KHARKOV NATIONAL UNIVERSITY OF RADIOELECTRONICS

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

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

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.

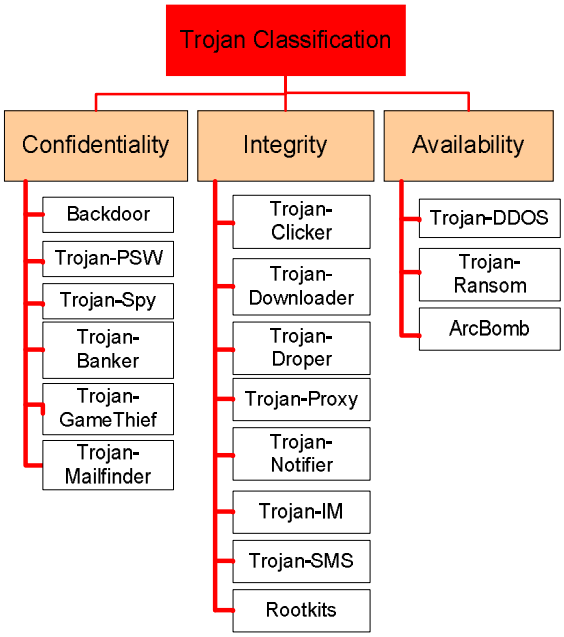

Figure 1. Software Trojan classification

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).

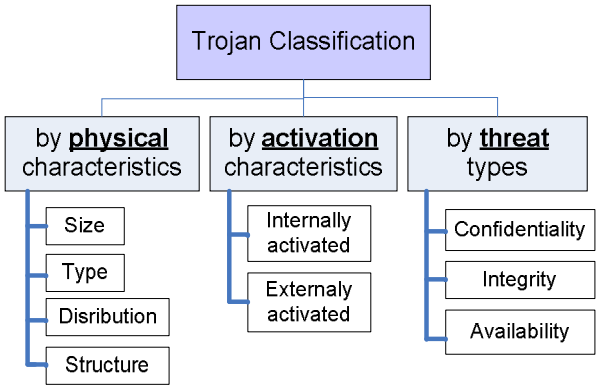

Figure 2. Hardware Trojan classification

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 симпозіуму «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 60×84$^{1}/_{8}$.
Умов. друк. арк. . Тираж: 150 прим.
Видано: СПД ФЛ Степанов В.В.
Вул. Ак. Павлова, 311, Харків, 61168, Україна