ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Μαυρομμάτης Δημήτριος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Επικ. Καθηγητής, Ξ. Δημητρόπουλος

Δευτέρα,25/06/2018, 13:00
Αίθουσα B108,Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

"ARTEMIS$_{ONOS}$: Εφαρμογή SDN για ανίχνευση και αυτόματη αντιμετώπιση επιθέσεων BGP Prefix Hijacking σε πραγματικό χρόνο"

ΠΕΡΙΛΗΨΗ

Το BGP Prefix Hijacking είναι μια συνεχής απειλή για το σύστημα δρομολόγησης του Διαδικτύου, έχοντας σημαντικές τεχνολογικές και οικονομικές επιπτώσεις παγκοσμίως. Η ερευνητική κοινότητα έχει απαντήσει με εξειδικευμένες τεχνικές ανίχνευσης και αντιμετώπισης, οι οποίες δεν έτυχαν ευρείας αποδοχής. Αντιθέτως, οι μηχανικοί δικτύων συνήθως ακολουθούν απλές, δοκιμασμένες πρακτικές, που όμως έχουν περιορισμούς (π.χ. ταχύτητα).

Σε αυτή την εργασία, δημιουργούμε μια SDN εφαρμογή που βασίζεται στο πρωτότυπο ARTEMIS και αξιοποιεί το ONOS, ένα δικτυακό λειτουργικό σύστημα τεχνολογικής αιχμής. Η εφαρμογή ονομάζεται ARTEMIS$_{ONOS}$ και χρησιμοποιεί σύγχρονες, κοινώς διαθέσιμες υπηρεσίες BGP streaming και ανιχνεύει με ακρίβεια διαφορετικούς τύπους hijack. Επιπλέον, αντιδρά αυτόματα με τα κατάλληλα αντίμετρα.

Το ARTEMIS$_{ONOS}$ είναι μια επίσημη εφαρμογή του ONOS και αξιοποιεί όλα τα οφέλη που προσφέρουν τα δίκτυα SDN. Συγκεκριμένα, το ARTEMIS$_{ONOS}$ είναι υλοποιημένο ως

αρθρωτή εφαρμογή πάνω στο OSGi framework, και χωρίζεται σε ξεχωριστά modules για την ανίχνευση και την επίλυση των επιθέσεων. Επιτυγχάνει υψηλή διαθεσιμότητα και κλιμάκωση μέσω της κατανεμημένης αρχιτεκτονικής του επιπέδου δεδομένου του δικτύου. Επίσης, λειτουργεί ανεξαρτήτως την διαδικτυακής του υποδομής (π.χ. συσκευές δικτύωσης), επιτρέποντας να έχει εύκολη ανάπτυξη αλλά και μειωμένη περιπλοκότητα. Επιπλέον, αν και η εφαρμογή είναι βασισμένη σε SDN, είναι συμβατή με το BGP, συνεπώς έτοιμη να χρησιμοποιηθεί σε επιχειρησιακό επίπεδο.

Αξιολογούμε την εργασία μας υλοποιώντας μια πλατφόρμα που εξομοιώνει τις επιθέσεις BGP Prefix Hijacking. Το ARTEMIS$_{ONOS}$ ανιχνεύει την επίθεση και εκκινεί την διαδικασία αντιμετώπισης εντός μερικών χιλιοστών του δευτερολέπτου. Αντιθέτως, η πλήρης αντιμετώπιση της επίθεσης επιτυγχάνεται σε δευτερόλεπτα, το χρόνο που απαιτείται από το BGP για να συγκλίνει. Παρόλο που το ARTEMIS$_{ONOS}$ είναι μια εφαρμογή που αντιδρά μετά τη εκκίνηση της επίθεσης, η αντιμετώπιση της σε ορισμένες περιπτώσεις είναι ταχύτερη από τη διάδοση της, προστατεύοντας το δίκτυο σχεδόν προληπτικά.

Mavromatis Dimitrios
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Assistant Professor, X. Dimitropoulos

Monday, 25/06/2018, 13:00
Room B108, Computer Science Dept., University of Crete

“ARTEMIS$_{ONOS}$: SDN-based Real-Time Detection and Automatic Mitigation of BGP Prefix Hijacking”

ABSTRACT

Prefix hijacking is a persistent and serious threat for the Internet's routing system, having a technical and financial impact on a global scale. The research community has developed several sophisticated prefix hijacking detection techniques, which nevertheless lack wide

adoption. On the other hand, network operators usually follow simple, tested practices, albeit with their own limitations (e.g., slow mitigation speed).

In the current work, we present a Software Defined Networking (SDN) application which is built upon the principles of the prototype ARTEMIS, such as self-monitoring, and utilizes ONOS, a carrier-grade SDN Operating System. The application is called ARTEMIS$_{ONOS}$; it uses modern, publicly available streaming services to monitor the BGP control plane in real-time, and accurately detects different types of hijacks. Moreover, it reacts automatically with a configurable mitigation countermeasure.

ARTEMIS$_{ONOS}$ is an official application of ONOS, and leverages several advantages of SDN. In particular, it provides the following features. ARTEMIS$_{ONOS}$ is developed as a modular application on top of the OSGi framework, containing a monitoring, a detection and a mitigation module. It achieves high availability and scalability through the distributed architecture of the network control plane, and is agnostic to the network infrastructure (BGP speakers, data-plane devices, etc) that it operates on, allowing for easy deployment and reduced operational complexity. Although ARTEMIS$_{ONOS}$ is an SDN application, it is fully compatible with BGP, and is thus ready to be used in operational environments.

We evaluate our work by implementing a framework that emulates prefix hijacks. We show that ARTEMIS$_{ONOS}$ detects the hijack and starts the mitigation process within milliseconds. On the contrary, mitigation is achieved in seconds; the time required for BGP to fully converge. Despite ARTEMIS$_{ONOS}$ being --in principle-- a reactive application, in some cases it is faster than the propagation of the actual hijack event, protecting some networks (the ones “close” to the victim) almost proactively.