מגישים: 200878627 יניב לידן
204736961 דן אברהם

עבודה 4 – תקשורת

שאלה 1:

א. תרחיש כזה יכול להיות במידה ומשתמש A שולח data-fragment ל-B. ה-fragment עובר בין נתבים ומגיע לנקודה שלא יכולה להעביר את כל ה-fragment אז היא מפצלת אותו ושולחת אותו בכמה חבילות כאשר אינן נשלחו במקור ממשתמש A אך הגיעו למשתמש B.

ב. הספקית ISP יכולה לנצל את השדות DSCP ו-ECN ב-IP Header כך שתזהה את החבילות שנשלחות ע"י המתחרים שלה ותיתן להן עדיפות נמוכה יותר בטיפול כך שהשירות שהמתחרים שלהם יתנו יהיה פחות טוב, דבר שעלול לגרום למעבר של לקוחות מהמתחרים אליהם.

שאלה 2:

א. מתקפות מסוג prefix hijack שפעלו בשנים האחרונות פעלו כך שהתוקף יצר רשת עם פרוטוקול שונה ל-gateway שגורם ל-routing tables להיות מאין רשתות וכך התוקף שם את הכתובת שלו ברשת זו. כך יכול התוקף לנצל את חוק ה-longest prefix match ע"י יצירת טווח קטן יותר של כתובות ברשת זו כך שתעבורת הנתונים ברשת תגיע אליו.

ב. Origin authentication מבטיח ניתוב בטוח ברשת ע"י שימוש ב-certifications וכן ב-resource public key infrastructure וכך מונע התקפות מסוג prefix hijack.

ג. Origin authentication לא יכול למנוע מתקפות בהן קיים certification לכתובת של התוקף והניתוב עובר דרך הרשת של התוקף אז Origin authentication לא יהיה יעיל.

ד. BGPSEC מצריך אישור של כל רשת חדשה, כך שהתוקף לא יכול ליצור רשת חדשה דרכה יעברו הנתונים ללא אישור ספציפי של הרשת.

ה. סדר העדיפויות של הניתובים עפ"י Ases ב-BGP רגיל:

I. לקוחות, שותפים, ספק.
II. קצרים, ארוכים.
III. אזורים גיאוגרפים.

ו. ב"מקרה 3" במאמר, הניתובים הנקבעים ע"י Ases ב-BGPSEC:

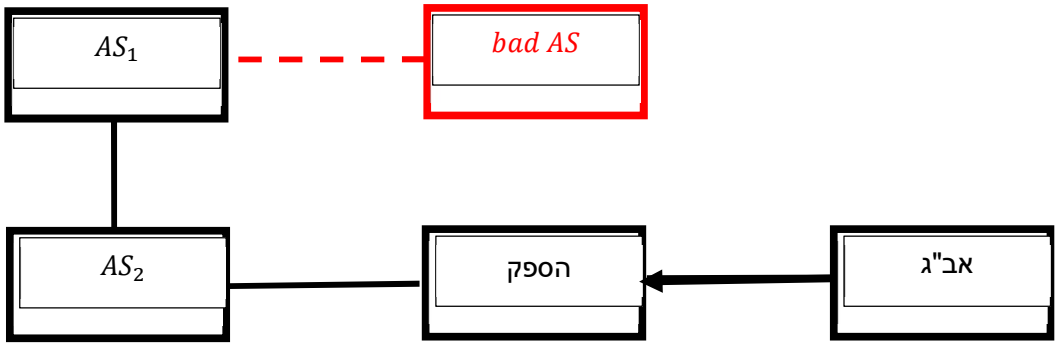
I. לקוחות, שותפים, ספק.
II. מאובטח, לא מאובטח.
III. אזורים גיאוגרפים.

ז. 3491 (client): (3491, 174), (21740, 174), (3536, 3365, 174)
21740(peer): (21740, 174)
3356(peer): (3356, 174)

ח. חסרון ראשון: התייחסות לניתובים מאובטחים עלולה לגרום ל- BGP wedgies בין ASים.
חסרון שני: ניתן לבצע את ההתקפות בגלל השימוש ב-BGP.

מגישים: 200878627 יניב לידן
204736961 דן אברהם

ט. ה-AS הזדוני מפרסם ל-ASים השכנים את הניתוב שלו כניתוב קצר בפרוטוקול BGP.
ה-ASים השכנים לא יוודאו זו בגלל ה-BGPSEC. וכך ייווצר מצב (בשרטוט) ש-AS_1 יעדיף לשלוח נתונים דרך ה-AS הזדוני מאשר דרך AS_2.



שאלה 3:

א. לרוב ב-WAN משתמשים ב over-provisioning גבוה כיוון שבמידה וקישור מסוים כושל ניתן להעביר אותו לקישור אחר ברשת (שקיים בעקבות ה over-provisioning).

ב. החיסרון בשימוש ב over-provisioning גבוה הוא ששימוש בפס רחב גורר עלויות גבוהות יותר, מה שמייקר את האחזקות.

ג. 4 מאפיינים ייחודיים לרשת הפנימית של גוגל לעומת WAN אחרות:

I. אפליקציות שדורשות רוחב פס גבוה יותר ברשת הפנימית יקבלו אותו ויפנו אותו או יאטו בהתאמה את קצב השידור במידה וצריך.
II. ברשת הפנימית של גוגל יש לחברה שליטה מלאה בכל המשאבים ברשת(יישומים, שרתים וכד').
III. יש שליטה ברוחב הפס.
IV. יש שליטה מלאה בתעבורת הנתונים ברשת ממקום אחד ייחודי.

ד. יתרון ראשון: הקצאה דינמית של רוחב הפס.
יתרון שני: שליטה ממקום אחד וייחודי (forwarding table).

שאלה 4:

א. חסרון ראשון: Round Robin מגביל את כמות החבילות בבקשה ולא מתייחסת לגודל החבילות, לכן ייתכן שבקשה ובה X חבילות קטנות יחסית תחכה הרבה לבקשה עם X חבילות גדולות בהרבה.
חסרון שני: Round Robin לא לוקח בחשבון תלויות בין חבילות כלומר, אם בבקשה מסוימת יש חבילות שתלויות בחבילות אחרות שנמצאות בבקשה אחרת ייתכן שהיא תשלח את החבילות שלה לפני שהחבילות שבהן היא תלויה יישלחו קודם.

ב. השיטה הנלמדה לפתור את החסרונות של Round Robin היא למשקל את הבקשות וליצור מאין priority queue כך שניתן לתת עדיפות לבקשות לפי גודל החבילות ולפי תלויות בניהן.

מגישים: 200878627 יניב לידן
204736961 דן אברהם

ג. נעטוף את חבילת ה-IPv6 בחבילה של IPv4 בנתב B, ונוריד את העטיפה בנתב E כך שהנתבים C, D שלא תומכים ב-IPv6 יוכלו להעביר את החבילה.

שאלה 5:

כיוון שאלגוריתם distance-vector מתבסס על אלגוריתם Bellman-Ford, ובכל איטרציה כל ראוטר ברשת מקבל ושולח לכל השכנים את ה distance-vector, הזמן שייקח (בהנחה שנגדיר כל ראוטר כקודקוד וכל DV כקשת) הוא הזמן של אלגוריתם Bellman-Ford שהוא $O(VE)$, כלומר O של מספר הראוטרים כפול מספר ה-transitions בין הראוטרים.

שאלה 6:

א. נגדיר A ו-B שני מחשבים.
נבצע tracert מ-A ל-B. אם אין תגובה, נבצע את התהליך מחדש עבור השכנים של A.
אם עדיין אין תגובה נסיק שיש packet loss. נאתר את הנתב הראשון ממנו לא הייתה תגובה ונעריך כי הוא הנתב הבעייתי.

ב. נגדיר A ו-B שני מחשבים.
נשלח PING מ-A ל-B ובאופן דומה לסעיף א' נעריך את מיקומו של הנתב הבעייתי תוך חיסכון מירבי במספר החבילות שנשלחות.

ג. כיוון שאנו מוצאים packet loss ייתכן והנתב הבעייתי העביר חבילה שלא טופלה היטב במקום או שהוא לא העביר אותה, לכן אם העביר חבילה שלא טופלה היטב היא עלולה להיאבד באחד בנתב שאינו בהכרח בעייתי ולכן בשיטות המצוינות בסעיפים א' ו-ב' אי אפשר להגיד בוודאות שהשרת שמצאנו הוא הבעייתי, אלא המיקום עצמו.

שאלה 7:

N'	A	B	C	D
	0	$3,B$	∞	∞
A		$3,B$	∞	∞
AB			$13,B$	$11,B$
ABD			$12,B$	
$ABDC$	0	$3,B$	$12,B$	$11,B$