אינטרנט, מַעֲשֶׂה אוֹרְגִים

נכתב ע"י אמיר שגיא

הקדמה

"...הירו אקרמן יושב בחדרו שבשכונת יעלים בערד. הוא מביט מרוצה במסך שעה שקליינט הטורנט נוגס במהירות 2 מגה לשנייה דרך ISO ההתקנה של Debian 8.0. הוא נעזר בשלושה עמיתים אליהם הוא מחובר באריג - הרחוק מבניהם נמצא בצד השני של העיר, ואילו לקרוב מבניהם קיים קו ראיה המשמש את קישור לייזר ה-ethernet שביניהם. מזמן הוא נטש את תדרי הג'יגה בעת התחברות לרשת. שבב הרדיו בכרטיס האלחוטי שלו מדלג ביעילות האופיינית למודולצית spread spectrum באזור ה-700 מה"צ בין ערוצי טלוויזיה נטושים.

את יכולת הבלוטות' הוא ביטל ממזמן, אין לו צורך בה וממילא הוא נגד זיהום אלקטרומגנטי - מהסיבה הזו הראוטר חי בגג, מוזן ע"י POE ממרכזית הרשת הביתית. את הזמן הוא מנצל לעיון נוסף בחוברת ההדרכה של חבילת OpenBTS 4.2, איתה יוכל להפעיל תא GSM מקומי, 120 מג"צ מתחת לתדר הסטנדרטי. משם, עם קצת מינהור VoIP, יוכל לתעל שיחות לתא סלולארי נוסף שפועל באריג תל אביב. אכן, נראה ששינוי עומד באופק. מאותת לו שההורדה הסתיימה, שעה שהוא סוגר חלון מפני הקור המדברי".[54321]

נשמע כמו קטע מספר של ניל סטיבנסון? לא בדיוק - מדובר בעתיד לא כל כך דמיוני לעולם הרדיו הדיגיטלי, עתיד אותו פרויקט אריג עוזר לעצב. הסיפור מניח שישראל, כמדינות נוספות בעולם, הלכה בעקבות יוזמת שיחרור התדרים בתחום 470-790 מגה"צ, הידועים בשם "TV white-space"[6]. השינוי כמובן לא נעשה באופן מתוכנן, אלא לאחר ששלל גורמים הביאו אותה להכרה בכשלון מדיניות הקצאת התדרים, במיוחד לאור הגידול הגיאומטרי בדרישה לרוחב פס. אבל אנחנו כאן כדי לדבר על אריג, ולשם כך אנחנו צריכים תחילה כמה הגדרות.

[1] White space radio by Carlson @ 470 MHz - http://www.carlsonwireless.com/products/RuralConnect.pdf
[2] Frequency-hopping spread spectrum - http://en.wikipedia.org/wiki/FHSS
[3] OpenBTS - http://en.wikipedia.org/wiki/OpenBTS
[4] תקשורת אופטית - http://en.wikipedia.org/wiki/Free-space_optical_communication
[5] spread spectrum מודולצית - http://en.wikipedia.org/wiki/Spread_spectrum
[6] FCC white-space decision - http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-260A1.pdf

מושגים

אריג: אריג (Mesh) הינה טופולוגיות רשת. לרוב רשתות שאינם מפגינות מבנה מובהק אחר (Star, Bus, וכו') מסווגת כאריג.

אריג-קהילתי: קבוצת משתמשים המקיימים תקשורת דיגיטלית ביניהם, לרבות WiFi, Ethernet, Optical fiber ליצירת רשת בטופולוגית אריג.

אינטרנט: לצורך הדיון נניח כי מדובר בצאצאה של ARPANET, רשת המחשבים דרכה אנו גולשים ל-wikipedia.org כיום.

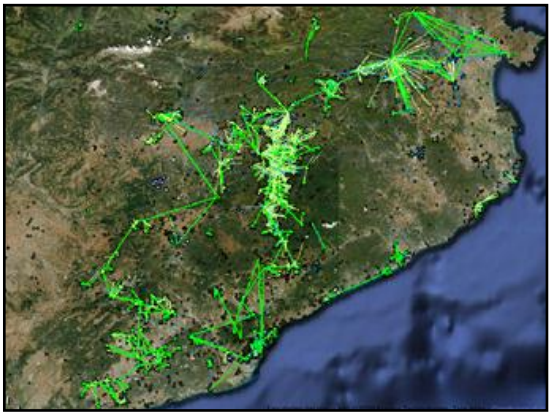
ספק-אינטרנט: כמה שהמושג נשמע ברור, הוא אולי זה שדורש הכי הרבה הבהרה: השם מבוסס על ההנחה שלאינטרנט מבנה אפשרי יחיד והיררכי. האמת היא שקיים מבנה אפשרי נוסף, שטוח, וביניהם אפשר לדמיין אינסוף מבני הכלאה. משתמש שמחובר לספק ומריץ שרת כלשהו, כגון Skype, הופך לחלק מהאינטרנט, ומכאן שניתן לראות בו עצמו כספק-אינטרנט.

שורש הסתירה בתפיסת האינטרנט כמשהו שעבורו קיים מקור יחיד. להמחשה, הנה תרגיל מחשבתי: דמיינו רשת אריג בעלת n צמתים, המחוברת ל-ARPANET דרך צומת מוצא יחיד. כעת שחקו עם הערך של n עד שהמשפט הבא יקבל ערך אמת: "האריג הוא האינטרנט". בשלב זה הופך האריג לספק האינטרנט של ספק האינטרנט. עבורי n=1.

אריג הוא גם שם העמותה שבמסגרתה פועל הפרויקט, אז אולי מכאן כדאי להמשיך בתיאור הנפשות הפועלות.

מי אנחנו?

עמותת אריג - **קהילת רשת האריג בישראל** פועלת לביסוס וקידום קהילת האריג בישראל. הרעיון הבסיסי פשוט - לרתום חומרה שברשותנו על מנת ליצור רשת שאינה דומה לשום רשת תקשורת שאנו מכירים עד כה - מבוזרת, בבעלות קהילתית, שביסודה עקרון חופש זרימת המידע ונגישותו. רשת שכזו כמובן תהווה תקדים בכל הנוגע לכמות המשתתפים שיוכלו לקחת בה חלק כמו גם בכמות המידע שתוכל להעביר על גבי תשתית שיתופית.



[מפת רשת guifi.net שבקטלוניה]

קהילות אריג פועלות זה זמן רב במגוון מקומות בעולם, כדוגמאת רשת freifunk.de החלוצית בגרמניה, רשת funkfeuer.at שבוינה, רשת awmn.net הפועלת בין איים ביוון, ורבות נוספות - כולן רשתות המונות אלפי משתתפים. בקטלוניה שבספרד, ביתה של אחת מרשתות האריג הגדולות בעולם, נערך זה עתה כנס IS4CWN[7], אירוע העוסק בסוגיות שונות הקשורות לרשתות אריג בהיבט בינלאומי. Guifi.net היא הראשונה שהחלה בפריסת רשת סיבים אופטיים כחלק מפיתוח הרשת, ובשיתוף עם ה-cat TLD. כבר מחוברת ל-IX CATNIX בברצלונה.

תיאור טכני

ברשת אריג אלחוטית, כל קודקוד הוא נתב המסוגל לשדר ולקלוט הודעות בסביבתו וכל צלע היא קישור אלחוטי הנוצר בין שני נתבים המצויים בטווח קליטה זה מזה. נתב מהווה מקור מידע וכן צומת ממסר להודעות המועברות בין נתבים אחרים. כל נתב מריץ פרוטוקול ניתוב האחראי ל:

1. **פרסום עצמי** - פרסום נוכחותו בהודעות Broadcast כך ששכניו יוכלו ללמוד על קיומו.
2. **גילוי שכנים** - נתב מאזין להודעות פרסום ובכך לומד מי נמצא בסביבתו המקומית.
3. **פרסום ושידור חוזר של הודעות טופולוגיה** - כל נתב מפרסם באופן מחזורי את טופולוגית הרשת הסמוכה לו. נתבים גם משדרים שנית הודעות שנקלטו מנתבים אחרים בסביבתם, ובכך מאפשרים להודעות להתפשט בקפיצות ברדיוס קבוע כלשהו.
4. **תחזוק טבלת ניתוב** - מבנה נתונים שבעזרתו יוכל לקדם הודעה הממוענת לכל צומת אחר ברשת, אם לא ישירות ליעדה אז לפחות בכיוון כללי שיקרב אותה לשם.

משימת הפרוטוקול היא למזער את כמות ההודעות המשמשות ליצירת הרשת ועדכון טבלאות הניתוב בנתבים ביחס לכמות המידע הממשי שזורם בה. חשוב לזכור שמבנה הרשת מצוי בשינוי תמידי - לדוגמא, צומת שלא יפרסם את קיומו יוסר מטבלאות הניתוב לאחר פרק זמן מסויים, דבר שמקנה יכולת 'ריפוי-עצמי' לרשת. עדכון מבנה הרשת הוא תהליך אוטומטי ושקוף למשתמש, שאחראי להתקנת פרוטוקול הניתוב בלבד. דוגמאות בולטות למימושי פרוטוקולים הם: OLSR, BATMAN ו-BMX.

[7] מצגת פרויקט אריג מהכנס: http://taproot.org.il/content/presentation/is4cwn/2012/is4cwn-2012.tar.bz2

כיצד רוקחים צומת אריג ? נעזר במודל השכבות (ההפוך) של **OSI**:

Physical	נחפש חומרת רדיו מתאימה לתדרי היעד, 2.4 גה"צ לרשתות g802.11 או 5 גה"ץ לרשתות a802.11. נקודת המפתח היא קיום דרייבר שיאפשר לנו שליטה מלאה על מאפייני הרדיו של החומרה. אנו עושים שימוש בהפצת OpenWRT לשם כך, המתמחה בחומרת Emedded, תוך התייעצות עם דף החומרה הנתמכת.
Data Link	בניית שכבת קישוריות זו היא משימתו של פרוטוקול הניתוב. הפקודה הבאה במערכת מבוססת OpenWRT תדאג להתקנת חבילת OSLR, המממשת פרוטוקול אריג כשרת הפועל בחסות מערכת ההפעלה: root@OpenWrt:~# opkg update && opkg install olsrd אופציה נוספת היא לעשות שימוש בפרוטוקול BATMAN, הפועל כמודול ברמת הקרנל - לשם כך כבר נצטרך לקנפג ולבנות קרנל מתאים עם תמיכה במודול. אופציה שלישית היא לא להשתמש כלל בפרוטוקול אריג! במידה והרשת סטטית, נגדיר מראש טבלאות ניתוב בכל נתב. פתרון זה אמנם אינו גמיש, מועד לטעויות וקשה לתחזוקה, אך עדיין מהווה מימוש אידאלי לרשתות קטנות.
Network	השמת כתובת ברשת היא משימה אליה נצטרך להתכונן מעט, תוך מימוש מערכת שתבטיח את יחידות כל כתובת ברשת. המשימה הופכת יותר מסובכת אם בכוונתנו להשם כתובות IPv6 במקביל לכתובות IPv4. מכל מקום הגדרות אלו הן דבר שנספק למימוש פרוטוקול הניתוב בו נשתמש, למשל בקובץ olsrd.conf.
Transport	מרגע ששכבת ה-Network קיימת, העובדה שמדובר ברשת אריג שקופה לפרוטוקולים משכבה זו כגון UDP, TCP וכו'. מה שחשוב להבין הוא שבכל רגע נתון הניתוב לעבר אתר יעד ב-ARPANET יכול לצאת לכיוון צומת gateway אחר כתוצאה משינוי בטופולוגית האריג / תמחור נתיבים וכו'.
Application	גם כאן נוכל לעשות שימוש בפרוטוקולים מוכרים. שימוש ב-HTTPS, SSH וכו' הופך קריטי בשל השימוש בתווך הרדיו, אליו כל אחד יכול להאזין.

עד לפני מספר שנים היכולת להפעיל ראוטרים צרכניים במתכונת של רשת אריג היתה רחוקה מלהיות פשוטה, ובוודאי שלא מה שמתכנני המוצר חשבו עליו. שחרור קוד המקור של נתב מפורסם בשם Linksys WRT54G, הביא לפריחה של קוד פתוח סביבו, לרבות הפצות לינוקס כגון OpenWRT הקרויה על שמו. שחרור הקוד נעשה בעקבות הגילוי כי הוא מכיל קוד GPL, מה שמחייב את שחרורו גם כן. ב-2003, בסוף הליך משפטי אולצה Linksys משפטית לעשות כן.

עם הריבוי בכמות ומגוון החומרה עבור פרוטוקולי 802.11, מאמץ רב הושקע בהשגת יכולות שליטה מלאות על אופי פעולת שבבי הרדיו, לרבות תמיכה במוד monitor בו השבב קולט תעבורה מבלי להיות משויך ל-access point, מוד ad-hoc המאפשר ליצור רשת ללא AP, או מוד mesh המאפשר יצירת רשת אריג. די להביט בכמות הדרייברים להם בוצע הינדוס הפוך בכדי להתרשם מכמות המאמץ שהושקעה ב"שיחרור" חומרת הרדיו שפותחה עבור 802.11. כמובן שנעדיף דרייברים שפותחו כקוד פתוח, שכן ביצועיהם ויציבותם עדיפים על פני כאלו שהונדסו לאחור.

עיון בפלט (חלקי) של שרת olsrd בעת פעולה מסביר קצת מה קורה מאחורי הקלעים:

```
# olsrd -d --config ./olsr.conf
*** olsr.org - 0.6.2-git_d14ce85-hash_122963f7f79c8c44d97e9af319b969ff - ***
Build date: 2012-03-12 04:00:03 on openwrt-test-node-01
http://www.olsr.org

Debug level: 1
IpVersion: 4                                                    #1
...
NIC Changes Pollrate 3.00
FIBMetric: flat
Hysteresis disabled
TC redundancy 2
MPR coverage 3
Link quality fish eye 1                                         #2
LQ Algorithm: etx_ff                                            #3
setting ifs_in_curr_cfg = 0
       IPv4 broadcast: 255.255.255.255                          #4
       IPC host: 127.0.0.1
Plugin: olsrd_txtinfo.so.0.1
Plugin param key:"accept" val: "127.0.0.1"
       IPv4 broadcast/multicast : 255.255.255.255
       Mode      : mesh
       IPv6 multicast      : ::
       HELLO emission/validity : 0.00/0.00
       TC emission/validity   : 0.00/0.00
       MID emission/validity  : 0.00/0.00
       HNA emission/validity  : 0.00/0.00                       #5
       Autodetect changes    : no
...
---- Interface configuration ----
Checking tap1:
       Not a wireless interface                                 #6
       Metric: 0
       MTU - IPhdr: 1472
       Index 7
       Address:114.134.23.236
       Netmask:255.255.255.240
       Broadcast address:255.255.255.255
New main address: 114.134.23.236
Using 'etx_ff' algorithm for lq calculation.
TC: add entry 114.134.23.236
RIB: add prefix 114.134.23.236/32 from 114.134.23.236
...
Scheduler started - polling every 0.050000 ms                   #7
...
```

1. OLSR תומך בהקמת אריגים מבוססי IPv6 או IPv4.
2. הגדרה המאפשרת לנתב שלנו לעקוב ביתר אדיקות אחרי שינויים בסביבתו הקרובה. רשתות אריג סבלו בעבר ממגבלת גודל שנבעה מהגידול האקספוננציאלי שחל בכמות הודעות הבקרה ביחס לגידול במספר הצמתים ברשת. עקרון ה-Fish-Eye מקנה לצמתים תמונת עולם מוטה (עדכנית יותר) לטובת צמתים קרובים יותר, ובכך מקטין את כמות הודעות הבקרה השייכות לצמתים מרוחקים.
3. שיטת אומדן טיב הקשרים ברשת - אנו עוסקים בתקשורת אלחוטית בה אנו מצפים שחלק מההודעות לא יגיע ליעדן בשל הפרעות בתווך. עם זאת קיימות שיטות שונות לאומדן מרחק בין צמתים (לדוגמא ספירת מספר הדילוגים בין צמתים לעומת סכימת טיב הקשרים ביניהם). כאן אנו מגדירים שימוש בשיטת אומדן בשם etx_ff.
4. כתובת ה-broadcast , דרכה מודיע הצומת שלנו על קיומו.
5. קיצור ל-"Host Network Announcement" - רשתות (subnets) אותן אנו מפרסמים כנגישות דרכנו - לדוגמא HNA של 0.0.0.0/0 בעצם אומר שאנחנו צומת מוצא עבור כל כתובת.
6. ניתן לקנפג את olsrd להשתמש בממשקים שאינם אלחוטיים כלל וכן בתרחישים מעורבים.
7. זהו - מאותו רגע שרת olsrd מבצע את משימות הפרוטוקול באופן מחזורי.

מרגע שאנו לומדים על צומת כלשהו, הוא הופך נגיש עבורנו, לרבות רשתות HNA (או HNA6) עליהן הוא מכריז. לדוגמא, ברירת המחדל של צמתים ברשת freifunk.de היא להריץ דף HTTP הכולל מידע בסיסי אודותם, בו ניתן לקרוא הודעות שמפעיל הצומת בחר להוסיף. כאמור, היתרון המרכזי בשימוש ב-OLSR על פני ניתוב סטטי הוא תמיכת הרשת בהופעה/העלמות של צמתים כפי שניתן לצפות ברשת אריג.

לאחר זמן המתנה קצר נוכל לבדוק את מודעות הצומת שלנו לסביבתו באריג:

```
$ wget -q -O- http://127.0.0.1:2006/all | head -n 32
Table: Links
Local IP     Remote IP    Hyst.  LQ     NLQ    Cost
114.134.23.236      114.134.23.225      0.00   1.000  1.000  1.000

Table: Neighbors
IP address   SYM    MPR    MPRS   Will.  2 Hop Neighbors
114.134.23.64YES    YES    NO     3      18

Table: Topology
Dest. IP     Last hop IP  LQ     NLQ    Cost
10.22.1.128         10.22.2.0    0.921  0.788  INFINITE
10.22.2.64          10.22.3.0    0.596  0.944  1.774
10.22.2.224         10.22.3.0    1.000  1.000  1.000
10.22.2.64          10.22.4.0    0.635  0.839  1.875
114.130.1.66        114.135.0.1  0.827  0.450  2.680
114.12.92.82        114.161.0.1  1.000  1.000  INFINITE
114.13.1.2          114.13.1.1   0.788  0.843  1.504
114.13.1.5          114.13.1.1   0.835  0.886  1.351
114.13.2.14         114.13.1.1   0.847  0.944  1.249
114.13.1.121        114.13.1.1   0.780  0.792  1.617
114.8.8.3           114.85.1.1   0.298  0.195  17.111
114.13.8.33         114.85.1.1   0.298  0.195  17.111
```

```
114.8.0.101          114.85.1.1    0.195  0.298  17.111
114.129.2.5          114.129.2.1   1.000  1.000  1.000
…
```

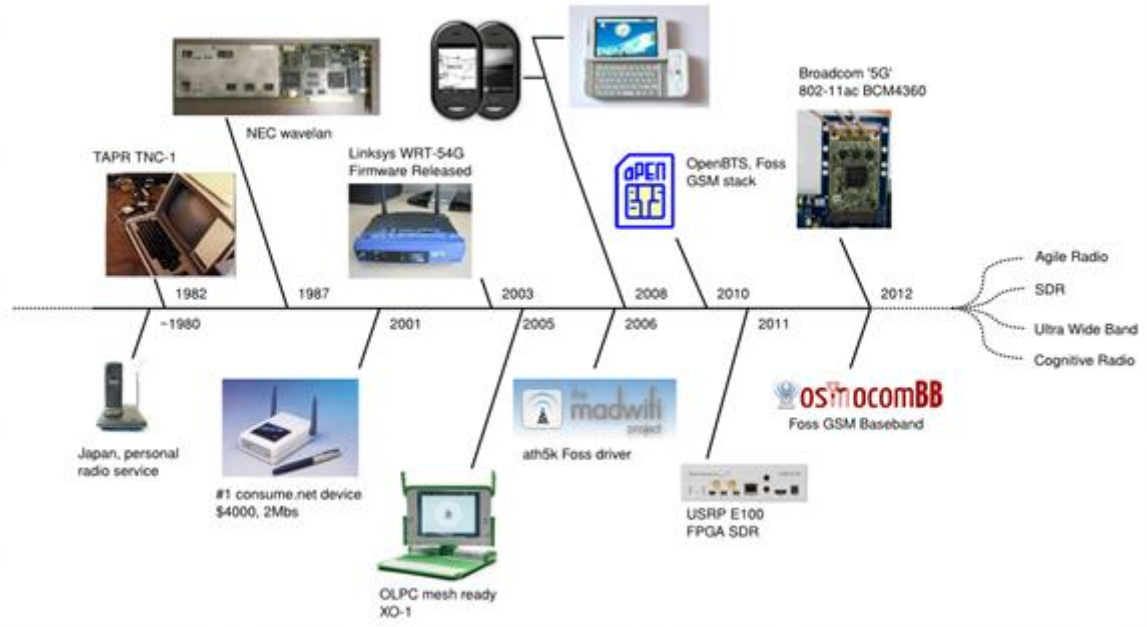
כאן אנו רואים את טבלת הטופולוגיה של הרשת מנקודת ראותו של הנתב שלנו, ממנה ניתן להפיק מפה/טבלת ניתוב מלאה של הרשת. שדה ה-cost מתאר את איכות הקשר לפי שיטת האומדן שבחרנו. כמובן שאפשר להרחיב עוד רבות על הצד הטכני, אך קודם אולי כדאי לתת קצת רקע כללי על הפרויקט.

היסטוריה

מושג הרשת הקהילתית מקדים את טכנולוגית Wi-Fi בכמה עשרות שנים - עד כדי כך שאפשר להתחקות אחריו עמוק לתוך ימי הזוהר של חובבי הרדיו, אי שם בסוף שנות ה-70. הרעיון אז היה שמפעיל Ham יחברו מעין מודם למכשירי הרדיו שלהם שיאפשר להם להעביר קבצים בין אחד לשני. ב-1978 כבר הועבר קובץ ה ASCII הראשון בין מפעילי Ham. ה-TNC-1, מעין מודם דיגיטלי לתדרי 144 MHz, בעזרתו הוקם קישור חובבים מבוסס packets ראשון כבר ב-1982! בתמונה של ארגון TAPR ניתן לראות ערימת מכשירי TNC ומאחוריה הכיתוב: packet-radio revolution!

אלא, שלא לי, וכנראה שגם לא לכם יש מכשיר TNC-1, וגם מהפכה לא ממש ראינו. מה שכן יש לנו זה ראוטרים, נטבוקים, לפטופים עם מחברי mini-PCIe המאפשרים שידרוג של מודולי הרדיו, סמארפונים, בעתיד הלא רחוק כרטיסי SDR (רדיו נשלט תוכנה) ועוד. מה משמעות הדברים? בעיקר שהשעה כשרה. גלובליזציה, מיזעור, שיפור ביכולת עיבוד אותות ופיתוחים שונים ברמת הפרוטוקולים הופכים את הצ'יפים האלחוטיים של היום לזמינים, חזקים וגמישים לאין שיעור ביחס לעבר, והיד עוד נטויה.

מה הספקנו לראות בעשר השנים האחרונות? פתיחת קוד המקור של אחד הנתבים הנפוצים בשוק, הופעת דרייברים מבוססי קוד פתוח, טלפוני quad-band התומכים בארבעה תדרי פעולה, וזאת בנוסף לתמיכה ב-bluetooth, GPS, Wi-Fi ולעיתים גם WiMax. הופעת קוד מקור להפעלת תחנת GSM מפרויקט OpenBTS, ומשלימו, פרויקט osmocomBB לפיתוח קוד עבור שכבת ה-baseband ב-GSM, עבור מכשירים ניידים עצמם. MIMO (טכנולוגיית ריבוי אנטנות), חידושים בנצילות הספקטרום הודות לשיטות מתקדמות למודולציה, ריבוב, ועוד. האמת היא, כי קצרה היריעה מלתאר את כל החידושים הללו, אבל אולי על אחד שווה להתעכב - **SDR**.



[חומרת רדיו, תמונת מבט היסטורית]

רדיו נשלט תוכנה

מזה זמן רב הורגלנו לחשוב שכל מכשיר רדיו נועד לפעול בתחום תדרים יחיד. אלו מבין הקוראים שמכנים סמארטפונים בשמם המדויק - מחשבים שגם יודעים לדבר dual/tri/quad-band, ממזמן הפנימו שהדבר עתיד להשתנות, מהר מכפי שנדמה לנו. SDR ו-GNUradio הם נושאים שראויים למאמר משלהם, אך נסתפק בלציין שמדובר במערכות מאוד גמישות בכל הנוגע לתדרי הרדיו והאופן בו הם פועלים.

העיקרון המנחה בעיצובם הוא שימוש בתוכנה עד נקודת ההשקה עם מודול השידור/קליטה, תוך שימוש ברכיבי FPGA על מנת לשנות את התנהגות החומרה בהתאמה לתדר וליישום בו עובד המכשיר. הנ"ל מאפשר להגדיר את אופי פעולתם באמצעות קוד, מהר, ובצורות שעד כה הצריכו מכשירים יעודיים יקרים מאוד. הרשימה הזו ממחישה בדיוק כמה מאמץ מושקע כרגע בתחום. קשה לצפות את ההשלכות המדויקות של טכנולוגיה זו על תחום הסלולר, ה-Wi-Fi והרדיו בכלל. מה שבטוח שזו תהווה את אחד האתגרים הגדולים ביותר בדרך לעיצוב מדיניות רגולציה בתחום, בישראל ובעולם כולו.

אריג, השוואה טופולוגית

כאמור, אריג הוא בראש וראשונה מבנה טופולוגי. אז מה החידוש שבו? ובכן באינטרנט כיום המבנה ההיררכי דומיננטי, והעניין עוד יותר מובהק כשמדובר בתשתיות הפיזיות. דוגמאות למבנים היררכים:

- הפרדה בין ספקי Tier 1, 2 ו-3[8] לרבות קיבולת התעבורה שלרשותם, וההתקשרויות ביניהם. אף שהרשתות עצמן מכילות מספר רב של קישורי גיבוי ואינה באמת נראית כפירמידה, המבנה הארגוני מסחרי שעומד מאחוריה כן.
- מבנה ה-PKI המשמש אותנו עבור תעודות SSL חתומות, שבראשו עומדים מספר מצומצם של גופים מסחרים בשל הקושי לעמוד בדרישות שלו. נתיב האימות לכל תעודת SSL מוביל לאחד מה-Root CA.
- מערכת ה-DNS, לרבות 13 שרתי השורש שבראשה.

מרבית הדוגמאות למבנים מבוזרים לקוחים משכבת האפליקציה: bittorrent, skype ,Tor ועוד.

מובן שלכל טופולוגיה יתרונות וחסרונות. טיפשי יהיה לטעון כאילו זו עדיפה על זו, משום שהדבר תלוי בתפקיד היישום ובהקשר בו הוא פועל. ננתח את היתרונות המרכזיים שבטופולוגית אריג:

- קשה לביתור - פרוטוקולי ניתוב ידעו לחוש בקשר משובש/מנותק ולאגף אותו, כמו גם לחזור להשתמש בו כשישוב לפעול באופן תקין. משמעות הדבר היא שיש לשבש מספר גדול של קשרים במקביל על מנת להתקיף בהצלחה את הרשת.
- מונע ריכוזיות שליטה - ביסוס אמצעי שליטה/שיבוש/ניתור על הרשת מצריכה פריסה פיזית של צמתים לאורכה ולרוחבה. מגבלת הכוח הפועלת על כל צומת נובעת ממבנה הרשת עצמו.

חסרונות המרכזיים של טופולוגית אריג:

- קצבי תעבורה נמוכים: עבור כל קפיצה בנתיב תקשורת מרובה צמתים בין מקור ליעד אנחנו יכולים לצפות לירידה של קרוב לחצי ברוחב הפס, מה שמשאיר בדר"כ מעט רוחב פס אחרי מספר מצומצם של קפיצות בין צמתים.
- הקושי שבביזור - יישום שירותים הופך קשה במקרים מסויימים אם אנחנו מסרבים לבטוח בגורם ריכוזי כלשהו. דוגמא לכך היא הקושי שבמימוש מערכת DNS מבוזרת - פתרונות לרוב יבצעו המרה כלשהי של זמן/חישוב/זיכרון על מנת להשוות את הביצועים של מערכת ריכוזית.

אחד השינויים המהותיים שפרויקט אריג רוצה לבסס הוא שימוש במבנה מבוזר בשכבת הקישוריות עצמה.

[8] ספקי Tier 1 - ספקים "שרואים" את כל האינטרנט, כלומר אינם צריכים לשלם דמי מעבר עבור גישה לחלק כלשהו של האינטרנט.

בחזרה לארץ הקודש...

איך נולד פרויקט אריג? תחילת הסיפור מחזיר אותנו לקטלוניה, לכנס Battle-Mesh v4 בו השתתפתי. הכנס, שזו היתה האיטרציה הרביעית שלו, נולד כתוצאה ממשפט שנזרק לעבר אחד ממפתחי פרוטוקול BATMAN מצידם של מפתחי OLSR. האוויריה בין המפתחים התחממה והוחלט לערוך תחרות שתכריע אחת ולתמיד מי מבין הפרוטוקולים עדיף. מהמפגש נולדה מסורת נודדת, בה פורסים רשת בדיקה באיזור בו מתקיים הכנס, המשמשת לבחינת תפקודי הפרוטוקולים, מפגש והחלפת רעיונות באופן כללי.

עם החזרה לארץ גיליתי שמעט מאוד אנשים מכירים את הנושא. תחושה מוזרה החלה להתלוות לכל פעם שבה היה מתברר לי שכל הרשתות באזור בו אני נמצא נעולות! כיצד משכנעים כל כך הרבה אנשים להתקין רשת אלחוטית ובו בזמן שאסור/מפחיד/לא כדאי לברר מה יקרה אם נאפשר להן לתקשר אחת עם השנייה. משם הדרך לרישום הדומיין http://arig.org.il היתה קצרה.

כיצד פסח רעיון רשתות האריג הקהילתיות על ישראל עד היום? אחרי הכל לא חסרות פה חברות העוסקות בתחום האלחוט, החל מיישומיו הצבאיים וכלה בפיתוחי WiMax. לשכת המדען הראשי מפעילה זוג מאגדים, RESCUE ו-CORNET בנושאי רשתות לשימוש כוחות הצלה ורדיו קוגניטיבי, בהתאמה. במקביל מתכננת עיריית תל אביב להרחיב את פרויקט הרשת האלחוטית בשדרות בן גוריון על סמך "הצלחת הפרויקט", ואף השכלנו בנתיים ללמוד מיוזמו, אלון סולר, ש"העירייה יכולה לבחור אילו תכנים יוצגו בדף הבית של הגולש כאשר הוא משתמש בשירות". חמוש בידע הנ"ל אני מוכן להסתכן בהערכה.

כאמור לרשתות אריג אלחוטיות יש היסטוריה ארוכה, ואחת הבעיות עם היסטוריה היא שאפשר ללמוד ממנה יותר מדי. רשת אריג לא תפעל בארץ במתכונת של תשתית קישוריות ראשית, פשוט מהסיבה שבישראל לא חסר אינטרנט, לפחות לא באופן שבו הוא חסר כאן. מה שכן רלוונטי לישראל הוא נושא הפרטיות, חופש המידע ועצם שפע אמצעי התקשורת שבהשג ידינו. מנקודת מבט זו אין סיבה שלא ננסה להפעיל אותם במתכונת שונה, אדרבא אם נשקול את הפוטנציאל שטמון בכך.

עוד דבר בולט שלומדים מפרויקטים שנעשו, הוא שקשה מאוד להפעיל רשתות כאלו ללא מעורבות קהילתית לאורך זמן. סוד כוחו של האריג טמון במעורבות אישית של כל אחד הלוקח חלק בהפעלתו. מובן שהכוונה היא לא להפוך את כל חברי קהילת אריג לאשפי סיסטם, אבל הנכונות להפעיל צומת בסופו של יום נשארת בידיהם. זה מה שהופך רשת אריג לקהילת אריג.

הפוטנציאל

רשת אריג מציעה מגוון יתרונות, אבל השימוש בהם מאוד תלוי בהקשר בו פועלת הרשת ונקודת מבטו של המפעיל. מפת האינטרסים ללא ספק סבוכה: אח גדול בעיר קטנה מעוניין בהפעלת רשת אריג כדי ליירט/לסנן/לנטר תעבורת אינטרנט. חברה מסחרית תרצה להוסיף פרסומות לעמודי אינטרנט כמודל עסקי. ספק סלולר מעוניין לפרוס אריג femto-cells דרך לקוחותיו כדי להוריד עומס מהרשת הראשית ולסייע בהגשת שירותי LTE. מורדים בעיר חמאת שבסוריה ירצו להקים אריג על מנת להבטיח יכולת תקשורת מול נסיונות שיבוש ממסדיים. כוחות סיוע בהאיטי יבקשו להקים אריג כדי לבסס ערוצי תיאום בעת אסון. קיבוץ ירצה להציע שיחות חינם בשטחו ואילו ראש עיר יפרוש אינטרנט "חינם" בשדרה, אפיל אם הוא לא באמת עונה על צרכי התושבים. הרשימה כמובן עוד ארוכה...

על מה יסכימו כולם? קרוב לוודאי שרק על הפוטנציאל הגלום ברשת, עבורם.

לא נתעלם מהיתרון מרכזי אחר של רשתות אריג אלחוטיות, והוא עלות הקמה נמוכה בשילוב עם פשטות הפעלה יחסית, לפחות כשמדובר ב-Wi-Fi. המשותף לכפרים באפריקה העושים שימוש בפרויקט village- telco, או רשתות אריג המספקות קישוריות בנפאל, הוא שנבחרו כפתרון היעיל ביותר כלכלית לביסוס תשתית תקשורת.

דבר נוסף שכדאי לשים אליו לב הוא ששירותים מסויימים דווקא מתאימים יותר לרוץ על רשתות אריג מאשר דרך ARPANET. קחו לדוגמא שירות כמו רשתות חברתיות - מימוש מבוזר כמו זה של Diaspora יותר מתאים לרוץ ברשת אריג מהסיבה הפשוטה שאופי התקשורת בחלקה הארי מקומי ממילא, ובאופן כללי נכון עבור כל שירותי ה-geo-social. דוגמאות נוספת היא שירותי איסוף נתונים מבוזרים כגון רשתות חישה אלחוטיות, או שירותי caching מקומיים מבוזרים.

פחד, אי-ודאות וספק

כמה תשובות שיעזרו לקורא לזהות, לעבד ולהפריך טענות נפוצות ששומעים בהקשר של רשתות אלחוטיות לא מאובטחות. חלק מהדברים מובאים בתגובה למאמר של עו"ד יהונתן קלינגר מהגליון השלושים וחמישה.

השמיים נופלים! ברשתות פתוחות כולם יכולים להאזין לי!

ובכן אין כל הבדל בין רשתות אלחוטיות פתוחות ורשתות סלולר מהבחינה שבשתיהן לתעבורת המידע יכול להאזין צד שלישי באופן פסיבי. רמת האבטחה נגזרת מפרוטוקולי התעבורה וההצפנה בהם נעשה שימוש, לרבות המצאות אפשרית של פגמים ביישום שלהם.

כניסה לא מאובטחת לרשת חברתית דרך HTTP ישאיר את המשתמש חשוף, אך זהו תרחיש חלול, משום שכל שהוא בסך הכל מתאר משתמש לא אחראי. שורש העניין כאן הוא לא התווך האלחוטי, אלא חוסר ידע בסיסי בנוגע לשימוש באינטרנט, שהביא לכך שלא נעשה שימוש ב-HTTPS. מרבית האשמה במקרים אלו מונחת ממילא עם מפעילי האתר שאינם מבצעים redirection לגישה דרך פרוטוקול מוצפן.

ומה לגבי גישה שאכן בוצעה דרך HTTPS? ובכן כאן כשל אבטחתי תלוי בהמצאות פגם תיאורתי או ישומי בפרוטוקול או במודל האמון. גם כאן ניתן להשוות את הדברים לבעיות אבטחה שנמצאו בפרוטוקול GSM בפרוטוקול ההצפנה A5/1 או בהתקפות נוכחיות או עתידיות על UMTS, או התקפות side-channel שנותרות רלוונטיות עבור שניהם.

השמיים נופלים! רשתות פתוחות מהוות סכנה למידע שלי!

ומה לגבי הצורך של משתמשים ברשת מאובטחת לשימושם הפרטי? ובכן לשם כך קיים פתרון טכני פשוט המאפשר הגשת זוג רשתות בו זמנית על ידי אותו נתב, הראשונה מאובטחת ופרטית ואילו השניה פתוחה, כאשר המשתמש בוחר באיזה מידה הוא רוצה לחלוק או לא את חיבור ה-uplink שלו.

אם אתם עדיין בדעה שזה מסוכן, אתם מוזמנים לקרוא את עמדתו של חוקר האבטחה ברוס שנייר בנושא.

השמיים נופלים! רשתות פתוחות יאפשרו גישה לתוכן שאינו חוקי באופן אנונימי!

כדי לא לדרדר את איכות הדיון נסתפק בכך שמספיק שאדם אשר מעוניין בגישה לחומר מהסוג הזה ילמד על דרך אחת לגשת לאינטרנט באופן אנונימי ומכן והלאה הוא יעדיף לעשות זאת מביתו ולא מפינת רחוב.

השמיים נופלים! ברשתות פתוחות המידע שלך מסכן אותי!

הנה קטע מתוך המאמר של יהונתן העוסק באחריות משפטית בעת שיתוף אינטרנט:

> "...אדם משתף את הרשת האלחוטית שלו, הרי שכל מי שמתחבר יכול להשתמש בה כדי לעשות פלאים לא חוקיים: החל מהורדה של חומר פדופילי, דרך שיתוף קבצים לא חוקי והרצת מניות, ועד פרסום טוקבקים בבלוגים שיהיו לשון הרע. אם יתקבל תזכיר חוק חשיפת גולשים... אדם יקבל תביעה על סמך כתובת ה- IP שלו, וזאת כאשר הוא השאיר את הרשת שלו פתוחה למשתמשים".

בוא נשים את הדברים בפרופורציה. בין גלישה אנונימית ורשתות אלחוטיות פתוחות יתכן קשר, אך הוא לא חד ערכי ובוודאי לא הכרחי. כפי שהזכרתי קיימים מגוון כלים משכבת האפליקציה המאפשרים את אותה יכולת - כלים קיימים שכל תכליתם לטשטש את הזהות בין IP ומשתמשים. המסקנה המתבקשת היא שהרעיון לקשור את המושגים משתמש וכתובת IP הוא מוטעה, ומכל מקום לא ישים.

אנחנו, כקוראים טכניים, לא יכולים להשלים עם מציאות שבה אדם מואשם במעשה על סמך כתובת ה-IP שלו בלבד - ראיה מסוג זה יכולה לשמש לכל היותר כראיה תומכת, שלבדה מותירה מעט חוץ מספק סביר. נדמיין מצב בו שוכנעו כל מפעילי הרשתות הפתוחות לנעול את רשתותיהם. מתיישב פלוני בבית קפה, רוכש קפה ומאפה. בתמורה מקבל את סיסמת הגישה לרשת. בשלב הבא הוא מפעיל את שרת ה-Tor שלו וגולש בצורה אנונימית. מה השגנו בכך? לא הרבה. דגש אחרון: בתיאור הנ"ל הנחנו שאיבטוח הרשת הוא משימה שבכוחו של כל אחד לעשות, אף שאנחנו מודעים היטב לקושי שכרוך בכך.

ונשארת תלויה שאלה המחיר. בעת נעילת הרשתות שלנו עוד ועוד אנו מוותרים על האפשרות לחקור מה ניתן לבנות בגישה הפוכה, על ידי שיתוף, קישור ובעיקר התעקשות על אופי נייטרלי לרשת. האם אלו הטיעונים שבעבורם נזנח את הרעיון? השאלה האמיתית שצריכה להשאל היא כיצד לבנות רשת שבד בבד תאפשר חופש ביטוי אנונימי, ובמקביל תדרוש הזדהות במקומות המעטים בהם הוא באמת נחוץ.

האינטרנט ישאר מקום רווי סכנות, במיוחד אם אתה מגיע ללא כל ידע בסיסי על אופן פעולתו. השורה התחתונה היא ששכבת הלינק, אותה מיישמים פרוטוקולי אריג מספיק נמוכה כדי שמרבית האיומים לא יהיו יחודיים עבורה, ובמרבית המקרים מקבילים לאיומים זהים מתחום הסלולאר.

הלאה! לדברים יותר מעניינים!

פעילות

אז מה נקודת המבט של אריג'ניקים? ובכן עיקר המטרה שלנו היא ללמד ולחלוק כיצד להשתמש בטכנולוגיות הללו לטובת הקהילה. נכון להיום אנו עוזרים בהפעלת רשתות וצמתי אריג במספר מוקדים בארץ, אולם פיתוח תוכנה הוא החלק שבו נעשית מרבית הפעילות כרגע. נכון להיום אנחנו עובדים על הכלים הבאים, כולם משוחררים כקוד פתוח:

- **Mesh DB** הוא מסד נתונים יעודי לרשתות אריג, שלאחרונה זכה ל-web-service משלו - ממשק מכונה שיאפשר לנו לפרסם נתונים על הרשת הפועלת בארץ. שכנוע קהילות אריג נוספות לתמוך ב-API הנ"ל יאפשר מחזור יישומים וחסכון עצום בעבודה כפולה. לדוגמא את 'יישום המפה', המציג את מבנה הרשת ניתן יהיה להפנות ל-API של קהילה כלשהי ופשוט לצפות ממנו לעבוד, בדומה מאוד ל-OpenSocial.
- **Arig Web-app** הוא יישום האינטרנט הרץ על גבי אתר הבית של אריג. היישום נמצא בפיתוח של מספר יכולות, לדוגמא איפשור שיתוף תמונות-פנורמה מגגות בתים, על מנת להקל על מציאת שכנים עימם ניתן יהיה להקים קישור רדיו על מנת להרחיב את הרשת.
- שירות יצירת תמונת קושחה לנתבים מצויים בישראל on-demand, מבוסס OpenWRT, שיקל על הצטרפות לרשת המקומית, למשל דרך קנפוג מוכן מראש של כתובת ה-IPv6 עבור הנתב.

סיכום

למרות מאמר ארוך מהמצופה, קשה לראות בו יותר כמבוא לנושא. קיימים היבטים רבים שלא היה אפשר לסקר, כמו נושא הקצאת תדרים בעולם ובישראל בפרט, מינוף IPv6 ברשתות אריג, DN42 כ-backbone וירטואלי לרשתות אריג בעולם ועוד.

איך לוקחים חלק? בתור התחלה אפשר כולם מוזמנים להגיד שלום דרך רשימת התפוצה של הפרוייקט, שם מתנהלים רוב הדיונים בקשר לפרויקט. השלב הבא הוא לקחת ראוטר להתקין עליו הפצת קוד פתוח כגון OpenWRT כדי לקבל הרגשה של איך דברים נראים. משם הדרך לקוד צריכה להיות פשוטה...

בנוסף, לאחר האקאתון ראשון מוצלח בעיר ערד בקרוב נקיים גרסה קצת יותר נגישה בתל-אביב, אליו כולם מוזמנים. מקווה לראות אותכם שם!

על המחבר

אמיר שגיא הוא מתכנת, פעיל קוד פתוח ואחד ממייסדי פרויקט אריג. תגובות / יצירת קשר אפשר לשלוח ל: digitalwhisper@taproot.org.il.