על שתי שיטות ל־BGP Security הדרגתי

עומר שכטר

עבודת סיום בקורס: "67828 פרוטוקולים לרשתות תקשורת והאינטרנט: תאוריה ומעשה"

מוגש למרצה: ד"ר מיכאל שפירא

תקציר

פרוטוקול הניתוב BGP הוא פרוטוקול הניתוב העיקרי בתעבורת interdomain ברשת האינטרנט. הפרוטוקול חשוף למספר בעיות אבטחה ידועות המשבשות את הגלישה העולמית בראשית מדי פעם בהיקפים שונים. בעבודה זו נסקור שני מאמרים מאמצע העשור הראשון של שנות האלפיים המציעים פתרונות ותיקונים שונים לפרוטוקול ומטפלים לכאורה בחולשות האבטחה. נשווה את הגישות ביניהם, ננתח אותם, נבין את יתרונותיהם וחסרותיהם הכלליים ואחד לעומת השני וננסה להציג התקדמות קלה בניסיון שהם מציעים לשיפור הפרוטוקול.

תוכן עניינים

1 הקדמה

הפרוטוקול BGP[1] משמש לניתוב ברשת האינטרנט מראשיתה. האינטרנט מחולקת לעשרות אלפי "רשתות־עצמאיות" (Autonomous System), אשר כל אחת מהן יכולה להיות חברה גדולה, ספק ולקוחותיו, אוניברסיטה וכן הלאה. בעוד ניתוב תעבורה בתוך רשת עצמאית שכזו הוא פשוט, שכן טופולוגיית הרשת ידועה והיא מנוהלת על ידי אדם יחיד שמנסה למקסם מהירות, ניתוב בין הרשתות האלה הוא אתגר מורכב יותר. זאת שכן הטופולוגיה של רשת האינטרנט ככלל אינה ידועה, ואת הניסיון למקסם מהירות על חשבון הכול מחליפים שיקולים כלכליים בין הרשתות השונות. פרוטוקול ה־BGP נועד לאפשר זאת, הפרוטוקול דואג שכל רשת תיידע את הרשתות השכנות לה על מסלולים שהיא יודעת, בהתאם לאינטרס העסקי שלה, ובנוסף דואג שכל רשת תלמד מהמידע שהתקבל משכנותיה אילו מסלולים לבחור - בהתאם לאינטרסים העסקיים שלה. לסוגיית הניתוב הפרוטוקול נחשב להצלחה. למרות שאין זה מובנה בו, הוכח כי הוא יציב[2] בתנאים הקיימים, הוא התפתח ממצב של רשת אינטרנט קטנה לאינטרנט הגלובלית של היום וכל ניסיון גלישה שלנו ברשת כיום הוא הוכחה להצלחת הפרוטוקול.

בניגוד לעצם הניתוב עצמו, לפרוטוקול יש חולשות אבטחה מהותיות, שגורמות הלכה למעשה לבעיות ניתוב. כפרוטוקול שצמח ברשת קטנה המורכבת מגופים שניתן לסמוך עליהם ועכשיו משומש במערכת גלובלית, הפרוטוקול אינו מכיל כיום שום דרך לוודא את נכונות המידע המעבר מרשת לרשת במסגרת תהליך העדכון של מסלולים. למעשה, כל נתב BGP של אחת הרשתות־העצמאיות יכול להעביר כל מסלול שיחפוץ בכך לשכניו והם יאמינו לו,

[1] Y. Rekhter, T. Li, and S. Hares, **A Border Gateway Protocol 4 (BGP-4)**, *RFC 4271*, 2006

[2] L. Gao and J. Rexford, **Stable Internet routing without global coordination**, *IEEE/ACM Trans. on Networking, vol. 9, no. 6, pp. 681–692*, 2001

ואף יבחרו בחלק מהמסלולים שהוא מספק, בהתאם לשיקוליהם. בשל מספר תכונות מובנות בפרוטוקול, שנפרט בהמשך (דוגמת חיפוש אחר הקידומת הקצרה ביותר ליעד), נתב יכול בוודאות לכפות על שאר הרשתות לאמץ מסלול שהוא מספק להם ולגרום לו לפעפע אל כל רשת האינטרנט, דבר שיגרום לכל תעבורת רשת המיועדת למקום מסויים לעבור דרכו.

בשנת 2000 פורסם המאמר הראשון המרכזי בניסיון לאבטח את הפרוטוקול[3], ניסיון זה דורש הקמת שרת מרכזי לאימות ומעבר לחתימה על כל חבילת מידע שנשלחת. הצעה זו דורשת החלפת כל החומרה והתכנה שמתעסקת עם BGP בכל העולם, צעד שלא סביר שיתרחש - ואכן אינו מתרחש. בשנים שלאחר פרסום הניסיון הזה התחילו לעלות נסיונות רבים לתקן את פרוטוקול ה־BGP תוך כוונה שהצעות אלו יהיו ישימות, בניגוד ל־sBGP.

בעבודה זו נסקור שני מאמרים המתיימרים להציע פתרון לבעיות האבטחה של BGP, תוך ניסיון לישימות של ההצעות.

- G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. D. McDaniel, and A. D. Rubin, **Working around BGP: An Incremental Approach to Improving Security and Accuracy in Interdomain Routing**, *NDSS.* 2003
- J. Karlin, S. Forrest, and J. Rexford, **Pretty good BGP: Improving BGP by cautiously adopting routes**, *14th IEEE International Conference on Network Protocols*, 2006

ראשית נסכם בקיצור נמרץ את תוכן המאמרים ונעלה נקודות חשובות העולות מהן. בהמשך נשווה את הגישות בשני המאמרים - בנקודת המוצא, בדרך הפתרון, בהנחות ההיתכנות, בבדיקת הנכונות של ההצעה ועוד. בהמשך נבדוק את היתרונות והחסרונות העולים מכל אחד מהמאמרים וננסה למצוא את הנקודות החלשות בהם. לבסוף ננסה, עד כמה שענוותינו ושכלינו מאפשרים, להציע התקדמות קטנה בשיפור אבטחת BGP.

2 תקציר המאמרים

2.1 המאמר הראשון

במאמר זה מוצע שימוש בכלי חיצוני הקרוי במאמר IRV המשומש בצמוד לנתב ה־BGP. הכלי מאפשר לאמת נתוני BGP על ידי הצד המקבל. ה־IRV ישב על שרת ייעודי שיישאל על אודות מסלולים שמתאפשר להגיע ממנו והאם הם אמיתיים. לדוגמה, כאשר רשת־עצמאית מקבלת משכנתה דיווח על מסלול אטקרטיבי לקידומת, היא תעבור על כל הרשתות באמצע ותשאל את שרת ה־IRV של כל אחד מהם האם תת־המסלול הקשור בהם אמיתי. מעבר כזה בכל הדרך מאפשר לוודא לחלוטין כי המסלול אמיתי.

שרת כזה יאפשר בנוסף לוידוא נכונות של מסלול גם חלוקת נתונים נוספים בין הרשתות העצמאיות, דבר שלטענת הכותבים ישפר את הניתוב בין הרשתות.

2.2 המאמר השני

הצעת הפתרון במאמר זה היא יוריסטיקה לבחירת מסלולים הנלמדים משכנים. הרעיון המרכזי במאמר נוגע לכך שניתן בנקל לזהות את מרבית המסלולים הבעייתיים על ידי אימוץ זהיר של מידע חדש.

> "BGP routers can avoid selecting and propagating these routes [i.e. the bad routes, O.S.] if they are cautious about adopting new reachability information"

הדרך לעשות כן אליבא דמאמר היא שמסלולים לא מוכרים יתקבלו בחשדנות ולא ייבחרו ישר. דרך זו תתמודד בקלות עם כל בעיות הגדרה של נתבים, סיבה שגורמת לפי הכותבים לרבות מהתקלות. המאמר מציע לאמץ מרווח חשדנות שבו כל מסלול חדש שמופיע לא מתקבל עד ששרד את המרווח. נתב ה־BGP מתבקש במשך תקופת אתחול ללמוד את היסטוריית המסלולים השונים כדי ללמוד מה נחשב "מסלול נורמלי", קרי מהו המקור של קידומת מסויימת ואילו רשתות נמצאות בסביבתה. לאחר תקופת האתחול, מסלולים המתאימים למה שידוע מההיסטוריה על הקידומת ויתאימו לכך יתקבלו, מסלולים חדשים שאינם חופפים להיסטוריה (קרי, מגיעים אל קידומת מסויימת על ידי מסלול שאינו מכיל שכנים מוכרים היסטורית אל הרשת העצמאית המתאימה לקידומת) לא יתקבלו אלא לאחר תקופת חשדנות שרירותית. המאמר מציע שני פרמטרים להגדרת הנתב - $h,\ s$. הראשון, H מתייחס לכמה זמן עובר על שמסלול נחשב לכזה ש־"נראה לאחרונה". ערכו לא יכול להיות נמוך שכן אחרת

[3] S. Kent, C. Lynn, and K. Seo, **Secure border gateway protocol (S-BGP)**, *IEEE Journal on Selected Areas in Communications*, 18(4):582–592, 2000

מסלולים תקינים ייראו חשודים, ומצד שני הוא לא יכול גבוה שכן אז הוא יגרום למסלולים רעים להפוך למקובלים. השני, s, מתייחס לתקופת החשדנות, שהיא כמה יש לחכות לפני שמסלול חשוד מתקבל. הערך אמור להיות ארוך מספיק כדי לאפשר למנהל הרשת לבדוק את הבעיה בעצמו. במאמר עצמו מצטטים טענה כי 45% משגיאות הגדרה (שגורמות למסלולים שגויים להידווח לשאר הרשת) שורדים פחות מ־24 שעות[4]. מסיבות אלה במאמר הם מציעים להגדיר $s = 24\,\text{hours}$ ו־$h = 10\,\text{days}$.

בנוסף ליוריסטיקה הזו, מציעים הכותבים להקים שרות דיווח תקלות אינטרנטי, שבו מנהלי רשת יוכלו לדווח על ממצאים חשודים שהם מוצאים, לפנות לאחראים המתאימים וכך למנוע במהרה בעיות הגדרה למיניהם. כל מנהל רשת של רשת־עצמאית יזין את הקידומות שהוא אחראי עליהם ודרך ליצור עמו קשר. כך אם הוא הגדיר לא נכון את הנתבים שלו וגרם להפצת מסלולים שגויים הוא ידווח על כך מיד, במקום לסבול מההשלכות החמורות לכך על הרשת שלו. בנוסף, כך הוא יוכל לדווח על בעיות מהר וליצור קשר עם מנהלי־רשת אחרים ולברר איתם לגבי מסלולים חשודים, ולמנוע ממידע שלו להגיע אליהם בטעות.

> "If these two operators are informed of each suspicious route that PGBGP finds, the operating overhead could be minimized and routes could be verified by the most knowledgeable parties."

3 השוואת המאמרים

3.1 נקודת מוצא

שני המאמרים נכתבו בשנים שלאחר פרסום המאמר על sBGP וההבנה כי פרוטוקול BGP מכיל בעיות אבטחה חמורות, ושניהם מתייחסים אליו. כל אחד מהמאמרים יוצא מנקודת הנחה שהקורא מכיר את sBGP, מודע ליתרונותיו וחסרונותיו ולעובדה שיש אי־הצלחה בהטמעתו ברחבי הרשת. שני המאמרים אם כן יוצאים מנקודת הנחה שכל פתרון לבעיית ה־BGP צריך להתייחס לשאלת היישומיות, קרי - איך ניתן להתחיל להשתמש בו בעולם האמיתי מבלי לכפות על עשרות אלפי ארגונים עסקיים ברחבי העולם להחליף את הציוד שלהם, שכיום עובד לכאורה פרט למקרי תקלה נדירים לכאורה. הכותרת של המאמר הראשון אף מתייחסת לכך ישירות וכותבת "An Incremental Approch", המאמר השני מציין כבר בהתחלה, בתקצירו, כי "PGBGP is incrementally deployable and offers significant security benefits to early adopters".

מבחינת הכישלון באימוץ sBGP ניתן לציין, לפי המאמרים, שני מרכיבים מהותיים: השינוי בפרוטוקול עצמו והריכוזיות של הפתרון[5]. כל אחד מהמאמרים מנסה להסביר מדוע הוא אינו עורך שינויים בפרוטוקול עצמו אלא רק בשוליים ומדוע הפתרון שלו אינו ריכוזי, אך כל מאמר עושה זאת בדרכים שונות. בעוד המאמר הראשון מחייב הקצאה ייעודית של חומרה (עבור שרת ה־IRV של כל רשת־עצמאית), דבר שהיה אחד הסיבות כאמור לכישלון sBGP, המאמר השני מנסה להסתייג ככל שניתן מחיוב הקצאת חומרה. בפרק 6 שעוסק ביישום והטעמה מוצעות שלוש דרכים לאפשר עבודה על BGP קלאסי יחד עם PGBGP. האפשרויות הן ששני הדברים יעבדו על הנתב, שינוי שלטענת המאמר דורש אך ורק שינוי בתכנה ולא בחומרה; הפרדת השימוש לנתב ולשרת, אשר במקרה זה הנתב יעביר את כל המידע אל השרת שינתחו וינחה במידת הצורך את הנתב בבחירה; האפשרות השלישית היא הטעמת שתי הפונקציות על שני שרתים נפרדים, לטענת הכותבים אפשרות זו תמנע כל שינוי שהוא לנתבים אבל תגדיל את העומס על השרתים. ניכר, אם כן, כי בחזית החומרתית המאמר השני התייחס יותר לסוגייה והעלה הצעות פתרון טובות ומגוונות יותר.

המאמר הראשון טורח להבהיר כבר בעמוד השני כי אין הוא משנה כלל את הפרוטוקול:

> "We have designed IRV as a separate protocol because of the difficulty in changing widely deployed protocols such as BGP. For similar reason, IRV is meant to be incementally deployable."

במאמר השני נכתב גם כן בשורה הראשונה בפרק 6, העוסק ביישום הפרוטוקול כי:

> "PGBGP does not require any changes to the BGP protocol, allowing on AS to deploy it when other ASs do not."

[4] R. Mahajan, D. Wetherall, and T. Anderson, **Understanding BGP misconfiguration**, *Proc. ACM SIGCOMM, pp. 3–16*, 2002

[5] המאמר הראשון מצטט לדוגמה את G. Huston, **Scaling interdomain routing**, *Internet Protocol Journal, 4(4)*, 2001 כדי לטעון שכל תכונה או פונקציה של ניתוב צריכה להיעשות על ידי פרוטוקול נפרד, ולכן קבלת המסלולים צריכה להיעשות בנפרד מבחירתם.

מבחינת גורמי הסיכון, שני המאמרים מסתמכים ומצטטים את המאמר של מרפי[6] ומחלקים את האיומים לפיו. חלוקה אחת של גורמי סיכון הם נסיונות מכוונים להגדרה שקרית של מסלולים במטרה להשתלט על תעבורה לעומת נסיונות שנובעים מטעויות אנוש בהגדרת מסלולים או נתבים פגומים.

3.2 הנחות היתכנות

הפתרון המוצע במאמר הראשון נראה כמו ניסיון להמיר את sBGP מאחריות של הצד השולח (שחותם על כל הודעת UPDATE) לאחריות הצד המקבל. ההמרה הזו גורמת לכך שחסרונות רבים הנמצאים בלב sBGP נמצאים גם בהצעה זו, אולי פרט להטמעה ההדרגית של ההצעה. ההצעה דורשת הקמה של שרת מרכזי שיאפשר לכל נתב לדעת היכן נמצא שרת ה־IRV של כל רשת־עצמאית, עניין מסובך שדורש שכל רשת־עצמאית תעדכן בו מידע בהתאם לשינויים אצלה, דבר שכמובן אינו דרישה במאמר השני (אבל כן הצעה משנית בו). דבר זה הנוגד את הטענה בעמוד 3 במאמר כי "The essence of the IRV architecture is decentralized query system". בנוסף להקמת שרת מרכזי, יש לדאוג לקו תקשורת רציף מאובטח בין שרת IRV של רשת עצמאית לשרתים אחרים, ולמעשה אין הסבר לכמה מהם, אך בהכרח מדובר בעשרות או מאות רק לשרתי הרשתות־העצמאיות הגדולות. המאמר מציע שילוב של IPSec או TLS כדי לדאוג לאבטחת הקו ואמינותו, דבר שייאט בהכרח את השידור, קל וחומר כשמדובר בקו מאובטח לשרתים רבים.

במאמר השני דווקא ניכר הניסיון הרב של המחברים לשכנע שהצעתם אפשרית למימוש. אחת הבדיקות שמבצעים המחברים היא לראות האם גם מימוש חלקי של ההצעה שלהם נותן תוצאות אפקטיביות עבור האינטרנט כולה (בעוד מנגנון ה־IRV יעיל רק לרשתות־עצמאיות שמשתמשות ב־IRV ולמסלולים שבכל הקודקודים שלהם יש IRV, דרישה מאוד חזקה משאר הרשתות באינטרנט). בבדיקה שלהם ניכר שמספיק שחלק זעיר מהרשתות (אך הגדולות בהן) תאמצנה את הצעתם ומספר המסלולים השקריים בכל הרשת יפחת דרמטית. בסיכום המאמר נכתב במפורש:

> "PGBGP is highly effective at blocking the spread of hijacked routes, even with relatively small-scale deployments, PGBGP can protect 97% of ASs from malicious prefix routes and 85% from bogus sub-preix routes when deployed only on the 62 core ASs in our study network."

הטמעה של ההצעה רק ברשתות הגדולות היא גם סבירה יותר. הרשתות־העצמאיות הגדולות הן בעלות המשאבים הרבים ביותר ומנהלי־הרשת בעלי הידע הרב ביותר, ולכן הטעמה של טכנולוגיה חדישה שם סבירה יותר מהטמעתה באוניברסיטה או בספק אינטרנט קטן.

3.3 דרך פתרון

3.3.1 המאמר הראשון

מנגנון השאילתות המוצע במאמר הראשון באמצעות IRV מסוכן ואף נפיץ כאשר אנו עוסקים במערכת שכלליה מקדשים את האינטרס העסקי מסחרי, שלרוב מוגן בסודיות. לפי הפרוטוקול, רוב המסלולים, אם לא כולם, המגיעים לכל רשת המיישמת את הפרוטוקול הולכות לתשאל את כל הקדקודים במסלול האם המסלול העובר בהן חוקי. הכותבים אמנם מציינים כי (עמוד 4):

> "the IRV need not respond uniformly to all requesters; and IRV may be configured to restrict access to particular data to a list of authorized requesters."

אך יישום הפרוטוקול יגרום לכך שהרשתות־העצמאיות הגדולות יקבלו המוני בקשות כל יום על מסלולים שונים העוברים דרכם ואם ישיבו להן - יגלו על הדרך מידע עסקי על קשריהם עם רשתות אחרות. בנוסף, רשת זדונית יכולה לנצל את הפרוטוקול כדי לשאול שאלות על מסלולים לא קיימים כדי לאסוף מידע על הקשרים העסקיים של רשת מסויימת עם רשתות אחרות. אם הרשת עונה, היא מגלה סודות מסחריים לגורם עוין, אם לא - הפרוטוקול הלכה למעשה לא עובד, שכן הוא בנוי כולו על ההסכמה של רשתות לחשוף מידע על מסלולים העוברים בהן. כל השמת הגבלה על המידע תגרום לכך שהפרוטוקול יהיה לא יעיל באופן חלקי (התייחסות נוספת לכך בפרק 4.2). נשים לב שבעיה זו קיימת ב־sBGP (ולמעשה מיובאת משם, אך שם באופן חמור יותר, שכן שם המידע חתום, וסוד עסקי חתום מסוכן יותר מסוד עסקי לא חתום), אך פה קיימת בהיקף רחב יותר, שכן בעוד ב־sBGP היא כוללת רק חשיפת מידע על מסלולים קיימים (שכן רק על מסלולים חתומים), פה כאמור רשת עוינת יכולה לזייף מסלולים ולשאול עליהם שרת IRV אשר לו אין אפשרות לדעת אם המשך המסלול אמיתי או לא, שכן הוא אינו חתום. ניתן לנחש שבעוד לארגונים קטנים או כאלו ללא מטרות רווח (אוניברסיטאות לדוגמה) לא תהיה בעיה

[6] S. Murphy, **BGP Security Vulnerabilities Analysis**, *Internet Research Task Force*, 2002

אמיתית לאמץ את ההצעה, ארגונים גדולים או מסחריים ינסו להימנע מכל ניסיון המחייב אותם לתת מידע אודות ההעדפות הפנימיות שלהם, וכל עוד הרשתות־העצמאיות המרכזיות הגדולות, מה שקרוי Tier 1, לא ימשיכו לעדכן על מסלולים שקריים - המסלולים האלה יפעפעו לרוב הרשת (כפי שניתן לראות בגרפים של המאמר השני). נרצה להודות שאמנם כאמור השינוי יהיה קשה יותר בארגונים גדולים, אך הוא כן סביר יותר ברשתות־עצמאיות קטנות יותר, כך אפשר לפתור את רוב בעיות ההגדרה של נתבים הנפוצות יותר בארגונים קטנים.

חולשה קלה נוספת במאמר היא שאין כלל לכל כמה זמן יש לבדוק IRV. במאמר עצמו נכתב "IRV does not mandate when queries are sent." (עמוד 4). בדיקה תכופה מדיי תגרום לעומס על השרתים ותאט קבלה של מסלולים חדשים ואת עבודת כל הפרוטוקול. בדיקה לא תכופה מספיק תחמיץ את המטרה ותאפשר למסלולים רעים להתגנב פנימה. שיפור למאמר יהיה בדיקה אמפירית על ידי נתב BGP והפעלת IRV בזמנים משתנים כדי לבדוק עלות/תועלת אופטימלית, אך במאמר הראשון אין כלל בדיקות אמפיריות של הטענות, עניין המופיע בשפע במאמר השני.

החיסרון הגדול ביותר ב־IRV הוא, לפחות לפי המאמר עצמו שמודה בכך, ההצעה לא יודעת להתמודד כמו שצריך עם נסיונות אקטיביים לזיוף בעלות על קידומות. עם טעויות הגדרה אכן ישנה התמודדות, אך במידה של זיוף בעלות יש לעבור לפי הפרוטוקול על כל הרשתות־העצמאיות ולשאול אותן אם עובר דרכן המסלול המתאים, ולבסוף לשאול את הרשת בקצה המסלול אם היא הבעלים של קידומת IP מסויימת. המאמר מודה כי (עמוד 8):

> "existing governing bodies [i.e. ICANN, ARIN, RIPE etc., O.S.] do not provide such validation infrastructure, and the technical challenges to doing so indicate that deployment in the near term is highly unlikley ... IRV cannot provide strong prefix ownership validation without governing authority"

החיסרון זה, מסתמך על דרישה שקיימת ב־sBGP והוא חלק אינהרנטי מהמאמר הראשון.

חשוב להדגיש כי בעיות רבות מגיעות מ־sBGP, חלקן מודגמות מעלה. כל פתרון שניתן לבעיה ב־sBGP כנראה יתקן בעיה ב־IRV. התלות הזו אמנם טובה, שכן sBGP היא הצעה מוכרת ומערכת מצד אחד ולכן אפשר לשער שרבים עובדים על הטמעתה ופתרון בעיות בה, אך מצד שני 14 שנים מפרסום ההצעה של sBGP עדיין איננו רואים התקדמות ניכרת בתחום בצד היישומי, מה שאומר שאולי היא לעולם לא תצליח.

בסעיף 6.2 במאמר, כותבי המאמר מודים על בעיה שלדעתינו אינה חמורה כמו שהם מציגים אותה. הבעיה שמועלה בתור שאלה היא, אם בעיות רבות כ"כ בנוגע לניתוב BGP נגרמות ממנהלי־מערכת שמגדירים לא נכון את הנתבים שלהם, מה יבטיח לנו שהם יגדירו נכון את שרתי ה־IRV שלהם?

> "The fundamental limitation of any supervisory system is that it is only as good as the data in it ... Unfortunately, many operators still configures routers by entering configuration commands ... this is a source of many problems, ... Would not that lead to divergence and uselessness of data as with the IRR?"

בניגוד להגדרות BGP שעוברות שינויים מדי פעם, הנתונים העיקריים בשרת ה־IRV לא אמורות לדעתינו להשתנות הרבה כלל וכלל. השרת אמור להכיל את האישור על בעלות על קידומות IP (ברגע שבו זה יהיה אפשרי), נתונים על שכנים ומסלולים אפשריים, מידע על הבעלים ואיך לגשת לאחראים על הרשת ולא הרבה יותר מכך. כל מידע נוסף שיתווסף גורע, ואילו הנתונים האלו עצמם ישתנו לעתים רחוקות מאוד, אם בכלל. על כן, איננו חושבים שזו בעיה חמורה כלל כמו שהמחברים של המאמר הראשון כותבים.

חשוב לציין שכל הבעיות שהצגנו מעלה מאפיינות את המאמר הראשון בלבד, ולא את המאמר השני.

3.3.2 המאמר השני

בניגוד למאמר הראשון, במאמר השני מודעים לחלק מחולשות הצעתם ואף מקדישים פרק ייעודי, פרק 8, לסיקור החולשות של הפרוטוקול תחת הכותרת "Limitation of PGBGP". מטרת עבודה זו אינה סיכום של המאמרים ועל כן לא נביא את החולשות המלאות כפי שמובאות במאמר אלא בקיצור, אך ננסה להרחיב דווקא בחלקים אותם כותבי המאמר מנסים להצניע. החולשה העיקרית היא שניסיון זדוני מתמשך יכול לעקוף את PGBGP ללא מאמץ מעבר לזמן שדרוש לחכות. לאחר מספיק זמן של שידור של מסלול שגוי באופן זדוני (או אפילו, טעות אנוש שנמשכת זמן רב) הפרוטוקול יפסיק לחשוד במסלול ויקבל אותו. יריב חכם פשוט יחכה מספיק זמן וישיג אותם תוצאות שאותן היה משיג בלא־זמן כיום. נשים לב שלאחר זמן מועט של דיווח על המסלול החשוד יכולים מנהלי־הרשת של רשתות־עצמאיות שונות להתחיל לפעול באמצעים מסויימים נגד רשת־עצמאית המתנהגת כך (לדוגמה, כאשר נניח הרשת־העצמאית פקיסטן טלקום תתחיל להכריז בעלות על הקידומת של גוגל, ייקח זמן למסלול לפעפע ומנהלי־רשת יתחילו לנסות לנסות להשיג את האחראים על הרשת של פקיסטן טלקום במטרה לגרום להם להפסיק. ההשהייה הזו עדיפה על המצב כרגע, אך כאמור, יריב זדוני יסרב כמובן). במאמר נכתב על כך בלקוניות, יותר מדיי לקוניות, כך:

"If a bogus route were to pass through the delay phase unnoticed, it would eventually propagate as occurs with BGP today"

באופן דומה, חסרון של הצעת המאמר השני על פני המאמר הראשון הוא שאין בה שום התגברות על Path Shortening Attack. מהמאמר עצמו אין אנו יכולים להיות בטוחים אם ה־PGBGP יראה בכך מסלול חדש וחשוד - שכן לא ברור איך אותה יוריסטיקה תגיב לגבי חלק מהמצבים של Path Shortening Attack. לדוגמה, לרשת־עצמאית א' יש מסלול לרשת ב' דרך ג', לאחר זמן מה היא מחליפה למסלול דרך ד', ואח"כ היא תקבל UPDATE של מסלול קצר יותר דרך ג', שהוא הלכה למעשה המסלול הקודם אחרי זריקת קדקודים ממנו. האם המסלול החדש הזה ייכנס למשפחת המסלולים החשודים וידווח, או שמא הוא יחשב כחלק מהנורמלי ויתועדף? אין לכך תשובה במאמר, ועל כן ניתן להניח שחלק מהיישומים של PGBGP עלולים לתעדף מסלולים שנבחרו מתוך Path Shortening Attack, בעוד המאמר הראשון דואג באמצעות IRV לוודא תקינות של כל מסלול חדש, ולכן מסלול מקוצר עם קדקודים שנזרקו לא יתקבל אצלו כלל.

המאמר השני מבקש כחלק מדרך הפתרון שלו ליצור היסטוריה של מסלולים אמינים. לצורך כך יש להפעיל את תכנת ה־PGBGP למשך תקופת זמן קצובה (h ימים) שבמהלכה הנתב לומד מה נחשב "נורמלי". אמנם זו בסה"כ הצורה הסבירה ביותר שניתן להעלות על הדעת, אך קיים בה חיסרון, והוא שההצלחה תלויה לחלוטין בתאריך הפעלת התכנה. ייתכן שבשל צירוף מקרים, שאינו נדיר ברשת האינטרנט, תכנת ה־PGBGP תתחיל לפעול בדיוק ביום שיש בו ניסיון מכוון לפגיעה או אפילו טעות בהגדרה שתגרום לנתב להאמין שמסלול שקרי הוא נורמלי. אח"כ תיקון שלו יהיה קשה במקצת, שכן בניגוד לנתב BGP רגיל שיחזור למסלול הנכון אחרי שהמסלול הרע יעלם, נתב PGBGP ידבוק במסלול הרע זמן רב ולא יחליף עד אשר לא תהיה לו ברירה. אנו רוצים לציין שהחסרון כשלעצמו אינו שהמנגנון מאפשר כאלו מצבים, שכן זה רק סימפטום לכך שההצעה אינה מושלמת אלא, כפי שכתבו המחברים, מדובר ביוריסטיקה לבחירת מסלולים טובים, ויוריסטיקה כשלעצמה אינה פתרון מושלם. מה שכן, החסרון הוא התלות וההסתמכות על מזל, שבו שני מפעילי רשת יאמצו את אותה הטכנולוגיה שבוע אחרי שבוע וכל אחד מהם ייתקל בהתנהגות שונה של הרשת, מצב שאינו רצוי.

3.4 סוף דבר

בסיכומו של דבר, מבחינת חולשות, IRV מפגין חולשות רבות יותר לגבי סבירות היישום שלו, היות שהוא דורש שיתוף פעולה רב יותר של רוב הרשת כדי לתפקד, בעוד PGBGP מבקש רק מחלק קטן ומרכזי שיתוף פעולה. לעומת זאת, IRV מתמודד טוב יותר עם נסיונות זיוף אקטיביים של מסלולים, שהוא הדבר כשלעצמו איתו אנו מנסים להתמודד. אמנם גם PGBGP מתמודד עם מסלולים בעייתיים, אך הוא סובל מ־False Positives ובסופו של יום הוא רק יוריסטיקה שמאפשרת לנחש, באופן טוב אך לנחש, מסלולים טובים על פני רעים. יש לציין אבל שדרך ההתמודדות של PGBGP מהירה יותר מבחינת תקורה מאשר של IRV.

4 השלב הבא

נבקש להציע שני שיפורים קטנים לנסיונות האבטחה של BGP כפי שהוצגו קודם במאמרים הראשון והשני. השיפורים הם תוספות קטנות ואינן כמובן משתוות להצעות הנהדרות שהוצעו בשני המאמרים. אנו מקווים בצניעותינו שהצעותינו תתקבלנה בהבנה למרות פשטותן, שכן כוונתן טובה.

4.1 אימות תקשורת

נרצה להציע שיפור קל למה שהוצע בשני המאמרים שבהם עסקנו, במטרה לשפר את עמידותם בפני נסיונות הכרזה שגויה של בעלות על קידומות. ההצעה שלנו רלוונטית בעיקר עבור המאמר השני, שכן היא אינה משפרת במאום את התפקוד של IRV כל עוד הוא מיושם על כל רשת האינטרנט. היות שאנחנו לא מאמינים שדבר שכזה סביר או ישים, מלכתחילה אנחנו מתייחסים בעיקר להצעת ה־PGBGP ונסב את תשומת הלב לכך שהצעתנו שימושית גם עבור IRV במידה שהוא לא מיושם על כל רשת האינטרנט.

בשני המאמרים מתווסף לנו, בנוסף לנתב ה־BGP, גם שרת המדבר את הפרוטוקול של ההצעה החדשה (IRV או PGBGP, תלוי במאמר) שמאפשר לבחון מסלולים ולאתר מסלולים חשודים. בהינתן מצב שבו ניתוב הרשת עובד (לדוגמה, "המצב הנורמלי" של PGBGP), נרצה להציע שבהינתן קבלת UPDATE על מסלול חדש יבצע וידוא של המסלול החדש באמצעות הישן. השרת שלנו ישלח הודעה (בסגנון ping) ל־AS המיועד דרך המסלול המוצע החדש שגילינו, ואז תשאל דרך המסלול הקיים, הישן, את ה־AS המיועד אם ההודעה שלנו הגיעה אליו. את ההודעה נשלח לשרת המיועד שהוא מריץ (IRV או PGBGP), זאת במידה שהרשת־העצמאית המיועדת אכן מריצה שרת שכזה (המקרה שלא מטופל בפסקאות הבאות). במידה שהוא ישיב שכן, אנו יודעים בוודאות

שהמסלול החדש אליו כשר, שכן ההנחה שלנו היא שהמסלול המקורי כשר אף הוא, ולכן מהתשובה של הרשת־העצמאית המיועדת נדע שהגענו אליה דרך המסלול החדש. אחרת, אם נשאל את הרשת־העצמאית המיועדת אם התקבלה הודעה ולא התקבלה, נדע שהמסלול החדש שהוצע לנו הוא זיוף. נשים לב שהשיטה שהצענו טובה גם ל־Prefix Hijacking וגם ל־Sub Prefix Hijacking, שכן כל דיווח על מסלול שאינו מוכר לנו ועדיף על מסלול נוכחי ליעד קיים ייבדק כך. חיסרון בהצעה שלנו הוא שהצעתנו אינה מטפלת כלל בנושא של Path Spoofing דוגמת Path Shortening Attack, שכן במקרה כזה נקבל תשובה חיובית מהרשת־העצמאית המיועדת על כך שתגובתינו הגיעה אליה, אך לא נוכל לזהות כך שאכן מתבצע Path Spoofing. נרצה לטעון שזהו אינו חיסרון מהותי, ונצטט את המאמר השני (פרק 2) באומרו:

> "Path spoofing attack are currently the least common of the three form of attack [the others being Prefix hijack and Sub-prefix hijack. O.S.]. One reason is that a malicious agent must gain access to a BGP router in order to perform a path spoofing attack."

נטען שתחת הנחה מקלה סבירה, נוכל להשתמש באותו מנגנון גם ללא דרישה שהרשת־העצמאית המיועדת מריצה שרת IRV או PGBPG. הנחתנו היא שרוב הרשתות־העצמאיות אינן זקוקות למסלול ניתוב לרוב הרשתות־העצמאיות האחרות, שכן לעולם לא תהיה תקשורת ביניהן. לדוגמה, הרשת העצמאית של "מכון אוסלן למדע ומחקר" הקוריאני (רשת־עצמאית מספר 38664) ככל הנראה לעולם לא תנווט שום תעבורה ל־"רשת לוויני גילת בע"מ" הישראלית (רשת־עצמאית 56804), שכן רוב תעבורת הרשת מרוב הרשתות־העצמאיות מנותב בסופו של דבר אל קבוצה קטנה יחסית של רשתות־עצמאיות, ואלו כמובן שתי דוגמאות אקראיות מבין עשרות אלפי רשת־עצמאית ממוצעת ברוב המקרים לא תנווט לאוניברסיטה נידחת או למשתמשים של ספק אינטרנט קטן (או אפילו בינוני). באמצעות הנחה זו נתאר מנגנון דומה למנגנון שהוצע קודם שיאפשר לנו לוודא שמסלול חדש שמדווח לנו הוא אכן מסלול אמיתי, אבל אך ורק למסלולים שנשתמש בהם. היות שרוב המסלולים שנקבל לצורך ניתוב הם חסרי־תועלת לפי ההנחה, המנגנון שלנו ישומש פעמים מעטות (יחסית לכמות הרשתות־העצמאיות הקיימות) וכך התקורה הגבוהה יחסית בשימוש שלו יהיו מזעריים ביחס הכולל. נרצה אבל, להציע שמצב זה ייבדק אמפירית. אנחנו חושבים שנתונים סטטיסטיים על אחוז הניתוב ההולך מרשת־עצמאית ממוצעת (והשונות בניתוב) אל כל רשת־עצמאית אחרת יוכל ללמד אותנו רבות על ניתוב תעבורה באינטרנט, ואף יוכל לשפר את נסיוננו להתמודד עם בעיות בתחום.

המנגנון יפעל כך - מצב מסויים יהיה מצב של בדיקה שבו יילמד מה הוא מצב "נורמלי", בדומה ל־PGBGP. לאחר המצב הזה כל מסלול שקיים ייחשב למסלול אמיתי. היה ובקבלת UPDATE יתגלה לנו מסלול טוב יותר מהמסלול הקיים, נתייחס אליו בחשדנות, בדומה ל־PGBGP ונשמור אותו אצלנו בטבלה מרוכזת (את קבלתו, פרסומו וכדומה נבצע בהתאם להנחיות של PGBGP, שהמנגנון שלנו פועל מעליו). כל עוד אין תוכן לנתב ליעד המסויים הזה, אין שום עניין בשאלה האם המסלול החדש כשר או אם לאו. בהינתן שמישהו בתוך הרשת־העצמאית שלנו מעוניין לשלוח חבילת־מידע לרשת־עצמאית אחרת, שיש לנו שני מסלולים אליה (אחד מהם בטבלה), נשלח את חלקה הראשון של ההודעה דרך המסלול המקורי (הנורמלי) וחלקה השני דרך המסלול החדש. את פיצול ההודעה ל־2 אפשר לעשות דרך המנגנונים המוכרים של TCP לפיצול חבילות או מעקב אחרי הסדר שלהם (איננו מתייחסים למצב בו החבילה אינה חבילת TCP אלא UDP או כל פרוטוקול אחר), אם נקבל הודעה על כך שהחלק השני של ההודעה לא הגיע נדע כי יש בעיה במסלול החדש לעומת הישן, ונוכל להבין כי מדובר במסלול פגום שנחטף. המנגנון עצמו הוא יקר שכן הוא עוצר את שליחת ההודעה המקורית לזמן מה עד אשר יש לנו אישור שהחבילה הגיע, אך זהו זמן קצר וחד־פעמי, שהחל ממנו המסלול נחשב לאמין ונשתמש בו ללא שינוי עד אשר יגיע אלינו מסלול חדש לשימוש. נרצה לטעון כי בהנחה שיש נתב זדוני באמצע המסלול המנסה לעבוד עלינו שהמסלול תקין, אין לו דרך לדעת מה להחזיר לנו, שכן אין לו את כל המידע (חלק מהתקשורת נשלחת דרכו וחלק לו), ומהא־סימטריות התקשורת ברשת, לא בטוח שהמסלול חזרה עובר דרכו. אלו בטוחות שמאפשרות לנו להגביר את הביטחון שלנו במסלול הקיים.

4.2 אימות נתיב

נרצה להציע פתרון לחולשה במנגנון ה־IRV מהמאמר הראשון על ידי שימוש בטכניקה מתחום ההצפנה. כפי שהצבענו מעלה בפרק 3.3.1, שרת ה־IRV מתבקש לענות על שאלות לגבי שכנים, שאלות שכוללות חשיפת מידע על נתונים עסקיים פנימיים. לדוגמה, רשת־עצמאית תוכל לנסות לברר כך האם שכנתה מונעת ממנה מסלולים מסויימים, כמודגם באיור:

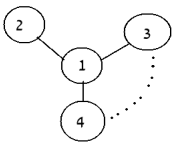
1. רשת־עצמאית 2 מעדכנת את רשת־עצמאית 1 לגבי בעלות על קידומת מסויימת.
2. רשת־עצמאית 1 מעדכנת את רשת־עצמאית 3 על קיום מסלול דרכה לרשת־עצמאית 2 ולקידומת שהיא בעליה. היא אינה מעדכנת בכך את רשת־עצמאית 4 מסיבות כלכליות.

3. עם פעפוע המידע ברשת, רשת־עצמאית 4 מעודכנת על קיומו של מסלול לקידומת בבעלות 2 שעוברת דרך הרשתות־העצמאיות 3, 1.

4. בהתאם לפרוטוקול ה־IRV רשת־עצמאית 4 שואלת את רשת־עצמאית 1 האם יש מסלול ממנה ל־3 ול־2.

(א) אם רשת־עצמאית 1 תענה את האמת, אזי רשת־עצמאית 4 תדע ששכנתה מסתירה ממנה מידע וכך תגלה חלק מהסודות הכלכליים של 1.

(ב) אם רשת־עצמאית 1 תענה בשקר, אזי רשת־עצמאית 4 תימנע מלבחור מסלול כשר, ולמעשה ייתכן שתגרום למסלול להתפוגג מכול האינטרנט שכן הוא יוכרז כמסלול פסול ברשת הדיווח המוצעת.



נשים לב שבעיה זו חמורה יותר ב־sBGP כפי שכתבנו מעלה, שכן שם הסודות המסחריים חתומים הלכה למעשה עם הצפנה, ועל כן לא ניתן אפילו לשקר למי שרוצים.

נרצה לטעון כי יש שני דברים בעייתים במה שהצגנו קודם, כאשר שרת IRV של רשת־עצמאית נשאל לגבי מסלול. הראשון הוא שהשרת יודע ישירות מה תהיה תוצאת תשובתו. "אמת" תמיד תכפה אמיתות מסלול ו־"שקר" תמיד זניחה שלו. לא ניתן לשאול את השאלה באופן אחר ("האם אין מסלול בינך לבין 3?") שכן עצם שאילת השאלה מראה על עניין במסלול מסויים. בכך שהשרת יודע מה השאלה ומה השפעת תשובתו, הוא יוכל כך לבחור בצורה מושכלת את תשובתו - נניח, אם יחסיה של רשת־עצמאית 1 עם 4 חשובים, הוא יעדיף לשקר ולגרום לקריסה של מסלול גדול של רשתות שאינן קשורות אליו כהוא זה. הבעיה השנייה היא שאין לו שום סיבה להניח שהשאלה הגיעה ממישהו קשור, לדוגמה, 4 יכול סתם לרצות לבדוק את עומק היחסים בינו לבין 1 ולהתחיל לשאולו שאלות אקראיות על מסלולים כדי להבין בערך מה קורה גם אם הוא לא יודע על מסלול מסוים העובר דרך 3.

לדעתינו ניתן לפתור בעיה זו באמצעות הצפנה. השיטה שנרצה להשתמש בה מכונה הצפנה הומומורפית[7] שהתגלתה ב־2009, ואמנם במקור הייתה מסובכת מאוד, אך כיום היא "מספיק פשוטה כדי שניתן יהיה להסבירה באמצעות פוסט בבלוג"[8]. הרעיון בהצפנה זו, שבהינתן טקסט m, פונקציית הצפנה E ופונקציה **חשיבה כללית כלשהי** f מתקיים כי $E(f(m)) = f(E(m))$. קרי, ניתן לבצע פעולות על הטקסט המוצפן, ותוצאות הפעולות תהיה ההצפנה של ביצוע הפעולות על הטקסט המקורי. נתאר באמצעות שיטה זו שיפור לשרתי ה־IRV כך שמצד אחד שרת לא יוכל לדעת חד־חד־ערכית מה תהיה ההשלכה של תשובתו, ומהצד השני יהיה בטוח שהוא עונה לצד הקשור בעניין.

4.2.1 הפרוטוקול

אנו מניחים, כמו במאמר הראשון, שלכל רשת־עצמאית ישנו שרת IRV. לכל רשת־עצמאית ישנו מפתח־הצפנה ופונקציות הצפנה ופענוח של שיטת הצפנה הומומורפית, המפתח הפומבי שלה יכול להיות מאוחסן בשרת ה־IRV כחלק משאר הפרטים המפורסמים שם. כל שרת יכיל את רשימת כל המסלולים שנתב ה־BGP פרסם, ולמי הוא פרסם אותם. בנוסף, נגדיר שתי משפחות פונקציות הידועות לכל, והן פונקציית התחילית p_{m_2} שמקבלת מחרוזתm_1 ובודקת האם מחרוזת m_2 קבועה מסויימת תחילית של m_1, אם כן מחזיר 1, אחרת 0; ופונקציית התחילית ההפוכה $\overline{p_{m_2}}$ (שהיא הפעלת הפונקציה הבוליאנית not על הפונקציה p_{m_2}).

בהינתן מסלול שנלמד מרשת־עצמאית x לרשת־עצמאית y לקידומת IP מסויימת α שבבעלות רשת־עצמאית z (ייתכן כי $x = z$, אין זה משנה), שרת ה־IRV של y יבצע את הפעולות הבאות:

1. יקודד את המסלול שהתקבל בצורה סטנדרטית - $z, \ldots, x, y$ בדיוק כפי שנלמד מ־x עם אותם NEXT HOP.

---

[7] C Gentry, **Fully homomorphic encryption scheme**, PhD thesis, Stanford University, 2009. http://crypto.stanford.edu/craig & C Gentry, **Fully homomorphic encryption using ideal lattices**, *STOC pp. 169-178*, 2009.

[8] הציטוט מהמאמר Craig Gentry, Amit Sahai, Brent Waters, **Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based**, *CRYPTO 2013 Lecture Notes in Computer Science Volume 8042, pp 75-92*, 2013. הפוסט בלוג עצמו של פרופ' בועז ברק וד"ר צביקה ברקרסקי (חלק א', בסופו קישור לחלק ב') - http://windowsontheory.org/2012/05/01/the-swiss-army-knife-of-cryptography/

2. יבקש משרת ה־IRV של x את $E_x(m)$ כאשר E_x היא ההצפנה לפי המפתח של x וכאשר m הוא המסלול של x לקידומת α כפי שמקודד בצורה הסטנדרטית.

3. יטיל מטבע הוגן כדי לבחור $f \in \{p, \overline{p}\}$ (p ־ 0, $\overline{p}$ ־ 1), יחשב את $f(E_x(m))$ וישלח את התוצאה ל־x.

4. x מקבל את $E_x(f(m))$, מפענח את הקלט לפי המפתח שלו ומקבל את $f(m)$, שהוא ביט יחיד של 0 או 1. הוא מחזיר אותו ל־y.

5. אם כעת y יבדוק לפי המטבע שלו מה הוציא f וידע האם מדובר בתחילית או לא (לדוגמה, אם $f = \overline{p}$ והתקבל 0, הוא ידע שאכן מדובר בתחילית).

את הפעולות האלה יבצע y לכל רשת־עצמאית במסלול שהוא קיבל מ־x. לכל רשת כזו שרת ה־IRV של y ירצה לבדוק האם המסלול הוא ישיר (אין קפיצות בו, וכל אחד במסלול הוא שכן של מי שהוא אמור להיות בו). נניח המסלול נראה כך ־ z, x, y (לשם הפשטות, אך הדבר נכון לכל מסלול), y ירצה לדעת האם באמת z העביר ל־x מסלול אליו. ניתן לבצע זאת באותו אופן כמו 5 הצעדים קודם, רק שהפעם מה שיישלח תהיה רשימת האנשים ש־z עדכן אותם (תת־קבוצה של רשימת השכנים שלו) והפונקציות ש־y ייחשב הן s_x ־ שמקבלת מחרוזת m_1 ובודקת האם x נמצאת בתוכה, והפונקציה $\overline{s_x}$ שהיא שלילה שלה.

כעת, נוכל להשתמש באותה הצפנה כדי להוכיח שאנחנו אכן "קשורים". הכוונה בקשורים, זה שאיננו הולכים לשאול סתם את השרת הבא במסלול, אלא שהוא ידע ששכן שלו עדכן אותנו במסלול אליו. נשתמש בחתימה דיגיטלית באמצעות המפתח הפרטי והמפתח הפומבי של כל שרת. הפעם, בניגוד ל־sBGP שבו מה שנחתם הם מסלולים שלמים שכוללים מידע רב על שותפיות, הדבר היחיד שיחתם זה שנכון לזמן מסוים יש קשרי שכנות בין x לבין y (כולל TTL שבו הודעה זו תפסיק להיות בתוקף). כך y יוכל להוכיח ל־z או לכל מי שנמצא לפני x במסלול שהוא שואל אותם את השאלה הזו כדי לוודא מסלול שאכן הגיע לידיעתו והוא לא שואל אותם סתם כדי להשיג מידע, אלא על משהו קונקרטי.

4.2.2 נכונות

נשים לב שבעת שאילת שרת ה־IRV עכשיו, הוא אינו יכול לדעת מה תהיה ההשפעה של התשובה שהוא מחזיר בסוף צעד 4, זאת בשל השימוש בשתי פונקציות שתוצאותן מוצפנת. כך גם הוא לא יוכל לתכנן מראש האם כדאי לו לבחור מסלול אמיתי שעובר דרכו או שקרי. למעשה, הוא אינו יודע בשום שלב מה הוא נשאל ומה הוא עונה, ועל כן הוא אינו מפסיד כלום מלענות את התשובה הנכונה, או מרוויח מאום מלתת תשובה שגויה. כעת כל הקדקודים במסלול נתון ידעו שאין להם יתרון בלשקר, וכך בסוף בדיקה נוכל להניח בהסתברות גבוהה יותר מאשר בשימוש רגיל ב־IRV שאכן המסלול שלנו אמיתי (או שקרי) על ידי שאילת כל הקדקודים באמצע. בנוסף, נשים לב ששרת IRV שיעדיף לא לענות לפנייה אוטומטית יוודע כאחד המנסה להסתיר מידע מאוד מסוים לגורם מאוד מסוים, דבר שהלכה למעשה יחשוף מידע על חלק מהאינטרסים העסקיים שלו, שאותם הוא מנסה להסתיר על ידי כך שהוא אינו עונה לפנייה. השיפור שהצענו גם יאפשר לשרתים לדעת לאן מגיע המידע שהם מפרסמים בסופו של דבר וכך יוכל לעזור להם למנוע מאינטרס עסקי לדלוף בלא ידיעתם לגורם בעל־עניין. לדוגמה, באיור מעלה, גם ללא שרת IRV 4 יכול לחשוד ש־1 לא מספר לו מידע מרגע שהגיע אליו המסלול ל־2 דרך 3 ו־1, אך ברגע ש־1 יישאל על ידי 4 לכך, 1 יוכל להתחיל לדון עם 3 בנושא ולבקש ממנו לא לפרסם את המסלול הזה לכל רשת־עצמאית שדרכה המסלול יוודע ל־4. כך 1 יוכל לדעת לשמור טוב יותר על האינטרסים העסקיים שלו.

בכיוון ההוכחה של הקשר והשכנות, אנחנו משתמשים בנכונות של חתימה דיגיטלית, טכניקה ותיקה ומוכרת בתחום המאפשרת לנו לדעת בוודאות ששואל השאלה אכן שואל אותה מתוך קשר ושכנות.

5 סיכום

פרוטוקול ה־BGP ימשיך כנראה בעתיד הנראה לעין לשמש כפרוטוקול הניתוב המרכזי ברשת, למרות חולשותיו. סקרנו שתי הצעות בנות עשור לערך לתקנו שכל אחת מציעה גישה אחרת - גישה כוללנית הפותרת בעיות רבות אל מול גישה יוריסטית המאפשרת להימנע מהן בהסתברות גבוהה. אף על פי ששתי ההצעות מגיעות מנקודת מוצא משותפת, כל אחת מהן לקחה את הצעתה לכיוון אחרת, ואף הראתה חולשות בחלקים שונים - סיכוי יישום לעומת הצלחה ברורה בהתגברות על התקפות. בסוף עבודתנו הצענו שתי הצעות קטנות שמנסות לתת מענה לשתי בעיות בפרוטוקול, והן האם מסלול חדש אכן מוביל ליעד מסויים, והאם המסלול שמדווח לי הוא אכן המסלול האמיתי שדרכו אעבור בפועל. הצעתינו הראשונה הייתה ניסיון לנצל כלי ישן ומוכר דוגמת TCP יחד עם הכלים בשני המאמרים ולרתום את מנגנון דיווח החבילות האובדות שלו לצורך בדיקה. הצעתינו השנייה כללה שימוש בכלי הצפנתי חדש לצורך התגברות על מכשול עסקי ביישום הצעה מאחד המאמרים. תוך כדי הצענו גם לבדוק התפלגות נתוני תעבורה בין רשתות־עצמאיות שונות כדי לתמוך בהשערה שהעלינו.