Hardware Trojans and Other Threats against Embedded Systems

Christof Paar
Horst Görtz Institute for IT-Security
Ruhr Universität Bochum, Germany
and University of Massachusetts Amherst
christof.paar@rub.de

ABSTRACT

Countless systems ranging from consumer electronics to military equipment are dependent on integrated circuits (ICs). A surprisingly large number of such systems are already security-critical, e.g., automotive electronics, medical devices, or SCADA systems. If the underlying ICs in such applications are maliciously manipulated through hardware Trojans, the security of the entire system can be compromised. In recent years, hardware Trojans have drawn the attention of the scientific community and government. Initially, the primary attacker model was a malicious foundry that could alter the design, i.e., introduce hardware Trojans which could interfere with the functionality of a chip. Many other attacker models exist too. For instance, a legitimate IC manufacturer, such as a consumer electronics company, might be in cohort with a national intelligence agency and could alter its products in a way that compromises their security.

Even though hardware Trojans have been studied for a decade or so in the literature, little is known about how they might look, and what the "use cases" for them is. We describe two applications for low-level hardware manipulations. One introduces an ASIC Trojans by sub-transistor changes, and the other is a novel type of fault-injection attacks against FPGAs.

As an example for an extremely stealthy manipulations, we show how a dangerous Trojans can be introduced by merely changing the dopant polarity of selected existing transistors of a design. The Trojan manipulates the digital post-processing of Intel's cryptographically secure random number generator used in the Ivy Bridge processors. The adversary is capable of exactly controlling the entropy of the RNG. For example, the attacker can reduce the RNG's entropy to 40 bits of randomness. Due to the AES-based one-way function after the entropy extracting, the Trojan is very difficult to detect. Crucially, this approach does not require to add new circuits to the IC. Since the modified circuit appears legitimate on all wiring layers (including all metal and polysilicon), our family of Trojans is resistant to many detection techniques, including fine-grain optical inspection and checking against "golden chips".

As a second "use case", we show how an adversary can extract cryptographic keys from an unknown FPGA design. The attack, coined bitstream fault injection (BiFI), systematically manipulates the bitstream by changing *random* LUT contents, configures the target device, and collects the resulting faulty ciphertexts. The ciphertexts are used to recover the key by testing a set of hypotheses, e.g., that the ciphertext is the plaintext XORed with the key. The attack only needs a black-box assumption about the bitstream structure and format. It was verified by considering a set of 3rd party AES designs on different standard FPGAs. In 15 out of 16 designs, we were able to extract the AES key.

BIOGRAPHY

Christof Paar has the Chair for Embedded Security at Ruhr University Bochum, Germany, and is affiliated professor at the University of Massachusetts Amherst. He co-founded CHES, the leading international conference on applied cryptography. Christof's research interests include efficient crypto implementations, hardware security, and security analysis of real-world systems. He holds an ERC Advanced Grant in hardware security and is spokesperson for two doctoral research schools, UbiCrypt and SecHuman. Christof has over 180 peer-reviewed publications and he is co-author of the textbook Understanding Cryptography. He is Fellow of the IEEE and was recipient of an NSF CAREER Award, the German IT Security Award and the Innovation Prize NRW. He has given numerous invited talks, including presentations at MIT, Yale, Stanford, IBM Labs and Intel.

REFERENCES

[1] G.T. Becker, F. Regazzoni, C. Paar, W.P. Burleson. Stealthy Dopant-Level Hardware Trojans. Cryptographic Hardware and Embedded Systems – CHES 2013, 197-214

[2] P. Swierczynski, G.T. Becker, A. Moradi, C. Paar.- Bitstream Fault Intjections (BiFI) - Automated Fault Attacks against SRAM-based FPGAs. IEEE Transactions on Computers, to appear.

This material is based upon work partially supported by the National Science Foundation under grants No. CNS-1318497 and CNS-1421352, as well as ERC grant No. 695022

ASIA CCS '17, April 02-06, 2017, Abu Dhabi, United Arab Emirates
ACM 978-1-4503-4944-4/17/04.
http://dx.doi.org/10.1145/3052973.3053885