ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Επταμηνιτάκης Γεώργιος

Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Επόπτης Μεταπτυχιακής Εργασίας: Αναπλ. Καθηγητής, Ξ. Δημητρόπουλος

Παρασκευή, 18 Μαρτίου 2022, ώρα 12:00 μ.μ.

Join Zoom Meeting

https://zoom.us/j/99097016946

" BPHS: Ένα εργαλείο προσομοίωσης επιθέσεων προθέματος BGP που υποστηρίζει φιλτράρισμα RPKI"

ΠΕΡΙΛΗΨΗ

Το πρωτόκολλο *BGP (Border Gateway Protocol)* χρησιμοποιείτε από τα Αυ- τόνομα Συστήματα (όπως, Comcast, AT&T, COSMOTE) ώστε να διαφημίζουν στο Internet μονοπάτια δρομολόγησης για το σύνολο του χώρου IP διευθύνσεων (δηλαδή, IPv4/IPv6 προθέματα δικτύου) και να εγκαθιδρύουν inter/intra-domain διαδρομές στο Internet. Παρά την επεκτασιμότητα και την δυνατότητα να εκφράζει πολύπλοκες πολιτικές δρομολόγησης, το BGP (από το σχεδιασμό του) δεν διαθέτει κανένα μηχανισμό ασφάλειας, όπως είναι η πιστοποίηση των διαφημιζόμενων διαδρομών. Έτσι, ένα Αυτόνομο Σύστημα έχει την δυνατότητα να διαφημίζει παράνομες διαδρομές για προθέματα IP που δεν κατέχει. Αυτές οι παράνομες ανακοινώσεις διαδίδονται και μολύνουν πολλά Αυτόνομα Συστήματα ή και ακόμα ολόκληρο το Internet, με αποτέλεσμα να επηρεάζουν τη διαθεσιμότητα, την ακεραιότητα και το απόρρητο των επικοινωνιών. Το φαινόμενο αυτό ονομάζεται *πειρατεία προθέματος BGP (ή BGP prefix hijacking*) και μπορεί να προκληθεί είτε από λάθος παραμετροποιήσεις δρομολογητών, είτε από κακόβουλες επιθέσεις.

Το *RPKI (Resource Public Key Infrastructure)* είναι ένα ιεραρχικό σύστημα πι- στοποίησης που στοχεύει στην προστασία του Internet από αυτές τις επιθέσεις πειρατείας προθέματος BGP, εισάγοντας την πιστοποίηση ιδιοκτησίας προθέματος IP. Παρά τον σημαντικό του ρόλο στην ασφάλεια του Internet, η ανάπτυξη του RPKI είναι αργή (χρησιμοποιείτε περίπου από το 20% των Αυτόνομων Συστημάτων στο Internet) λόγω της περιορισμένης υιοθέτησης του από τα περισσότερα Αυτόνομα Συστήματα (δηλαδή, προστατεύει ένα Αυτόνομο Σύστημα μόνο όταν ένας μεγάλος αριθμός από Αυτόνομα Σύστηματα το χρησιμοποιεί ήδη) και λόγω των πολύπλοκων μηχανισμών του που οδηγούν σε ανθρώπινα λάθη.

Αρκετές ερευνητικές εργασίες έχουν προσπαθήσει να εκτιμήσουν τον αντίκτυπο των επιθέσεων πειρατείας προθέματος BGP και τα οφέλη της υιοθέτησης του RPKI στο Internet μέσω αλγορίθμων προσομοίωσης που μοντελοποιούν το γράφημα του Internet και το πρωτόκολλο BGP. Ωστόσο, δεν υπάρχει καμία σχετική εργασία που να προτείνει έναν προσομοιωτή BGP ο οποίος να επιτρέπει στους διαχειριστές δικτύων να αξιολογούν γρήγορα και εύκολα την ευπάθεια των Αυτόνομων Συστημάτων τους σε επιθέσεις πειρατείας προθέματος BGP και να διεξάγουν την έρευνα τους μέσω ενός φιλικού προς τον χρήστη εργαλείου (ή υπηρεσίας) προσομοίωσης BGP.

Σε αυτή την εργασία, εισάγουμε το *BPHS*, το πρώτο εργαλείο προσομοίωσης επιθέσεων πειρατείας προθέματος BGP που επιτρέπει στους διαχειριστές δικτύων (α) να αξιολογούν την ευπάθεια των Αυτόνομων Συστημάτων τους σε επιθέσεις προθέματος BGP και (β) να μετρούν τα οφέλη της υιοθέτησης του RPKI στο Internet, γρήγορα και εύκολα, μέσω μιας φιλικής προς τον χρήστη web εφαρμογής.

Αξιολογούμε το BPHS αναπαράγοντας πραγματικές ιστορικές επιθέσεις προθέματος BGP που εντοπίστηκαν στο Διαδίκτυο και αποκαλύπτουμε τα οφέλη της υιοθέτησης του RPKI πραγματοποιώντας μια συγκριτική μελέτη (χρησιμοποιώντας το BPHS) που δείχνει το ποσοστό επιτυχίας των επιθέσεων για διαφορετικά σενάρια φιλτραρίσματος RPKI. Επιπλέον, εξάγουμε δύο λίστες κατάταξης που δείχνουν τα πιο ευάλωτα Αυτόνομα Συστήματα και τις πιο ευάλωτες χώρες σε επιθέσεις πειρατείας προθέματος BGP, συμπεριλαμβανομένων των πιο ευάλωτων Ελληνικών Αυτόνομων Συστημάτων. Τα αποτελέσματα της αξιολόγησης δείχνουν ότι το BPHS εκτιμά τον αντίκτυπο των επιθέσεων με υψηλή ακρίβεια και ότι το φιλτράρισμα RPKI στην ραχοκοκαλιά του Internet μειώνει σημαντικά τις επιθέσεις προθέματος BGP.

University of Crete

Computer Science Department

M.Sc. Thesis

Eptaminitakis Georgios

Master's Thesis Supervisor: Associate Professor, X. Dimitropoulos

Friday, 18 March 2022, 12:00 p.m.

Join Zoom Meeting

https://zoom.us/j/99097016946

"BPHS: A BGP Prefix Hijacking Simulation Tool Supporting RPKI filtering"

ABSTRACT

The *Border Gateway Protocol* (BGP) is used by the Autonomous Systems (e.g., Comcast, AT&T, COSMOTE) to advertise AS paths for the corresponding routed IP address space (i.e., IPv4/IPv6 network prefixes) and establish inter/intra-domain routes in the Internet. Despite its scalability and capabilities of expressing complex routing policies, BGP lacks many security features by design, like the authentication of the advertised routes. Thus, an Autonomous System (AS) is able to advertise illegitimate routes for IP prefixes that it does not own. These advertisements propagate and "pollute" many ASes, or even the entire Internet, affecting service availability, integrity, and confidentiality of communications. This phenomenon is called *BGP prefix hijacking* and can be caused by either router misconfigurations or malicious attacks.

The *Resource Public Key Infrastructure* (RPKI) is a hierarchical certification system that aims to protect the Internet against these BGP prefix hijacking attacks, introducing IP prefix ownership authentication. Despite its crucial role in Internet security, RPKI deployment is slow (i.e., around 20% of the total ASes on the Internet) due to its limited adoption from most ASes (i.e., it protects an AS only if a large number of other ASes already use it) and due to its complex mechanisms resulting in human errors.

Several research works have tried to measure the impact of the BGP prefix hijacking attacks and the benefits of the RPKI adoption in the Internet through BGP simulation algorithms that model the Internet graph and the BGP protocol. However, there is not any related work proposing a BGP simulator enabling network operators to quickly and easily assess the vulnerability of their Autonomous Systems to BGP prefix hijacking attacks and conduct their study through a user-friendly and plug&play BGP simulation tool or service.

In this thesis, we introduce *BPHS*, the first BGP Prefix Hijacking Simulation tool that enables network operators to quickly and easily (a) assess the vulnerability of their Autonomous Systems to BGP prefix hijacks and (b) measure the benefits of the RPKI's adoption in the Internet, through a user-friendly web application.

We evaluate BPHS by replaying real historical hijacks detected in the Internet and reveal the benefits of the RPKI adoption by conducting a comparative study (using BPHS) showing the attacker's success rate for different RPKI filtering scenarios. In addition, we extract two rankings lists showing the most vulnerable ASes and countries to BGP prefix hijacking attacks, including the most vulnerable Greek ASes. The evaluation results show that BPHS estimates the impact of a hijack with high accuracy and that the RPKI filtering in the Internet backbone significantly reduces the BGP attacks.