|  |  |  |
| --- | --- | --- |
|  | **Reference** | **Comments:** |
|  | J. Lei and Z. T. Li, “Using network attack graph to predict the future attacks,” Proc.Second Int. Conf. Commun. Netw. China, ChinaCom 2007, pp. 403–407, 2008. | **Teodor**: As the title and abstract suggests this paper is about making predictions. They have an attack graph with probability values tied to it. They do not say how you should obtain the probabilities, but they are used to guess which attack path the attackers are working on.  **Heiko**: The authors create attack graphs from IDS-Data and predict attacks based on IDS events. They did an experimental validation, but they used honeypots for it which may not be representative. |
|  | B. C. Cheng, G. T. Liao, C. C. Huang, and M. T. Yu, “A novel probabilistic matching algorithm for multi-stage attack forecasts,” IEEE J. Sel.Areas Commun., vol. 29, no. 7, pp. 1438–1448, 2011. | **Teodor:** My experience is that papers with the word “novel” in the title seldom are particularly novel, and are often hard to understand. This is no exception. They appear to present a solution that inspect attack graphs and guess what the attackers are up to from the number of matched steps in the graph. It should probably be included.  **Pekka:** I consider this is a good paper and should be included for the following reasons:  1) According to the authors they present an apparently novel method named JEAN (Judge Evaluation Attack intension) for (predicting? / projecting) possible attacks. The method is a probability based approach. The authors demonstrate the method is more accurate and less labor intensive than LCS (Longest Common Subsequence) based approaches. The authors state “JEAN aims to provide a reasonable projection value for all possible stored attack sequences and to do the best matching of inputs”.  2) The article presents an impressive review of (apparently) predictive methods (-2011)  Although the results seem to be impressive it is quite hard to follow the validity of paper’s scientific process  **Roman:** This paper is really hard to understand but it is good I think. It gives very good review on existing predictive methods and probabilistic matching model. They write on specific attack prediction with comparison analysis and using experimental results shows really good work. They found out that is very hard to forecast multi-stage attack. |
|  | E. Santos Jr., “A Cognitive Architecture for Adversary Intent Inferencing: Knowledge Structure and Computation,” Proc SPIE 17th Annu. Int.Symp. Aerospace/Defense Sens. Control. Vol 5091, pp. 182–193, 2003. | **Teodor:** This is a very abstract paper about predicting adversaries’ action in any domain. It could be discussed in our paper, but I do not think it describes a solution. For example, “case based recognition” (which is like the attack graph papers I have read) is discussed, but no mathematical model is presented.  **Heiko:** This paper talks about using prediction for COA and mission planing, therefore it may fit pretty good in our work. Unfortunately, it is a very sophisticated model, therefore it is hard to verify and it is not clear for me how to make a mission planing support tool out of that (which is a goal of this research). |
|  | R. Colbaugh and K. Glass, “Predictive defense against evolving adversaries,” ISI 2012 - 2012 IEEE Int.Conf. Intell. Secur. Informatics Cyberspace, Border, Immigr. Secur., pp. 18–23, 2012. | **Teodor**: This paper addresses prediction with machine learning and game theory. Complex stuff! They apply it to spam to predict how spam evolve over time and tested it with real data. I am unable to assess how reasonable their solution is, but it should probably included.  **Dennis**: They make an assumption on triggering event…..which in some ways is a leap of faith.  How can you know a triggering event when it happens, isn’t that a look back determination or do we consider every event a potential triggering event.  The definitions of topological properties (transitivity, community structure, and core-periphery structure) may have some direct translation to contextualizing cyber events.  The discussion of neighbors the modeling framework may also be important.  Provides a useful approach as a point of departure for M&S of cyber systems and of organizing behavioral issues.   Appears it may have some overtones into TTPs?  The case studies are interesting, but this paper looked to me like predicting which of these 3 events are most likely as opposed to what is next.  Think some of the organizational concepts and classification schemes are potentially useful in a true prediction state. |
|  | A. Sarabi and M. Bailey, “Predicting Cyber Security Incidents Using Feature-Based Characterization of Network-Level Malicious Activities Categories and Subject Descriptors,” Int.Work. Secur. Priv. Anal. (SPA ’15), pp. 3–9, 2015. | **Dennis**: This paper has some value, but I was left a little confused as to what that was. Didn’t think some of the results were explained well enough (but that could be my issue alone). Good that it concentrates on false positives/negatives, but again……did not see a tie to architecture or final result. Gives good idea as to data sets that could be used for testing.  **Heiko**: Based on the assumption that IP address space prefixes have a small entropy of 'badness', this paper predicts future incidents. Unfortunately, it is not clear if this is valid assumption |
|  | S. J. Yang, A. Stotz, J. Holsopple, M. Sudit, and M. Kuhl, “High level information fusion for tracking and projection of multistage cyber attacks,” Inf.Fusion, vol. 10, no. 1, pp. 107–121, 2009. | **Tracy**: This paper introduces information fusion to provide situation awareness and threat prediction. A fusion system is proposed for the tracking and projection of multistage attacks. They use the term threat projection for prediction (like projecting a missile trajectory). The paper separates modelling of cyber-attack method from modelling of the network configuration. Predictions are performed independently on the two models, then fused to determine the targeted entities. They reference two previously existing tools/systems. First, they use INformation Fusion Engine for Real-time Decision-making (INFERD) to detect, correlate, and associate alerts that are part of multistage attack tracks. Second, Threat Assessment for Network Data and Information (TANDI) considers the current network status, and results from these tools are combined to determine next most likely targets. The system has several limitations. But this is one of the few papers reviewed the provided predictions.  **Margaret**: |
|  | X. Qin and W. Lee, “Attack plan recognition and prediction using causal networks,” Proc. - Annu.Comput. Secur. Appl. Conf. ACSAC, pp. 370–379, 2004. | **Tracy:**  **Pekka and Bernt**: Paper presents a method to recognize likely attacker goal and subgoals based on events and the Bayesian networks generated from attack trees. As the likely goal(s) is/are resolved, one is able to predict potential upcoming attacks. In this study the attack trees are constructed with expert knowledge. The authors conduct a probabilistic inference from events to correlate and analyze attack scenarios |
|  | O. Sheyner and J. M. J. M. Win, “Tools for Generating and Analyzing Attack Graphs,” in Formal Methods for Components and Objects, Springer Berlin / Heidelberg, 2004, pp. 344–371. | **Teodor**: I see this as an attack graph paper without any ambition of making predictions of what will happen next or when it will happen. I think it is out of scope for that reason and that we need to include pretty much every attack graph paper if we include this one.  **Margaret**: |
|  | W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, S. Dubus, and A. Martin, “Success Likelihood of Ongoing Attacks for Intrusion Detection and Response Systems,” 2009 Int.Conf. Comput. Sci. Eng., pp. 83–91, 2009. | **Teodor**: The words they use leads the thought to prediction of what attackers are doing, but I can’t find that really being done in the paper. As I understand Fig 3 they just associate objective with attacks and say which objectives that are possible given what they have seen from alerts etc. I think this is borderline case which we could include or could exclude.  **Margaret**: |
|  | B. A. Prakash, “Prediction Using Propagation: From Flu Trends to Cybersecurity,” IEEE Intell.Syst., vol. 31, no. 1, pp. 84–88, 2016. | **Dennis**: This approach is modeled after the Google Flu Trends model, although paper does not go into it in detail.  Authors make claims (for example) that low-prevalence feature based approaches appear to yield lower prediction errors. But details were not given, as were no formulas. Approach may have merit, but not enough information presented to allow for a reasonable evaluation of the technique and doesn’t allow us to decide what bearing (if any) this approach may have on our problem.  **Heiko**: This paper takes models for describing flu infections by analyzing twitter and uses them to model malware infections by monitoring information by AV tools. By the information given in the paper, it is hard to to determine the quality and relevance of this approach.  **Roman**: This paper doesn’t have any good implications on cyber prediction. It is word prediction there but with no correlation to our cause. |
|  | S. Noel and S. Jajodia, “Optimal IDS sensor placement and alert prioritization using attack graphs,” J. Netw.Syst. Manag., vol. 16, no. 3, pp. 259–275, 2008. | **Dennis**: There is not enough detail in this paper.  **Margaret**: |
|  | B. Bell, E. Santos Jr, and S. M. Brown, “Making adversary decision modeling tractable with intent inference and information fusion,” Proc. 11th Conf.Comput. Gener. Forces Behav. Represent., pp. 535–542, 2002. | **Dennis**: Similar to other two papers from Santos in this review, and like the others it sheds some light into the architecture of a predictive system (so see other reviews above). In this paper some key concepts concern classes of hypothesis (descriptive, predictive, and diagnostic). The authors present an argument that examines user intent inference and adversary intent inference. They present some constructs that include capturing observations, interpreting raw information to compute fused (higher level) information (although this could also be thought of as the data to useable information process) and then models of the user. They lay out the challenges with those 3 constructs and then present a very high level (no math) summary of the intelligence cycle approach. What is good from this paper is there are some (again) architectural items and lessons learned that will be valuable in a recommended approach to our prediction problem. .  **Tracy**: The paper articulates the challenges facing adversary decision modeling. They introduce an approach that employs intent inference, probabilistic reasoning, information fusion, and intelligent agents. They also introduce a notional computational architecture that, given observations of an adversary's actions and reactions, automatically generate hypotheses about the adversary's intent. But it is all very high level. There are no actual examples or implementation details. The paper is useful to list, because intent is related to prediction. But the paper makes no predictions. |
|  | K. Rieck and P. Laskov, “Language models for detection of unknown attacks in network traffic,” J. Comput.Virol., vol. 2, no. 4, pp. 243–256, 2007. | **Dennis**: Compare the problem to natural language detection and byte sequences. The byte sequences can be represented as n-grams…and n-grams have already been applied to intrusion detection problems. Base things on vector space and utilize distance functions (through unsupervised learning) to examine semantic differences in the “language” which translates into attack/normal data. Key here is that the approach yielded high results and in some cases out performed Snort (expected, since these are unknown signatures). Testing results also showed that this approach should be combined with a signature detection schema, presumably to remove all the “knowns” before engaging in language processing. Highly relevant to our problem and in the case of using multiple analytics to identify unknown attacks, this approach appears to be useful. Again, should be part of architecture considerations.  **Tracy**: The paper takes network traffic, converts connection payloads to n-grams and words, then uses language models and unsupervised learning for anomaly detection/intrusion detection. This is a first step towards automatic generation of attack signatures, and automated defenses. The paper had good results (few false positives). The paper made no predictions and had no prediction model. But the technique / model in this paper could apply to the known vulnerability / unknown attack model of our problem. |
|  | K. M. Vamvoudakis et al., "Formulating Cyber-Security as Convex Optimization Problems", In: “Control of Cyber-Physical Systems,” vol. 449, pp. 23–42, 2013. | **Tracy**: The paper developed a graph-based technique to correlate isolated attack scenarios from isolated alerts. They converted attack trees to Bayesian networks, and conducted probabilistic inference to evaluate the likelihood of attack goal(s) and predict potential upcoming attacks. Some assumptions are made, and expert knowledge is required, but likely attacks on assets are predicted.  **Pekka and Bernt**: The paper does not fully meet the inclusion criteria after all, and should not be included. While providing a mathematical model of resource allocation in cyber attack context, the assumptions necessary for conducting the analysis are limited by their applicability in more general scenarios. |
|  | D. a Gilmour, L. S. Krause, L. a Lehman, I. Distributed, and I. Systems, “Intent Driven Adversarial Modeling,” Knowl.Creat. Diffus. Util. | **Dennis**: The concept driving this research is to be able to effectively model adversarial actions in the environment where the adversary is not necessarily doctrine based, but rather less organized/predictable. The Emergent Adversarial Modeling System (EAMS) is intended to supply realistic and emergent Red force behavior by concentrating on intent in asymmetric conflict. Small discussion of Effects Based Operation. Scenario for this is physical military operation (not cyber) so some level of “laws of physics” had to be obeyed.  Addresses the issue of predictive adversary modeling by considering the adversary a “system”. Does mention soft factors which slightly line up with the center of Boyd’s OODA loop and how those influence intent ….which IMHO is consistent with Boyd’s theory. Incorporation of these soft factors into EAMS.  [NOTE: sometimes when evaluating papers, I look for architectural components that may be part of or influence the structure of a solution. This paper has many of those]. Present components of multiple sources of inputs, necessary for more realistic model. Defines also the Bayesian approaches to adversary axioms/beliefs/goals/actions. Other architectural comment is that there were multiple engines that represented the adversary, a much more realistic approach. There was no mathematics given, but rather both an ontology (appendix) and a structure for the multiple analytic engines. Both I think are useful as inputs to a prediction architecture, but again, no formulas.  **Tracy**: The paper mentions Bayesian Networks, but does not elaborate. There are no equations or math. The paper focuses on ground force / air force simulation, not cyber. The paper is similar to other Santos co-authored papers in our review. It presents a high level architecture, Emergent Adversarial Modeling System (EAMS), to model adversarial behavior based on adversaries' axioms, beliefs, goals, and actions, and generates possible courses of action. So the paper presents some level of prediction. Its also relevant because intent is a component of prediction. Quote from the conclusions, “Intent can be used effectively to influence the actions of an adversarial force.” |
|  | S. Noel, E. Robertson, and S. Jajodia, “Correlating intrusion events and building attack scenarios through attack graph distances,” Proc. - Annu.Comput. Secur. Appl. Conf. ACSAC, pp. 350–359, 2004. | **Pekka and Bernt**: Paper presents a simple (and fast) method for correlating intrusion events and building attack scenario based on precomputed attack graph distances. As output the method indicates likely attack scenarios based on the correlation of intrusion events. As a secondary output, an overall relevancy score is computed for each resulting attack scenario, although evident usability for it is not provided.  **Roman:** This attack graph and IDS paper gives a roadmap for using attack graphsin attack scenarios and events. This is more real time solution and building a model for network vulnerabilities by using Nessuss, than prediction.  **Tracy**:  The paper maps network intrusion events to an attack graph. Then they compute attack graph distances. The distances are used to determine attacks with high causal correlation. For inputs they use network traffic and machine vulnerabilities. Their outputs were correlated multi-step attacks identified in post-processed network traffic, and a relevancy score. They claim real-time performance. While an impressive Intrusion Detection System, it is not a predictive system. |
|  | J. Bean, “CHAracterization of Relevant Attributes using Cyber Trajectory Similarities CHAracterization of Relevant Attributes using Cyber by,” 2009. | **Pekka and Bernt**: The paper does not fully meet the inclusion criteria after all. In best case scenario, the output of the study could be used as input parameters/variables of actual predictions  **Heiko**: This paper is not about predicting something but about finding similarities between attacks. Therefore it does not really fit our inclusion criteria. |
|  | T. Sommestad and F. Sandström, “An empirical test of the accuracy of an attack graph analysis tool,” Inf.Comput. Secur., vol. 23, no. 5, pp. 516–531, Nov. 2015. | **Pekka and Bernt:** Although the article does not fully meet the inclusion criteria, it should be included as it emphasizes the poor predictive capabilities of current attack graphs. Paper presents a comparison between attack graph analysis and empirical data from an exercise and highlights poor prediction accuracy of attack graph analysis. The authors state that attack graph analysis' poor prediction capability is due to inaccurate vulnerability scans and improper interpretation of privileges that vulnerabilities grant.  **Teodor**: I think we can cite this paper and discuss the accuracy issue, but its I not a paper meeting our criterions.  **Roman:** This practical paper is good work about accuracy and we can of course cite it, butis more discussing analysis of attack graphs than prediction we need to focus. Chapter 4 we could use. Some thoughts about |
|  | X. Ou, S. R. Rajagopalan, and S. Sakthivelmurugan, “An Empirical Approach to Modeling Uncertainty in Intrusion Analysis,” in 2009 Annual Computer Security Applications Conference, 2009, pp. 494–503. | **Pekka and Bernt:** Although the article does not fully meet the inclusion criteria, it should be included as it provides a method and a tool to model uncertainties in intrusion detection. Uncertainty of the intrusion can be used as a parameter value when making predictions. The paper presents an empirical rule-based reasoning system for correlating alerts and log data for detecting multi-stage attacks, and identifying compromised machines |
|  | B. Zhu and A. a. Ghorbani, “Alert correlation for extracting attack strategies,” Int. J. Netw.Secur., vol. 3, no. 3, pp. 244–258, 2006. | **Pekka:** The paper seems to present a correlation based method for extracting attack strategies (attack graphs) from intrusion alerts. The authors concentrate on explaining about the details of the applied correlation method, that is a neural-network-based approach to computing correlation of events. The output of this paper can possibly be used as an input of actual prediction methods. Although the article does not fully meet the inclusion criteria as it is not capable to predict, maybe it should be included as well?  **Margaret:**  **Roman:** This paper is describing alert correlation and some approaches where we could find potential of discovering unknown attack patterns. Maybe we should try to build ours own ACM representation scheme - UCM (Unknown Correlation Matrix) based on this methodology. Forward statistical correlation strength – what alert is most likely to happen next. Goals of alerts analysis to understand security landscape and prevent future attacks. We should look for correlation probabilities. It shows technique how to handle a big data alerts. Automated analysis techniques on top of the attack graph in predictions could help to reduce analysis work. |
|  | V. Degeler, R. French, and K. Jones, “Self-Healing Intrusion Detection System Concept,” Proc. - 2nd IEEE Int. Conf. Big Data Secur. Cloud, IEEE BigDataSecurity 2016, 2nd IEEE Int. Conf. High Perform. Smart Comput. IEEE HPSC 2016 IEEE Int. Conf. Intell. Data Secur. IEEE IDS 2016, pp. 351–356, 2016. | **Teodor**: This is a paper that stays on the conceptual level and say little about how you should realize their solution in practice. There are diagrams (figure 3/4) saying that an identified attack should lead to a reaction, but they do not say how this should be done.  **Dennis**: Article states it is looking at intrusion detection, which does not appear to be predictive. Looks for anomalous events in a stream of constructed event sequences. Paper clearly applies since it is looking for the known vulnerability, unknown signature and presents a solution approach albeit not truly predictive. Paper does make a good statement, that any method should keep both false negatives and false positives at a minimum (Capt. Obvious, I know…..but well stated). Do negative selection on entities that don’t match it. Does a positive to see if it matches prior self-set (isn’t this straight up signature matching???). Uses danger theory as the approach. DT is in-line real time processing and is post event. Figures 3 and 4 allude to a more active defense and automation approach (IMHO). |
|  | Lee, S., Lee, D.H., Kim, K.J., 2006. A conceptual design of knowledge-based real-time cyber-threat early warning system. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 4331 LNCS, 1006–1017. | **Teodor:** I do not have the access to the PDF, but this seems to be a paper that could meet our inclusion criterions. |
|  | Shen, D., Chen, G., Cruz, Jr., J.B., Haynes, L., Kruger, M., Blasch, E., 2007. A Markov game theoretic data fusion approach for cyber situational awareness 3, 65710F. | **Teodor:** A bit abstract, but focuses on our issue. |
|  | Robinson, D., Cybenko, G., 2012. A Cyber-based Behavioral Model. J. Def. Model. Simul. 9, 195–203. | **Teodor:** Focuses on user behaviors and seems to be useful for detecting insiders or anomalies. But that is also the case for much IDS research, which we ignore. |
|  | Shen D., Chen, G., Blasch, E., Tadda, G., 2007. Adaptive Markov Game Theoretic Approach for Cyber Network Defense. | **Roman:** The Authors tried to generate primitive prediction of cyber attacker’s intents. The primitive prediction can be used before it is refined. High level data fusion based on Markov game model, is proposed to capture new or unknown threats. The Markov game method (stochastic) is used to estimate the possible cyber-attack with uncertainty and information is not defined. Methodology was studying red and blue team with different domain properties. They also mentioned suboptimal technique which is used for reasoning in chess, backgammon and monopoly. They also used Fiticious play to learn these unknown properties. Each player starts with some initial beliefs and chooses the best response to those beliefs. They build game simulation platform based on open source network – practically is the way to test the unknown threats through visualization and experiment. They simulated by events. |
|  | Morris, T.I., Mayron, L.M., Smith, W.B., Knepper, M.M., Ita, R., Fox, K.L., 2011. A perceptually-relevant model-based cyber threat prediction method for enterprise mission assurance. 2011 IEEE Int. Multi-Disciplinary Conf. Cogn. Methods Situat. Aware. Decis. Support. CogSIMA 2011 60–65. | **Teodor:** Only the title says something on prediction. The rest is more about intelligence processing or so.  **Roman:** Paper with really focusing on enterprise intelligence processing and not much valuable for prediction. |
|  | Giacobe, N., 2010. Application of the JDL data fusion process model for cyber security. SPIE Defense, Secur. … 7710, 77100R–77100R–10. | **Teodor:** A short review paper. It that Yang et al. (2009) are the ones that have done something on prediction.  **Roman:** This paper used descriptive model. There are some assumptions types of algorithm and is more analyzing approach and knowing attacker capabilities (for example using Metasploit). |
|  | Skopik, F., Bleier, T., Fiedler, R., 2012. Information management and sharing for national cyber situational awareness. ISSE 2012 Secur. Electron. Bus. Process. Highlights Inf. Secur. Solut. Eur. 2012 Conf. 217–227. | **Teodor:** On information sharing and not prediction.  **Roman:** This paper is orientated on Austrian CAIS project which uses Delphi method – forecasting technique, also was inspired by bio informatics models and innovative tools for attack simulations. They suggest that manifestation and impact of attacks is very similar and so they introduced reactive approach. |
|  | Greitzer, F.L., Frincke, D.A., 2010. Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In: Advances in Information Security. pp. 85–113. | **Teodor:** Focused on insiders, but clearly about anticipating attacks from them. On the other hand, the predictions seems to be about who will be malicious rather than when they will attack or how likely it is that someone will attack.  **Roman:** It is truly insider threat perspective, form psychological and motivation approach. Also warns thatmistaken prediction of potential insider crime has a lot of negative consequences for individuals and organization.The key to prediction is to incorporate traditional cyber audit data with demographical and organizational data of the employee.They suggested that any data monitoring needed to predict model should be based on actual behavior and events. In chapter 4 they gave a predictive conceptual modeling approach with psychosocial and cyber indicators (Data, Observations, Indicator, Behavior). It is interesting how they combined data fusion and analysis like predictive classification (Machine Learning, Model-based reasoning and Heuristic rules). The predictive classification analyze a vast amount of noisy data which are all the time changeable. Reasoner (insider threat problem) like executive function form knowledge base is explained. To provide warning signs of cyber-attacks they suggested to evaluate demographic, behavioral and psychosocial data indicators based on case studies. The prediction should be tested against of set of a real cases. They gave usable predictive indicators, for developing framework. |
|  | Yang, S.J., Byers, S., Holsopple, J., Argauer, B., Fava, D., 2008. Intrusion activity projection for cyber situational awareness. IEEE Int. Conf. Intell. Secur. Informatics, 2008, IEEE ISI 2008 167–172. | **Teodor:** Seems very relevant.  **Roman:** Behavior trends for projections of future intrusions are based on Variable Length Markov Models.They put four elements for projecting cyber-attack actions (capability, opportunity, intent and behavior). They researched that estimation and attacker exact capability is not possible. Extremely conservative way is to assume that all attacker are able to execute all known and unknown exploitation methods, and on the other way that attacker used services, which he/she used before. Capability alone is not enough to estimate future attack actions. They had developed a prototype of virtual terrain model with algorithms for cyber intrusion projection. In examine they discovered that capability and opportunity is effective to project most cyber attack actions (they quantified the results in numbers). They used 13-step attack. Problems are always decoy and stealthy attacks. |
|  | Kopylec, J., D’Amico, A., Goodall, J., 2007. Visualizing cascading failures in critical cyber infrastructures. In: IFIP International Federation for Information Processing. pp. 351–364. | **Teodor:** This is not about adversarial attacks, but on dependencies between systems.  **Roman:** It is more about Critical infrastructure procedures, GIS, Disaster plan for software based attacks. The design Cascade (software system) that visually presents the physical vulnerabilities. It is interesting in combined sensors and GIS data that provide sophisticated visualization. RISK MANAGEMENT + INFRASTRUCTURE SIMULATION SYSTEM |