Proceedings of the IEEE

AUGUST 2014 / VOL. 102 / NO. 8

CONTENTS

SPECIAL ISSUE

TRUSTWORTHY HARDWARE

Edited by R. Karri and F. Koushanfar

1126 **Physical Unclonable Functions and Applications: A Tutorial**
By C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas
|INVITED PAPER| This paper is a tutorial on ongoing work in physical-disorder-based security, security analysis, and implementation choices.

1142 **Public Physical Unclonable Functions**
By M. Potkonjak and V. Goudar
|INVITED PAPER| This paper surveys the time-bounded or public PUFs, including their design and security evaluation and the new protocols that they can support.

1157 **Microcontrollers as (In)Security Devices for Pervasive Computing Applications**
By D. Strobel, D. Oswald, B. Richter, F. Schellenberg, and C. Paar
|INVITED PAPER| This paper discusses possible threats to embedded systems using two microcontroller case studies.

1174 **Trustworthiness of Medical Devices and Body Area Networks**
By M. Zhang, A. Raghunathan, and N. K. Jha
|CONTRIBUTED PAPER| This paper surveys the threat landscape of medical embedded devices and the merits and shortcomings of existing defenses.

1189 **Mobile Trusted Computing**
By N. Asokan, J.-E. Ekberg, K. Kostiainen, A. Rajan, C. Rozas, A.-R. Sadeghi, S. Schulz, and C. Wachsmann
|INVITED PAPER| This paper surveys the trusted computing features in mobile computing platforms.

1207 **Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain**
By U. Guin, K. Huang, D. DiMase, J. M. Carulli, Jr., M. Tehranipoor, and Y. Makris
|INVITED PAPER| This paper surveys the state of the art in counterfeiting and detection technologies.

1229 **Hardware Trojan Attacks: Threat Analysis and Countermeasures**
By S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan
|INVITED PAPER| This paper is a survey of the state-of-the-art Trojan attacks, modeling, and countermeasures.

1248 **FPGA Security: Motivations, Features, and Applications**
By S. M. Trimberger and J. J. Moore
|INVITED PAPER| This paper discusses all aspects of FPGA security and trust.

1266 **Regaining Trust in VLSI Design: Design-for-Trust Techniques**
By J. Rajendran, O. Sinanoglu, and R. Karri
|INVITED PAPER| This paper surveys how concepts in VLSI test can be adopted in the context of hardware security and trust and design-for-trust techniques.

1283 **A Primer on Hardware Security: Models, Methods, and Metrics**
By M. Rostami, F. Koushanfar, and R. Karri
|INVITED PAPER| The paper is a primer on hardware security threat models, metrics, and remedies.

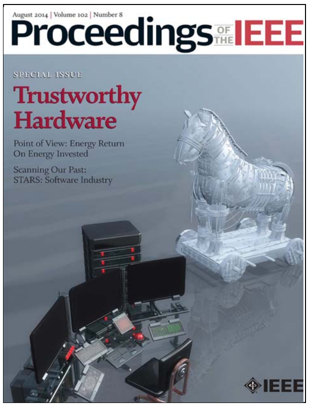
DEPARTMENTS

1118 POINT OF VIEW
Energy Return On Energy Invested (EROI): A Quintessential but Possibly Inadequate Metric for Sustainability in a Solar-Powered World?
By W. F. Pickard

1123 SCANNING THE ISSUE
Trustworthy Hardware
By R. Karri and F. Koushanfar

1296 SCANNING OUR PAST
STARS: Software Industry
By B. Grad

1304 FUTURE SPECIAL ISSUES/SPECIAL SECTIONS


August 2014 | Volume 102 | Number 8
Proceedings of the IEEE
SPECIAL ISSUE
Trustworthy Hardware
Point of View: Energy Return On Energy Invested
Scanning Our Past: STARS: Software Industry
IEEE

On the Cover: On this month's cover, security issues are highlighted in general by the illustration of the Trojan horse which the Greeks used successfully to breach the city of Troy.