על אנונימיות ופרטיות ברשת

"On the Internet, nobody knows you're a dog."

The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20) only for academic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

בשבחה של אנונימיות

ביום-יום אנחנו נהנים (ודורשים) מאנונימיות:

- הצבעות בקלפי
- הבעת דעה (אנונימית או תחת שם כינוי)
- הדלפת מידע "לגיטימית" תוך הגנה על המדליף
- במבחני הערכה (או סיטואציות דומות דוגמת שליחת מאמרים לכנס באופן אנונימי)
- הפגנות המוניות

⇐ אנונימיות מביאה לחופש ביטוי

בחסרונה של אנונימיות

אנשים מבצעים פעולות לא חוקיות (או על גבול החוקיות) תוך ניצול האנונימיות:

- הוצאת דיבה (ללא חשש מתביעה)
- החלפת קבצים
- תקיפות מחשבים (ללא חשש מתביעה)
- הונאות מחשב
- Spam
- החלפת אינפורמציה למטרות לא חוקיות

בשבחה של פרטיות

לכולם יש סודות:

- סטודנט שפתר את בעיית העצירה
- סודות מסחריים של חברות
- מידע רפואי
- מידע חסוי (מידע הקשור לאימוץ ולקטינים)
- מידע פרטי ואישי
- E-commerce

בחסרונה של פרטיות

ישנם מקרים בהם נרצה "לפרוץ" לפרטיות של מישהו (למען מטרה טובה):

- לזהות מידע בעייתי ברשות אדם (פדופיל)
- לזהות אדם שביצע פעולות לא חוקיות
- לזהות אדם העומד לבצע פעולה לא חוקית
- (בעצם כל סיבה שמצדיקה ציתות או חיפוש בחפציו של אדם...)

בעיות פרטיות ואנונימיות ברשת

- מצב הפרטיות והאנונימיות ברשת הינו מורכב
- ישנן לא מעט סיטואציות בהן אנו נהנים מאנונימיות ... לכאורה
- לרוב, מי שמנסה לאתר מי ביצע פעולה מסוימת יכול לזהות את כתובת ה-IP של מבצע הפעולה
- ע"י שילוב עם המידע בידי ה-ISP ניתן לזהות המחשב ממנו בוצעה הפעולה ה"אנונימית"

בעיות פרטיות ואנונימיות ברשת (המשך)

- מרבית המידע העובר ברשת איננו מוצפן ומאובטח כראוי
- לפיכך, כל פריט מידע שמגיע לרשת האינטרנט הוא בחזקת public's knowledge
- מכיוון שאיננו שולטים על העתקתו, שמירתו במטמון, ועוד, הרי שהמידע גם איננו ניתן לעצירה
- לדוגמא http://jya.com/ida-orrd.htm
- או קוד ה-DeCSS

בעיות פרטיות ואנונימיות ברשת (המשך)

- Everything you say may be used...
- למספר רשויות בטחון (ה-NSA, ה-GCHQ, וחברים) ישנה מערכת בשם Echelon המאזינה לכל התעבורה הדיגטלית שהם מסוגלים לשים את ידיהם עליה
- המערכת מסננת את המידע המעניין לצורך אנליזה אנושית

בעיות פרטיות ואנונימיות ברשת (המשך)

המידע הנשלח ברשת חשוף אם כך ל:

- ציתות
- איסוף ושמירה
- Tracing (לצורך זיהוי המקור)

בנוסף, ניתן לזהות את מבצע הפעולה ע"י חקר ה-log של המערכת בה בוצעה פעולה (או ה-log של רכיבי רשת)

בעיות פרטיות – המחשב הביתי

הרבה חברות מבססות את המודל העסקי שלהן על איסוף אינפורמיה על המשתמש:

- spyware
- מעקב דרך cookies
- data mining
- איסוף מידע בעולם הפיסי

spyware

- תוכנה שעוקבת אחר המשתמש
- מותקנת כך שתוכל לאסוף מידע על המשתמש
- לרוב מסתירה את עצמה מהמשתמש וקשה להסירה (תלויית מערכת הפעלה*)
- שולחת את המידע החוצה לחברה שאוספת את המידע (לרוב למטרות פרסומיות)
- בעלת מאפייני התנהגות של סוס טרויאני
- ישנן מספר תוכנות ל"טיפול" בתוכנות אלה

מעקב אחרי פירורי עוגיה (cookie crumbs)

- חברות מסוימות אוספות מידע על הרגלי גלישה ע"י השתלת cookie במחשבו של המשתמש
- ה-cookie מאפשר לזהות לקוח חוזר ולאסוך מידע אודותיו (דוגמת google.com)
- בנוסף, יש חברות אשר שותלות cookies במגוון אתרים
- הלקוח שגולש למספר אתרים שונים נתון למעקב של חברות אלה

שתילת עוגיות

- בשונה מ-spyware להשתלת עוגיות יש את היכולת לעבוד על כל מערכות ההפעלה
- בנוסף, אין בשתילת העוגיה שום פעילות לא חוקית – הדפדפן מבקש עבור המשתמש את העוגיה, ואם הוא לא עושה כן, העוגיה איננה מועברת
- הפתרון הפשוט להגן כנגד עוגיות הוא פשוט לא לאפשר אותן (פוגע בנוחות)

Data Mining

- חברת Walmart סרקה את מאגר הנתונים של לקוחותיה, וגילתה כי 90% מהאנשים שרכשו חיתולים ובירה היו צפויים לרכוש את הירחון sports illustrated
- הידע הזה איפשר לה לשנות את מבנה החנויות ולהשיג תשואה גבוה יותר

Data Mining (המשך)

- היום ישנן שיטות data mining מתקדמות, היודעות לאסוף מידע ממאגרי נתונים גדולים ו"לא מוסדרים" לכאורה
- ע"י אנליזה של מאגר הקניות שביצעתם בעבר, והשוואתו לאנשים אחרים, ניתן ל"פלח" אתכם, ולהבין מה תרכשו בעתיד
- ע"י אנליזה של הדואר שלכם, ניתן להסיק מה נושאי העניין שלכם, ולכן להציע לכם פרסומות שסביר להניח שיעבדו עבורכם

Data Mining – לא הכל רע

- חייבים להבין שרובנו, בסופו של דבר, נהנים מה-data mining הזה
- הצעות שבאמת עוזרות לנו (ספרים מוזלים ב-amazon) או מידע חשוב (data mining שנעשה ע"י קופות חולים) הן דבר שרובנו רוצים
- עם זאת, הבעיה היא מה עושה החברה עם המידע הנצבר
- הבעיה היא, לרוב, העברת המידע לצד שלישי

Data Mining – הזוית החוקית

- ברוב המדינות המתוקנות ישנן חוקים הנוגעים לניהול מאגרי מידע
- בחלק מן המדינות הללו ישנן הגבלות על הזכויות של בעל מאגר הנתונים להעביר אינפורמציה לצד שלישי

- למיטב ידיעתי – בארץ בעל מאגר המידע חייב לרשום אותו, אך איננו מוגבל בנוגע להעברת המידע לצד שלישי
- כיום יש הצעת חוק בנושא שתמנע העברת מידע ללא אישור של המשתמש

העולם האמיתי

- בלשים וריגול עסקי היו קיימים עוד לפני עידן האינטרנט
- באופן מפתיע, הם מצליחים לבצע את עבודתם:
  - מעקב פיזי
  - חיטוט בפחי אשפה (trash-analysis)
  - פיתוי
  - איסוף סמוי מעובדי הארגון (באירועים חברתיים, במתן הטבות וכו')
  - social engineering

Anonymizer

- שרת המוכן ל"כסות" על אחרים
- שרת שכזה הוא בעצם proxy אשר מסיר את כל השדות המזהים של התקשורת שהוא מקבל
- לדוגמא, גלישה באמצעות Anonymizer מתבצעת ע"י התחברות לשרת ה-Anonymizer ובקשה ממנו להביא דפים מאתר אחר
- אפשר לשלוח כך גם דואר, ולבצע מספר רב של פעולות

Anonymizer (המשך)

- כדי להגן על המשתמש, שרת ה-Anonymizer צריך להמנע מלשמור log של הבקשות (ומקורותיהן)
- ניתן להתחבר משרת Anonymizer אחד לאחר, ובכך להקטין את הסיכון לחשיפה
- עדיין ניתן לבצע מעקב אחרי תוכן החבילות ולעקוב אחריה דרך הנתבים ושרתי ה-Anonymizers

Remailer

- Remailer הוא שרת Anonymizer עבור תעבורת דואר
- ישנם remailer-ים המאפשרים גם קבלת דואר
- לצורך כך מוגדר שם כינוי (pseudonym) למשתמש
- שרת ה-remailer דואג להעברה "בטוחה" ולא ניתנת למעקב לאדם האמיתי
- שרתים אלה מצמצמים מאוד את כמות הדואר הנשלח דרכם, למטרות מניעת Spam

הצבעה אלקטרונית (Electronic Voting)

פרוטוקולי הצבעות אלקטרוניים הם מסובכים עקב מגוון הדרישות הסותרות שאנו דורשים מהם:

- פרטיות – לא ניתן לזהות מי הצביע עבור מי
- בטיחות – כל משתתף יכול להצביע פעם אחת, ומי שיכול להצביע הוא מורשה לכך
- אמינות – ספירת הקולות נעשית כך שניתן לוודא שאין רמאות ושכל הקולות הכשרים נספרים
- ניתנות לבדיקה – משתתף יכול לוודא שקולו נקלט ונספר כראוי
- עמידות בפני מכירת קולות אפקטיבית

הצבעה אלקטרונית ורשתות ערבול (Electronic Voting and Mix nets)

- אנו נציג כרגע את אחד הרכיבים המשמשים בפרוטוקולי הצבעות אלקטרוניות, והמשמש לצרכי השגת פרטיות
- נניח כי יש לנו מספר רב של קולות כולם מסודרים בסדר מסוים (לדוגמא שעת ההצבעה)
- אנחנו מעוניינים לערבל אותם בצורה כזו שלאחר הערבול, לא ניתן לזהות את הפרמוטציה שהופעלה
- הערבול נקרא Mix Net ובפרוטוקולים רבים יש מספר שכבות של Mix Nets (שמספיק שאחת מהם תהיה אמינה ותערבל את ההודעות בלי לנסות לעקוב אחריהן, כדי שהערבול יצליח)

רשתות ערבול

- נציין כי ההודעות שיש לערבל מוצפנות תחת מפתח פומבי מסויים (כדי להגן על פרטיות המצביעים)
- אבחנה: יש חובה על שכבת הערבול לא רק לסדר מחדש את ההודעות, אלא גם לשנות את תוכנן
- השיטה הנפוצה הראשונה מבוססת על הצפנה בשכבות (כלומר ההודעה מוצפנית תחת מספר מפתחות פומביים)
- השיטה השנייה (שלא נרחיב עליה את הדיבור) מבוססת על "הצפנה מחדש" (re-encryption)

רשתות ערבול מבוססות שכבות

- נניח כי יש t שרתי ערבול ולכל אחד מהם מפתח פומבי מתאים (PK_i) כאשר המפתחות ידועים לכל המשתמשים במערכת
- תוך התעלמות ממבנה ההודעה המוצפנית m (שמכילה את פתק ההצבעה) כל מצביע מחשב את $PK_1(PK_2(PK_3(...(PK_t(m))...)))$ ושולח את הערך המוצפן לשרת הערבול הראשון
- השרת מפענח את כל הערכים שקיבל, מפעיל עליהם פרמוטציה רנדומית, ושולח את הערכים שקיבל לשרת הערבול השני

רשתות ערבול מבוססות שכבות (המשך)

- השרת השני מפענח את כל הערכים שקיבל, מפעיל על הסדר שלהם פרמוטציה רנדומית ושולח הלאה
- כך התהליך נמשך עד שההודעה m מגיעה לשרתים שאחראים על הספירה

- ניתן להראות שבצורה זו, מספיק שהשרתים לא משתפים פעולה אחד עם השני, לא ניתן למצוא מ-m את $PK_1(PK_2(PK_3(...(PK_t(m))...)))$ ולהפך
- לכן, לא ניתן לגלות (בהנחה ש-m איננה מכילה את זהות המצביע), מי הצביע עבור איזו מפלגה
- הערה: כדי שהאמור לעיל יהיה נכון, פונקציית ההצפנה חייבת להיות רנדומית

רשתות ערבול מבוססות הצפנה מחדש (Re-encryption)

- כמו קודם, נניח כי יש t שרתי ערבול אבל מפתח פומבי ישנו רק לשרת שסופר את הקולות
- כדי שאורך ההודעות המוצפנות לא יגדל ככל שיש יותר שרתי עירבול, וכדי שהמצביעים יצטרכו לדעת רק מפתח פומבי אחד, הם מצפינים את הצבעתם תחת המפתח של השרת הסופר
- את ההודעה המוצפנית הם שולחים לשרת הערבול הראשון, שמבצע Re-encryption של כל ההודעות, כך שהכתב הגלוי לא משתנה, אבל כתב הסתר משתנה
- וכך המידע ממשיך עד הגיעו לשרת שסופר את הקולות

רשתות ערבול – הערות כלליות

- חשוב לזכור כי שרתי הערבול עשויים לנסות ולהשמיט קולות, או לשנות את הקולות
- לכן, הם לא סתם מגרילים פרמוטציה, הם מוכיחים (תוך שימוש בפרוטוקולים קריפטוגרפיים) שהם אינם מרמים, ושהם לא החליפו או מחקו קולות וכו'
- הוכחות אלה (Zero Knowledge Proofs) לא מוסרות שום מידע על הפרמוטציה שנבחרה

ניתוב בצל (onion routing)

- נרצה למנוע מעקב אחרי חבילות ב-on-line
- כמו כן, נרצה למנוע שימוש ב-traffic analysis לצרכי מעקב
- לצורך כך, נגדיר מספר נתבי בצל (onion routers) אשר משמשים לצורך הבטחת אנונימיות

ניתוב בצל (המשך)

- לכל נתב/משתמש P_i יהיה מפתח פומבי PK_i
- אם משתמש s מעוניין בשליחת הודעה m למשתמש r הוא מבצע את הצעדים הבאים:
  - מדפן את ההודעה לאורך נתון וקבוע
  - בוחר באקראי מספר נתבים (עם חזרות, המספר חסום) ומקבל סדרה של נתבים P_i
  - *לאחר מכן, המשתמש מצפין את m תחת המפתחות הפומביים של הנתבים ושולח ל P_1 את*

$$PK_1(P_2, PK_2(P_3, PK_3(\ldots(P_t, PK_t(P_r, PK_r(m)))\ldots)))$$

ניתוב בצל (המשך)

- נתב המקבל את ה"בצל" מפענח את ההודעה שקיבל ומוצא את היעד הבא
- כדי למנוע זיהוי של כמה נתבים נותרו בדרך – הנתב מוסיף מידע דמה בסוף החבילה
- יש להמנע מהוספת מידע דמה שיזוהה ע"י הנתב הבא (כך הוא ידע מה מספר הנתבים שהחבילה עברה דרכם)

ניתוב בצל (המשך)

- כדי למנוע traffic analysis על הנתבים לשמור על נפח תעבורה קבוע ביניהם ע"י שליחת חבילות דמה
- *מספיק שאחד מהנתבים בדרך הוא אמין ומבצע את תפקידו נאמנה כדי שלא ניתן יהיה לאתר את החבילה* (בהנחה שחבילות הדמה אינן ניתנות לאבחנה מחבילות רגילות)

חתימה ייעודית (designated verifier signature)

- נניח כי זוג חברות מנהלות משא ומתן עסקי
- במהלך המו"מ עוברות הצעות לחוזה בין הצדדים
- ההצעות עוברות בדואר אלקטרוני וכדי למנוע זיוף של הצעה מאחד הצדדים – ההודעות חתומות

- במקרה כזה, נוצרת "זיקה חוזית" אשר הצדדים לא בהכרח מעוניינים לייצר
- בנוסף, אחד הצדדים מסוגל להוכיח לאחרים את דבר קיום ההסכם הסופי – דבר אשר לא בהכרח נרצה בו

חתימה ייעודית (המשך)

- חתימה ייעודית היא חתימה אשר החותם מכוון את חתימתו למקבל
- המקבל יכול לוודא את החתימה
- אך אף אחד ממנו אינו יכול לוודא כי החתימה תקפה
- לרוב, דרישה זו ממומשת ע"י שימוש בחתימה אשר גם המקבל היה יכול לייצר (באופן הדומה ל-MAC)

חתימות להדלפה אנונימית ומאומתת (ring signatures)

- שר מעוניין להדליף מידע מישיבת הממשלה לעיתונאי בצורה אנונימית
- הוא יכול לשלוח מידע לעיתונאי דרך שרת anonymizer
- במקרה זה, העיתונאי לא יאמין להודעה
- הוא יכול לחתום על ההודעה באמצעות חתימה דיגיטלית
- במקרה זה – הוא איננו אנונימי

חתימות להדלפה אנונימית ומאומתת (ring signatures)

- ring signatures הינן חתימות בהן החותם מוכיח כי הוא אחד מקבוצה
- אין צורך לקבוע את הקבוצה מראש
- אין דרך לדעת מי מהחברים בקבוצה הוא החותם האמיתי
- אין צורך לייצר מפתחות חתימה פומביים מיוחדים לצורך כך (ניתן ל"התעלק" על מפתחות חתימה קיימים)
- בצורה זו, השר יכול לחתום בתור אחד מחברי הממשלה, והעיתונאי יכול לוודא את החתימה

דוגמא ל-ring signatures

- נניח שימוש ב-RSA (אפשר לעבוד עם כל שיטת חתימה)
- כמו-כן, נניח כי יש בידינו פונקציית הצפנה בטוחה (AES) ופונקציית תמצות בטוחה

- יהיו r חברי הקבוצה בעלי r מפתחות RSA ציבוריים מן הצורה (n_i, e_i)
- נסמן הצפנה של מחרוזת x תחת (n_i, e_i) ב- $f_i(x)$

דוגמא ל-ring signatures (המשך)

- יהי b מספר סיביות הארוך משמעותית מכל אורכי המודולי (n_i)
- נגדיר את הפונקציות הבאות:

עבור $m = q_i n_i + r_i$:

$$g_i(m) = \begin{cases} q_i n_i + f_i(r) & if\ (q_i+1)n_i \le 2^b \\ m & else \end{cases}$$

- יהי s חבר הקבוצה המעוניין להדליף את המידע (ולכן הוא מסוגל לחשב את $f_s^{-1}(x)$)
- כמו כן נגדיר את $C_{k,v}(y_1, y_2, \ldots, y_r)$ להיות

$$C_{k,v}(y_1, y_2, \ldots, y_r) = E_k(y_r\ XOR\ E_k(y_{r-1}\ XOR \ldots E_k(y_1\ XOR\ v)\ldots))$$

דוגמא ל-ring signatures (המשך)

אלגוריתם החתימה ע"י s על הודעה m:

- חשב $k=h(m)$
- בחר v באופן אקראי (באורך b סיביות)
- בחר עבור כל $i \neq s$ ערך x_i אקראי (באורך b סיביות) וחשב $y_i=g_i(x_i)$
- מצא y_s כך ש- $C_{k,v}(y_1, y_2, \ldots, y_r)=v$
- חשב $x_s=g_s^{-1}(y_s)$
- החתימה היא $(P_1, P_2, \ldots, P_r; v; x_1, x_2, \ldots, x_r)$ כאשר P_i הוא המפתח הפומבי של i

דוגמא ל-ring signatures (המשך)

בדיקת החתימה על הודעה m:

- חשב $k=h(m)$
- *לכל* i *חשב את* $y_i=g_i(x_i)$
- *בדוק כי* $C_{k,v}(y_1, y_2, \ldots, y_r)=v$

חתימות עיוורות (blind signatures) וכסף אלקטרוני

- בעתיד כסף אלקטרוני יהיה בשימוש
- ה"מטבעות" יחתמו ע"י רשות שזכותה להנפיק מטבעות (לדוגמא, בנק)
- מכיוון שכל מטבע נוצר ע"י הבנק, הוא יכול לעקוב אחרי מי קיבל ממנו את המטבעות, ומה הוא עשה איתם
- יש כאן פגיעה בפרטיות! ניתן לזהות תורמים למפלגות, מיטיבים אנונימיים, וכו'

חתימות עיוורות וכסף אלקטרוני

- את "הטבעת" המטבעות מבצע הבנק בתמורה לכסף אמיתי (מחסיר מהחשבון)
- המטבע הוא בעצם מעין צ'ק שהבנק משלם למי ש"מפקיד" את הצ'ק
- נתעלם מהמנגנונים שמונעים ממישהו להפקיד פעמיים את אותו צ'ק (או להשתמש בו פעמיים)

חתימות עיוורות וכסף אלקטרוני (המשך)

- לכן, לצרכי פרטיות, המשתמש הוא זה שיציע את הצ'ק שעליו יחתום הבנק
- הבנק לא יידע על מה הוא חותם...
- אבל יוכל לזהות ניסיונות רמאות

חתימות עיוורות - דוגמא

- נרצה שבעל המפתח הפומבי (n_U, e_U) (והפרטי המתאים) יחתום על הודעה m
- נבחר כ-100 מחרוזות $m_1, m_2, \ldots, m_{100}$ בעלות תוכן זהה
- כמו כן נבחר באקראי כ-100 גורמים מעוורים $a_1, a_2, \ldots, a_{100}$
- נבקש חתימה על אחד מ-100 הערכים
- $m_1 a_1^{e_U}, m_2 a_2^{e_U}, \ldots, m_{100} a_{100}^{e_U}$
- **החותם** יבחר באקראי $1 \le r \le 100$ ויבקש את $a_1, a_2, \ldots a_{r-1}, a_{r+1}, \ldots, a_{100}$

חתימות עיוורות - דוגמא (המשך)

- לאחר קבלת 99 ערכי a_i החותם יכול לבדוק את 99 ההודעות הרלוונטיות (האם הן כאלה שהוא מוכן לחתום עליהן)
- אם הבדיקה מצליחה הוא חותם על $m_r a_r^{e_U}$
- כלומר הוא שולח חזרה את $sig = (m_r a_r^{e_U})^{d_U} = m_r^{d_U} a_r$
- המקבל שיודע את a_r מחשב את $m_r^{d_U}$ ויש לו חתימה תקיפה (שחתם הבנק) על m_r
- *החותם איננו יודע את m_r וזאת למרות שחתם עליו!*

הצפנת תעבורה

- ניתן למנוע מ"האח הגדול" לקרוא את הדואר שלנו ע״י הצפנתו
- בצורה זו ניתן להסתיר את המידע העובר בתקשורת
- עם זאת, בסיטואציה זו, גם תקשורות שאנו מעוניינים ש"האח הגדול" יאזין להן עמידות בפניו

שירותי ליווי למפתח (Key Escrow)

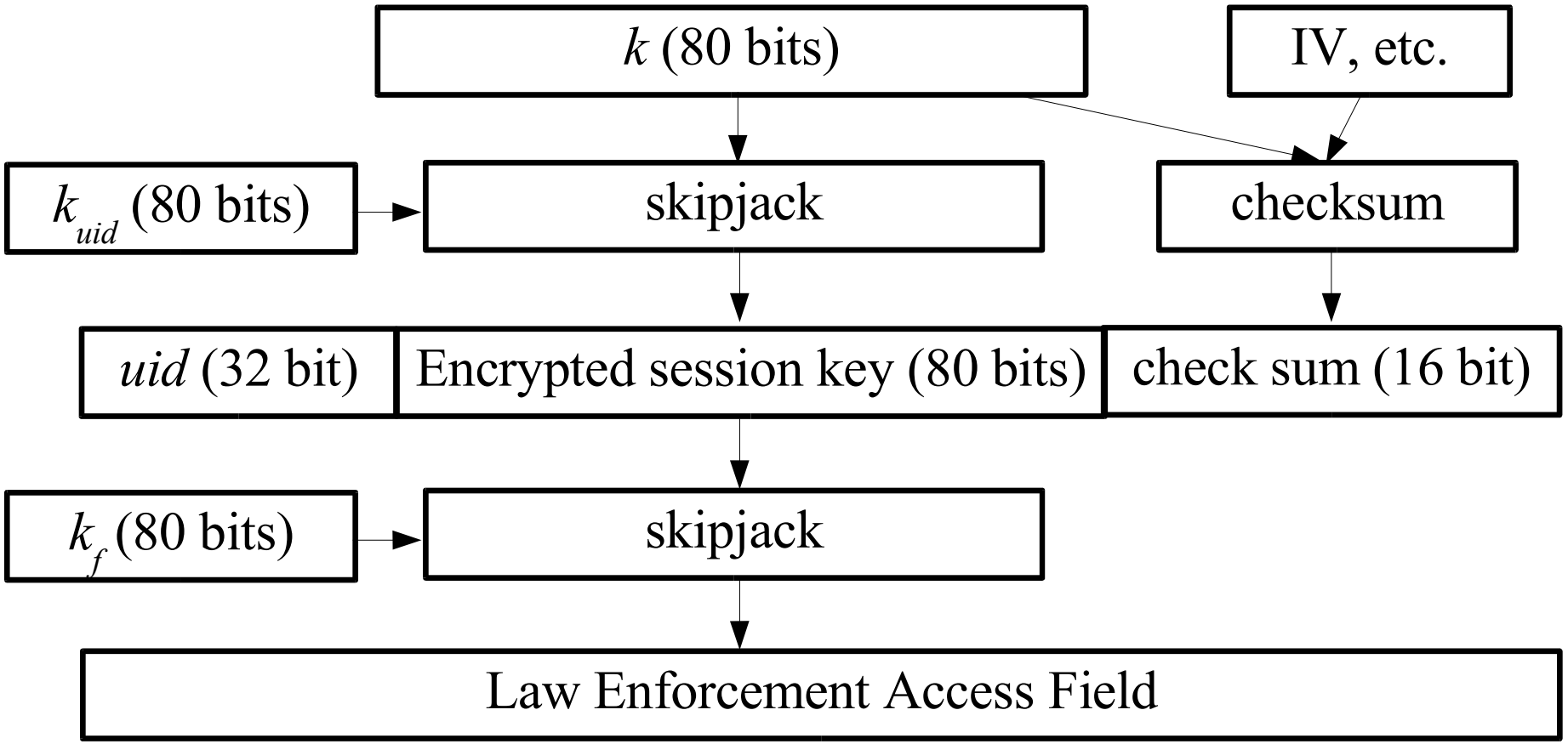
- רעיון ה-key escrow הוא בבסיסו שליחת המפתח ששימש להצפנת המידע יחד עם המידע
- כמובן, שהמפתח איננו נשלח גלוי
- דרישות ממערכת key escrow:
  - המידע המועבר מוצפן
  - לגוף רשמי יש את האפשרות לפענח את השיחה
  - הגוף הרשמי יכול לפענח את השיחה רק לאחר צו שופט (או גוף מבקר)

FIPS 185 (Skipjack,KEA)

- לכל רכיב המממש את התקן יש מספר יחודי – uid ומפתח ייחודי של המכשיר k_{uid}
- *כמו כן, לכל הרכיבים ממשפחה מסוימת ישנו "מפתח משפחה"* k_f הידוע לרשויות
- משתמש לצורך הצפנה בצופן Skipjack (גודל בלוק 64 סיביות, גודל מפתח 80 סיביות)
- שני צדדים המעוניינים לשחוח ביניהם מסכימים על מפתח סודי משותף k בן 80 סיביות (תוך שימוש ב-KEA) שמבוסס על Diffie-Hellman

FIPS 185 (Skipjack,KEA)

* הרכיב המצפין מחשב LEAF:



FIPS 185 (Skipjack,KEA)

- כשהרשות מעוניינת לפענח הודעה מוצפנית, היא מפענחת את ה-LEAF ומשחזרת את ה-*uid*
- בהנתן ה-*uid*, היא ניגשת לטבלה האוצרת את כל זוגות ה-(uid, k_{uid}) ומשחזרת את k_{uid}
- באמצעות k_{uid} הרשות מפענחת את ה-encrypted session key ומוצאת את k.

אבל ...

- כעת הרשות מסוגלת לפענח כל הודעה מוצפנית, ללא בקרה!
- לכן, את הטבלה של זוגות ה-(uid,k_{uid}) לא שומרת רשות אכיפת החוק
- הטבלה מחולקת תוך שימוש בסכימת חלוקת סוד (secret sharing scheme) לשני גופים בלתי תלויים
- רק כאשר שני הגופים מוסרים את השתף שלהם, יכולה הרשות לשחזר את k_{uid}

סוגיות נוספות

- מרגע שניתנה לרשות גישה ל-k_{uid} היא מסוגלת לקרוא גם הודעות קודמות (כאלה שעבורן הצו המאפשר ציטוט אינו תקף)
- גם מנגנון המבטיח שינוי חד-כיווני כל יום של k_{uid} לערך אחר, יאפשר לרשות לפענח גם את כל ההודעות העתידיות
- הרכיב יכול לשבש את ה-LEAF שהוא מוציא (ע"י שינוי מצד המשתמש)

מספר פתרונות לסוגיות שהועלו

- פתרון לבעיית מציאת המפתח היא partial key escrow בו הרכיב מצהיר רק על חלק מהמפתח שנבחר k
- בצורה זו, הרשות המאזינה צריכה להשקיע מאמץ בכל הודעה שברצונה לפענח (ולא יכולה לפענח את כל התקשורת)
- ישנן מנגנונים קריפטוגרפיים המאפשרים לרכיב ההצפנה להוכיח כי הוא אכן מצהיר על המפתח (חלק המפתח) הנכון באופן שאיננו מדליף שום מידע על המפתח k