

Ανίχνευση Επιθέσεων σε Ασύρματα Δίκτυα μέσω Αναγνώρισης Ανωμαλιών στη Δικτυακή Κίνηση

Δημήτριος Πολίτης

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ

27 Φεβρουαρίου 2017

Περίγραμμα Παρουσίασης

- 1 Εισαγωγή
- 2 Κίνητρο - Υπόβαθρο
- 3 Απειλές σε Ασύρματα Δίκτυα
- 4 Ανίχνευση Εισβολών με Ανάλυση της κίνησης

Ασφάλεια ΠΣ

Ασφάλεια Πληροφοριακών Συστημάτων

- Τα πληροφοριακά συστήματα ενσωματώνονται στην καθημερινότητά μας
- Η ασφάλεια των ΠΣ γίνεται απαραίτητη

Αποτροπή Πρόσβασης - Ανίχνευση Επιθέσεων

- Το πρώτο επίπεδο ασφάλειας είναι η αποτροπή πρόσβασης IPS
 - Κωδικοί πρόσβασης
 - Two factor authentication
- Το δεύτερο επίπεδο είναι η ανίχνευση επιθέσεων IDS
- Το τρίτο επίπεδο είναι η ανοχή - αντίδραση (response and tolerance)

Διαφορές Ασύρματων - Ενσύρματων Δικτύων

Διαφορές Ασύρματων - Ενσύρματων Δικτύων

- Δεν υπάρχει απομόνωση φυσικού μέσου.
- Δεν υπάρχει ισχυρή δικτυακή υποδομή
- Μεγάλη κινητικότητα κόμβων
- Παρεμβολές, θόρυβος, απώλειες πακέτων, θερμοκρασία, υγρασία
- Πληθώρα πελατών που εισέρχονται και εξέρχονται τυχαία

Οι διαφορές στους δυο τύπους δικτύων επιβάλλουν την μελέτη νέων μεθόδων ανίχνευσης επιθέσεων στα ασύρματα δίκτυα.

Τύποι Ασύρματων Δικτύων

Τύποι Ασύρματων Δικτύων

- Wireless local area networks
- Wireless personal area networks
- Wireless sensor networks
- Ad hoc networks
- Mobile telephony
- Wireless mesh networks
- Cyber physical systems

Απειλές Ασύρματων Δικτύων

- Silencing
- Spoofing
- Sybil attack
- Jamming
- Tampering
- Node capture
- Sinkhole attack
- Denial of service
- Selective forwarding
- Wormhole attack
- Blackhole attack
- Routing request flooding attack
- Routing request disrupt attack
- Eavesdropping

Συστήματα IDS

Κύριες Λειτουργίες IDS

- Συλλογή δεδομένων δικτυακής κίνησης
- Ανάλυση δεδομένων με χρήση τεχνικών ανίχνευσης επιθέσεων

Μετρικές Αποτελεσματικότητας IDS

- False Positive Rate (FPR)
- False Negative Rate (FNR)
- Detection Rate (DR)

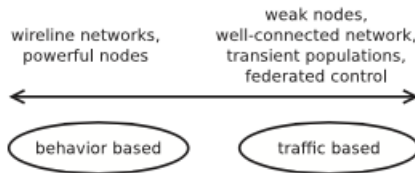
Η ευαισθησία του συστήματος ανίχνευσης υπολογίζεται από τη σχέση:

$$DR = 1 - FPR - FNR$$

Συλλογή και Ανάλυση Δεδομένων

Συλλογή Δεδομένων

- traffic based collection
- behavior based collection

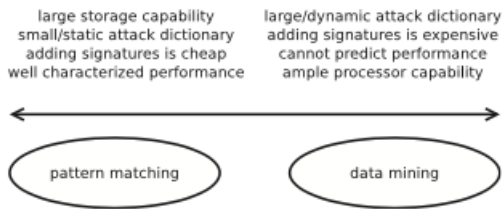


Σχήμα: Διαδικασία συλλογής δεδομένων

Συλλογή και Ανάλυση Δεδομένων

Ανάλυση Δεδομένων

- data minning
- pattern matching



Σχήμα: Διαδικασία ανάλυσης δεδομένων

Ανίχνευση Επιθέσεων

Ανίχνευση Επιθέσεων

- anomaly based
- specification based
- reputation based management
- signature based

Τύποι Ανωμαλιών στη Δικτυακή Κίνηση

Κύριοι Τύποι αποκλίσεων

- point anomalies
- context anomalies
- collective anomalies

Τρόποι Λειτουργίας Τεχνικών Ανίχνευσης

Με βάση τα δεδομένα εκπαίδευσης

- Supervised Methods
- Semisupervised Methods
- Unsupervised Methods

Με βάση τον αλγόριθμο ανίχνευσης

- Classification based (Neural Networks, Bayesian Networks, Support Vector Machines, Rule-Based)
- Nearest Neighbor Based
- Clustering Based
- Statistical Based (Parametric, non-Parametric)
- Information Theory Based

Αποτελεσματικότητα Ανίχνευσης anomaly based

Πλεονεκτήματα

- Δεν αναζητούν κάτι συγκεκριμένο - όχι attack dictionaries
- Μεγάλο πλήθος εφαρμογών
- Ενδείκνεται για ασύρματους κόμβους με μικρό αποθηκευτικό χώρο

Μειονεκτήματα

- Ψψηλό FPR
- Δυσκολία κατά τη δημιουργία του μοντέλου και των δεδομένων εκπαίδευσης

Βιβλιογραφία II



Chatzigiannakis, V., S. Papavassiliou, M. Grammatikou, και B. Maglaris: *Hierarchical anomaly detection in distributed large-scale sensor networks*.



11th IEEE Symposium on Computers and Communications (ISCC'06), 2006.



Deng, Hongmei, R. Xu, J. Li, F. Zhang, R. Levy, και Wenke Lee: *Agent-based cooperative anomaly detection for wireless ad hoc networks*.

12th International Conference on Parallel and Distributed Systems - (ICPADS'06), 2006.

Βιβλιογραφία IV

-  Li, Fudong, Nathan Clarke, Maria Papadaki, και Paul Dowland:
Behaviour profiling on mobile devices.
2010 International Conference on Emerging Security
Technologies, 2010.
-  Limthong, Kriangkrai: *Performance of interval-based features
in anomaly detection by using machine learning approach.*
International Journal of Machine Learning and Computing,
4(3):292–299, 2014.

Βιβλιογραφία VI

- Patwardhan, A., J. Parker, A. Joshi, M. Iorga, και T. Karygiannis: *Secure routing and intrusion detection in ad hoc networks*.
Third IEEE International Conference on Pervasive Computing and Communications, 2005.
- Rajasegarar, S., C. Leckie, και M. Palaniswami: *Anomaly detection in wireless sensor networks*.
IEEE Wireless Communications, 15(4):34–40, 2008.
- Samfat, D. και R. Molva: *Idamn: an intrusion detection architecture for mobile networks*.
IEEE Journal on Selected Areas in Communications, 15(7):1373–1380, 1997.

Βιβλιογραφία VII



Turcotte, Melissa: *Anomaly detection in dynamic networks*.
2014.



Zhang, Yongguang και Wenke Lee: *Intrusion detection in wireless ad-hoc networks*.

Proceedings of the 6th annual international conference on
Mobile computing and networking - MobiCom '00, 2000.