purportedly mathematically unbreakable [7].

The emergence of hardware Trojans embedded in third- *how can we comparatively assess security levels of IP cores,*

Figure 1: Control Values Histogram and the Best-Fit Normal Distribution for UART Module (a) Genuine (b) Trojan Type 1 (c) Trojan Type 2 (d) Trojan Type 3 (e) Trojan Type 4 (f) Trojan Type 5 (g) Trojan Type 6 (h) Trojan Type 7 (i) Trojan Type 8 (j) Trojan Type 9

Table 1: Security Metric for genuine and Trojan-Infected RS232 Circuits

	Gen	T1	T2	T3	T4	T5	T6	T7	T8	T9
Rare Nodes (Y/N)	N	N	N	N	N	N	N	N	Y	N
K-W Test:	5.45e-02	1.59e-03	4.17e-03	3.97e-03	6.65e-03	4.29e-03	2.90e-03	4.17e-03	1.86e-01	1.99e-03
Security Metric:	5.45e-02	1.59e-03	4.17e-03	3.97e-03	6.65e-03	4.29e-03	2.90e-03	4.17e-03	0	1.99e-03

inserted Trojan, or that the target circuit is likely vulnerable to hardware Trojan attacks. At the second level, for all of the control values corresponding to the entire circuit, we fit the measured distribution with a normal distribution to set a boundary of security for K-W Test parameter p. As shown in the Table 1, the genuine circuit is assigned the highest security level.

From figure 1 (a), it is apparent that there are several low controllability nodes so that the golden model is potentially vulnerable to attacks. For example, it shows that the majority of control values are distributed within a range [-3,-1], but that there exist several nodes with low probabilities. However, there do not exist any nodes below the boundary 3 outlined in Step II of Section 2.

Figures 1 (b) - (j) indicate that the inclusion of hardware Trojans deteriorate the security level of the target circuit by largely affecting the control value distribution. The inserted Trojans have shifted the peak control values distribution to the left such that the accumulation of node control values are found to be at -6 whereas the original control values were found to be distributed around -2. The large number of nodes with low controllability indicates that the IP core is an easy target for attacks, or that the IP core may already contain malicious logic. In either event, the cost to exhaustively include all testing patterns in an effort to trigger any malicious logic would be prohibitively exorbitant.

As we mentioned earlier, the real power of the proposed metric is to provide a quantitative metric for IP users to compare security levels of IP cores with similar functionality, but supplied by different vendors. It also provides IP vendors with another means of supporting their claim that their IP cores are more secure than others.

5. CONCLUSION

A security metric is developed to quantitatively measure the security level of any IP core. The developed metric provides IP users with a valuable reference attempting to compare the quality of IP cores (with the same or similar functionality). The metric has been demonstrated on an RS232 module, along with nine unique Trojan designs, that the insertion malicious logic will degrade the module's security.

Acknowledgements

This work was funded in part by the NSF grant CNS 0958510, 1319105, and Intel.

6. REFERENCES

[1] https://esc.isis.poly.edu/ .

[2] https://www.trust-hub.org/ .

[3] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar. Trojan detection using IC fingerprinting. In IEEE Symposium on Security and Privacy, pages 296{310, 2007.

[4] E. Greenbaum. Open source semiconductor core licensing. Harvard Journal of Law & Technology, 25(1):131{157, 2011.

[5] Y. Jin and Y. Makris. Hardware Trojans in wireless cryptographic ICs. IEEE Design and Test of Computers, 27:26{35, 2010.

[6] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor. Trustworthy hardware: Identifying and classifying hardware Trojans. IEEE Computer, 43(10):39{46, 2010.

[7] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In Advances in Cryptology { CRYPTO'99, pages 789{789. 1999.

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

[9] A. Waksman, M. Suozzo, and S. Sethumadhavan. FANCI: Identification of stealthy malicious logic using boolean functional analysis. In Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, CCS '13, pages 697{708, 2013.