Deceptive Cyber Defense for IIoT

Daniel Fraunholz, Hans D. Schotten
Intelligent Networks
German Research Center for Artificial Intelligence
D-67663 Kaiserslautern, Germany
Email: {daniel.fraunholz,hans_dieter.schotten}@dfki.de

***Abstract*—Standard cyber security hardly copes with uprising cyber crime and espionage intrusion techniques. Simultaneously recent advances in industrial applications are coming along with a rising demand for interconnectivity which lead to new cyber security threats. Deceptive defense mechanisms are able to provide high level threat intelligence and harden industrial systems. The intention of this work is to develop a deceptive cyber security framework with highly adaptive features. The system will need a minimum of configuration and maintenance. Additionally state-of-the-art weaknesses like scope, fingerprinting and generalization will be eliminated.**

I. Introduction

The Industrial Internet of Things (IIoT) is a novel paradigm that brings vast advantages in economic efficiency for industrial applications. It is rapidly gaining ground and expected to grow up to 50 billion devices by 2020 [1]. A crucial change is the fusion of cyber and physical world. Critical infrastructures like power plants, hospitals, traffic management systems and also industrial production environments are highly endangered. IIoT design criteria implicates new security risks. Major risks are the vast amount of devices, the wireless communication and the ad-hoc networking. Existing security solutions are e.g. firewalls, rule-based intrusion detection and prevention and anti virus. These solutions are not suitable to ensure a certain security level in respect to volatile signatures, encryption, zero-day exploits, inside attacks and physical attacks. To support mitigation of these threats, deceptive systems are an eligible solution. But available deception systems lack in several features. Often they can be fingerprinted and bypassed or even evaded by intruders. In section II an overview of deceptive technologies in general plus current research on adaptive features for deceptive systems is depicted. Section III focuses on the relation between design criteria and the perception of the intruder. To do so psychological models are employed and current research for Human-Computer-Interaction, game and decision theory are motivated. Technical aspects of context-aware deception systems plus current implementations are illustrated in IV. In section V supportive research work is presented. Finally, a conclusion is drawn in VI.

II. State-of-the-Art Deception Methods

Deception techniques were first described by Clifford Stoll 1989 [2]. Since this time many implementations were made for a vast amount of protocols [3] [4] [5], resource types [6] [7] [8] and interaction-levels [9] [10] [11]. Recently a new research field for deceptive systems with adaptive abilities is emerging [12]. Several of the research aspects of this work are also targeted in former research, including adaptive deployment [13] [14], service learning [15] and game-theory-based interaction [16] [17].

III. Psychological Aspects of Deception

For deception techniques the human psychology is crucial to understand and to consider for the system design. Relevant research fields are general psychology, Human-Computer-Interaction (HMI), game theory and decision theory.

A. General Psychology

While human motives are highly ambivalent and hardly to determine, motivation is easily influenced by the situation. In respect to the relation between motivation and volition, it is likely that human behavior can be influenced by system induced stimuli. For example by handicapping intrusion attempts, frustration can be increased. Like FA theory postulates, this can lead to aggression and decreased cautiousness. Another approach is to increase aggression by insulting the intruder [18].

B. Human-Computer-Interaction

More technical related is the theoretical background of the perception of interaction by the intruder. Several models are deployed to deduct design criteria for deceptive systems. Such models are choice under risk model, advanced cognitive motivation model, GOMS, Herczeg model and Seven Stages-of-Action. Premature results show that by applying these models the intruders perception of the interaction can be controlled.

C. Game and Decision Theory

All interaction stages will be analyzed by a game and decision theoretical point of view. One key aspect is the deployment of deceptive systems. The second key aspect is the intensification of the interaction between deception system and intruder to amplify threat intelligence. One example is to block, redirect or accept the actions of the intruder and by this to maximize the information gain per interaction.

IV. Context-aware System Features

The technical focus of this work is to implement several context-aware features in a framework. Per definition this framework is optimized for minimal configuration and maintenance input. To achieve this, machine learning algorithms are employed and modified by the addition of heuristic estimations of optimal input parameters.

A. Environment Adaptive Deployment

An important stage in deception is the deployment. The deceptive system needs to be unidentified as intrusion detection but needs to attract the intruders interests. To avoid identification or fingerprinting the deceptive system observes the environment and determines an optimal deploying strategy. For the framework an active scan engine, called nmap [19], is used to observe a computer network. Based on the results an ontology is build and analyzed by the use of machine learning methods. To complete the process the deployment is realized by a state-of-the-art deployment engine, namely honeyd. Continuing research considers broader resource types, like tokens and client-side deception.

B. Automated Service Learning

Like the environment adaption, service learning focuses on anti-fingerprinting techniques. But in contrary it tries to mimic just one service. This service can be deployed on a deceptive system or as a deceptive service on a real system. Even if in state-of-the-art taxonomies of deceptive systems context-awareness is not considered, this systems interaction is classified as a high-interaction deceptive system, regarding to the intense interaction between intruder and system. Depending on the quality of deception the intruders intention may be deducted from the interaction, therefore a high quality learning of services is aspired.

C. Intelligent Interaction

If the communication e.g. service protocol is well-understood from intruder and system, it is possible to manipulate the progression of the intruder in achieving her objective. This feature will employ the results from III and try to manipulate the intruders behaviour. It will be designed to maximize the information gain in respect to e.g. obtained input commands, uploaded files or specific metrics.

V. Auxiliary Research

Several side-studies are conducted to support the system development. A model of different intruders is developed, an validation environment is designed and partly implemented and a long-term field study is started.

A. Intruder Model

Since intruder skills, intentions and resources are highly different, relevant features were clustered and a taxonomy was developed. This taxonomy is able to classify intrusion and potentially increase threat intelligence.

B. Validation Environment

Since deployments in the wild are always risky, an environment was designed to validate the deceptive system and in later stages to simulate intrusions and evaluate different counter measure methods. The environment consists of eight entities, were six of them simulating production machines, one simulates the intruder and the last one represents the deception system. Additionally a monitoring unit is employed for state-of-the-art intrusion and anomaly detection within the network communication.

C. Deceptive Systems in the Wild

Since deceptive systems are highly depended on psychological factors the internet is a realistic environment. To gain experience in real intrusion scenarios a long-term study on deceptive systems in the internet is ongoing. First results are that the investigated service is mostly attacked by bots. These attacks are very frequent, one system observed 45.000 intrusion attempts at one day. All attempts will be investigated for patterns and correlations. Additionally the concept of fake deception systems will be investigated.

VI. Conclusion

This work presents several adaptation features which enable deception based cyber defense to support the mitigation of uprising threats for IIoT applications.

References

[1] E. Dave, "The internet of things how the next evolution of the internet is changing everything," 2011.

[2] C. Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York, NY, USA: Doubleday, 1989.

[3] L. Rist, "Conpot," 2015. [Online]. Available: https://github.com/mushorg/conpot

[4] P. Sylvain, "rpdy," 2015. [Online]. Available: https://github.com/citronneur/rdpy

[5] "Mailoney," 2015. [Online]. Available: https://github.com/awhitehatter/mailoney

[6] L. Rist, "Honeyprint," 2016. [Online]. Available: https://github.com/glaslos/honeyprint

[7] B. Alexander, "honeypot-camera," 2015. [Online]. Available: https://github.com/alexbredo/honeypot-camera

[8] S. Poeplau, "Ghostusb," 2015. [Online]. Available: https://github.com/honeynet/ghost-usb-honeypot

[9] N. Provos, "Honeyd," 2007. [Online]. Available: http://www.honeyd.org/

[10] "Kippo," 2015. [Online]. Available: https://github.com/desaster/kippo

[11] "Sebek," 2008. [Online]. Available: https://github.com/honeynet/sebek

[12] W. Zanoramy, A. Zakaria, and L. M. Kiah, "A review of dynamic and intelligent honeypots," in *ScienceAsia*, 2013, pp. 1–5.

[13] H. Christopher and H. Brian, "Automated honeynet deployment for dynamic network environment," in *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*, ser. HICSS '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 4880–4889. [Online]. Available: http://dx.doi.org/10.1109/HICSS.2013.110

[14] C. Leita, K. Mermoud, and M. Dacier, "Scriptgen: an automated script generation tool for honeyd," in *21st Annual Computer Security Applications Conference (ACSAC'05)*, Dec 2005, pp. 12 pp.–214.

[15] C. Vishal, T. Alok, and C. Tzicker, *Towards Automatic Learning of Valid Services for Honeypots*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 469–469. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-30555-2_55

[16] G. Wagener, R. State, T. Engel, and A. Dulaunoy, "Adaptive and self-configurable honeypots," in *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*, May 2011, pp. 345–352.

[17] A. Pauna and I. Bica, "Rassh - reinforced adaptive ssh honeypot," in *Communications (COMM), 2014 10th International Conference on*, May 2014, pp. 1–6.

[18] G. Wagener, R. State, A. Dulaunoy, and T. Engel, "Heliza: talking dirty to the attackers," *Journal in Computer Virology*, vol. 7, no. 3, pp. 221–232, 2011. [Online]. Available: http://dx.doi.org/10.1007/s11416-010-0150-4

[19] F. Vaskovich, "The art of port scanning," *Phrack Magazine*, vol. 7, 1997.