

August / September 2009, Volume 5, Number 2

EU research:

CoMiFin

..-..DIESIS

Supply chain

assurance

3rd SCADA

Symposium



SCADA security

CFI BCM

scenario and cost

ECN

European CIIP Newsletter

CRITIS 2009

Conference:

Register now!

**> About ECN**

ECN is co-ordinated with

The European Commission, was initiated by Dr. Andrea Servida,

and is now coached and supervised by Angelo Marino.

For 2007-2009, the ECN is financed by the IRRIIS project.

The IRRIIS project is an IST FP6 IP,

funded by the European Commission

under contract no 027568

**>For ECN registration send any email to:**

subscribe@ciip-newsletter.org

**>Article can be submitted to be published to:**

submit@ciip-newsletter.org

**>Questions about articles to the editors can be sent to:**

editor@ciip-newsletter.org

**>General comments are directed to:**

info@ciip-newsletter.org

**>Download site for specific issues:**

http://irriis.org

http://www.ci2rco.org

**The copyright stays with the editors and authors respectively, however**

**people are encouraged to distribute this CIIP Newsletter**

**>Founders and Editors**

Eyal Adar CEO iTcon, eyal@itcon-ltd.com

 Bernhard M. Hämmerli, HTA, Initiator and Main Editor bmhaemmerli@acris.ch

Eric Luiijf, TNO Defence, Security and Safety, eric.luiijf@tno.nl

**>Country specific Editors**

For Germany: Heinz Thielmann, Prof. emeritus, heinz.thielmann@t-online.de

For Italy: Louisa Franchina, ISCOM, luisa.franchina@comunicazioni.it

For France: Michel Riguidel, ENST, riguidel@enst.fr

For Spain: Javier Lopez, UMA, jlm@lcc.uma.es

For Finland: Hannu Kari, HUT, kari@tcs.hut.fi

**> Spelling:**

British English is used except for US contributions

|  |
| --- |
| **Introduction** |
| Intro | European R&D and dependenciesby Eric Luiijf& Bernhard Hämmerli | 4 |
| **European Activities** |
| CoMiFin Project | CoMiFin: Middleware for Monitoring Financial Critical Infrastructureby Barry P. Mulcahy | 6 |
| DIESIS | DIESIS – Designing a Research Facility for CIPErich Rome et. Al | 8 |
| **Countery Specific Issues** |  |
| SWISS-CIP Strategy | Developing a national CIP strategy: Swiss experiences and resultsby Stefan Brem | 13 |
| **Method and Models** |  |
| Supply chain assurance | An Overview of Software Supply Chain Integrityby Paul Kurtz | 15 |

Table of Content

Financial bodies, as well as businesses and ordinary people worldwide, are increasingly reliant on this financial infrastructure for conducting their day-to-day finan-cial activities. As of today, the overall number of transactions being conducted over the finan-cial ICT infrastructure amounts to millions per hour worldwide and several trillions of dollars/euros moved around the world every day. The SWIFT Circuit handled on 15th October 2008 (that years peak day): 17,860,068 messages, or approximately 206 messages per second on average.

CoMiFin: Middleware for Monitoring

Financial Critical Infrastructure

The goal of the FP7 STREP project CoMiFin is to create a federated, distributed and collaborative network of agents for enhancing trustworthy-ness and dependability of financial infrastructures.

An increasing amount of this traffic is being carried over pub-licly accessible commun-ication media (such as the Internet), and involves commodity hardware and software. This trend towards the “webification” of critical financial services, such as home banking, online trading and remote payments provides for 24-hour service availability and im-proves user-friendliness. How-ever, it exposes such services and the supporting ICT infra-structure to massive, coordinated Internet-based attacks and frauds that are not being effectively countered by any single organisation.

The main purpose of the CoMiFin STREP is to strategically target the EU technological and institutional approach in financial infrastruc-ture protection (FIP). Speci-fically, CoMiFin aims to provide “an infra-structure level monitoring, noti-fication and mitigation” middle-ware as an essential element of FIP.

**Threat Model**

Several technologies and good practices enable thorough analysis of the events related to a specific domain, for example, the network traffic within an ISP. However, current monitoring approaches are inadequate to deal with coor-dinated and distributed attacks on a large scale. Even well protected and highly secure financial institution networks are vulnerable to complex and coordinated frauds involving multiple actors spread over different countries. In these cases, the monitoring and detection systems whose scope is limited to each individual organisation are unable to detect potential attacks and provide early alerts. To be effective, the monitoring activities have to involve multiple participants possibly distributed over disparate organisational, administrative and geographical domains.

“One-in-a-thousand-year events seem to be happening annually, and one in a hundred year events are occurring weekly at the moment. All our risk models need to be reviewed, updated and re-applied”

Lord Turner, February 2009

**The CoMiFin Approach**

In CoMiFin, we have a long-term research agenda aimed at developing a comprehensive approach to financial infrastructure protection. In contrast to existing work, we do not restrict our atten-tion to protecting each individual financial domain, but rather focus on the entire financial ecosystem as a whole. Our specific objective in the CoMiFin project is to devise a scalable distributed monitoring subsystem. This system will provide the relevant IT components of each participating financial domain with early notifications about faults and other potentially malicious activity


origin-nating at remote sites (possibly be-longing to other critical infrastruc-tures). Thus, enabling those compo-nents should trigger the necessary protective mechanisms in a timely fashion.

Barry P. Mulcahy

Dr. Barry P. Mulcahy is a Security Research Fellow for the Telecommunications So-ftware & Systems Group (TSSG) at the Waterford In-stitute of technology (WIT). He received his BSc from University College Cork (UCC) in 2001 and his PhD in distributed security systems in 2008. He has worked as a lecturer in computer secur-ity at UCC and on a number of different national and international projects in the field of IT security. These include EI, SFI and FP7 projects. Barry is actively involved in the FP7 project CoMiFin: Communication Middle-ware for Monitoring Financial Critical Infra-structure. His re-search interests include secure workflows, distributed security, privacy and trust management systems. Barry regularly serves on technical programme com-mittees and as a reviewer for conferences in his research areas.

e-mail: bmulcahy@tssg.org

Financial actors collectively gene-rate massive amounts of event data whose processing can no longer be effectively accomplished by existing centralised solutions. CoMiFin pro-vides a distri-buted event aggre-gation and correlation system based on an unmanaged network infrastructure (the Internet), thereby providing resilience under failure scenarios including operational failures and deliberate breaches.

The primary objective of this intel-ligence cloud is to leverage the computational and storage resour-ces available at each participant attached to the cloud in order to mine the event stream delivered for potentially dangerous patterns of activity and other anomalies. This is a non-trivial task requiring a holistic and cooperative approach across multiple elements of a financial infrastructure, such as disparate financial and telecom-munication networks, various middleware platforms, and other interconnecting components.

**The CoMiFin Technical
Architecture**

The vector for the next disruption or attack on financial CI is an un-known quantity. In order to be effective as an early warning sys-tem for financial CI, any system must be capable of identifying and disseminating informa-tion about emerging threats in real-time.

The CoMiFin architecture is a highly scalable and robust monitoring software system that enables con-sistent sharing of operational con-ditions amongst all of the inter-dependent parties including utilities providers, such as telecommuni-cation service and electricity providers.

The system is designed to meet a variety of non-functional require-ments, such as responsiveness, predictability, security and trust. Interfaces with existing network management systems deployed in individual financial domains (for example, various IBM Tivoli pro-ducts) facilitate effective domain specific monitoring and manage-ment policies.

CoMiFin innovates across a spec-trum of distributed computing technologies including (but not limited to): semantic overlay networking enhanced with trusted and secure group formation; highly scalable event processing; and new techniques for intrusion de-tection and mitigation strategies.

On joining the CoMiFin intelligence cloud, more secure agreements can be reached by subsets of participants. These interest-based agreements allow partici-pants to subscribe to the so-called semantic rooms. These rooms are exclusive virtual spaces where partici-pants can share interest-based events and information at a higher level of security. This could include infor-mation on fault notifications, ser-vice interruptions, DDoS and any other cyber-attacks.

**Theoperational inde-pendence of financial actors is unaffected**

The CoMiFin system is strictly an information sharing medium for all elements of financial CI. While actors in the system may be dependent on each other for services at a business level, the independence of their internal infrastructures and their freedom to act on information provided by CoMiFin is not affected by their participation in the system.
This allows each actor to tailor their response to emerging threats based on local domain know-ledge, the level of trust associated with the source of the information, and the relevance that they place in the information provided via CoMiFin. This real-time information support allows mitigation strategies to be implemented by financial actors in a timely and appropriate manner.

**The CoMiFin Community**

As part of the engagement process with the financial community, the project has close ties with the Co-ordination action project PARSIFAL, which purpose is bringing together the financial industry and research stakeholders in order to better establish trustworthy better protect CFI.

In addition, a Financial Advisory Board (FAB) has been established for the project. The CoMiFin FAB is chaired by Mr. Thomas Kohler of UBS Zurich and has members from across the European financial land-scape. The board includes both national and international service providers and steers the project with their operative knowledge of CFI.

The CoMiFin Consortium is actively cooperating with the FAB and other financial bodies in the areas of: requirements analysis, regu-latory policies, prototyping and assessment, and dissemination of the results.

**The CoMiFin Consortium**

The CoMiFin Consortium consists of 9 partners: ElsagDatamat (IT), Technische Universität Darmstadt (DE), IBM (IL), Waterford Institute of Technology (IE), Ministry of Economics and Finance of Italy (IT), OptXware (HU), KreditTilsynet (NO), University of Modena (IT) and Consorzio Interuniversitario Nazionale per l‘Informatica (IT). This represents an ideal mix of commercial, academic and finan-cial interests in the field of FIP.

If you would like to find out more about CoMiFin please visit our

website at www.comifin.eu or

email info@comifin.eu.

CoMiFin: Middleware for Monitoring ...|Barry P. Mulcahy

European CIIP Newsletter 2013**|**5/2

**7**

Financial bodies, as well s busiesses and ordinary people worldwide, are increasingly reliant on this financial infrastructure for conducting their day-to-day finan-cial activities. As of today, the overall number of transactions being conducted over the finan-cial ICT infrastructure amounts to millions per hour worldwide and several trillions of dollars/euros moved around the world every day. The SWIFT Circuit handled on 15th October 2008 (that years peak day): 17,860,068 messages, or approximately 206 messages per second on average.

An increasing amount of this traffic is being carried over pub-licly accessible commun-ication media (such as the Internet), and involves commodity hardware and software. This trend towards the “webification” of critical financial services, such as home banking, online trading and remote payments provides for 24-hour service availability and im-proves user-friendliness. How-ever, it exposes such services and the supporting ICT infra-structure to massive, coordinated Internet-based attacks and frauds that are not being effectively countered by any single organisation.

The main purpose of the CoMiFin STREP is to strategically target the EU technological and institutional approach in financial infrastruc-ture protection (FIP). Speci-fically, CoMiFin aims to provide “an infra-structure level monitoring, noti-fication and mitigation” middle-ware as an essential element of FIP.

**Threat Model**

Several technologies and good practices enable thorough analysis of the events related to a specific domain, for example, the network traffic within an ISP. However, current monitoring approaches are inadequate to deal with coor-dinated and distributed

attacks on a large scale. Even well protected and highly secure financial institution networks are vulnerable to complex and coordinated frauds involving multiple actors spread over different countries. In these cases, the monitoring and detection systems whose scope is limited to each individual organisation are unable to detect potential attacks and provide early alerts. To be effective, the monitoring activities have to involve multiple participants possibly distributed over disparate organisational, administrative and geographical domains.

**The CoMiFin Approach**

In CoMiFin, we have a long-term research agenda aimed at developing a comprehensive approach to financial infrastructure protection. In contrast to existing work, we do not restrict our atten-tion to protecting each individual financial domain, but rather focus on the entire financial ecosystem as a whole. Our specific objective in the CoMiFin project is to devise a scalable distributed monitoring subsystem. This system will provide the relevant IT components of each participating financial domain with early notifications about faults and other potentially malicious activity origin-nating at remote sites (possibly be-longing to other critical infrastruc-tures). Thus, enabling those compo-nents should trigger the necessary protective mechanisms in a timely fashion.

Financial actors collectively gene-rate massive amounts of event data whose processing can no longer be effectively accomplished by existing centralised solutions. CoMiFin pro-vides a distri-buted event aggre-gation and correlation system based on an unmanaged network infrastructure (the Internet), thereby providing resilience under failure scenarios including operational failures and deliberate breaches.

The primary objective of this intel-ligence cloud is to leverage the computational and storage resour-ces available at each participant attached to the cloud in order to mine the event stream delivered for potentially dangerous patterns of activity and other anomalies. This is a non-trivial task requiring a holistic and cooperative approach across multiple elements of a financial infrastructure, such as disparate financial and telecom-munication networks, various middleware platforms, and other interconnecting components.

**The CoMiFin Technical
Architecture**

The vector for the next disruption or attack on financial CI is an un-known quantity. In order to be effective as an early warning sys-tem for financial CI, any system must be capable of identifying and disseminating informa-tion about emerging threats in real-time.

The CoMiFin architecture is a highly scalable and robust monitoring software system that enables con-sistent sharing of operational con-ditions amongst all of the inter-dependent parties including utilities providers, such as telecommuni-cation service and electricity providers.

The system is designed to meet a variety of non-functional require-ments, such as responsiveness, predictability, security and trust. Interfaces with existing network management systems deployed in individual financial domains (for example, various IBM Tivoli pro-ducts) facilitate effective domain specific monitoring and manage-ment policies.

CoMiFin innovates across a spec-trum of distributed computing technologies including (but not limited to): semantic overlay networking enhanced with trusted and secure group formation; highly scalable event processing; and new techniques for intrusion de-tection and mitigation strategies.

On joining the CoMiFin intelligence cloud, more secure agreements can be reached by subsets of participants. These interest-based agreements allow partici-pants to subscribe to the so-called semantic rooms. These rooms are exclusive virtual spaces where partici-pants can share interest-based events and information at a higher level of security. This could include infor-mation on fault notifications, ser-vice interruptions, DDoS and any other cyber-attacks.

**Theoperational inde-pendence of financial actors is unaffected**

The CoMiFin system is strictly an information sharing medium for all elements of financial CI. While actors in the system may be dependent on each other for services at a business level, the independence of their internal infrastructures and their freedom to act on information provided by CoMiFin is not affected by their participation in the system.
This allows each actor to tailor their response to emerging threats based on local domain know-ledge, the level of trust associated with the source of the information, and the relevance that they place in the information provided via CoMiFin. This real-time information support allows mitigation strategies to be implemented by financial actors in a timely and appropriate manner.

**The CoMiFin Community**

As part of the engagement process with the financial community, the project has close ties with the Co-ordination action project PARSIFAL, which purpose is bringing together the financial industry and research stakeholders in order to better establish trustworthy better protect CFI.

In addition, a Financial Advisory Board (FAB) has been established for the project. The CoMiFin FAB is chaired by Mr. Thomas Kohler of UBS Zurich and has members from across the European financial land-scape. The board includes both national and international service providers and steers the project with their operative knowledge of CFI.

The CoMiFin Consortium is actively cooperating with the FAB and other financial bodies in the areas of: requirements analysis, regu-latory policies, prototyping and assessment, and dissemination of the results.

**The CoMiFin Consortium**

The CoMiFin Consortium consists of 9 partners: ElsagDatamat (IT), TechnischeUniversität Darmstadt (DE), IBM (IL), Waterford Institute of Technology (IE), Ministry of Economics and Finance of Italy (IT), OptXware (HU), KreditTilsynet (NO), University of Modena (IT) and ConsorzioInteruniversitarioNazionale per l‘Informatica (IT). This represents an ideal mix of commercial, academic and finan-cial interests in the field of FIP.

If you would like to find out more about CoMiFin please visit our

website at www.comifin.eu or

emailinfo@comifin.eu.