

# Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years

James CLARKE<sup>1</sup>, Bernhard HÄMMERLI<sup>2</sup>, Henning ARENDT<sup>3</sup>, Aljosa PASIC<sup>3</sup>

<sup>1</sup>Waterford Institute of Technology, Cork Road, Waterford, Ireland

Tel: +353719166628, Fax: + 35351302902, Email: jclarke@tssg.org

<sup>2</sup>Acris GmbH, Bodenhofstrasse 29 6005 Luzern, Switzerland

Tel: +41795417787, Fax: +41795417787, Email: bmhaemmerli@acris.ch

<sup>4</sup>25, Calle De Albarracin, Madrid, Spain

Tel: +34914408800, Fax: +34917543252, Email: aljosa.pasic@atosresearch.eu

**Abstract:** This paper, entitled **Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the next 5 years**, will describe the outcomes of a recently held workshop of the same name held on 24-25<sup>th</sup> September 2007 in Frankfurt, Germany. The workshop was well attended by stakeholders from the financial industry and researchers from the ICT Security and Critical Information Infrastructure Protection areas. The participants over the two day workshop held working group sessions in order to discuss and elaborate a strategic plan and research challenges associated with “massively distributed critical financial infrastructure protection (FIP)” and “trust in new value added business chains”. It is the intention of the authors to present this paper, if accepted, in the submitted workshop entitled **Converging Technical and Non-Technical Consumer Needs in ICT Trust, Security and Dependability across disciplines**.

**Keywords:** Trust, Security, Dependability, Financial Infrastructure Protection (CIP)

## 1. Introduction

A number of coordinated activities supported by ICT Unit F.5 Security [1] have taken place over the last years and resulted in setting the scene for the establishment of a dedicated workshop on Financial Infrastructure Protection (FIP). In May 2006, the IST FP6 SecurIST[2] project organised the Joint SecurIST, Mobile & Wireless Workshop[3]. Its main purpose was to bring together the ICT Trust, Security and Dependability research community with the Mobile and Wireless research community to discuss and propose future research areas of common and mutual benefit to their constituencies. An incisive keynote address "Banking in 2015 and its Impact on Technology, namely on Mobile Technology[4]" formed a basis for an important scenario used within a number of intensive working sessions. In September 2006, a Workshop was organized by the IST FP6 ESFORS[5] project entitled Joint Workshop on Software and Services Development, Security & Dependability [6]. Within working sessions, major research topics were discussed that would contribute to the provision of CIIP in the finance industry.

These above workshops main organisers, chairs and some of their participant's follow up activities further culminated in the financial industry communities coming together with the ICT TSD and CIIP research communities in a workshop specifically dedicated to FIP. The workshop entitled *Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years* was held on 24-25<sup>th</sup> September 2007 in Frankfurt. The event was organised and hosted by the European Finance Forum in close cooperation with European Commission's JRC and INFISO-F5 Unit Security. The workshop was attended by representative stakeholders from the EU and global financial industry and researchers from the ICT Security and Critical Information Infrastructure Protection domains (academic and industry). The workshop served as an excellent platform for a structured strategic dialogue between these Stakeholders. The focus of a number of working group sessions over the two day workshop was on jointly developing scenarios, consequent strategic plans and research directions associated with the **protection of massively distributed critical financial infrastructures and services and trust in new value-added business chains**.

The workshop addressed issues that span beyond a single financial institution or national market. It specifically addressed global, cross border and multi-member state issues and correlations, which may impact or destabilize critical ICT-based financial infrastructures of the European economy. This paper will present the results and challenges discussed and elaborated at the Workshop.

## 2. Objectives

The rapid growth and deployment of Information and Communication Technologies (ICTs) that we are experiencing today is having profound impact on the financial service industry. On the one hand, the ICT infrastructures over which critical financial services are being delivered are becoming ever more interconnected, open and ubiquitous, but at the same time, ever more fragile and vulnerable to failure and cyber-attacks. On the other hand, over the coming years, it is expected that in the financial sector, the level of self-service will become significantly higher than today, with ubiquitous and mobile banking becoming strong market drivers. Industrialisation, business process outsourcing and number of intervening actors in the service value creation chain will further increase, changing the way financial services will be composed and delivered, while continuing to guarantee their very high-level of trustworthiness. This, in turn, would require: defining trustworthiness and new levels of trust in the ever increasing supply chain, and improving reliability of highly distributed infrastructures while dealing at the same time with severe constraints over business continuity management. Security and privacy in both the clients and the client advisors behaviour will be a key success factor for banking and, more broadly, for the financial industry.

## 3 Methodology

In view of the above objectives, in early 2007, an Organization committee was convened in order to prepare a workshop event on *Challenges for the Protection of Critical ICT-Based Financial Infrastructures for the Next 5 Years*. The workshop was held on 24-25 Sept 2007 in Frankfurt, Germany, and attracted nearly 40 attendees from major EU and global financial industry players and key members from the ICT Trust, Security and Dependability (TSD) and Critical information infrastructure protection (CIIP) research communities (academia and industry). The workshop served as an excellent platform for a structured strategic dialogue between these Stakeholders. The focus was on:

- How the situation in the European financial sector will evolve over the next 5 years in the two main themes of the workshop: protection of massively distributed critical financial infrastructures; and, trust in new added value business chains;
- Developing joint scenarios and consequent strategic plans and research directions on how future trustworthy financial services could be constructed and delivered over critical ICT-based service infrastructures and how these latter could be protected from any kind of cyber-threat.

The workshop outcomes were twofold:

- (1) Bringing together the relevant stakeholders types (Financial industry, ICT TSD and CIIP researchers) to engage in dialogue and stimulate collaborative research actions in view of the EU's FP7 call for R&D proposals in the area of critical infrastructure protection, including the protection of ICT-based critical financial infrastructures;
- (2) Provide input to future strategic research directions that the European Commission will support in its next work programme for ICT security Research, for the period 2009-2010.

In the workshop, three dedicated working sessions entitled (1) Trust in new value-added Business chains, (2) Protection of Massively Distributed critical Financial Services and (3) Protection of the Critical Base Infrastructure. Each session was broken in two partners: firstly, scenario definition and second, based on the scenarios from part 1, the discussion, definition and agreement of research topics considered beneficial and necessary for continued mutual collaboration between all the stakeholders, which are described in the next section of the paper.

## 4 Trust in new value-added Business chains

In part 1 of the session, the group decided to first categorise the detailed scenarios into a number of high level research topics upon which the key challenges and issues could be brainstormed. These high level topics included the following:

- Addressing the Quantification/Scale issues – Information overload, dynamicity and complexity of systems. Can we look at it from another perspective and use the large amounts of available data in order to quantify/adjudge the risks or levels of crime increase/decrease.
- Widening and different areas of players/counterparts e.g. foreign/non foreign, banks/service providers, Technologists and User Aspects – more access, control of their data;
- Consideration of the Global Dimension;
- Definition and design of trust elements (models, authority, metrics to enable measurement and rating of CIP layers of protection, etc.).

In the second part of the session, the participants brainstormed and discussed the major immediate and future challenges that need to be tackled in order to realise a Trust framework in new value-added business chains. These challenges are highlighted below:

1. **Trust, especially in the financial systems infrastructure**, is a global challenge: Identifying institutions that build up trust – whom we can trust and who earns trust. Empirical question of who builds up trust? Trust Authority Model: Trusted Authority needs definition of liability and then you can use it in a constructive way. Is it banks, is it government, is it safe?
2. **Trusted collaborations** Collaboration with third parties and dealing with communities both within and outside EU (new players that change the rules bring the need to adapt to these rules and do business with them; and, need to be collaborative between countries, and not limited to EU only). Furthermore, banks should evolve to be the partners of the business.
3. **Optimised / New business processes** Secure and Critical cores of businesses need larger distribution. There is also a factor of High volume and speed. Quantities are changing qualities – millions/billions using it so critical mass is creating changes. Need to think how to get high performance at low cost; how to unify the natural processes with the banking processes (both from technical and organisational way); how to catalyse creation processes by getting people together that don't ordinarily work together; how to break economic monopolies by identifying new potential users, new applications; how to mix and combine banking businesses; how to develop a model for business impact.
4. **Business Ratings and Regulation** Clear observation of Ratings and Ranking industries build up. Need to think about new areas of observation and regulation (both soft regulation and Gentleman's agreement). Need for structuring of information for selection and rating structures. Credit ratings parameters need to be researched and built – semantic, grid systems to simulate the ratings that are being provided. The need for processes and means for quicker response times in emergency cases.
5. **Empowering the end-users** End user capabilities and giving more power to end users: What are the expectations of the customers? Does it include the ability for them to refuse the technical ways we can suggest? Also, establishing "User friendliness" of our TSD solutions. End user should be part of the model descriptions from the start.
6. **Two-side authentication** (of users and clients at the same time) and **Anonymity aspects** (who will manage this? EU, Trusted Third Party Association?)
7. **Security of Systems** Banks communication systems need to be studied. There is need to protect the extranet with firewalls while dealing with huge volumes. There is a need to create or increase confidence in internet based systems in general. As we increase speed and magnitude and things get more complex, we need to redefine the risk criteria. Therefore, we need new modelling techniques for risk to deal with quantification in this new environment. There is also a need for more reliability on software models and for investigating the use and impact of Open source software in the banking sector. Regarding using the mobile terminal for data vaulting, the large challenge is not only to standardise the vault data, but

also today's mobiles are not broadly equipped with the necessary features to support this concept of mobile data vaults.

8. **Interdependencies** There is need to understand the interdependencies between the multi-point, multi-distribution environment. Electricity could serve as example for ensuring and rating the CIP layers of protection.
9. **Cyber crime** is developing on the basis of mobility and speed. There is a need for further research on modelling of attacks, on phishing (identification and avoidance and stamping out of phishing), and on developing a concept of a minimal tolerance to attacks and faults.

## 5 Protection of Massively Distributed critical Financial Services.

The goals pursued by the participants within this session included the following:

- Identity federation in the supply chain based on trust levels that each participant needs to reach through certification
- Disaster, Outsourcing, Moving: transient organisational phases increase risks but for the speed and simplicity during these phases often the additional risks are neither controlled nor internally communicated. Also, the lower level of trust during these phases is not communicated partners and tracked.
- Society need to profit from convergence, for example tracking and localisation of goods
- Self healing systems, systems designed for flexibility. Individual nodes should have more intelligence. Self-conscious nodes.
- Accepted Polymorphic identities, for each identity representation some attributes are mandatory others are discretionary.
- Socio economic trends drive towards
  - Online accessible real-time services
  - Further industrialization and commoditization of financial service supply chain
  - Privacy protection for customers
- Exposure to online organized crime requires new approach to security modelling into business logic (misuse cases)
- Catastrophic events transiently change risk appetite, meaning that trust (to devices and individuals) increases during recovery phase without trustworthiness having changed

The group then discussed the impact of these observations on the financial infrastructure. It was argued that the industry looks for federation of identities in market places (single sign on) as well as for supply chain integration (trust delegation). In B2B scenarios, some participants proposed that a European Agency would offer such a federation service.

The individual citizen, however, would like to prevent that relationships between her single (trans)actions can be established and prefers several separate identities, and more explicit choices of what can be done with her information. In the consumer world, we might look at more and more free services (paid by advertisement) with virtually no privacy and as an alternative paid service with guaranteed privacy. The request towards the legislation is to force service providers to offer greatest flexibility how each information item is handled.

Exposures to risks around online organized crime as well as catastrophic events require tested and reliable modes of information sharing between international enterprises, which imply that state driven crisis management frameworks can not stop at the national boundaries either.

Increasing distribution and connectivity in the infrastructure will ask for systems that are designed for reliability and contain the intelligence to cope with extra-ordinary situations. This creates new challenges in terms of distributed intelligence and interoperability. Last, but not least, resilient and cost-effective management of multi-owned infrastructures poses new challenges as we

see a move from exception management to performance management that detects service degradations.

Prevention of identity theft was the foremost discussion topic that all participants have seen as a key challenge. Clear standards on how identity information needs to be protected and when strong authentication is required would help. It is essential that the risk is not transferred to the consumer when careless service providers go for the cheapest option.

Rather than promoting (state sponsored) single identity representations, we should allow for polymorphic identities and correspondingly bring more convenience into handling multiple identities. Another interesting opportunity could then be to increase the trust level by combining 2-3 identities that are semi-trusted to reach a higher trust level.

The group discussed that similar to other science domains (e.g. pharmaceutical), it would be desirable to nurture a venture capitalist funded environment where IT driven financial services innovation are created and financial service providers are increasingly investing into IT enabled European innovation potential.

New dimensions of scalability were discussed in several contexts and it was argued that for true scalability, it must be possible to design systems without a single dispatching or single back-end system.

## 6 Protection of the Critical Base Infrastructure

In the first part of the session, the group identified the following scenarios summarized below:

**1. End-user protection in a highly distributed environment (mobility):** Mobility is becoming one of the main differentiators within the financial services, providing the end user to access to the financial services anytime, anywhere. This situation creates also some security deficiencies, related mainly with user terminals, privacy, malware detection and reaction, etc.

**2. Secure communication channels (Internet),** this was one of the most controversial scenarios, taking into account that the secure communication channel is in principle part of the supposed Internet security infrastructure and protocols topic. It was noted by some group members that it could not be part of this R&D initiative.

**3. In a catastrophic disaster, critical infrastructure recovery methods:** One of the main concerns is related with the critical single points of failure, what could happen in case one of the main European infrastructure nodes would be down, how could the rest of the infrastructure recover from such a situation.

**4. Regulatory issues, collaboration environments.** Define a collaborative framework, managed and controlled by automatic processes that keep up-to-date every individual European entity (banks, government, police, etc.) with the possible threats environment.

Once the possible scenarios were defined and clarified, during the second part of the session, the team identified the main challenges associated within those scenarios.

One of the main goals are the personal data protection (privacy), the way to define an identity and authentication management that guaranties the security within the user access taking into account the mobile environment. In addition to the protection of personal data and to having strong authentication methods, the quality of service and service availability are also important challenges to be discussed and analyzed within the scenarios defined above.

One of the main concerns of financial entities is related with the real time proactive and trusted data sharing environment, the possibility to define a federation system where the financial entities could share threats, risks and some other important information in order to apply the pertinent protection measurements. In order to go ahead with the previous topic, one important goal is the standardization, within the different interfaces, but also the interface standardization between communication entities.

Risk assessment and risk modelling were also some important topics discussed during the session, identifying possible risk and quantifying the impact based on those risks. For this topic, one important research area is the attack simulation and the possibility to identify cascading effects.

Other important topics discussed during the session included the following:

- European regulatory and laws enforcements
- Resiliency, redundancy, reliability of highly distributed financial environments
- Advanced behaviour detection, prevention and reaction mechanisms (i.e. heuristic analysis)
- Robust segmentation (of services and applications)
- Managing the organization of business aspects following merging of companies

## 7 Conclusions

The workshop held on 24-25 Sept. 2007 brought together the stakeholders in the Financial Industry and the European RTD community members from ICT Trust, Security and Dependability and Critical Information Infrastructure Protection. The event made it abundantly clear that a significant amount of R&D must take place in a coordinated fashion in order to protect massively distributed Critical Financial Services and provide trust in new Value Added Business Chains.

The outcomes of this workshop included the following:

- In each of the scenarios, new technologies and associated risks were identified;
- Exposure to online organized crime requires new approaches to be addressed;
- Secure communication channels are required (current and future Internet);
- Regulatory issues in collaboration environments need to be addressed;
- Significant joint efforts of academia, stakeholders and regulators are needed.

Within the intensive working group sessions of the workshop, a number of scenarios, requirements and research topics were elaborated, discussed and considered in three dedicated Theme-based sessions. These were found to be beneficial and necessary for continued mutual collaboration between the stakeholders. The main outcomes of each session are as follows:

### Session/Theme 1: Trust in new value-added Business chains

- **Trust and trusted collaborations**, especially in the financial systems infrastructure, is a global challenge:
- **Optimised / New business processes**, which are secure and critical in larger, faster and more complex environments and its distribution.
- **Business Ratings and Regulation** require clear observation of Ratings and Ranking industries and new areas of observation and regulation;
- **Empowering the end-users** with enhanced capabilities and giving more power to End users. Examination of the expectations, roles and awareness of the customers is required from the start;
- **Two-side authentication** (of users and clients at the same time) and **Anonymity aspects** (who will manage this? EU, Trusted Third Party Association?)
- **Security of Systems** including internet-based, mobile-based, Banks communication and other financial infrastructure systems need to be studied;
- **Interdependencies** between the multi-point, multi-distribution environment. Electricity could serve as example for ensuring and rating the CIP layers of protection.
- **Cyber crime** is developing on the basis of mobility and speed. There is a need for further research on modelling of attacks, on phishing (identification and avoidance and stamping out of phishing), and on developing a concept of a minimal tolerance to attacks and faults.

### Session/Theme 2: Protection of Massively Distributed critical Financial Services

- Socio economic trends drive towards:
  - Online accessible real-time services;
  - Further industrialization and commoditization of financial service supply chains;
  - Privacy protection for customers;
- Exposure to online organized crime requires new approach to security modelling into business logic (misuse cases);

- Catastrophic events transiently change risk appetite, meaning that trust (to devices and individuals) increases during recovery phase without trustworthiness having changed;
- Block attackers: Deception, counterattacks, international collaboration;
- Internationally coordinated law enforcement;
- Protection and competitive advantage through investing with small innovative companies;
- 3 corrective actions: Protect the brand; Collaboration; and, Inform Public;
- Collaboration in both reactive as well as pro-active areas;
- Identity management:
  - Need for Polymorphic identities: We are citizen, consumer, employee, patient, bank customer, etc;
  - We need to improve the fundamentals of identity;
  - Combine 2-3 identities that are semi-trusted to reach a higher trust level;
  - European agency as the federator for ID mgmt systems in B2B scenarios;
  - Passports are voluntary.... ID cards are mandatory;
  - Liability for B2B transactions is bound to strong identification;
  - Some identity attributes are core/mandatory others are discretionary;
  - Under the new upcoming telecom law, victims need to be informed about possible data breaches.

### **Session/Theme 3: Protection of the Critical Base Infrastructure**

- Personal Data (privacy) protection, improvements in identity management and authentication methods, considering a mobile environment (anytime – anywhere);
- Quality of Service + Availability;
- Real Time Proactive and Trusted data sharing environment between financial and non financial entities (federation of trusted relations);
- Interfaces standardisation, risk assessment, risk modelling;
- Attack simulation facilities (cascading effects);
- European regulatory and laws enforcements;
- Resiliency, redundancy, reliability of highly distributed financial environment;
- Advanced behaviour detection, prevention and reaction mechanisms (heuristic analysis);
- Composition of trust;
- Robust and secure segmentation (of services and applications);
- Managing the organization of business aspects following merging of companies.

Throughout the workshop, a number of realistic cooperation mechanisms were presented by the European Commission. These could benefit the bringing together of the financial industry stakeholders with the communities of Security and CIIP researchers and help build up stronger and fruitful collaborations in the future. In order to capitalise on the successful workshop reported here in this paper to carry out further analyses, it was deemed necessary that a project or number of collaborative projects should be formed bringing together the relevant stakeholders including financial industry industrial members in order to follow up on these findings. The organisers intend to follow up on these activities. The full workshop report is available on the European Commission web site under ICT FP7 Security and also at the European Finance Forum web site[7].

## **References**

- [1] [http://ec.europa.eu/dgs/information\\_society/directory/index\\_en.htm#Dir%20F](http://ec.europa.eu/dgs/information_society/directory/index_en.htm#Dir%20F)
- [2] <http://www.securitytaskforce.eu/>
- [3] Workshop report available at [http://www.securitytaskforce.org/dmdocuments/jointws\\_report\\_v1july0707\\_reportonly.pdf](http://www.securitytaskforce.org/dmdocuments/jointws_report_v1july0707_reportonly.pdf)
- [4] Presented by Thomas Kohler, Head Information Risk Control, UBS Global Wealth Management
- [5] <http://www.esfors.org>

[6] Workshop report available at

[http://www.esfors.org/index.php?option=com\\_remository&Itemid=66&func=fileinfo&id=52](http://www.esfors.org/index.php?option=com_remository&Itemid=66&func=fileinfo&id=52)

[7] Report stored at <http://www.europeanfinanceforum.org/> under CIP