Rilevamento delle Intrusioni tramite Classificazione Multilivello

Tesi di Laurea Magistrale in Ingegneria Informatica

L. Scalavino

Relatore: Prof. Giuseppe Lo Re

Correlatore: Prof. Alessandra De Paola

Rilevamento delle Intrusioni tramite Classificazione Multilivello

Tesi di Laurea di
Ludovico Scalavino

Relatore:
Prof. Giuseppe Lo Re

Correlatore:
Prof. Alessandra De Paola

Sommario

In questo lavoro di tesi viene affrontato un problema che affligge il rilevamento delle intrusioni tramite metodi di machine learning : l'incapacità dei classificatori più utilizzati di ottenere alte prestazioni uniformemente per tutte le classi di attacco.
La ricerca di una soluzione ha portato allo sviluppo di un metodo innovativo: il Classificatore Esperto Multilivello (CEM), che combina diversi classificatori dello stato dell'arte per migliorarne le prestazioni relativamente alle singole classi di attacco. In questa tesi sono descritte tutte le fasi della ricerca (analisi dei metodi classici, analisi del dataset utilizzato, descrizione del CEM) e la valutazione sperimentale dei metodi classici e del metodo proposto. Risultati sperimentali suggeriscono come il metodo progettato soddisfi i requisiti preposti, ottenendo i miglioramenti prestazionali ricercati.

INDICE

1. INTRODUZIONE

Nel mondo moderno, l'**informazione** rappresenta una delle risorse più importanti per imprese e organizzazioni, così come per i singoli individui.

Una buona gestione, conservazione e comunicazione delle informazioni tra diversi componenti delle organizzazioni ricoprono un ruolo fondamentale nella massimizzazione della produttività in ambiente lavorativo.

I sistemi relativi all'***Information Technology*** **(IT)** ricoprono, dunque, un ruolo critico per permettere ad enti produttivi e fornitori di servizi di raggiungere con successo gli obiettivi di business desiderati.

Con il termine IT si identificano tutti i metodi e le tecnologie che sfruttano reti, calcolatori e impianti di telecomunicazione per recuperare, trasmettere e manipolare **dati** o **informazioni** in qualsiasi formato elettronico.

Per quanto detto appare evidente il contributo dell'IT relativamente allo sviluppo di aziende e organizzazioni. L'impiego di tecnologie informatiche permette infatti di riscontrare numerosi benefici in molte attività lavorative, di seguito illustrati.

Fra questi, uno dei principali consiste nella possibilità di **accesso remoto** ai dati; i sistemi di IT infatti permettono l'accesso ai dati (personali o aziendali) da qualsiasi dispositivo collegato alla rete, fornendo così la possibilità di interagire con le informazioni desiderate da ogni posizione. Ciò, oltre ad aumentare significativamente la produttività grazie all'aumento di accessibilità ai dati, permette l'instaurazione di forme innovative di rapporti lavorativi come il lavoro da remoto o lo *smart working*.

Come per ogni risorsa di valore è necessario garantire che le informazioni siano protette da eventuali minacce. Esse rappresentano infatti un bene tanto prezioso quanto sensibile e sono spesso obiettivo di utenti malintenzionati, che potrebbero tentare di appropriarsene o, più genericamente, comprometterne la sicurezza. La presenza di questi rischi ha fatto sì che, parallelamente allo sviluppo di applicazioni IT, venissero ideati **sistemi di sicurezza informatica** mirati a contrastarli.

Una possibile soluzione per difendere risorse informatiche da pericoli che possano minarne la sicurezza potrebbe consistere nell'implementazione di un sistema

completamente sicuro, in grado di prevenire tali attacchi per mezzo di misure estremamente stringenti [63], per esempio controlli rigorosi delle identità; la realizzazione di un tale sistema è tuttavia impraticabile [64] a causa di una varietà di fattori:

- è attualmente impossibile ottenere un software completamente privo di bug; il codice necessario per implementare sistemi di sicurezza avanzata e affidabile risulta molto complesso a causa dei numerosi requisiti da soddisfare. L'interazione delle molte componenti necessarie per la costruzione di un tale meccanismo ne rende pressoché impraticabile un'implementazione priva di errori.
- la base di meccanismi di sicurezza già esistente e installata nei sistemi di tutto il mondo rende particolarmente ostica la transizione su larga scala a un nuovo sistema, per quanto sicuro (nell'eventualità in cui sia implementato).
- anche individuando un sistema di sicurezza privo di vulnerabilità bisognerebbe affrontare le criticità intrinsecamente presenti nei metodi di crittografia utilizzati; essi non sono infatti privi di punti deboli: le password generate possono essere individuate da un attaccante e interi sistemi crittografici possono essere attaccati e aggirati, come già avvenuto in passato.
- anche un sistema perfettamente sicuro e privo di vulnerabilità potrebbe essere soggetto ad utilizzi non appropriati da parte di utenti interni che, maliziosamente o meno, potrebbero abusare dei propri privilegi; bisogna infatti tener conto del fattore umano, spesso necessario nella gestione dei sistemi di sicurezza.
- è stato mostrato che la relazione tra il livello di controllo della sicurezza e l'efficienza per gli utenti è di proporzionalità inversa: più il primo è stringente, più la seconda risulta ridotta.

Per quanto detto è inevitabile la creazione di sistemi contenenti vulnerabilità, che devono essere affrontate efficacemente. È dunque essenziale identificare le possibili **minacce** presentate da entità esterne ai sistemi al fine di progettare sistemi e tecniche mirati alla protezione delle informazioni elaborate nei sistemi informatici. La disciplina che si occupa di tale protezione prende il nome di **Sicurezza Informatica** (

in Inglese *Computer Security*), così definita dal NIST (*Nation Institute of Standards and Technology*)[65]:

la protezione fornita a un sistema informativo automatizzato con lo scopo di raggiungere gli obiettivi applicabili di preservare l'integrità, disponibilità e confidenzialità delle risorse del sistema informativo (includendo hardware, software, firmware, informazioni/dati e telecomunicazioni).

Esistono molteplici rischi e contromisure relativi alla trasmissione di informazioni sulla rete. Una delle più grandi minacce è rappresentata dalle **intrusioni** non autorizzate in sistemi informatici o reti di calcolatori da parte di utenti malevoli o software maligno.

Questo tipo di attacchi presenta rischi di grave entità per un sistema informatico. Un'intrusione effettuata da un utente indesiderato (spesso chiamato *hacker*) può essere identificata come appartenente a una di tre classi: un *masquerader* è un individuo non autorizzato all'utilizzo di una risorsa del sistema e che vi accede sfruttando l'identità di un utente legittimo; un *misfeasor* è un utente legittimo che accede a dati, programmi o risorse per le quali non ha autorizzazione di accesso oppure abusa dei privilegi posseduti; un **utente clandestino** è un individuo che ottiene ottiene il controllo della supervisione di un sistema e lo utilizza per eludere il controllo degli accessi e la raccolta di log riguardanti l'attività del sistema.

Le intrusioni effettuate da software comportano l'ingresso di **malware** (cioè software malevolo) nel sistema: **virus**, **worm**, **trojan horse** possono innestarsi nelle macchine del sistema utilizzando come mezzo di trasmissione la rete o anche dispositivi fisici infetti.

Appare evidente come gli ingressi indesiderati in un sistema informatico possano causare danni di entità immensa. L'intrusione da parte di hacker può portare a conseguenze catastrofiche per un'organizzazione: interrompere il funzionamento di server web, estrarre password, manipolare o estrarre informazioni riservate da database sono soltanto alcune delle azioni distruttive che un intruso potrebbe portare a termine; l'ingresso di software malevolo costituisce una minaccia altrettanto grave, in quanto malware come quelli sopra menzionati possono causare la distruzione di grandi quantità di dati oppure la creazione di punti di accesso per facilitare il successivo ingresso di hacker.

Le contromisure esistenti per affrontare il rischio di intrusioni si dividono in due categorie.

La prima, la **Prevenzione delle Intrusioni** (in Inglese *Intrusion Prevention* - IP), è anche la più complessa da attuare: per prevenire totalmente ingressi indesiderati nei sistemi informatici sarebbe necessario individuare ed eliminare ogni sua possibile vulnerabilità; un attaccante ha infatti bisogno di individuare una sola falla nella sicurezza per portare a termine un attacco mirato specificamente a sfruttarla per guadagnare l'accesso al sistema.

Nell'ambito della sicurezza informatica, dunque, il **Rilevamento delle Intrusioni** (in Inglese *Intrusion Detection* - ID) ha assunto un ruolo di fondamentale importanza.

Con rilevamento delle intrusioni si definisce la pratica di apprendere informazioni su di un attacco mirato al sistema, prima o anche dopo che sia stato portato a termine. Essendo la soluzione più plausibile fra le due illustrate, l'ID è stata recentemente oggetto di numerose ricerche; pur non permettendo una prevenzione assoluta delle intrusioni, che corrisponderebbe a una sicurezza totale, l'individuazione di tali attacchi apporta benefici di sicurezza non indifferenti.

Una rapida individuazione di un'intrusione potrebbe permettere di identificare e rimuovere dal sistema l'intruso, possibilmente prima che qualsiasi danno sia stato causato, oppure limitare i danni nel caso in cui l'attacco sia già stato portato a buon fine. Non è inoltre trascurabile l'azione deterrente che un buon sistema di rilevamento delle intrusioni può attuare nei confronti dei possibili attaccanti. È infine fondamentale la raccolta di informazioni collaterale all'opera di un sistema di ID: tali dati relativi alle tecniche di intrusione possono essere utilizzati per rafforzare i futuri sviluppi di sicurezza legati all'ID.

I sistemi di individuazione delle intrusioni si basano su di un principio fondante: è assunto che il comportamento degli intrusi presenti differenze quantificabili rispetto al comportamento degli utenti legittimi. Il confine tra i due comportamenti non è tuttavia ben definito, il che porta dunque all'inevitabile presenza di **falsi positivi**: istanze di utenti erroneamente identificati come intrusi nonostante fossero legittimi. Cercare di limitare i falsi positivi conduce tuttavia all'errore opposto: i **falsi negativi** rappresentano utenti malevoli identificati come legittimi. Quanto detto necessita la ricerca di un compromesso nell'implementazione di sistemi di ID; la complessità presentata da questa indagine è il motivo principale per cui la ricerca in quest'ambito

è attualmente particolarmente attiva**,** non avendo ancora individuato una soluzione globale per questo problema.

La tesi di ricerca qui presentata si propone di affrontare il problema dell'individuazione delle intrusioni sfruttando gli strumenti messi a disposizione dal *Machine Learning*, per la progettazione e realizzazione di un sistema di rilevamento delle intrusioni basato sulla combinazione di più classificatori per ottenere prestazioni superiori rispetto a quelle dei singoli metodi. Tale sistema ha lo scopo di superare le limitazioni riscontrate sperimentalmente in tali classificatori singoli mantenendo al contempo contenuto l'impegno temporale richiesto. La trattazione seguente sarà così suddivisa:

1. **Introduzione**;
2. **Stato dell'arte**: descrizione più approfondita del rilevamento delle intrusioni, delle sfide che presenta e delle tecniche più avanzate per affrontarle;
3. **Cenni teorici**: introduzione sintetica al *Machine Learning* e approfondimenti teorici sui classificatori trattati;
4. **Classificatore Esperto Multilivello**: presentazione del metodo proposto, descrizione della sua architettura e illustrazione del processo di sviluppo;
5. **Analisi del dataset**: descrizione del processo di ricerca del *dataset* da utilizzare;
6. **Analisi sperimentale**: resoconto della fase di studio applicativo, risultati delle analisi effettuate sui metodi classici e sul Classificatore Esperto Multilivello;
7. **Conclusioni**.

8. BIBLIOGRAFIA

[1] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.
[2] Małowidzki, M., Berezinski, P., & Mazur, M. (2015). Network intrusion detection: Half a kingdom for a good dataset. In Proceedings of NATO STO SAS-139 Workshop, Portugal.
[3] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security.
[4] Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., ... & Bouwman, J. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Scientific data, 3.
[5] He, H., & Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on knowledge and data engineering, 21(9), 1263-1284.
[6] Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2015). Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Communications Surveys & Tutorials, 18(1), 184-208.
[7] Beigi, E. B., Jazi, H. H., Stakhanova, N., & Ghorbani, A. A. (2014, October). Towards effective feature selection in machine learning-based botnet detection approaches. In 2014 IEEE Conference on Communications and Network Security (pp. 247-255). IEEE.
[8] Jazi, H. H., Gonzalez, H., Stakhanova, N., & Ghorbani, A. A. (2017). Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. Computer Networks, 121, 25-36.
[9] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018, January). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In ICISSP (pp. 108-116).
[10] Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., ... & Zissman, M. A. (2000, January). Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. In Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00 (Vol. 2, pp. 12-26). IEEE.
[11] Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA off-line intrusion detection evaluation. Computer networks, 34(4), 579-595.
[12] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE symposium on computational intelligence for security and defense applications (pp. 1-6). IEEE.
[13] McHugh, J. (2000). Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security (TISSEC), 3(4), 262-294.

[14] Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security, 31(3), 357-374.
[15] Saad, S., Traore, I., Ghorbani, A., Sayed, B., Zhao, D., Lu, W., ... & Hakimian, P. (2011, July). Detecting P2P botnets through network behavior analysis and machine learning. In 2011 Ninth annual international conference on privacy, security and trust (pp. 174-180). IEEE.
[16] KDD Cup 1999. Available on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, February 2020.
[17] Beer, F., Hofer, T., Karimi, D., & Bühler, U. (2017). A new attack composition for network security. In 10. DFN-Forum Kommunikationstechnologien. Gesellschaft für Informatik eV.
[18] Haider, W., Hu, J., Slay, J., Turnbull, B. P., & Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. Journal of Network and Computer Applications, 87, 185-192.
[19] Gogoi, P., Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2012, August). Packet and flow based network intrusion dataset. In International Conference on Contemporary Computing (pp. 322-334). Springer, Berlin, Heidelberg.
[20] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). Towards Generating Real-life Datasets for Network Intrusion Detection. IJ Network Security, 17(6), 683-701.
[21] Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 military communications and information systems conference (MilCIS) (pp. 1-6). IEEE.
[22] Garcia, S., Grill, M., Stiborek, J., & Zunino, A. (2014). An empirical comparison of botnet detection methods. computers & security, 45, 100-123.
[23] Aviv, A. J., & Haeberlen, A. (2011). Challenges in experimenting with botnet detection systems.
[24] Gharib, A., Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2016, December). An evaluation framework for intrusion detection dataset. In 2016 International Conference on Information Science and Security (ICISS) (pp. 1-6). IEEE.
[25] Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., ... & Halderman, J. A. (2014, November). The matter of heartbleed. In Proceedings of the 2014 conference on internet measurement conference (pp. 475-488).
[26] Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., ... & Vigna, G. (2009, November). Your botnet is my botnet: analysis of a botnet takeover. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 635-647).
[27] Schuba, C. L., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., & Zamboni, D. (1997, May). Analysis of a denial of service attack on TCP. In Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097) (pp. 208-223). IEEE.

[28] Lau, F., Rubin, S. H., Smith, M. H., & Trajkovic, L. (2000, October). Distributed denial of service attacks. In Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0 (Vol. 3, pp. 2275-2280). IEEE.
[29] Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE international symposium on secure software engineering (Vol. 1, pp. 13-15). IEEE.
[30] Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007, February). Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In NDSS (Vol. 2007, p. 12).
[31] Quinlan, J. R. (1986). Induction of decision trees. Machine learning, 1(1), 81-106.
[32] Safavian, S. R., & Landgrebe, D. (1991). A survey of decision tree classifier methodology. IEEE transactions on systems, man, and cybernetics, 21(3), 660-674.
[33] Swain, P. H., & Hauska, H. (1977). The decision tree classifier: Design and potential. IEEE Transactions on Geoscience Electronics, 15(3), 142-147.
[34] Russell, S., & Norvig, P. (2002). Artificial intelligence: a modern approach.
[35] Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.
[36] Kourou, K., Exarchos, T. P., Exarchos, K. P., Karamouzis, M. V., & Fotiadis, D. I. (2015). Machine learning applications in cancer prognosis and prediction. Computational and structural biotechnology journal, 13, 8-17.
[37] Kober, J., & Peters, J. (2009, May). Learning motor primitives for robotics. In 2009 IEEE International Conference on Robotics and Automation (pp. 2112-2118). IEEE.
[38] Koch, G., Zemel, R., & Salakhutdinov, R. (2015, July). Siamese neural networks for one-shot image recognition. In ICML deep learning workshop (Vol. 2).
[39] Zoph, B., Vasudevan, V., Shlens, J., & Le, Q. V. (2018). Learning transferable architectures for scalable image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 8697-8710).
[40] Wu, X., Kumar, V., Quinlan, J. R., Ghosh, J., Yang, Q., Motoda, H., ... & Zhou, Z. H. (2008). Top 10 algorithms in data mining. Knowledge and information systems, 14(1), 1-37.
[41] Hssina, B., Merbouha, A., Ezzikouri, H., & Erritali, M. (2014). A comparative study of decision tree ID3 and C4. 5. International Journal of Advanced Computer Science and Applications, 4(2), 13-19.
[42] Breiman, L. (1996). Out-of-bag estimation.
[43] Breiman, L. (1996). Bagging predictors. Machine learning, 24(2), 123-140.
[44] Polikar, R. (2006). Ensemble based systems in decision making. IEEE Circuits and systems magazine, 6(3), 21-45.
[45] Ho, T. K. (1998). The random subspace method for constructing decision forests. IEEE transactions on pattern analysis and machine intelligence, 20(8), 832-844.

[46] Schapire, R. E. (1990). The strength of weak learnability. Machine learning, 5(2), 197-227.
[47] Rish, I. (2001, August). An empirical study of the naive Bayes classifier. In IJCAI 2001 workshop on empirical methods in artificial intelligence (Vol. 3, No. 22, pp. 41-46).
[48] Zhang, H. (2005). Exploring conditions for the optimality of naive Bayes. International Journal of Pattern Recognition and Artificial Intelligence, 19(02), 183-198.
[49] Langley, P., Iba, W., & Thompson, K. (1992, July). An analysis of Bayesian classifiers. In Aaai (Vol. 90, pp. 223-228).
[50] Amor, N. B., Benferhat, S., & Elouedi, Z. (2004, March). Naive bayes vs decision trees in intrusion detection systems. In Proceedings of the 2004 ACM symposium on Applied computing (pp. 420-424).
[51] Duda, R. O., Hart, P. E., & Stork, D. G. (1973). Pattern classification and scene analysis (Vol. 3, pp. 731-739). New York: Wiley.
[52] Domingos, P., & Pazzani, M. (1997). On the optimality of the simple Bayesian classifier under zero-one loss. Machine learning, 29(2-3), 103-130.
[53] Langley, P., Iba, W., & Thomas, K. (1992). An analysis of Bayesian classi er. In proceedings of the Tenth National Conference of Artificial Intelligence.
[54] Kononenko, I. (1990). Automatic Knowledge Acquisition. Current trends in knowledge acquisition, 8, 190.
[55] Domingos, P., & Pazzani, M. (1996, July). Beyond independence: Conditions for the optimality of the simple bayesian classi er. In Proc. 13th Intl. Conf. Machine Learning (pp. 105-112).
[56] Friedman, N., Geiger, D., & Goldszmidt, M. (1997). Bayesian network classifiers. Machine learning, 29(2-3), 131-163.
[57] Arlot, S., & Celisse, A. (2010). A survey of cross-validation procedures for model selection. Statistics surveys, 4, 40-79.
[58] Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. Computers & Electrical Engineering, 40(1), 16-28.
[59] Wold, S., Esbensen, K., & Geladi, P. (1987). Principal component analysis. Chemometrics and intelligent laboratory systems, 2(1-3), 37-52.
[60] Zheng, A., & Casari, A. (2018). Feature engineering for machine learning: principles and techniques for data scientists. " O'Reilly Media, Inc.".
[61] Schapire, R. E., Freund, Y., Bartlett, P., & Lee, W. S. (1998). Boosting the margin: A new explanation for the effectiveness of voting methods. Annals of statistics, 26(5), 1651-1686.
[62] Wolpert, D. H. (1992). Stacked generalization. Neural networks, 5(2), 241-259.
[63] Viega, J., & McGraw, G. R. (2001). Building secure software: How to avoid security problems the right way, portable documents. Pearson Education.
[64] Sobh, T. S. (2006). Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces, 28(6), 670-694.

[65] Guttman, B., & Roback, E. A. (1995). An introduction to computer security: the NIST handbook. Diane Publishing.
[66] RFC4949, N. (2007). Internet Security Glossary, Version 2.
[67] Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India.
[68] Bace, R. G., & Mell, P. (2001). Intrusion detection systems.
[69] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. Ieee communications surveys & tutorials, 16(1), 303-336.
[70] Hornik, K., Stinchcombe, M., & White, H. (1989). Multilayer feedforward networks are universal approximators. Neural networks, 2(5), 359-366.
[71] Cannady, J. (1998, October). Artificial neural networks for misuse detection. In Proceedings of the 1998 National Information Systems Security Conference (NISSC'98) (pp. 443-456).
[72] Internet Security Scanner (ISS). IBM [Online]. Available: http://www.iss.net, accessed on Feb. 2015.
[73] Morel, B. (2011, October). Artificial intelligence and the future of cybersecurity. In Proceedings of the 4th ACM workshop on Security and artificial intelligence (pp. 93-98).
[74] Lippmann, R. P., & Cunningham, R. K. (2000). Improving intrusion detection performance using keyword selection and neural networks. Computer networks, 34(4), 597-603.
[75] Bivens, A., Palagiri, C., Smith, R., Szymanski, B., & Embrechts, M. (2002). Network-based intrusion detection using neural networks. Intelligent Engineering Systems through Artificial Neural Networks, 12(1), 579-584.
[76] Heckerman, D. (2008). A tutorial on learning with Bayesian networks. Innovations in Bayesian networks, 33-82.
[77] Nielsen, T. D., & Jensen, F. V. (2009). Bayesian networks and decision graphs. Springer Science & Business Media.
[78] Jemili, F., Zaghdoud, M., & Ahmed, M. B. (2007, May). A framework for an adaptive intrusion detection system using Bayesian network. In 2007 IEEE Intelligence and Security Informatics (pp. 66-70). IEEE.
[79] Kruegel, C., Mutz, D., Robertson, W., & Valeur, F. (2003, December). Bayesian event classification for intrusion detection. In 19th Annual Computer Security Applications Conference, 2003. Proceedings. (pp. 14-23). IEEE.
[80] Quinlan, J. R. (2014). C4. 5: programs for machine learning. Elsevier.
[81] Snort available at https://www.snort.org/, February 2021
[82] Kruegel, C., & Toth, T. (2003, September). Using decision trees to improve signature-based intrusion detection. In International Workshop on Recent Advances in Intrusion Detection (pp. 173-191). Springer, Berlin, Heidelberg.
[83] Bilge, L., Kirda, E., Kruegel, C., & Balduzzi, M. (2011, February). EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. In Ndss (pp. 1-17).

[84] Bilge, L., Sen, S., Balzarotti, D., Kirda, E., & Kruegel, C. (2014). Exposure: A passive dns analysis service to detect and report malicious domains. ACM Transactions on Information and System Security (TISSEC), 16(4), 1-28.
[85] Zhang, J., Zulkernine, M., & Haque, A. (2008). Random-forests-based network intrusion detection systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38(5), 649-659.
[86] Mukkamala, S., Sung, A. H., & Abraham, A. (2005). Intrusion detection using an ensemble of intelligent paradigms. Journal of network and computer applications, 28(2), 167-182.
[87] Friedman, J. H. (1991). Multivariate adaptive regression splines. The annals of statistics, 1-67.
[88] Bilge, L., Balzarotti, D., Robertson, W., Kirda, E., & Kruegel, C. (2012, December). Disclosure: detecting botnet command and control servers through large-scale netflow analysis. In Proceedings of the 28th Annual Computer Security Applications Conference (pp. 129-138).
[89] Goldberg, D. E., & Holland, J. H. (1988). Genetic algorithms and machine learning.
[90] Koza, J. R., & Koza, J. R. (1992). Genetic programming: on the programming of computers by means of natural selection (Vol. 1). MIT press.
[91] Li, W. (2004). Using genetic algorithm for network intrusion detection. Proceedings of the United States department of energy cyber security group, 1, 1-8.
[92] Lu, W., & Traore, I. (2004). Detecting new forms of network intrusion using genetic programming. Computational intelligence, 20(3), 475-494.
[93] Ariu, D., Tronci, R., & Giacinto, G. (2011). HMMPayl: An intrusion detection system based on Hidden Markov Models. computers & security, 30(4), 221-241.
[94] Joshi, S. S., & Phoha, V. V. (2005, March). Investigating hidden Markov models capabilities in anomaly detection. In Proceedings of the 43rd annual Southeast regional conference-Volume 1 (pp. 98-103).
[95] Lee, W., Stolfo, S. J., & Mok, K. W. (1999, May). A data mining framework for building intrusion detection models. In Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No. 99CB36344) (pp. 120-132). IEEE.
[96] Witten, I. H., & Frank, E. (2002). Data mining: practical machine learning tools and techniques with Java implementations. Acm Sigmod Record, 31(1), 76-77.
[97] Panda, M., & Patra, M. R. (2007). Network intrusion detection using naive bayes. International journal of computer science and network security, 7(12), 258-263.
[98] Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA data mining software: an update. ACM SIGKDD explorations newsletter, 11(1), 10-18.
[99] Vapnik, V. (2013). The nature of statistical learning theory. Springer science & business media.
[100] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert systems with applications, 39(1), 424-430.

[101] Hu, W., Liao, Y., & Vemuri, V. R. (2003, June). Robust Support Vector Machines for Anomaly Detection in Computer Security. In ICMLA (pp. 168-174).
[102] Baum, L. E., & Eagon, J. A. (1967). An inequality with applications to statistical estimation for probabilistic functions of Markov processes and to a model for ecology. Bulletin of the American Mathematical Society, 73(3), 360-363.
[103] Wang, L. (Ed.). (2005). Support vector machines: theory and applications (Vol. 177). Springer Science & Business Media.
[104] Agate V., De Paola A., Lo Re G., Morana M. A Platform for the Evaluation of Distributed Reputation Algorithms, (2019) Proceedings of the 2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications, DS-RT 2018, art. no. 8601020, pp. 182 – 189, DOI: 10.1109/DISTRA.2018.8601020
[105] De Paola A., Gaglio S., Lo Re G., Morana M. A hybrid system for malware detection on big data, (2018) INFOCOM 2018 - IEEE Conference on Computer Communications Workshops, pp. 45 – 50, DOI: 10.1109/INFCOMW.2018.8406963
[106] De Paola A., Favaloro S., Gaglio S., Lo Re G., Morana M., Malware detection through low-level features and stacked denoising autoencoders, (2018) CEUR Workshop Proceedings, 2058
[107] Concone F., De Paola A., Lo Re G., Morana M., Twitter analysis for real-Time malware discovery, (2017) 2017 AEIT International Annual Conference: Infrastructures for Energy and ICT: Opportunities for Fostering Innovation, AEIT 2017, 2017-January, pp. 1 – 6, DOI: 10.23919/AEIT.2017.8240551
[108] Agate V., De Paola A., Lo Re G., Morana M., Vulnerability evaluation of distributed reputation management systems, (2017) ValueTools 2016 - 10th EAI International Conference on Performance Evaluation Methodologies and Tools, pp. 235 – 242, DOI: 10.4108/eai.25-10-2016.2266868
[109] Agate V., De Paola A., Gaglio S., Lo Re G., Morana M., A framework for parallel assessment of reputation management systems, (2016) ACM International Conference Proceeding Series, 1164, pp. 121 – 128, DOI: 10.1145/2983468.2983474
[110] Agate V., de Paola A., Lo Re G., Morana M., A simulation framework for evaluating distributed reputation management systems, (2016) Advances in Intelligent Systems and Computing, 474, pp. 247 – 254, DOI: 10.1007/978-3-319-40162-1_27