FOREWORD

We warmly welcome you to SECRYPT 2009 - the International Conference on Security and Cryptography, which is held, this year, in Milan, Italy. This conference reflects a continuing effort to increase the dissemination of recent research among professionals who work on the fields of security and cryptography, especially for the five scientific areas included in the conference. SECRYPT is integrated as one of the modules of the ICETE joint conference.

The major goal of ICETE is to bring together researchers, engineers and practitioners interested in information and communication technologies, including e-business, wireless networks and information systems, security and cryptography, signal processing and multimedia applications. These are the main knowledge areas that define the four component conferences, namely: ICE-B, WINSYS, SECRYPT and SIGMAP, which together form the ICETE joint conference.

In the program for this joint conference, we have included keynote lectures, papers, and posters to present the widest possible view on these technical areas. With these tracks, we expect to appeal to a global audience of the engineers, scientists, business practitioners and policy experts, interested in the research topics of ICETE. All tracks focus on research related to real world applications and rely on contributions not only from the Academia but also from the industry, with different solutions for end-user applications and enabling technologies, in a diversity of communication environments. The proceedings demonstrate a number of new and innovative solutions for e-business and telecommunication, and demonstrate the vitality of these research areas.

ICETE has received 300 papers in total, with contributions from more than 50 different countries, from all continents, which demonstrates the success and global dimension of ICETE 2009. To evaluate each submission, a double blind paper evaluation method was used: each paper was reviewed by at least two experts from the International Program Committee, in a double-blind review process, and most papers had 3 reviews or more. In the end, 114 papers were selected for oral presentation and publication, corresponding to a 38% acceptance ratio. Of these only 34 were accepted as full papers (11% of submissions) and 80 as short papers. Additionally, 51 papers were accepted for poster presentation. These acceptance ratios demonstrate that ICETE 2009 strives to achieve a high quality standard which we will keep and enhance in order to ensure the success of next year conference, to be held in Milan/Italy. Furthermore, a short list of about 30 papers will be selected to appear in a book that will be published by Springer.

We would like to emphasize that SECRYPT 2009 includes outstanding keynote lectures in areas which are very relevant, nowadays. These talks are presented by distinguished researchers who are internationally renowned experts, and contribute to heighten the overall quality of the Conference.

A successful conference involves more than paper presentations; it is also a meeting place,
where ideas about new research projects and other ventures are discussed and debated. Therefore, a social event including a conference diner was organized for the evening of July 9 in order to promote this kind of social networking.

We would like to express our thanks, first of all, to the authors of the technical papers presented at the conference, whose work made possible to put together a high quality program. Next, we would like to thank all the members of the program committee and reviewers, who helped us with their expertise, dedication and time. We would also like to thank the invited speakers for their invaluable contribution, sharing their vision and knowledge. Naturally, a word of appreciation for the work of the secretariat and all other members of the organization, whose diligence in dealing with all organizational issues were essential and required a collaborative effort of a dedicated and highly capable team.

We hope that you will find these proceedings interesting and a helpful reference in the future for all those who need to address the areas of e-business and telecommunications.

Manu Malek  
Stevens Institute of Technology, U.S.A.

Eduardo Fernández-medina  
University of Castilla-La Mancha, Spain

Javier Hernando  
Technical University of Catalonia, Spain
## CONTENTS

### INVITED SPEAKERS

**Keynote Speakers**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Speaker</th>
<th>IS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Antennas in Wireless Communication Networks</td>
<td>Blagovest Shishkov</td>
<td>5</td>
</tr>
<tr>
<td>Protecting Information Privacy in the Electronic Society</td>
<td>Pierangela Samarati</td>
<td>19</td>
</tr>
<tr>
<td>E-Business Design - A Shift to Adaptability</td>
<td>David Marca</td>
<td>21</td>
</tr>
<tr>
<td>Cloud Computing - Fundamental Architecture &amp; Future Applications</td>
<td>Frank Leymann</td>
<td>31</td>
</tr>
<tr>
<td>Web 2.0: A Buzzword, a Serious Development, Just Fun, or What?</td>
<td>Gottfried Vossen</td>
<td>33</td>
</tr>
</tbody>
</table>

### ACCESS CONTROL AND INTRUSION DETECTION

**Full Papers**

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-Touch Financial Transaction Authentication</td>
<td>Daniel V. Bailey, John Brainard, Sebastian Rohde and Christof Paar</td>
<td>5</td>
</tr>
<tr>
<td>Service and Timeframe Dependent Unlinkable One-Time Pseudonyms</td>
<td>Kristof Verslype and Bart De Decker</td>
<td>13</td>
</tr>
</tbody>
</table>

**Short Papers**

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Anomaly-Based Web Application Firewall</td>
<td>Alejandro Perez-Villegas and Gonzalo Alvarez</td>
<td>23</td>
</tr>
<tr>
<td>Visual Programming Language for Security Requirements in Business Processes as Model-Driven Software Development</td>
<td>Mirad Zadic and Andrea Nowak</td>
<td>29</td>
</tr>
<tr>
<td>Finger Vein Verification Technology for Mobile Apparatus</td>
<td>Hideo Sato</td>
<td>37</td>
</tr>
<tr>
<td>Efficient Algorithms and Abstract Data Types for Local Inconsistency Isolation in Firewall ACLS</td>
<td>S. Pozo, A. J. Varela-Vaca, R. M. Gasca and R. Ceballos</td>
<td>42</td>
</tr>
</tbody>
</table>

### Posters

<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Authentication Framework - Requirements and Phase Design</td>
<td>Tomas Pelka, Jan Hajny and Petra Lambertova</td>
<td>57</td>
</tr>
<tr>
<td>Adding Expert Knowledge to Tan-Based Intrusion Detection Systems</td>
<td>S. Benferhat, A. Boudjelida and H. Drias</td>
<td>61</td>
</tr>
</tbody>
</table>
NETWORK SECURITY AND PROTOCOLS

FULL PAPERS

PREVENTING WORMHOLE ATTACK IN WIRELESS AD HOC NETWORKS USING COST-BASED SCHEMES
Marianne Amir Azer, Sherif Mohammed El-Kassas and Mady Saiid El-Soudani 69

AN OFFLINE PEER-TO-PEER BROADCASTING SCHEME WITH ANONYMITY
Shinsaku Kiyomoto, Kazuhide Fukushima and Keith M. Martin 75

NETWORK STACK OPTIMIZATION FOR IMPROVED IPSEC PERFORMANCE ON LINUX
Michael G. Iatrou, Artemios G. Voyiatzis and Dimitrios N. Serpanos 83

ATTACK GRAPH GENERATION WITH INFUSED FUZZY CLUSTERING
Sudip Misra, Mohammad S. Obaidat, Atig Bagchi, Ravindara Bhatt and Soumyala Ghosh 92

SHORT PAPERS

RFID AUTHENTICATION PROTOCOLS BASED ON ELLIPTIC CURVES - A Top-Down Evaluation Survey
Michael Hutter 101

FAST RE-ESTABLISHMENT OF IKEV2 SECURITY ASSOCIATIONS FOR RECOVERY OF IPSEC GATEWAYS IN MOBILE NETWORK
Peng Yang, Yuanchen Ma and Satoshi Yoshizawa 111

MONITORING NODE SELECTION ALGORITHM FOR INTRUSION DETECTION IN CONGESTED SENSOR NETWORK
Jaeun Choi, Myungjiong Lee, Gisung Kim and Sehun Kim 117

THROTTLING DDoS ATTACKS
Saraiah Gujjunoori, Taji Ali Syed, Madhu Babu J., Avinash D., Radhesh Mohandas and Alwyn R. Pais 121

ASSESSMENT OF MOBILE SECURITY PLATFORMS
Germán Retamosa and Jorge E. López de Vergara 127

POSTERS

SIMULATION OF AN IDENTITY-BASED CRYPTOGRAPHY SCHEME FOR AD HOC NETWORKS
Pura Mihai-Lică, Patriciu Victor Valeriu and Bica Ion 135

BEHAVIOR-BASED CLUSTERING FOR DISCRIMINATION BETWEEN FLASH CROWDS AND DDoS ATTACKS
Young Jun Heo, Jintae Oh and Jongsoo Jang 140

EVALUATION OF QUALITY AND SECURITY OF A VOIP NETWORK BASED ON ASTERISK AND OpenVPN
Rodrigo S. Miani, Dherik Barison and Leonardo de Souza Mendes 144

A TRAFFIC COHERENCE ANALYSIS MODEL FOR DDOS ATTACK DETECTION
Hamza Rahmani, Nabil Sahli and Farouk Kamoun 148
CRYPTOGRAPHIC TECHNIQUES AND KEY MANAGEMENT

FULL PAPERS

IMPLEMENTING TRUE RANDOM NUMBER GENERATORS IN FPGAS BY CHIP FILLING
Octavian Cret, Radu Tudoran, Alin Suciu and Tamas Györfi 167

QUANTUM SECURE DIRECT COMMUNICATION USING ENTANGLEMENT AND SUPER DENSE CODING
Ola M. Hegazy, Ayman M. Bahaa Eldin and Yasser H. Dakrouy 175

AN EFFICIENT GROUP KEY AGREEMENT PROTOCOL FOR HETEROGENEOUS ENVIRONMENT
Mounita Saha and Dipanwita Roy Chowdhury 182

CERTIFIED PSEUDONYMS COLLIGATED WITH MASTER SECRET KEY
Vijayakrishnan Pasupathinathan, Josef Pieprzyk and Huaxiong Wang 190

THE CHAMELEON CIPHER-192 (CC-192) - A Polymorphic Cipher
Magdy Saeb 198

SHORT PAPERS

A NEW ANALYSIS OF RC4 - A Data Mining Approach (J48)
Ali Movaghar and Mohsen HajSalehi Sichani 213

ON THE SECURITY OF TWO RING SIGNCRYPTION SCHEMES
S. Sree Vivek, S. Sharmila Deva Selvi and C. Pandu Rangan 219

PRACTICAL TRACEABLE ANONYMOUS IDENTIFICATION
Daniel Slamanig, Christian Stingl and Peter Schartner 225

INFORMATION-THEORETICALLY SECURE STRONG VERIFIABLE SECRET SHARING
Changlu Lin, Lein Harn and Dingfeng Ye 233

SAFE REVERSE AUCTIONS PROTOCOL - Adding Treatment Against Collusive Shill Bidding and Sniping Attacks
Guerra Ruy and Ribeiro Leonardo 239

A SECOND PREIMAGE ATTACK ON THE MERKLE-DAMGARD SCHEME WITH A PERMUTATION FOR HASH FUNCTIONS
Shiwei Chen and Chenhui Jin 245

ON THE SECURITY OF ADDING CONFIRMERS INTO DESIGNATED CONFIRMER SIGNATURES
Watari Senga and Hiroshi Doi 249
A CHAOS BASED ENCRYPTION METHOD USING DYNAMICAL SYSTEMS WITH STRANGE ATTRACTORS
Arash Sheikholeslam

INTERACTIVE SECRET SHARE MANAGEMENT
Constantin Catalin Dragan

EFFICIENT TRAITOR TRACING FOR CONTENT PROTECTION
Hongxia Jin

AD-HOC ON DEMAND AUTHENTICATION CHAIN PROTOCOL - An Authentication Protocol for Ad-hoc Networks
A. M. Hamad and W. I. Khedr

NMIX: AN IDEAL CANDIDATE FOR KEY MIXING
Dipanwita Roy Chowdhury and Jaydeb Bhauik

A NEW IMAGE ENCRYPTION ALGORITHM USING CELLULAR AUTOMATA
D. Roy Chowdhury and Mayank Varshney

TOOL SUPPORT FOR ACHIEVING QUALITATIVE SECURITY ASSESSMENTS OF CRITICAL INFRASTRUCTURES - The ESSAF Framework for Structured Qualitative Analysis
Nguyen Hanh Quyen, Köster Friedrich, Klaas Michael, Brenner Walter, Obermeier Sebastian and Brändle Markus

COLLABORATIVE SECURITY ASSESSMENTS IN EMBEDDED SYSTEMS DEVELOPMENT - The ESSAF Framework for Structured Qualitative Analysis
Friedrich Köster, Michael Klaas, Hanh Quyen Nguyen, Walter Brenner, Markus Braendle and Sebastian Obermeier

AN APPROACH FOR DESIGNING OF ENTERPRISE IT LANDSCAPES TO PERFORM QUANTITATIVE INFORMATION SECURITY RISK ASSESSMENT
Anton Romanov and Eiji Okamoto

IDENTIFYING SECURITY ELEMENTS FOR COOPERATIVE INFORMATION SYSTEMS
Nathalie Dagorn

MULTIPARTY COMPARISON - An Improved Multiparty Protocol for Comparison of Secret-shared Values
Tord Ingolf Reistad

THE DARK SIDE OF SECURITY BY OBSCURITY - and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime
Nicolas T. Courtois

FREE SECURITY SUITE 2 - Easy, Intuitive and Complete Free Security Suite with Web Browser Integration
Javier Corral-García, Carlos-Jorge del Arco González, José Luis González-Sánchez and José Luis Redondo García
SECURITY IN INFORMATION SYSTEMS AND SOFTWARE ENGINEERING

FULL PAPERS

SECURITY PATTERNS, TOWARDS A FURTHER LEVEL
Beatriz Gallego-Nicasio, Antonio Munoz, Antonio Maña and Daniel Serrano 349

SHORT PAPERS

ITERATED TRANSFORMATIONS AND QUANTITATIVE METRICS FOR SOFTWARE PROTECTION
Mariusz M. Jakubowski, Chit W. (Nick) Saw and Ramarathnam Venkatesan 359

PHISHPIN: AN INTEGRATED, IDENTITY-BASED ANTI-PHISHING APPROACH
Hicham Tout 369

ON THE NEED TO DIVIDE THE SIGNATURE CREATION ENVIRONMENT
Jorge L. Hernandez-Ardieta, Ana I. Gonzalez-Tablas, Benjamin Ramos and Arturo Ribagorda 375

AN ALTERNATIVE APPROACH FOR FORMULA MODELLING IN SECURITY METRICS
Felipe Marques Pires, Leonardo de Sousa Mendes and Rodrigo Sanches Miani 381

A SECURITY DESIGN PATTERN TAXONOMY BASED ON ATTACK PATTERNS - Findings of a Systematic Literature Review
Andreas Wiesauer and Johannes Sameitinger 387

ISEE: AN INFORMATION SECURITY ENGINEERING ENVIRONMENT
Jingde Cheng, Yuichi Goto and Daisuke Horie 395

POSTERS

MANAGING SECURITY OF GRID ARCHITECTURE WITH A GRID SECURITY OPERATION CENTER
Julien Bourgeois and Raheel Hassan 403

AUTHOR INDEX 409
FREE SECURITY SUITE 2
Easy, Intuitive and Complete Free Security Suite with Web Browser Integration

Javier Corral-Garcia, Carlos-Jorge del Arco González
José Luis González-Sánchez and José Luis Redondo García
Department of Computing and Telematic System Engineering, University of Extremadura, Cáceres, Spain
javiercg@unex.es, cdelarco@alumnos.unex.es, jlgo@unex.es, jliter@unex.es

Keywords: Free software, Security, Suite, Privacy, Network threats, Web browser extension.

Abstract: Nowadays there are many security suites to protect a system against threats from the network. However, users must purchase a license to use them. There is the possibility of installing some free-of-charge security tools (often Free Software tools), without license payments and avoiding illegal use of software. The disadvantages are that each tool focuses on monitoring only one security threat, leaving a lot of other aspects unprotected. Moreover, in most cases these tools run on command line, involving difficult configuration processes for non-expert users. We have developed a Free and easy to use suite that ensures the security of the systems in which it is installed, and designed for users who don’t have enough time, nor high knowledge about computer security, to protect their systems against threats from the network adequately. In order to achieve our objectives, we made a thorough study of the latest free software tools, with the aim of choosing the best for our suite, developing several easy and intuitive graphical interfaces for the command line tools, even modifying the source code of one of them, and developing an extension to integrate FSS-2 in the Mozilla Firefox browser.

1 INTRODUCTION

System and network security are fundamental cornerstones that seek to ensure the protection of information. Unfortunately they are not easy goals to achieve (De-Silva et al., 2007). The Internet has grown dramatically and evolved significantly over the past 10 years (Arlitt & Williamson, 2007) and, as the level of trade and commerce conducted over it increases, so does the requirement that the Internet is reliable and secure. Unfortunately, the quantity and complexity of security threats to the Internet is also increasing (Sandford et al., 2006). The Free Security Suite 2 project, or FSS-2, appears with the need to offer users a complete easy and intuitive tool to protect their systems against increasing threats.

Nowadays there are many security suites to protect a system. However, users must purchase a license to use these Software products. This fact means that, generally, the user decides to leave their system unprotected or using this software illegally, facing the consequences accordingly. There is the possibility of installing some free-of-charge security tools in order to solve the problems of the user, without license payments and avoiding illegal use of software. The disadvantages are that each tool focuses on monitoring only one security threat, leaving a lot of other aspects unprotected, in most cases, involving difficult configuration processes and a complex interface for non-expert users.

Our previous version, Free Security Suite (Castuera et al., 2004), emerged to solve these problems, by offering a free security suite that integrated several easy and intuitive tools to control various security aspects at the same time. FSS became the only application with such features, and nowadays it still has this singularity, due to the non-existence of another Free Software security suite.

However, throughout these years, the application has become obsolete. For this reason we have developed FSS-2, a new version adapted to current needs. The philosophy is the same one but with an improved suite, returning to make a thorough study of the latest free software tools, with the aim of choosing the best for our suite, developing easy and intuitive graphical interfaces, also modifying the source code of one tool, and developing an extension to integrate FSS-2 in the Mozilla Firefox browser (Firefox, 2009), so that it can be used more comfortably.
2 PREVIOUS ANALYSIS

We proposed to develop Free and easy to use tool, that ensure the security of the systems in which it is installed, and directs towards users who don’t have enough time, nor high knowledge about computer security, to adequately protect their systems. Thus, FSS-2 is a tool with easy use and configuration features, which controls the main aspects of security that concerns common users. We wanted to develop it as a Free Software tool, GPL licensed, among other reasons, so that its use would not involve any cost to any user. The source code is distributed with the tool and can be modified without restrictions, allowing anybody to improve its features or to adapt it to other specific requirements.

2.1 Tools Analysis

With the goal of making FSS-2 to strengthen the security of a system in as many aspects as possible, we previously performed a thorough analysis of the threats that presents nowadays a computer system, analyzing in depth the latest protection tools, in order to choose the most suitable to join FSS-2.

2.1.1 Anti-RootKit

FSS-2 includes Tripwire (2009), for to obtain and compare fingerprints of programs, and Chkrootkit (2009) and Rkhunter (2009), as a detection method if it is suspected that the rookit is already present in our system. These tools run on command line mode so we have developed an interface for each of them in order to make their use more intuitive to the user.

2.1.2 File Encryption

After analyzing many files encryption tools, we finally opted for ScramDisk (2009), which has an intuitive graphical interface that facilitates the task to the user.

2.1.3 e-Mail Encryption

GnuPG (2009) allows encrypt communications and data, with a key management system and access modules for all types of public key directories. It runs from the command line, so it was desirable to incorporate a graphical user manager to enable him to exploit all the opportunities offered by GnuPG. So, we were analyzed different possibilities, choosing GPA (2009) finally, due to its simplicity and its more intuitive use.

2.1.4 AntiPhising

Mozilla Firefox (Firefox, 2009) browser incorporates an antiphishing tool. It is GPL licensed, being chosen as the anti-phishing tool for FSS-2.

2.1.5 Firewall

We decided to include two tools: Firestarter (2009) is made for users who prefer an easy tool with good results; GuardDog is the option for users with higher knowledge and who wish to obtain a more advanced configuration from their firewall.

2.1.6 Antivirus

We have selected ClamAV (2009), a GPL licensed antivirus with support for Linux, simple updating method, and versions released often by their developers. ClamAV can be run on command line mode or on various graphical environments. In our suite, we have included the KlamAV environment (2009), which we considered it has the best features, providing exclusive options not included on others, and making habitual tasks such as updating of the Clam graphical environment easier.

2.1.7 Content Filter

FSS-2 includes the Dnsguardian tool (2009), GPL licensed, after analyzing various content filtering tools. However, it runs on command line. So, we have developed a graphical interface that replaces command mode, developing modifications on the source code of the application, with the objective of improving it substantially.

2.1.8 Anti-Spam

Users are able to install Thunderbird (2009) with a Bayesian filter incorporated, and also the installation and configuration of the CRM114 (2009) system to sort email messages using Kmail (2009) client. We have enabled an option in our application to access the Evolution (2009) mail client, because it presents an integrated anti-spam filter. CRM114 was chosen because it has obtained the best results according to our preferences.

3 DEVELOPMENT

We developed graphical interfaces that allow users to configure and run the tools explained above. Besides this, we had to develop interfaces for
execute script files and operating system commands, to achieve applications that run specific command line orders.

Our suite can be easily installed and configured on any Linux system because our data model is based on a collection of text files.

In addition, we made a modification in the source code of the Dansguardian tool, in order to obtain a configuration based on user groups, so that each group can have a set of predefined filtering options, because its initial configuration was too complex.

### 3.1 Mozilla Firefox Extension

Although the application can be executed differently, we developed an extension to include FSS-2 as a tool in the Mozilla Firefox browser, so that it can be used more comfortably.

### 3.2 Installation Scripts

The installation was performed through automated scripts to avoid complex configurations task when the user begins to run the suite.

### 3.3 Implementation

FSS-2 applications may be used separately, independent of the suite. The implementation has been carried out using C++ programming language together with Shell Script language and operating system GNU/Linux commands. The tools used have been Anjuta IDE and Glade interface designer, in addition to some official libraries.

### 4 FSS-2

The access to the application is done through Firefox browser by opening the Tools menu and choosing the FSS-2 option. The main window shows eight tabs that allow access to the different tools, each one indicating its basic functionality.

#### 4.1 Anti-rootkit

The Anti-rootkit tab provides access to rootkit detection applications through the intuitive graphical user interfaces that we developed. We carry out several options for Chkrootkit for: to start the rootkits analysis, to access the latest analysis results, and to search for and install new updates automatically. RKHunter add another option, updating its database and saving the files analyzed as authentic. With Tripwire we allow users to verify the files integrity.

#### 4.2 Antivirus

Using this tab, we include the KlamAV graphical interface in order to use the ClamAV antivirus. Thus, users can scan their systems (with the chance of scheduling this task), update antivirus, configure emails scanning, managing quarantine files, etc.

#### 4.3 Antispam

The Antispam tab provides access to the email clients included with FSS-2, in addition to the CRM114 tool that we integrated with KMail, due to the reasons set out in the tools analysis section, where we also explain the reasons for this choice.

#### 4.4 File Encryption

FSS-2 allows the user to create encrypted disk partitions and volumes. Data is encrypted in a container, and when the user has access to this data, it is opened and automatically decrypted, through the ScramDisk tool.

![Figure 1: GPA encryption tab FSS-2.](image)

#### 4.5 e-Mail Encryption

We allow performing the encryption of text messages for later e-mail data transmission. The tool is used through GPA graphical environment, which allows user to get all the GnuPG features in an easy and intuitive way. By means of the mentioned tools, it allows encryption, decryption, signature and document verification, besides import and export of public key.
4.6 Content Filter

Dansguardian, allows the control of Internet contents. We have developed a graphical environment for FSS-2 that allows users to use the tool in a comfortable and intuitive way. Also, we have realized a modification which consists on a configuration based on user groups, with the objective that each one can have a set of predefined filtering options, because its initial configuration seemed to be too complex to non-expert user.

4.7 Firewall

We had included two tools: Firestarter, for users who prefer an easy tool with good results, and GuardDog for users with higher knowledge and who wish to obtain a more advanced configuration.

4.8 Antiphising

The tool we offer is integrated into Mozilla Firefox web browser, however, FSS-2 incorporates a tab to enable/disable this protection in the browser.

4.9 General Preferences

Also, we have incorporated several options in order to automate various tasks, such as the execution of some tools or the whole suite at system start-up, or of different scheduled analysis.

5 CONCLUSIONS

We have developed an easy to use and Free tool that ensures the security of systems, and designed for users who don’t have enough time, nor high knowledge about computer security, to protect their systems against threats in an easy and intuitive way.

Thus, FSS-2 is a tool with easy use and configuration features, which controls the main aspects of security that concerns common users. Besides, as free tool, the source code is distributed and can be modified without restrictions, allowing everybody to improve its features.

We made a thorough study of the latest free software tools, with the aim of choosing the best for our suite, developing easy and intuitive graphical interfaces for command line tools, even modifying the source code of one of them.

We performed the installation of FSS-2 through different automated scripts to avoid complex configurations task when user begins to run the suite, and although the application can be executed differently, we developed an extension to include FSS-2 as a tool in the Mozilla Firefox browser, so it can be used more comfortably.

REFERENCES


