

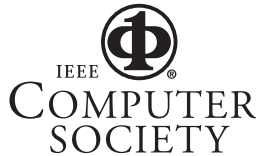
KHARKOV NATIONAL UNIVERSITY OF RADIOELECTRONICS

Proceedings of IEEE East-West Design & Test Symposium (EWDTS'09)

Copyright © 2009 by The Institute of Electrical and Electronics Engineers, Inc.

SPONSORED BY

IEEE Computer Society Test Technology Technical Council



Moscow, Russia, September 18 – 21, 2009

IEEE EAST-WEST DESIGN AND TEST SYMPOSIUM 2009 ORGANISING COMMITTEE

General Chairs

V. Hahanov – Ukraine
Y. Zorian – USA

General Vice-Chairs

D. Bikov - Russia
R. Ubar – Estonia

Program Chairs

S. Shoukourian – Armenia
D. Speranskiy – Russia

Program Vice-Chairs

M. Renovell – France
Z. Navabi – Iran

Steering Committee

M. Bondarenko – Ukraine
V. Hahanov – Ukraine
R. Ubar – Estonia
Y. Zorian – USA

Publicity Chairs

R. Ubar - Estonia
S. Mosin – Russia

Program Committee

E. Evdokimov – Ukraine
A. Chaterjee – USA
E. Gramatova – Slovakia
S. Hellebrand – Germany
A. Ivanov – Canada
M. Karavay – Russia
V. Kharchenko – Ukraine
K. Kuchukjan – Armenia
A. Matrosova – Russia
V. Melikyan - Armenia

O. Novak – Czech Republic

A. Orailoglu – USA
Z. Peng – Sweden
A. Petrenko – Ukraine
P. Prinetto – Italy
J. Raik – Estonia
A. Romankevich – Ukraine
A. Ryjov – Russia
R. Seinauskas – Lithuania
S. Sharshunov – Russia
A. Singh – USA
J. Skobtsov – Ukraine
A. Stempkovsky – Russia
V. Tverdokhlebov – Russia
V. Vardanian – Armenia
V. Yarmolik – Byelorussia
E. J. Aas – Norway
J. Abraham – USA
M. Adamski – Poland
A. Barkalov – Poland
R. Bazylevych – Ukraine
V. Djigan – Russia
A. Drozd – Ukraine
W. Kuzmicz – Poland

Organizing Committee

S. Chumachenko – Ukraine
N. Kulbakova – Ukraine
V. Obrizan – Ukraine
A. Kamkin – Russia
K. Petrosyanz – Russia
A. Sokolov – Russia
Y. Gubenko – Russia
M. Chupilko – Russia
E. Litvinova – Ukraine
O. Guz – Ukraine
G. Markosyan – Armenia

EWDTS CONTACT INFORMATION

Prof. Vladimir Hahanov
Design Automation Department
Kharkov National University of Radio Electronics,
14 Lenin ave,
Kharkov, 61166, Ukraine.

Tel.: +380 (57)-702-13-26
E-mail: hahanov@kture.kharkov.ua
Web: www.ewdtest.com/conf/

7th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS 2009)
 Moscow, Russia, September 18-21, 2009

The main target of the **IEEE East-West Design & Test Symposium** (EWDTS) is to exchange experiences between scientists and technologies of Eastern and Western Europe, as well as North America and other parts of the world, in the field of design, design automation and test of electronic circuits and systems. The symposium is typically held in countries around the Black Sea, the Baltic Sea and Central Asia region. We cordially invite you to participate and submit your contribution(s) to EWDTS'09 which covers (but is not limited to) the following topics:

- Analog, Mixed-Signal and RF Test
- Analysis and Optimization
- ATPG and High-Level Test
- Built-In Self Test
- Debug and Diagnosis
- Defect/Fault Tolerance and Reliability
- Design for Testability
- Design Verification and Validation
- EDA Tools for Design and Test
- Embedded Software Performance
- Failure Analysis, Defect and Fault
- FPGA Test
- HDL in test and test languages
- High-level Synthesis
- High-Performance Networks and Systems on a Chip
- Low-power Design
- Memory and Processor Test
- Modeling & Fault Simulation
- Network-on-Chip Design & Test
- Modeling and Synthesis of Embedded Systems
- Object-Oriented System Specification and Design
- On-Line Testing
- Power Issues in Design & Test
- Real Time Embedded Systems
- Reliability of Digital Systems
- Scan-Based Techniques
- Self-Repair and Reconfigurable Architectures
- System Level Modeling, Simulation & Test Generation
- System-in-Package and 3D Design & Test
- Using UML for Embedded System Specification
- CAD and EDA Tools, Methods and Algorithms
- Design and Process Engineering
- Logic, Schematic and System Synthesis
- Place and Route
- Thermal, Timing and Electrostatic Analysis of SoCs and Systems on Board
- Wireless and RFID Systems Synthesis
- Digital Satellite Television
- Signal and Information Processing in RF and Communication

The symposium is organized by Kharkov National University of Radio Electronics, in cooperation with Tallinn University of Technology, Institute for System Programming of RAS, and Moscow Institute of Electronics and Mathematics. It is sponsored by the IEEE Computer Society Test Technology Technical Council (TTTC) and financially supported by Cadence, JTAG Technologies, Kaspersky Lab, Synopsys, Mentor Graphics, Tallinn Technical University, Donetsk Institute of Road Transport, Moscow Institute of Electronics and Mathematics, Virage Logic, Echostar, Aldec, Teprocomp, DataArt Lab.



CONTENTS

Simulation-based Verification with APRICOT Framework using High-Level Decision Diagrams Maksim Jenihhin, Jaan Raik, Anton Chepurov, Raimund Ubar	13
Fault-Detection Capability Analysis of a Hardware-Scheduler IP-Core in Electromagnetic Interference Environment J. Tarrillo, L. Bolzani, F. Vargas, E. Gatti, F. Hernandez, L. Fraigi	17
Hardware Reduction in FPGA-Based Compositional Microprogram Control Units Barkalov A.A., Titarenko L.A., Miroshkin A.N.	21
Optimization of Control Units with Code Sharing Alexander A. Barkalov, Larisa A. Titarenko, Alexander S. Lavrik	27
SAT-Based Group Method for Verification of Logical Descriptions with Functional Indeterminacy Liudmila Cheremisinova, Dmitry Novikov	31
MicroTESK: Automation of Test Program Generation for Microprocessors Alexander Kamkin	35
Verification Methodology Based on Algorithmic State Machines and Cycle-Accurate Contract Specifications Sergey Frenkel and Alexander Kamkin	39
Coverage Method for FPGA Fault Logic Blocks by Spares Vladimir Hahanov, Eugenia Litvinova, Wajeb Gharibi, Olesya Guz	43
Testing and Verification of HDL-models for SoC components Vladimir Hahanov, Irina Hahanova, Ngene Christopher Umerah, Tiecoura Yves	48
The Model of Selecting Optimal Test Strategy and Conditions of ICs Testing During Manufacturing Sergey G. Mosin	54
A Technique to Accelerate the Vector Fitting Algorithm for Interconnect Simulation Gourary M.M., Rusakov S.G., Ulyanov S.L., Zharov M.M.	59
Frequency Domain Techniques for Simulation of Oscillators Gourary M.M., Rusakov S.G., Stempkovsky A.L., Ulyanov S.L., Zharov M.M.	63
Distributed RLC Interconnect: Estimation of Cross-coupling Effects H.J. Kadim, L.M. Coulibaly	67
Constrained-Random Verification for Synthesis: Tools and Results D. Bodean, G. Bodean, O. Ghincul	71
Discussion on Supervisory Control by Solving Automata Equation Victor Bushkov, Nina Yevtushenko, Tiziano Villa	77
Generalized Faulty Block Model for Automatic Test Pattern Generation F. Podyablonsky, N. Kascheev	80
Self Calibration Technique of Capacitor's Mismatching For 1.5 Bit Stage Pipeline ADC Vazgen Melikyan, Harutyun Stepanyan	84
Applied Library of Adaptive Lattice Filters for Nonstationary Signal Processing Victor I. Djigan	87
On-chip Measurements of Standard-Cell Propagation Delay S.O. Churayev, B.T. Matkarimov, T.T. Paltashev	93
FPGA FFT Implementation S.O. Churayev, B.T. Matkarimov	96

Reconfiguration and Hardware Agents in Testing and Repair of Distributed Systems G. Moiş, I.Ştefan, Sz. Enyedi, L. Miclea	99
Symmetrization in Digital Circuit Optimization Natalia Eliseeva, Jie-Hong R. Jiang, Natalia Kushik, Nina Yevtushenko	103
Embedded Processor Power Reduction via Power aware Custom Instruction Selection Hoda Ahmadinejad, Saeed Safari, and Hamid Noori	107
Level Quantization Effects in Digital Signal Processing by Discrete Fourier Transform Method Gamlet S. Khanyan	111
A New Paradigm in Design of IIR Digital Filters Vladislav A. Lesnikov, Alexander V. Chastikov, Tatiana V. Naumovich, Sergey V. Armishev	115
Evolutionary Approach to Test Generation of Sequential Digital Circuits with Multiple Observation Time Strategy Yu. A. Skobtsov, V. Yu. Skobtsov	119
SMT-based Test Program Generation for Cache-memory Testing Evgeni Kornikhin	124
Critical Path Test Generation in Asynchronous QDI Circuits Fahime Khoramnejad, Hossein Pedram	128
Model-driven & Component-based Development Method of Multi-core Parallel Simulation Models Nianle Su, Wenguang Yu, Hongtao Hou, Qun Li and Weiping Wang	135
Minimizing of Number of Discrete Device's Controllable Points Dmitriy Speranskiy, Ekaterina Ukolova	142
VHPI-compatible Simulation and Test Generation System Dmitriy Speranskiy, Ivan Ukolov	147
Fault Tolerant HASH function with Single Element Correction and Minimum Delay Overhead Costas A. Argyrides, Carlos A. Lisboa, Dhiraj K. Pradhan, Luigi Carro	151
Analysis of the Control Vector Optimal Structure for a Minimal-Time Circuit Optimization Process A.M. Zemliak, M.A. Torres, T.M. Markina	156
Parallel Simulation of Boolean Functions by Means of GPU Włodzimierz Bielecki, Alexander Chemeris, Svetlana Reznikova	162
Two-Criterial DSSS Synchronization Method Efficiency Research Kharchenko H.V., Tklich I.O., Vdovychenko Y.I.	165
An Efficient March Test for Detection of All Two-Operation Dynamic Faults from Subclass S_{av} Gurgen Harutyunyan, Hamazasp Avetisyan, Valery Vardanian, Y. Zorian	175
Large and Very Large-scale Placement Bazylevych R.P., Bazylevych L.V., Shcherb'yuk I.F.	179
An Educative Brain-Computer Interface Kirill Sorudeykin	183
Time-Hardware Resource: A Criterion of Efficiency of Digital Signal Search and Detection Devices Alexander Fridman	187
A New Principle of Dynamic Range Expansion by Analog-to-Digital Converting Elina A. Biberdorf, Stanislav S. Gritsutenko, Konstantin A. Firsanov	193
FREP: A Soft Error Resilient Pipelined RISC Architecture Viney Kumar, Rahul Raj Choudhary, Virendra Singh	196

System Remote Control of the Robotized Complex - Pegas Dmitry Bagayev, Evsyakov Artem	200
Use of Predicate Categories for Modelling of Operation of the Semantic Analyzer of the Linguistic Processor Nina Khairova, Natalia Sharonova	204
Methodological Aspects of Mathematical Modelling of Processes in a Corporate Ecological System Kozulia T.V., Sharonova N.V.	208
Getting Optimal Load Distribution Using Transport-Problem-Based Algorithm Yuri Ladyzhensky, Viatcheslav Kourkchi	212
Dialogue-based Optimizing Parallelizing Tool and C2HDL Converter Steinberg B., Abramov A., Alymova E., Baglij A., Guda S., Demin S., Dubrov D., Ivchenko A., Kravchenko E., Makoshenko D., Molotnikov Z., Morilev R., Nis Z., Petrenko V., Povazhniy A., Poluyan S., Skiba I., Suhoverkhov S., Shapovalov V., Steinberg O., Steinberg R.	216
The System for Automated Program Testing Steinberg B., Alimova E., Baglij A., Morilev R., Nis Z., Petrenko V., Steinberg R.	218
Development of the University Computing Network for Integrated Circuit Design Atkin E., Volkov Yu., Garmash A., Klyuev A., Semenov D., Shumikhin V.	221
Increase in Reliability of On-Line Testing Methods Using Natural Time Redundancy Drozd A., Antoshchuk S., Martinuk A., Drozd J.	223
An Algorithm of Carrier Recovery for Modem with M-ary Alphabets APK-Signals without PLL Victor V. Panteleev	230
At Most Attainable of Lengths a Symmetrical Digital Subscriber Line on xDSL-technologies: Engineering-Maintenance Methods of the Calculation Victor V. Panteleev, Nikolay I. Tarasov	234
New Approach to ADC Design Stanislav S. Gritsutenko	240
Simulation of Radiation Effects in SOI CMOS Circuits with BSIMSOI-RAD Macromodel K.O. Petrosjanc, I.A. Kharitonov, E.V. Orekhov, L.M. Sambursky, A.P. Yatmanov	243
Thermal Design System for Chip- and Board-level Electronic Components K.O. Petrosjanc, I.A. Kharitonov, N.I. Ryabov, P.A. Kozyanko	247
TCAD Modeling of Total Dose and Single Event Upsets in SOI CMOS MOSFETs K.O. Petrosjanc, I.A. Kharitonov, E.V. Orekhov, A.P. Yatmanov	251
Reduction in the number of PAL Macrocells for Moore FSM implemented with CPLD A. Barkalov, L. Titarenko, S. Chmielewski	255
Schematic Protection Method from Influence of Total Ionization Dose Effects on Threshold Voltage of MOS Transistors Vazgen Melikyan, Aristakes Hovsepyan, Tigran Harutyunyan	260
5V Tolerant Power clamps for Mixed-Voltage IC's in 65nm 2.5V Salicided CMOS Technology Vazgen Melikyan, Karen Sahakyan, Armen Nazaryan	263
Analysis and Optimization of Task Scheduling Algorithms for Computational Grids Morev N. V.	267
A Low Power and Cost Oriented Synthesis of the Common Model of Finite State Machine Adam Klimowicz, Tomasz Grzes, Valeri Soloviev	270

Comparison of Survivability & Fault Tolerance of Different MIP Standards Ayesha Zaman, M.L. Palash, Tanvir Atahary, Shahida Rafique	275
Hardware Description Language Based on Message Passing and Implicit Pipelining Dmitri Boulytchev, Oleg Medvedev	279
V-Transform: An Enhanced Polynomial Coefficient Based DC Test for Non-Linear Analog Circuits Suraj Sindia, Virendra Singh, Vishwani Agrawal	283
GA-Based Test Generation for Digitally-Assisted Adaptive Equalizers in High-Speed Serial Links Mohamed Abbas, Kwang-Ting (Tim) Cheng, Yasuo Furukawa, Satoshi Komatsu, Kunihiro Asada	287
Between Standard Cells and Transistors: Layout Templates for Regular Fabrics Mikhail Talalay, Konstantin Trushin, Oleg Venger	293
On-Chip Optical Interconnect: Analytical Modelling for Testing Interconnect Performance H J Kadim	300
The Problem of Trojan Inclusions in Software and Hardware Alexander Adamov, Alexander Saprykin	304
Design methods for modulo $2n+1$ multiply-add units C. Efstathiou, I. Voyiatzis, M. Prentakis	307
Geometrical Modeling and Discretization of Complex Solids on the Basis of R-functions Gomenyuk S.I., Choporov S.V., Lisnyak A.O.	313
Selective Hardening: an Enabler for Nanoelectronics Ilia Polian and John P. Hayes	316
Parameterized IP Infrastructures for Fault-Tolerant FPGA-Based Systems: Development, Assessment, Case-Study Kulanov Vitaliy, Kharchenko Vyacheslav, Perepelitsyn Artem	322
Generating Test Patterns for Sequential Circuits Using Random Patterns by PLI Functions M. H. Haghbayan, A. Yazdanpanah, S. Karamati, R. Saeedi, Z. Navabi	326
A New Online BIST Method for NoC Interconnects Elnaz Koopahi, Zainalabedin Navabi	332
Low Cost Error Tolerant Motion Estimation for H.264/AVC Standard M. H. Sargolzaie, M. Semsarzadeh, M. R. Hashemi, Z. Navabi	335
Method of Diagnosing FPGA with Use of Geometrical Images Epifanov A.S.	340
Performance Analysis of Asynchronous MIN with Variable Packets Length and Arbitrary Number of Hot-Spots Vyacheslav Evgrafov	344
System in Package. Diagnosis and Embedded Repair Vladimir Hahanov, Aleksey Sushanov, Yulia Stepanova, Alexander Gorobets	348
Technology for Faulty Blocks Coverage by Spares Hahanov Vladimir, Chumachenko Svetlana, Litvinova Eugenia, Zakharchenko Oleg, Kulbakova Natalka	353
The Unicast Feedback Models for Real-Time Control Protocol Babich A.V., Murad Ali Abbas	360
Algebra-Logical Repair Method for FPGA Logic Blocks Vladimir Hahanov, Sergey Galagan, Vitaliy Olchovoy, Aleksey Priymak	364

The Method of Fault Backtracing for HDL - Model Errors Searching Yevgeniya Syrevitch, Andrey Karasyov, Dariya Kucherenko	369
Handling Control Signals for the Scan Technology Olga Lukashenko, Dmitry Melnik, Vladimir Obrizan	373
Robust Audio Watermarking for Identification and Monitoring of Radiotelephone Transmissions in the Maritime Communication Vitaliy M. Koshevyy, Aleksandr V. Shishkin	377
An Interconnect BIST for Crosstalk Faults based on a Ring LFSR Tomasz Garbolino, Krzysztof Gucwa, Andrzej Hławiczka, Michał Kopeć	381
Generation of Minimal Leakage Input Vectors with Constrained NBTI Degradation Pramod Subramanyan, Ram Rakesh Jangir, Jaynarayan Tudu, Erik Larsson, Virendra Singh	385
Very Large-Scale Intractable Combinatorial Design Automation Problems – Clustering Approach for High Quality Solutions Roman Bazylevych and Lubov Bazylevych	389
Flexible and Topological Routing Roman Bazylevych and Lubov Bazylevych	390
An Algorithm for Testing Run-Length Constrained Channel Sequences Oleg Kurmaev	391
Constructing Test Sequences for Hardware Designs with Parallel Starting Operations Using Implicit FSM Models Mikhail Chupilko	393
Redundant Multi-Level One-Hot Residue Number System Based Error Correction Codes Somayyeh Jafarali Jassbi, Mehdi Hosseinzade, Keivan Navi	397
Parallel Fault Simulation Using Verilog PLI Mohammad Saeed Jahangiry, Sara Karamati, Zainalabedin Navabi	401
IEEE 1500 Compliant Test Wrapper Generation Tool for VHDL Models Sergey Mikhtonyuk, Maksim Davydov, Roman Hwang, Dmitry Shcherbin	406
Early Detection of Potentially Non-synchronized CDC Paths Using Structural Analysis Technique Dmitry Melnik, Olga Lukashenko, Sergey Zaychenko	411
An Editor for Assisted Translation of Italian Sign Language Nadereh Hatami, Paolo Prinetto, Gabriele Tiotto	415
Architecture Design and Technical Methodology for Bus Testing M.H. Haghbayan, Z. Navabi	419
Assertion Based Verification in TLM AmirAli Ghofrani, Fatemeh Javaheri, Zainalabedin Navabi	424
Flash-memories in Space Applications: Trends and Challenges Maurizio Caramia, Stefano Di Carlo, Michele Fabiano, Paolo Prinetto	429
Design Experience with TLM-2.0 Standard: A Case Study of the IP Lookup LC-trie Application of Network Processor Masoomeh Hashemi, Mahshid Sedghi, Morteza Analoui, Zainalabedin Navabi	433
Test Strategy in OSCI TLM-2.0 Mina Zolfy, Masoomeh Hashemi, Mahshid Sedghi, Zainalabedin Navabi and Ziaeddin Daeikozekanani	438
Synthesizing TLM-2.0 Communication Interfaces Nadereh Hatami, Paolo Prinetto	442

Advanced Topics of FSM Design Using FPGA Educational Boards and Web-Based Tools Alexander Sudnitson, Dmitri Mihhailov, and Margus Kruus	446
A Mixed HDL/PLI Test Package Nastaran Nemati, Majid Namaki-Shoushtari, Zainalabedin Navabi	450
Testing Methodologies on Communication Networks Nadereh Hatami, Paolo Prinetto, Gabriele Tiotto, Paola Elia	456
A Novel High Speed Residue to Binary Converter Design Based on the Three-Moduli Set $\{2n, 2n+1+1, 2n+1-1\}$ Muhammad Mehdi Lotfinejad, Mohammad Mosleh and Hamid Noori	460
Performance Evaluation of SAT-Based ATPG on Multi-Core Architectures Alejandro Czutro, Bernd Becker, Ilija Poljan	463
Intelligent Testbench Automation and Requirements Tracking Ivan Selivanov, Alexey Rabovoluk	471
Iterative Sectioning of High Dimensional Banded Matrices Dmytro Fedasyuk, Pavlo Serdyuk, Yuriy Semchyshyn	476
Estimating Time Characteristics of Parallel Applications in Technology of Orders Based Transparent Parallelizing Vitalij Pavlenko, Viktor Burdeinyi	480
Phase Pictures Properties of Technical Diagnostics Complex Objects Tverdokhlebov V.A.	483
Information Technology of Images Compression in Infocommunication Systems Alexander Yudin, Natalie Gulak, Natalie Korolyova	486
Technology of Cascade Structural Decoding Leonid Soroka, Vladimir Barannik, Anna Hahanova	490
Technology of the Data Processing on the Basis of Adaptive Spectral- Frequency Transformation of Multiadical Presentation of Images Vladimir Barannik, Sergey Sidchenko, Dmitriy Vasiliev	495
Compression Apertures Method - Color Different Images Konstantin Vasyuta, Dmitry Kalashnik, Stanislav Nikitchenko	499
Isotopic Levels Architectural Presentation of Images Relief Vladimir Barannik, Alexander Slobodyanyuk	502
Method and Mean of Computer's Memory Reliable Work Monitoring Utkina T.Yu., Ryabtsev V.G.	505
Extended Complete Switch as Ideal System Network Mikhail F. Karavay and Victor S. Podlazov	513
Image Compression: Comparative Analysis of Basic Algorithms Yevgeniya Sulema, Samira Ebrahimi Kahou	517
Networked VLSI and MEMS Designer for GRID Petrenko A.I.	521
Path Delay Fault Classification Based on ENF Analysis Matrosova A., Nikolaeva E.	526
COMPAS – Advanced Test Compressor Jiří Jeníček, Ondřej Novák	532
INVITED TALKS	538
AUTHORS INDEX	545

The Problem of Trojan Inclusions in Software and Hardware

Alexander Adamov, Alexander Saprykin
Kharkov National University of Radio Electronics,
Lenin ave, 14, Kharkov, 61166 Ukraine,
E-mail: Alexander.Adamov@dnt-lab.com

Abstract

This paper describes an information security threat implemented in software and hardware by means of malicious inclusions called Trojans. Creation of Trojans is mostly driven by criminal with the purpose of financial profit and sabotage.

The Trojans programs can steal money from your bank account, payment system, credit card numbers, and other personal information; use your computer as a part of “zombie” network to perform fraudulent actions of hacker.

The hardware Trojans can be embedded in safety critical, security and military systems, such as weapon control systems, battlefield communication systems, information collection and decision making systems, satellite electronics, banking systems, cryptosystems, etc.

The goal of the paper is to compare the security problem of high level computer systems with the same problem in hardware systems, such as System-on-Chip. Therefore, the class of Trojan malicious programs is considered in both environments: software and hardware.

1. Introduction

Nowadays e-crime and e-terrorism are the hottest topic in information security. Digital systems are everywhere in our life. And millions of computers are infected by malicious programs - malware, part of them are enslaved within botnets, launching distributed DoS attacks, working as anonymizers and spam senders.

Currently, every two seconds new malicious program appears according to Kaspersky Lab statistics [1]. All these samples are high level software for particular OS. Also many anti-virus solutions are available on the market to protect the users from security threats, such as malware, hacker attacks, spam.

The worse thing about malicious inclusions is that they can be found at hardware level as well. Such alterations can compromise the system by modifying its functionality, intercepting the data or blocking the work of the whole system. Fortunately, they are limited in proliferation and cannot infect other devices. In contrast to malicious programs, hardware malicious circuits are hardly-detectable. There is no unified protection solution, like Antivirus.

There are three main categories of malicious programs[2]:

- *Viruses* - program code that replicates on host system.
- *Worms (network worms)* – type of malicious programs, that spread by network channels, capable of overcoming the protection of computer systems and computer networks, as well as the creation and further copies proliferation, that are not always the same as the original ones, and implementation of other harmful effects.
- *Trojans* – programs that damage victim machines or threaten data integrity, or impair the functioning of the victim machine.

1. Hacker utilities and other malware.

Unlike, the world of hardware devices has only the one class of malware – Hardware Trojan (HT). Because, the chip’s IP cores cannot be modified by viruses when it is already synthesized into a die. And also there is no required communication channel for worm proliferation. Both those classes need the unified environment for reproduction and spreading. So the most popular threat implemented in hardware is Trojan circuit. The main purpose of HT is to steal confidential information, modify the functionality and transmitting data or block/destroy device.

HT can be implemented as hardware inclusions to application specific ICs (ASICs), microprocessors, digital signal processors (DSPs), or as IP core modifications for field programmable gate arrays (FPGA) [3].

2. Software Trojan Classification

Trojans can be classified mostly according to the actions that they carry out on victim machines. However they also can be divided by type of OS (Win32/64, Unix, MacOS, SymbOS, Windows Mobile) and programming language for cross-platform scripts (HTML, JavaScripts, Perl, PHP, etc.) [2].

Let us consider the Software Trojan (ST) classification by Kaspersky Lab grouped according to three IS threat types that ST may violate:

1. Confidentiality

- *Backdoor* - remote administration utilities that open infected machines to external control via a LAN or the Internet.
- *PSW Trojan* - steals passwords from the system.
- *Trojan-Spy* - includes a variety of spy programs and key loggers, all of which track and save user activity on the victim machine and then forward this information to the master.
- *Trojan-GameThief* - steals the user information pertaining to online games.
- *Trojan-Banker* - steals the user information pertaining to the banking system, the electronic money and plastic cards.
- *Trojan-Mailfinder* - provides unauthorized collection of user email addresses with the subsequent transfer to the attacker.

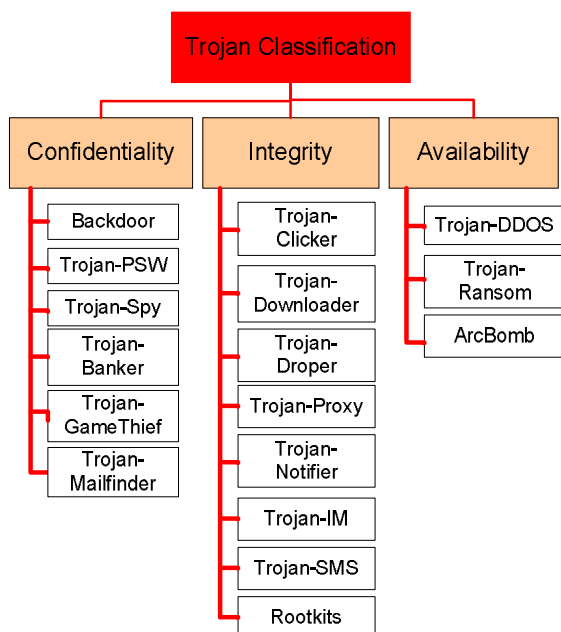


Figure 1. Software Trojan classification

2. Integrity

- *Trojan Clicker* - redirects victim machines to specified websites or other Internet resources.
- *Trojan Downloader* - downloads and installs new malware or adware on the victim machine.
- *Trojan Dropper* - used to install other malware on victim machines without the knowledge of the user.
- *Trojan Proxy* - function as a proxy server and provide anonymous access to the Internet from victim machines.
- *Trojan-Notifier* - inform the 'master' about an infected machine.
- *Trojan-IM* - steals user's account (login and password) from the Internet-pager (e.g., ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype, etc.)
- *Trojan-SMS* - used for unauthorized sending SMS-messages from the compromised mobile devices to expensive paid numbers that are stored in the malware body.
- *Rootkits* - a collection of programs used by a hacker to evade detection while trying to gain unauthorized access to a computer.

3. Availability

- *Trojan-DDoS* - performs an unauthorized DoS (Denial of Service) attack from infected computers to a computer-sacrifice with the specified address.
- *Trojan-Ransom* - used for unauthorized data modification on victim's computer to make it impossible to work with it or block the normal functioning of the computer.
- *ArcBomb* - archived files coded to sabotage the de-compressor when it attempts to open the infected archived file.

3. Hardware Trojan Classification

Hardware Trojans can be generally divided by three major criteria (Figure 2): physical characteristics, activation and threat type [4].

Physical characteristics are the following:

- size - large (macro) or small (transistor/wire);
- type - functional (changes original structure of design) or parametric (modifies existing logic);
- distribution - tight (localized in a small area) or loose (distributed all over circuit);

- structure – modify layout or no-change (affects Trojan physical footprint).

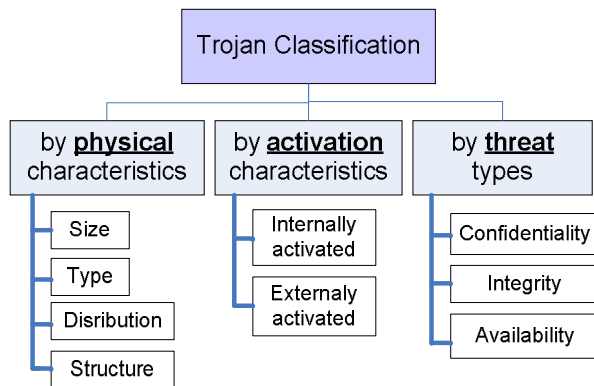


Figure 2. Hardware Trojan classification

HT has the following activation types:

- externally activated Trojans are triggered by signals from input pins.
- internally activated Trojans can be activated by internal logic (internal state, instruction, data, interrupt, clock) or can work all the time.

According to IS threat type that HT may violate:

- confidentiality threat,
- integrity threat,
- availability threat.

Hardware Trojans has the following set of characteristics:

- *Relatively small size compared to total chip area.* Trojans inclusions are small enough to be implanted without changing the chip dimensions and its pin count.
- *Invisibility and stealthy activation.* Being deeply embedded into the circuit Trojans are hardly observable. Moreover, theirs components can

be distributed all over the chip to make its detection less probable. Also Trojans may stay inactive during the whole working cycle until they are triggered by special condition.

- *Malicious activity.* Trojans have malicious intentions to steal confidential data or disrupt chip functionality.

4. Conclusion

From the both classifications given above it is obvious that for HT more attention was paid to implementation criteria, not to the functional features as it is done in software Trojan classification.

Software Trojans have the similar architecture and common execution environment. The functionality is the main difference of Trojan families.

Universal solution against HT, similar to software anti-viruses, does not exist. It makes the HT detection challenge very complicated and provides huge area for research.

5. References

- [1] E. Kaspesky, "Evolution of Malware and A-Malware. The Kaspersky Vision", Kaspersky Lab, 2008 www.kaspersky.com.
- [2] "Malware Classification", Kaspersky Lab, 2009 www.securelist.com
- [3] D. Colins, "Trust in Integrated Circuits (TIC)", DARPA Solicitation BAA07-24, 2007 (www.darpa.mil/mto/solicitations/baa07-24/index.html).
- [4] X. Wang, M. Tehranipoor and J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions", International Workshop on Hardware Oriented Security and Trust, 2008, pp. 15-22.

Camera-ready was prepared in Kharkov National University of Radio Electronics
by Dr. Svetlana Chumachenko
Lenin ave, 14, KNURE, Kharkov, 61166, Ukraine

Approved for publication: 31.08.2009. Format 60×84¹/₈.
Relative printer's sheets: . Circulation: 150 copies.
Published by SPD FL Stepanov V.V.
Ukraine, 61168, Kharkov, Ak. Pavlova st., 311

Матеріали симпозиуму «Схід-Захід Проектування та Діагностування – 2009»
Макет підготовлено у Харківському національному університеті радіоелектроніки
Редактори: Володимир Хаханов, Світлана Чумаченко
Пр. Леніна, 14, ХНУРЕ, Харків, 61166, Україна

Підписано до публікації: 31.08.2009. Формат 60×84¹/₈.
Умов. друк. арк. . Тираж: 150 прим.
Видано: СПД ФЛ Степанов В.В.
Вул. Ак. Павлова, 311, Харків, 61168, Україна