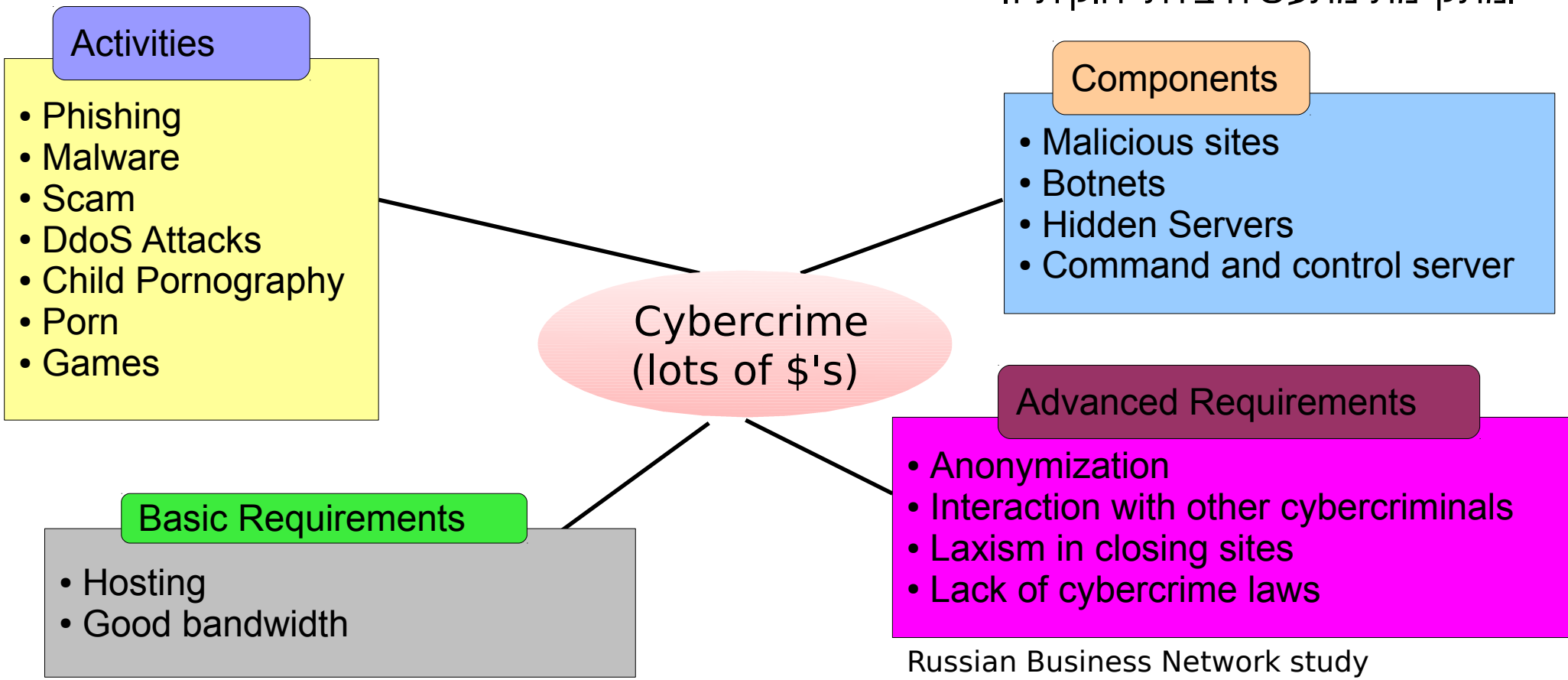
Michael and Ruth Ha'Efrati, Israel

Trojans used for industrial espionage in 2004/5 (4/2 years in prison and Damages of about 1M NIS)



Malware As A Service

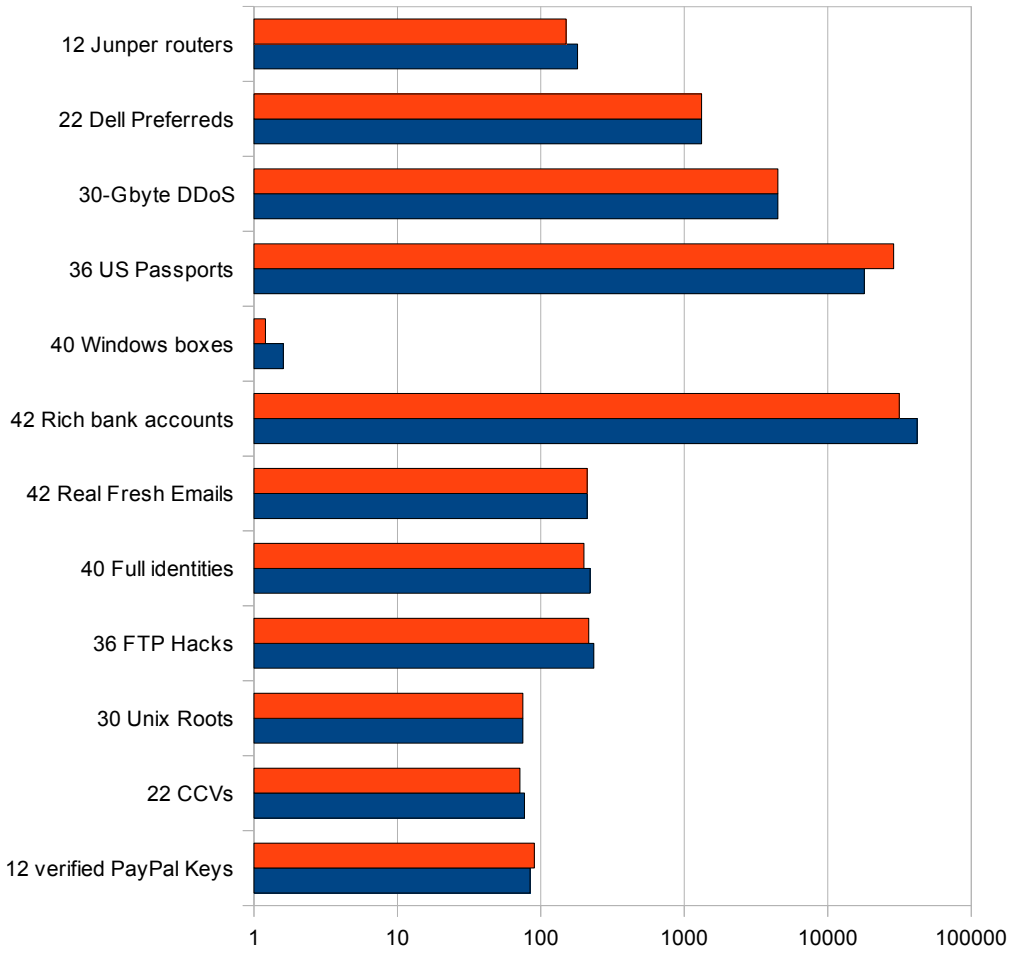
ה-(russion business network) RBN הוא חברה המציעה שירותי hacking
ומתקיימת מתעשיה בלתי חוקית זו



Russian Business Network study
http://www.bizeul.org/files/RBN_study.pdf

כתבה על RBN:
http://www.calcalist.co.il/internet/articles/0,7340,L-3082407,00.html

התמריץ הכלכלי



המחירים ב-$, בסולם לוגריתמי

דן גיר ודניאל קונווי החלו לפרסם בינואר 2008 מדד שנתי למחירי הכלכלה המחתרתית בעיתון IEEE Security & Privacy

- 0PI – The 0wned Price Index

נתונים נוספים מינואר 2009:

- בוטנטים: 100-200 לכל אלף הדבקות, תלוי במיקום
- שירותי דואר זבל: 0.01$ לכל 1000 אימיילים, לפחות 85% יימסרו
- כרטיס אשראי ללא CCV2: בין דולר לשלושה
- כרטיס אשראי עם CCV2: בין 1.5$ ל-10$ תלוי בארץ (ובכרטיס)

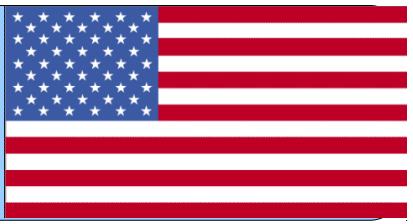
המחירים נקובים בדולר אמריקאי

http://geer.tinho.net/ieee/ieee.geer.0801.pdf
http://geer.tinho.net/ieee/ieee.sp.geer.0901.pdf

האבולוציה של התוקפים – hacking by countries

USA

Arranged for a soviet gas pipe to blow up by hiding vulnerabilities In SCADA systems (1982)

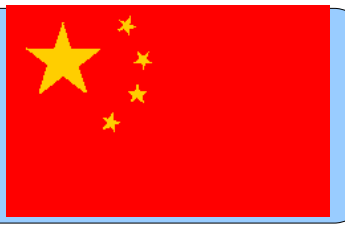


Russia

Attacks on Estonia's internet (following anti-Russian actions by Estonia) that shut down Esotnia's internet (2007)

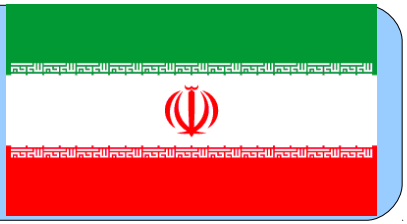
China

Hacking into RSA (EMC's security division) to obtain access to Lockheed Martin's servers (stealing plans of F-35) (2010-2011)



Iran

Hacking into a Dutch Certifying authority (Diginator) to access citizen's email accouts (2011)



הכר את האויב – מקורות מידע

- קבוצות דיון Newsgroups
  - 2600
  - Cult of the dead cow (CDC), etc
- מגזינים
  - Phrack
  - 2600
- כנסים
  - Defcon
  - 2600
  - Usenix
  - Black Hat
  - CCC
- CERT – Computer Emergency Response Team
- Bugtraq
- ועוד...

קישורים למקורות אלה ניתן למצוא באתר הקורס

מדיניות הגנה

מדיניות הגנה: קובעת על מה רוצים להגן וכנגד אילו איומים, במי בוטחים, כיצד מגיבים על התקפות וכו'.

לגבי כל אחד מהאיומים הפוטנציאליים, יש לשקול:

- האם ההתקפה היא מעשית?
- הנזק שעלול להיגרם כתוצאה מההתקפה
- עלות ההגנה נגד האיום
- פגיעה בנוחות המשתמש כתוצאה מההגנה

דוגמאות למדיניות הגנה

- אין הגנה
- הגנה ע"י הסתרה - Security by Obscurity
- הגנה ברמת המחשב - Host Security
  - רמת אבטחה גבוהה
  - לא ניתנת להרחבה, יוצאת מכלל שליטה
- הגנה ברמת הרשת - Network Security
  - הנחה: הרשת אינה חשופה להתקפות פנימיות
- שילוב של הגנה ברמת רשת והגנה ברמת המחשב

כתיבת מדיניות הגנה טובה

כאשר באים לכתוב מדיניות הגנה מומלץ:

- לבדוק כי הפונקציונליות של המערכת נשמרת
- לבדוק דרישות חוקיות (למשל, מידע רפואי חייב להשמר סודי)
- לצרף הסברים לאנשים (לא הסברים טכניים מדי!) כדי שאנשים יבינו מה הם צריכים לעשות
- להסביר מה על כל אדם במערכת לעשות (עובדים/מנהלים/אנשי system)
- מעקב אחרי המימוש (מה קורה אם מישהו עובר על המדיניות)
- תהליך עדכון וטיפול במקרים שלא מכוסים ע"י המדיניות
- למי מגיעים חשבונות ועל אילו מחשבים?
- רמת האבטחה הנדרשת מתחנה לפני שהיא תוכל לקבל שירות?
- כיצד מוגן מידע עסקי רגיש?
- כיצד מוגן מידע אישי רגיש? (גם מבחינת חוק)
- לבדוק עלויות מימוש המדיניות

כתיבת מדיניות הגנה טובה (המשך)

- אילו קבצים מותר להכניס מבחוץ?
- כיצד מתגוננים כנגד וירוסים?
- מי יכול להתחבר לרשת מבחוץ?
- האם לעובדים מותר להוציא חומר מהחברה? ואם כן מה דרישת האבטחה בביתם?
- כיצד אנשי ארגון שנמצאים אצל לקוחות יוכלו להתחבר לרשת הפנימית?
- מהן הדרישות לשרתי המסחר/השירותים האלקטרוניים?
- איזה מידע נחשב מסווג? כיצד הוא מוגן? האם מותר להוציאו?
- במקרה של מספר סניפים לחברה – מה היחס (האבטחתי) כלפי סניפים אחרים?
- האם יש חשבונות משותפים (לפרויקטים, למזכיר המטפל בדוא"ל של המנהלת)?
- מתי סוגרים חשבון (ולמי פונים במקרה של תקלה)?
- למי מהעובדים מותר להתקשר לתוך הארגון? מה דרישות האבטחה ממנו?
- מה לעשות לפני חיבור מחשב לרשת הפנימית?

הקושי בכתיבת מדיניות הגנה טובה

http://taosecurity.blogspot.com/2005/08/soccer-goal-security-i-found-this-ad.html

מנגנוני הגנה

- לאחר בחירת מדיניות ההגנה, יש לבחור מהם מנגנוני ההגנה שבעזרתם מממשים את מדיניות ההגנה.
- בקורס זה נלמד מנגנוני הגנה שונים, כגון:
  - הגנה פיסית
  - סיסמאות
  - Security protocols
  - Firewalls

יש לזכור:

- חוזקה של שרשרת האבטחה היא כחוזק החוליה החלשה ביותר שבה
- אפילו אם מנגנון בודד חסר, המערכת עלולה להיות לא בטוחה

So in war, the way is to avoid what is strong and to strike at what is weak.

Sun Tzu, The art of war

הגנה פיסית

הגנה פיסית

מערכות מחשב נתונות לאיומים פיזיקליים מוחשיים. חלקם מכוונים ליצור נזק, חלקם מזיקים לא בכוונה:

- הפסקות חשמל
- איתני טבע (רעידות אדמה, הצפות, שריפה)
- שדות חשמליים ומגנטיים חזקים
- גניבה פיזית של מחשב (במיוחד נייד) או אמצעי מחשוב אחר (טלפון, כרטיס חכם, וכו')
- חיתוך כבלי תקשורת
- הרס מכוון של חלקי מיחשוב (אלת בייסבול+מסך)
- גילוח שכבות סיליקון מכרטיסים חכמים
- וכדומה...

אמצעי הגנה פיזיים

- מבנים עמידים במקומות בטוחים
- הגנה כנגד ברקים
- גלאי אש, מתזים
- גנרטור חירום
- מספר יחידות יתירות (Redundancy)
- גיבויים בכספת עמידת אש
- גיבויים באתר נפרד
- מערכת תקשורת חירום (דרך מרכזיה נפרדת)
- נעילת ציוד (מחשבים ניידים, קופסאות דיסקים נעולות)

פגיעה "מבפנים" – עובדים ואורחים

- הגבלת הגישה הפיסית למערכת המחשב
  - שומר בכניסה
  - דלת כניסה עם קוד
  - דלת עם סורק רשתית העין / טביעת אצבע
- נעילת חומר רגיש בכספות
- רישום אחר מבקרים באתר
- מצלמות אבטחה
- שמירת מפתחות קריפטוגרפיים בזיכרון מיוחד
  - Disk on Key, Smart Card

קרינה אלקטרומגנטית

- מערכות המחשב פולטות קרינה:
  - המעבד (בד"כ קרינה חלשה, אבל עדיין שמישה לצורך התקפה)
  - ציוד היקפי (דיסקים, מדפסות וכו')
  - צגים (בד"כ קרינה חזקה מאוד)
  - קווי תקשורת
- אמצעי הגנה:
  - סיכוך קווי תקשורת, הפרדה מקווי טלפון
  - הגנה באמצעות כלוב פרדיי
  - יצירת רעש לבן שמסתיר את הקרינה

"זליגת" מידע פיסית

- מערכות המחשב פולטות מידע בדרכים נוספות:
  - זמן החישוב מעיד על איזו פעולה מבוצעת
  - רעש מהמעבד יכול לשמש למציאת אינפורמציה סודית המעובדת בתוכו
  - צריכת האנרגיה מוסרת אינפורמציה על הפעולה המתבצעת (היפוך ביט בזכרון מ-0 ל-1 דורשת יותר אנרגיה מהפעולה ההפוכה)
  - חום הנפלט מהמעבד יכול להעיד על פעולת החישוב המתבצעת בו
  - הרעש שהמעבד משמיע יכול להעיד אף הוא על מה מתרחש בתוכו

- אמצעי הגנה:
  - יצירת פעולות המסוככות על דברים אלה (צריכת אנרגיה קבועה לפעולה, צריכת זמן קבוע לפעולה, משתיק-קול)

Electro-magnetic Pulse (EMP)

- פצצות שמתפוצצות מעל האטמוספרה יכולות לייצר קרינה שהורסת את כל המערכות האלקטרוניות, כולל מחשבים ומערכות תקשורת, מבלי לפגוע בבני אדם ובעלי חיים.
- היום קיימות פצצות EMP שבנויות במזוודות קטנות. ניתן לשלוח אותן עם שליח לכל מקום.

ניתן להגן נגדן באופן חלקי תוך שימוש בכלים הבאים:

- כלוב פרדיי (לא יכול להגן על ערוצי תקשורת)
- טכנולוגיות ישנות (למשל שפופרות רדיו) רגישות פחות ל-EMP, מאשר VLSI. לכן, ניתן להגן על מערכות קריטיות ע"י בנייתן בטכנולוגיות ישנות
- שימוש בחשבוניות חרוזים ☺