Accenture Security

ARTIFICIAL INTELLIGENCE ON THE HORIZON OF CYBER SECURITY

Alice Silde

alise.silde@accenture.com

5th October, 2017

AGENDA

- Recap on Artificial Intelligence (AI)
- Current State of AI Technologies
- AI in Security Offence
- AI in Security Defence
- The Future of AI-Enabled Security
- Approach to Designing Intelligent Security Solutions
- Conclusions
- Q&A

AI RECAP

ARTIFICIAL INTELLIGENCE

- AI technologies **combine** different techniques and algorithms to **emulate human performance**, such as decision-making, learning, engaging in dialogue or task execution
- Machine Learning (ML) is typically a part of an AI solution

DIFFERENT TYPES AND CATEGORIES

Artificial Intelligence

- Strong or Weak
- Narrow or General
- Other

Machine Learning

- Supervised
- Unsupervised
- Reinforcement Learning
- Neural Networks
- Deep Neural Networks a.k.a. Deep Learning

MACHINE LEARNING

https://xkcd.com/1838/

ALGORITHM ADVANTAGES

- **Neural Networks and Deep Neural Networks** – speed; flexible learning; intuitiveness; complex non-linear functions
- **Intelligent Agents** - mobility; aim to accomplish tasks even despite contradictory objectives; adaptability to environments and user preferences; awareness of human error
- **Artificial Immune Systems** – dynamic and multi-layered structure (self-adaptability, self-organization); speed; distributed learning; robustness; selective response; diversity in detector generation; disposability
- **Genetic Algorithms** - adaptability to environments; selective response; speed; flexible and robust global search
- **Fuzzy Sets/Fuzzy Logic** - robustness of reasoning; human-friendliness

- Think Linux vs Windows

IMPACT OF AI ON GENERAL TECHNOLOGY

WHY DO WE NEED IT?

- Complex data
- Problem-solving
- Finding patterns
- Analysis and predictions
- High-dimensional problems
- Re-usability of non-pre-programmed software
- Controlled real-time/online operation

CURRENT CAPABILITIES

- Intuitive games [12] [13]
- Function optimization for problem-solving [6]
- Product design and manufacturing [7]
- Reporting and publishing [8]
- Medical diagnostics [8]
- Research [14]
- Intelligent assistants [9] [4]
- General augmentation of human ability to think and perform

500% INCREASE IN INTEREST IN 2015 SINCE 2014 AND A 200% INCREASE IN Q3 OF 2016 SINCE 2015 FROM 2010 THROUGH 2015, FUNDING IN THE AI SECTOR HAS MULTIPLIED NEARLY SEVENFOLD

– [4] BRANT, K. F., AUSTIN, T. 2016. GARTNER

HYPE TRAIN

- Disregard for actual business requirements
- Unawareness of cost and other implications of acquisition, deployment and operation
- Crafted demonstrations and proof-of-concept (PoC)
- Misunderstanding of the underlying technologies

LIMITATIONS AND PREDICTIONS

THERE IS STILL MUCH TO WORK ON…

- Data privacy considerations
- Difficulties with ambiguous data

BUT THE ADOPTION OF AI WILL CONTINUE

- AI is inevitably here to stay

"We predict that most of the world's largest 200 companies will utilize the full toolkit of big data and analytical tools to refine their offers and improve their customer experience by 2018."

[4] BRANT, K. F., AUSTIN, T. 2016.

- Adding intelligence to devices and software
- Transformation of economy and workplace
- Many desired solutions yet to be developed
- Increased availability and affordability

IMPACT OF AI ON SECURITY - ATTACK PERSPECTIVE

MALICIOUS AI

- In charge of important aspects of our lives
- Malevolent goals can be designed or introduced later
- Machine ethics face many challenges
- Unknown and unpredictable attack vectors

CREATING ADDITIONAL ATTACK VECTORS

- AI failure
- Difficulties in testing and debugging
- Challenges in monitoring, visualisation, analysis

AI VS AI

- Targeted model misleading
- Probing defensive mechanisms
- Deducing the type of model from the task it performs
- Using known or discovered 'blind spots'

CURRENT USE

- Augmentation of malware capabilities
- Automated reconnaissance tasks
- Scanning for vulnerabilities
- Using the gap in defensive expert skills

SOME EXAMPLES

- NMap Clustering [17]
- Markov Obfuscate [17]
- DeepHack [18]
- AppCrawler [34]
- Future Work

IMPACT OF AI ON SECURITY - DEFENCE PERSPECTIVE

CHALLENGE AND RESPONSE

"Defense against intelligent cyber weapons can be achieved only by intelligent software."
[3] TYUGU, E. 2011.

SECURITY CHALLENGES

- Volume of data
- Diversity of data sources and changing environments
- Diversity, volatility and lack of structure in data
- Requirement for speed of response
- Low fault tolerance

USEFUL AI CAPABILITIES

- Resource optimisation
- Increased staff productivity
- Reduced false-positive rates
- Reduced incident detection and response times
- More complete scenario coverage
- Feedback loop
- Interpretability

EARLY STEPS TOWARDS AI

- Integration into SDLC and automation
- Descriptive and diagnostic analysis
- Malware analysis
- Forecasting tools
- Anomaly detection

SOME EXAMPLES

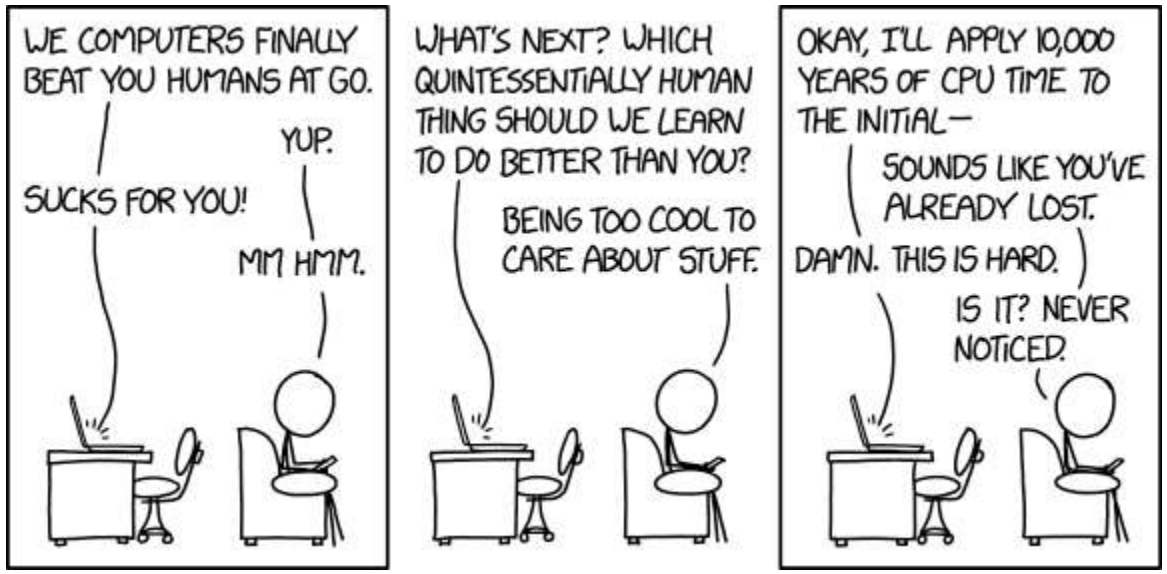
TOOLS

- ID Panel [17]
- PUMA Plugin [35]
- NeuroNet [31]
- Deep Instinct [43]
- DeepArmor [29]
- Mayhem [44]
- MWDCM [31]
- MMBot [47]

PROTOTYPES AND FRAMEWORKS

- Multi-Layered Security Model prototype [31]
- Machine Learning for detecting malicious websites [36]
- Machine Learning for identifying C&C communications [37]
- Deep Neural Networks for malware similarity analysis [33]
- Self-Organising Maps for detecting malicious intent [31]
- Neuro-Endocrine Immune System for tool orchestration [31]
- GAAIS – IDS for mobile networks [31]

WHERE ARE THE RESULTS?



https://xkcd.com/1875/

WHERE ARE THE RESULTS?

- Accuracy and reliability still needs improvement
- Testing and validation
- Training, tuning and calibration
- Cost of acquisition, deployment, operation/maintenance

THE FUTURE OF AI IN SECURITY

PREDICTIONS

- "The **rise of AI-enabled cyberattacks** is expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses.“ [22]
- "Cybersecurity could become **one of the best AI applications** that the business world has seen.“ [25]
- "By 2018, **25% of security products** used for detection **will have some form of machine learning** built into them.“ [30]
- "By 2020, **sophisticated criminals will be able to beat 80%** of the organizations who have deployed **advanced analytic systems**.“ [30]

POTENTIAL SOLUTIONS

- Lack of training data
  - Simulations and honeypots
- Need for context
  - Knowledge base; consolidation of security data
- Increased attack-space
  - Adversarial Training
- Steep learning curve
  - ‘Prior Knowledge’
- Limitations in learning
  - Handle the gaps by other means and other products
- Questionable accuracy and reliability
  - Focus on Narrow AI
- Expert skill gap
  - Design and deliver targeted training and education
- Need for intelligent decision support
  - Use multiple agents; Neuro-Endocrine Immune System for orchestration
- Paperwork and regulations

INTELLIGENT ANALYSIS OF SECURITY FINDINGS – AN APPROACH TO DESIGNING AI-BASED SOLUTIONS

“More than 92.85 percent of false cases are FPs even if the numbers of attack types for FP and FN are similar”
[49] HO, C., LAI, Y., CHEN, I., WANG, F., TAI, W. 2012.

Why

- Existing solutions are limited [50] [51] [52] [54]
- Higher error tolerance
- Inherent attack resistance

Other Pre-Considerations

- Strong need for context
- Requires a complex solution
- Might require a different approach than most existing solutions

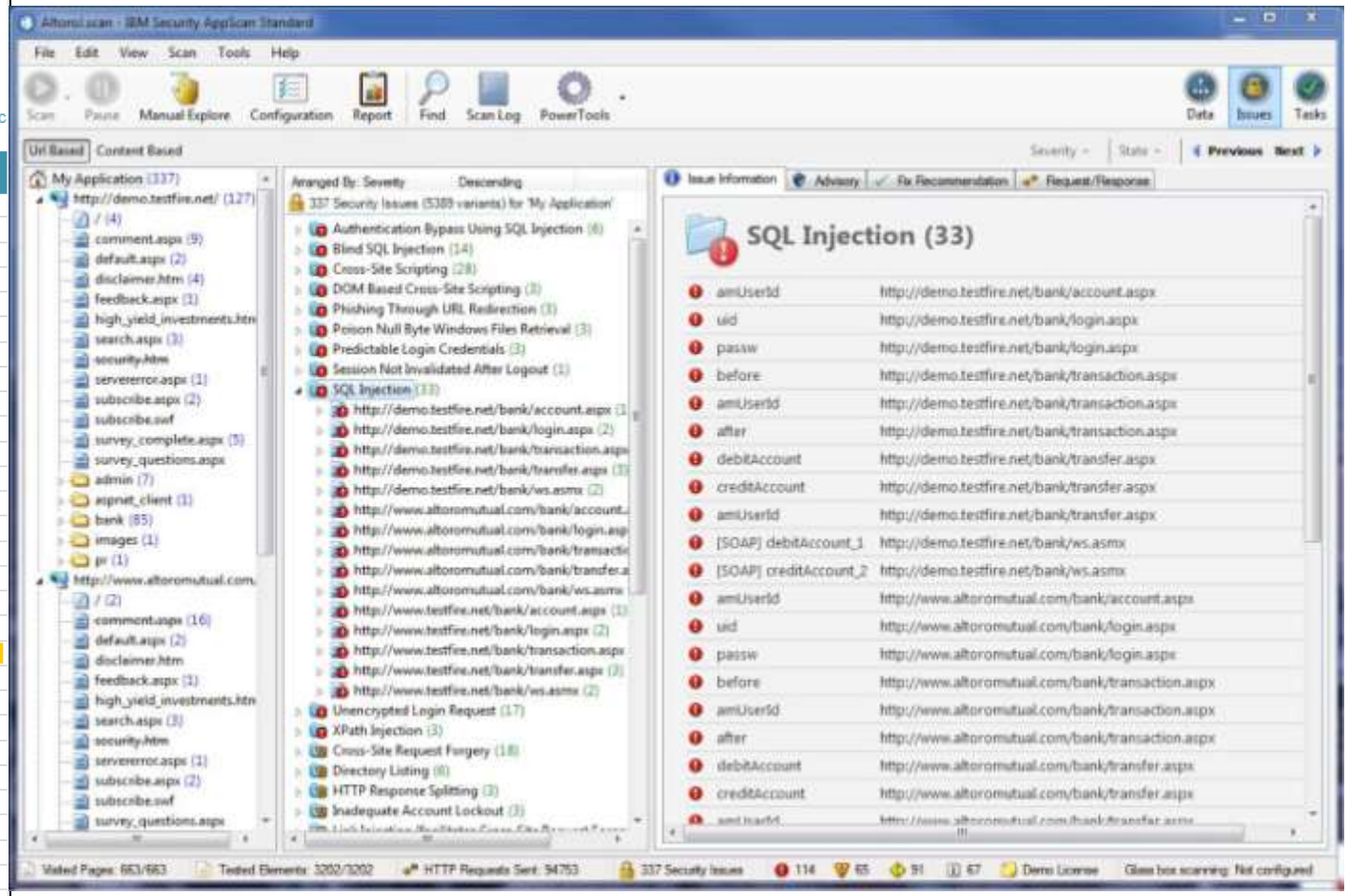
INTELLIGENT ANALYSIS OF SECURITY FINDINGS – AN APPROACH TO DESIGNING AI-BASED SOLUTIONS

Executive Summary

Issue Types 32

TOC

	Issue Type	Number of Issues
H	Authentication Bypass Using SQL Injection	1
H	Blind SQL Injection	1
H	Cross-Site Scripting	11
H	DOM Based Cross-Site Scripting	3
H	Poison Null Byte Windows Files Retrieval	1
H	Predictable Login Credentials	1
H	SQL Injection	12
H	Unencrypted Login Request	6
H	XPath Injection	1
M	Cross-Site Request Forgery	6
M	Directory Listing	2
M	HTTP Response Splitting	1
M	Inadequate Account Lockout	1
M	Link Injection (facilitates Cross-Site Request Forgery)	6
M	Open Redirect	2
M	Phishing Through Frames	6
M	Session Identifier Not Updated	1
L	Autocomplete HTML Attribute Not Disabled for Password Field	4
L	Database Error Pattern Found	16
L	Direct Access to Administration Pages	2
L	Email Address Pattern Found in Parameter Value	2
L	Hidden Directory Detected	3
L	Microsoft ASP.NET Debugging Enabled	3
L	Missing HttpOnly Attribute in Session Cookie	4
L	Permanent Cookie Contains Sensitive Session Information	1
L	Unencrypted __VIEWSTATE Parameter	4
L	Unsigned __VIEWSTATE Parameter	4
I	Application Error	15
I	Application Test Script Detected	1
I	Email Address Pattern Found	3
I	HTML Comments Sensitive Information Disclosure	5
I	Possible Server Path Disclosure Pattern Found	1



© IBM AppScan Standard

http://blog.watchfire.com/wfblog/2012/08/out-with-the-old-in-with-the-new-ibm-security-appscan-standard-86-released.html

https://www.ibm.com/developerworks/library/se-sql-injection-attacks/index.html

INTELLIGENT ANALYSIS OF SECURITY FINDINGS – AN APPROACH TO DESIGNING AI-BASED SOLUTIONS

- Involve field experts for feature engineering
- Labelling of true vulnerabilities
  - Good training data
  - Analysis of known attack patterns and signatures
  - Analysis of behavioural data from multiple sources
  - Adding context by proactive search
- Clustering/classification into vulnerability types
  - Use of a large and varied knowledge base – the context
  - Use different layers to analyse feature sets
- Assigning a severity/impact rating
  - Evaluation of exploitability – matching/labeling
  - Intuitive deep learning approach
  - Strong goal and reward engineering
  - DeepHack approach
- Potential to discover new attack and exploitation techniques

CONCLUSIONS

- AI is basically just a **smarter**, **more efficient** way to create digital products.
- It is important to **consider the implications** of true/general AI in its conception phase.
- AI-enabled solutions can **complement existing technologies**.
- The industry will benefit from **security specialists** with **AI** development **skills**
- Teaching AI to be a 'team player' could help **solve data ambiguity issues** and the **need for context**, which are common challenges in many fields

Q&A THANK YOU!

ACCENTURE LATVIA SECURITY PRACTICE

CYBER SECURITY TESTING · VULNERABILITY MANAGEMENT

SECURITY ADVISORY SERVICES · DATA PRIVACY & GDPR · SECURITY RISK ASSESSMENTS

ISO 27001 · SPLUNK

CREST Registered Penetration Tester

AppScan IBM Security

ISO-27001 Lead Auditor

CISA Certified Information Systems Auditor

splunk> Splunk Certified Power User

splunk> Splunk Certified Admin

C|EH Certified Ethical Hacker

C)PTE Certified Penetration Testing Engineer

C)DFE Certified Digital Forensics Examiner

Contact Latvia.SecurityST@accenture.com

REFERENCES

- [1] Horvath, M. 2017. “Artificial Intelligence and Application Security Vendors: Marketing Hype or Genuine Hope?” https://www.gartner.com/doc/3700418/artificial-intelligence-application-security-vendors Gartner
- [2] CybeRisk. 2016. “Application of Artificial Intelligence in Cyber Security” http://www.cyberisk.biz/application-artificial-intelligence-in-cyber-security/
- [3] Tyugu, E. 2011. “Artificial Intelligence in Cyber Defense” https://ccdcoe.org/iccc/materials/proceedings/tyugu.pdf
- [4] Brant, K. F., Austin, T. 2016. “Hype Cycle for Smart Machines, 2016” https://www.gartner.com/doc/3380751/hype-cycle-smart-machines- Gartner
- [5] Cardoza, C. 2017. “How artificial intelligence will make its mark on the software testing world” http://sdtimes.com/ai-mark-software-testing-world-sdtimes/ SD Times
- [6] Sutskever, I. 2017. “The State of AI” https://www.technologyreview.com/video/604431/the-state-of-ai/
- [7] Conti, M. 2017. “Incredible Inventions of Intuitive AI” https://www.youtube.com/watch?v=aR5N2Jl8k14 TedTalk
- [8] Andrews, W., Brant, K. F., Revang, M., Reynolds, M., Karamouzis, F., Hare, J. 2016. "Predicts 2017: Artificial Intelligence" https://www.gartner.com/doc/3519744/predicts--artificial-intelligence Gartner
- [9] Panetta, K. 2016. “Top 10 Strategic Technology Trends for 2017: Artificial Intelligence and Advanced Machine Learning” http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/ Gartner
- [10] Hof, R. D. 2017. “Deep Learning — With Massive Amounts of Computational Power, Machines Can Now Recognize Objects and Translate Speech in Real Time. Artificial Intelligence Is Finally Getting Smart" https://www.technologyreview.com/s/513696/deep-learning/
- [11] Meyer, D. 2016. “Recent Advances in Machine Learning and Their Application to Networking” https://www.youtube.com/watch?v=IUksoV7l8ww DevOps Networking Forum
- [12] ColdFusion. 2016. “Google's Deep Mind Explained! – Self Learning A.I.” https://www.youtube.com/watch?v=TnUYcTuZJpM
- [13] Bright, P. 2017. “Elon Musk's Dota 2 AI Beats the Professionals at their Own Game” https://arstechnica.com/gaming/2017/08/ai-bot-takes-on-the-pros-at-dota-2-and-wins/
- [14] Accenture Digital. 2017. “Digital Index Switzerland 2017” https://www.accenture.com/t00010101T000000Z__w__/ch-de/_acnmedia/PDF-55/Accenture-Digital-Index-Switzerland-2017.pdf#zoom=50 Accenture
- [15] Trabulsi, A. 2015. “Future of Artificial Intelligence” http://www.fujitsu.com/us/Images/Panel1_Andrew_Trabulsi.pdf
- [16] Cardoza, C. 2017. “Black Hat USA 2017: Machine learning is not a silver bullet for security” http://sdtimes.com/black-hat-usa-2017-machine-learning-not-silver-bullet-security/
- [17] Wolff, M., Wallace, B., Zhao, X. 2016. “Applied Machine Learning for Data Exfil and Other Fun Topics” https://www.youtube.com/watch?v=dGwH7m4N8DE BlackHat USA
- [18] Petro, D., Morris, B. 2017. “Weaponizing Machine Learning” https://www.youtube.com/watch?v=wbRx18VZlYA DefCon 25
- [19] Chio, C. 2016. “Machine Duping 101: Pwning Deep Learning Systems” https://www.youtube.com/watch?v=4Qw3WWaymhc DefCon 24
- [20] Anderson, H. 2017. “Bot vs Bot For Evading Machine Learning Malware Detection” https://www.blackhat.com/us-17/briefings.html#bot-vs.-bot-for-evading-machine-learning-malware-detection BlackHat USA
- [21] Pistono, F., Yampolskiy, R. V. 2016. “Unethical Research: How to Create a Malevolent Artificial Intelligence” https://arxiv.org/ftp/arxiv/papers/1605/1605.02817.pdf
- [22] Yampolskiy, R. V. 2017. “AI Is the Future of Cybersecurity, for Better and for Worse” https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse
- [23] Yampolskiy, R. V., Spellchecker, M. S. 2016. “Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures” https://arxiv.org/ftp/arxiv/papers/1610/1610.07997.pdf
- [24] Charisi, V., Dennis, L., Fisher, M., Lieck, R., Matthias, A., Slavkovik, M., Sombertzki, J., Winfield, A. F. T., Yampolskiy, R. V. 2017. “Towards Moral Autonomous Systems” https://arxiv.org/pdf/1703.04741.pdf
- [25] Rizkallah, J. 2017. “Is Cybersecurity A Second Coming For AI?” https://www.forbes.com/sites/forbestechcouncil/2017/05/23/is-cybersecurity-a-second-coming-for-ai/#10f179eb7c40 Forbes Technology Council
- [26] Rossi, B. 2017. “How AI has created an arms race in the battle against cybercrime” http://www.information-age.com/ai-created-arms-race-battle-cybercrime-123465117/
- [27] Greenberg, A. 2016. “Obama’s Concerned an AI Could Hack America’s Nukes” https://www.wired.com/2016/10/obamas-concerned-ai-hack-americas-nukes/ Wired

REFERENCES

- [28] Yampolskiy, R. V. 2016. “Fighting malevolent AI: artificial intelligence, meet cybersecurity” https://theconversation.com/fighting-malevolent-ai-artificial-intelligence-meet-cybersecurity-60361
- [29] Hoffman, K. 2017. “For black and white hats, AI is shaking up infosec” https://www.the-parallax.com/2017/03/27/hackers-ai-artificial-intelligence-infosec/
- [30] Litan, A., Bussa, T., Ahlm, E. 2016. "The Fast-Evolving State of Security Analytics, 2016" https://www.gartner.com/doc/3274217/fastevolving-state-security-analytics- Gartner
- [31] Dilek, S., Cakir, H., Aydin, M. 2015. “Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review” https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf
- [32] Rehman, A., Saba, T. 2014. “Evaluation of artificial intelligent techniques to secure information in enterprises” https://link.springer.com/article/10.1007/s10462-012-9372-9
- [33] Berlin, K. 2016. “An AI Approach to Malware Similarity Analysis: Mapping the Malware Genome With a Deep Neural Network” https://mediaexchange.accenture.com/media/t/1_ao6yp1n1 BlackHat USA
- [34] Sasi, R. 2016. “Security Automation Based on Artificial Intelligence” https://www.youtube.com/watch?v=JhliHQ4BlGI Positive Hack Days
- [35] Sanz, B., Santos, I., Laorden, C., Ugarte-pedero, X., Garcia Bringas, P., Alvarez, G. 2012. “PUMA: Permission Usage to Detect Malware in Android” https://link.springer.com/chapter/10.1007/978-3-642-33018-6_30
- [36] Beard, A., Thyagarajan, A. 2016. “Detecting Malicious websites using Machine Learning” https://www.youtube.com/watch?v=IY3BjqVZAEw BSides DC
- [37] Nelms, T. 2015. “Practical Machine Learning for Network Security” https://www.youtube.com/watch?v=wg0F6i8EFr0 ShmooCon
- [38] Group J1. 2016. “Artificial Intelligence Within Cyber Security” https://www.youtube.com/watch?v=1JzPeaVXS7k
- [39] Barthur, A. 2016. “Cybersecurity with AI” https://www.youtube.com/watch?v=nUNmcfD4TzQ H2O.ai
- [40] Sevy, R., Montgomery, J. 2015. “Using Machine Learning Solutions to Solve Serious Security Problems” https://www.youtube.com/watch?v=48O6L_DfE2o Central Ohio InfoSec Summit
- [41] Chio, C. 2015. “Detecting Network Intrusions With Machine Learning Based Anomaly Detection Techniques” https://www.youtube.com/watch?v=c71gt-I8Lik Positive Hack Days
- [42] Russinovich, M. 2017. “Machine Learning and the Cloud: Disrupting Threat Detection and Prevention” https://www.youtube.com/watch?v=fRklX97iGIw RSA Conference
- [43] Emerging Technology. 2016. “Machine-Learning Algorithm Combs the Darknet for Zero Day Exploits, and Finds Them” https://www.technologyreview.com/s/602115/machine-learning-algorithm-combs-the-darknet-for-zero-day-exploits-and-finds-them/ MIT Technology Review
- [44] Tkacik, D. 2016. “CMU-spinoff ForAllSecure wins $2 million top prize at the DARPA Cyber Grand Challenge” https://www.cylab.cmu.edu/news_events/news/2016/cmu-spinoff-forallsecure-wins-2-million-top-prize-at-the-darpa-cyber-grand-challenge.html Carnegie Mellon University CyLab
- [45] Emma. 2017. “What’s the Deal with Artificial Intelligence in Cyber Security?” https://business.f-secure.com/whats-the-deal-with-artificiai-intelligence-in-cyber-security F-Secure
- [46] Choudhury, S. R. 2017. “Cyber threats are growing more serious, and artificial intelligence could be the key to security” https://www.cnbc.com/2017/04/17/darktrace-on-why-artificial-intelligence-is-key-in-cybersecurity.html CNBC
- [47] Gaustad, E. 2017. “Applied Machine Learning: Defeating Modern Malicious Documents” https://www.youtube.com/watch?v=ZAuCEgA3itI RSA Conference
- [48] Ismail, N. 2017. “The role of AI in cyber security” http://www.information-age.com/role-ai-cyber-security-123465795/
- [49] Ho, C., Lai, Y., Chen, I., Wang, F., Tai, W. 2012. “Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems” http://ieeexplore.ieee.org/abstract/document/6163595/
- [50] Marshak, D., Due, K. 2016. “Intelligent Finding Analytics: Your Cognitive Computing Application Security Expert” https://securityintelligence.com/intelligent-finding-analytics-cognitive-computing-application-security-expert/ IBM SecurityIntelligence
- [51] Marshak, D., Duer, K. 2016. “How to Leverage Cognitive Technology to Think Like a Security Expert” https://goo.gl/5vVoCc IBM Security

REFERENCES

- [52] Grieco, G. 2015. “Toward large-scale vulnerability discovery using Machine Learning” https://www.youtube.com/watch?v=9n6qxaUhcxo DefCamp; Grieco, G., Grinblat, G. L., Uzal, L., Rawat, S., Feist, J., Mouner, L. 2016. “”Toward Large-Scale Vulnerability Discovery Using Machine Learning” https://dl.acm.org/citation.cfm?id=2857720; The VDiscover Tool: http://www.vdiscover.org/
- [53] Nahari, H. 2016. “Machine Learning: No, It Can't Do That!” https://www.youtube.com/watch?v=M588VYrBqJI YOW! Conference
- [54] Yamaguchi, F., Lindner, F., Rieck, K. 2011. Vulnerability Extrapolation: Assisted Discovery of Vulnerabilities using Machine Learning https://www.usenix.org/legacy/events/woot11/tech/final_files/Yamaguchi.pdf
- [55] Akyol, E., Baikalov, I., Jou, S., Krasser, S. 2017. “AI and Machine Learning in CyberSecurity: What Is the Difference” https://www.youtube.com/watch?v=WOy5KN6J4h8 ITSPmagazine