Computer Security Symposium 2017
23 - 25 October 2017

ハードウエアの安全性についての評価

ヴァスコンセロス　ヴァルガス　ダニロ[1]　櫻井　幸一[1]

概要：デバイスの台数は毎日増えていますが、そのデバイスに信頼できるでしょうか？オフソーシングと大規模なサプライチェーンは、この問題をさらに複雑にしています。使用パターンに基づいてデバイスを評価する方法があれば、これは単純化されます。提案アイデアはどのデバイスでも動作範囲外でランダムまたはゼロ出力を持つ必要があるということです。したがって、提案アイデアは、動作範囲外のパターンまたは関係をチェックするシステムを使用します。

キーワード：自動チェック、ハードウェア、信頼チェック

Hardware Trust-Check System

Danilo Vasconcellos Vargas[1]　Kouichi Sakurai[1]

Abstract: The number of electronic devices is multiplying every day but can we trust them? Off-sourcing and large supply chains make this question even more complicated. This would be simplified if we could have a method to evaluate any device given its usage patterns. The idea is that any device should have random or zero output outside of its working range. Therefore, the proposed idea uses a system that check for patterns or relationships outside the area of usage.

Keywords: Automatic Check, Hardware, Trust-check

1. Introduction

Nowadays, electronic devices can be found almost everywhere. From cars, factories to refrigerators and washing machines. The demand for many types of devices continue to increase. Many functions that were previously done without the need of any electronic circuit were replaced by more complex electronic solutions. The improvement in quality is sometimes questionable but the need for more devices is a reality of the modern world. Moreover, the internet of things [2] and wereable devices [5] should increase the demand even further.

The devices are surely increasing but can we trust them? With large supply chains and off-sourcing answering this question becomes increasingly complicated [18].

In this paper, we propose a different approach which is more general and can potentially identify many types of malicious hardware.

2. Related Works

Here, we review some of the literature regarding hardware security and trust check as well as related subjects.

2.1 Hardware Trojan

There are many types of malicious code that can be inserted in electronic devices. One of the most dangerous malicious code is the trojan. Many tools were developed for hardware trojan detection [12], [17]:

- Power based analysis - A transition into a trojan will draw current from the power distribution. Power based analysis use this to try to identify trojans [1],[24].

[1] 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

- Timing based signal analysis - The additional load added by a trojan will make the original circuit slower and this delay can be used to recognize the presence of trojans [13], [14].
- Trojan activation methods - Some methods try to activate the trojan itself. By doing this the identification of the trojan is faciliated. Sometimes this methods is used in combination with the other methods described above [25], [3].

2.2 Machine Learning and Statistical Based Approaches

Other approaches try to identify trojans by analysing the netlist of the IC [8], [11].

However there are many other state-of-the-art machine learning which might improve the results. For example, Evolutionary neural networks [19], [16], Learning Classifier Systems [21], [23], [22], [20],[7], [15], [6], [10] and deep neural networks [4],[9].

3. Proposed Approach

The proposed approach is based on the idea that output for out of the range input should be either noise, a constant value or some output correlated with the input. Research on anomaly detection is based on a similar hypothesis. Naturally, an anomaly does not mean that the IC is malicious. However, for a IC to be malicious it must be anomalous.

Figure 1 illustrates the behavior of a system of a non-malicious IC while Figure 2 illustrates the output of a IC which might be malicious.

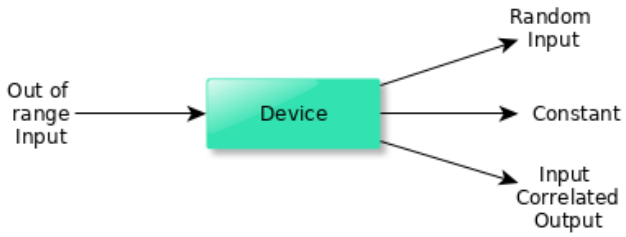

図 1 Expected output from a well-designed non-malicious IC.

4. Discussion

Thus, with this approach an automatic screening can be made to auxiliate the check for malicious devices. In fact, when a system is identified as possibly malicious it will necessarily have a pattern of output. This output pattern can be used to investigate any similarity with stored data

図 2 Expected output from a possibly malicious IC.

(i.e., the system is leaking information) or normal output from a different range of input (i.e., possible trojan).

参考文献

[1] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar. Trojan detection using ic fingerprinting. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 296–310. IEEE, 2007.

[2] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[3] M. Banga, M. Chandrasekar, L. Fang, and M. S. Hsiao. Guided test generation for isolation and detection of embedded trojans in ics. In *Proceedings of the 18th ACM Great Lakes symposium on VLSI*, pages 363–366. ACM, 2008.

[4] Y. Bengio. Learning deep architectures for ai. *Foundations and Trends® in Machine Learning*, 2(1):1–127, 2009.

[5] M. Billinghurst and T. Starner. Wearable devices: new ways to manage information. *Computer*, 32(1):57–64, 1999.

[6] A. Bonarini, C. Bonacina, and M. Matteucci. Fuzzy and crisp representations of real-valued input for learning classifier systems. *Learning Classifier Systems*, pages 107–124, 2000.

[7] M. V. Butz and O. Herbort. Context-dependent predictions and cognitive arm control with xcsf. In *Proceedings of the 10th annual conference on Genetic and evolutionary computation*, pages 1357–1364. ACM, 2008.

[8] R. S. Chakraborty, F. G. Wolff, S. Paul, C. A. Papachristou, and S. Bhunia. Mero: A statistical approach for hardware trojan detection. In *CHES*, volume 5747, pages 396–410. Springer, 2009.

[9] G. Hinton, S. Osindero, and Y. Teh. A fast learning algorithm for deep belief nets. *Neural computation*, 18(7):1527–1554, 2006.

[10] G. Howard, L. Bull, and P. Lanzi. Towards continuous actions in continuous space and time using self-adaptive constructivism in neural XCSF. In *Proceedings of the 11th Annual conference on Genetic and evolutionary computation*, pages 1219–1226. ACM, 2009.

[11] Y. Jin and Y. Makris. Hardware trojan detection using path delay fingerprint. In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pages 51–57. IEEE, 2008.

[12] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor. Trustworthy hardware: Identifying and classifying hardware trojans. *Computer*, 43(10):39–46, 2010.

[13] J. Li and J. Lach. At-speed delay characterization for ic authentication and trojan horse detection. In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pages 8–14. IEEE, 2008.

[14] D. Rai and J. Lach. Performance of delay-based

trojan detection techniques under parameter variations. In *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pages 58–65. IEEE, 2009.

[15] P. Stalph and M. Butz. Learning local linear jacobians for flexible and adaptive robot arm control. *Genetic programming and evolvable machines*, 13(2):137–157, 2012.

[16] K. Stanley and R. Miikkulainen. Evolving neural networks through augmenting topologies. *Evolutionary computation*, 10(2):99–127, 2002.

[17] M. Tehranipoor, H. Salmani, X. Zhang, M. Wang, R. Karri, J. Rajendran, and K. Rosenfeld. Trustworthy hardware: Trojan detection and design-for-trust challenges. *Computer*, 44(7):66–74, 2011.

[18] M. Tehranipoor and C. Wang. *Introduction to hardware security and trust*. Springer Science & Business Media, 2011.

[19] D. V. Vargas and J. Murata. Spectrum-diverse neuroevolution with unified neural models. *IEEE Transactions on Neural Networks and Learning Systems*.

[20] D. V. Vargas, H. Takano, and J. Murata. Continuous adaptive reinforcement learning with the evolution of self organizing classifiers. In *Development and Learning and Epigenetic Robotics (ICDL), 2013 IEEE Third Joint International Conference on*, pages 1–2. IEEE, 2013.

[21] D. V. Vargas, H. Takano, and J. Murata. Self organizing classifiers and niched fitness. In *Proceedings of the fifteenth annual conference on Genetic and evolutionary computation conference*, pages 1109–1116. ACM, 2013.

[22] D. V. Vargas, H. Takano, and J. Murata. Novelty-organizing team of classifiers-a team-individual multi-objective approach to reinforcement learning. In *SICE Annual Conference (SICE), 2014 Proceedings of the*, pages 1785–1792. IEEE, 2014.

[23] D. V. Vargas, H. Takano, and J. Murata. Novelty-organizing team of classifiers in noisy and dynamic environments. In *Evolutionary Computation (CEC), 2015 IEEE Congress on*, pages 2937–2944. IEEE, 2015.

[24] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic. Hardware trojan detection and isolation using current integration and localized current analysis. In *Defect and Fault Tolerance of VLSI Systems, 2008. DFTVS'08. IEEE International Symposium on*, pages 87–95. IEEE, 2008.

[25] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty. Towards trojan-free trusted ics: Problem analysis and detection scheme. In *Proceedings of the conference on Design, automation and test in Europe*, pages 1362–1365. ACM, 2008.