Title:	Version:
Deliverable D1.1 **First Working Session report**	1.1

Project Number:	Project Acronym:	Project Title:
258212	CoMiFin-ICA	Communication Middleware for Monitoring Financial Critical Infrastructure – International Cooperation Aspects

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
2010-09-30	2010-10-31	R – PU

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission Services), RE – Restricted to a group defined by the consortium (including the Commission Services), CO – Confidential, only for members of the consortium (including the Commission Services)

Responsible and Editor/Author:	Organization:	Contributing WP:
Giorgia Lodi	CINI	WP1

Authors (organizations):
Roberto Baldoni (CINI), Giorgia Lodi (CINI), Mirco Marchetti (UoM), Robert Glass (Sandia), Walter Beyeler (Sandia), Barry Mulcahy (WIT), György Csertán (OPT), Hamza Ghani (TUD), Atle Dingsør (KRD), Luca Nicoletti (MEF), Virgilio Audisio (ED), Eliezer Dekel (IBM)

Abstract:

This report describes the principal outcomes that emerged in the discussion carried out during the first CoMiFin-ICA working session between the CoMiFin research group and Sandia Laboratories (US) people.

Keywords:

Adoption, Adaptation, Critical Infrastructures, Network analysis, Cyber security, Collaboration Models, Information sharing

Revision History

The following table describes the main revision changes done in the document and the responsible for the revision.

Revision	Date	Description	Author (Organization)
v0.1	2010-10-14	Document creation, TOC	Giorgia Lodi (CINI)
v0.2	2010-10-29	Executive summary, Section 1 and Section 2	Giorgia Lodi (CINI), Mirco Marchetti (UoM), Robert Glass (Sandia), Walter Beyeler (Sandia), Barry Mulcahy (WIT), György Csertán (OPT), Hamza Ghani (TUD), Atle Dingsør (KRD), Luca Nicoletti (MEF), Virgilio Audisio (ED), Eliezer Dekel (IBM)
V1.1	2010-12-01	General revision of the deliverable	Giorgia Lodi (CINI)

Executive Summary

This deliverable describes the *principal outcomes* of the first CoMiFin-ICA working session carried out in collaboration with people from Sandia Laboratories (US). The working session was held in Rome, in conjunction with the first CoMiFin-ICA workshop, whose principal outcomes will be extensively discussed in CoMiFin-ICA D1.2 deliverable.

The main *objective* of the working session was to identify possible international cooperation activities between the CoMiFin consortium and the Sandia Laboratories.
Starting from the main principal objectives of the CoMiFin-ICA proposal, we identified two broad research areas that have been investigated and discussed during the working session day:

1. *Collaboration Models for large scale Critical Infrastructures: research challenges and applications*
2. *Organizational, Social and Technological Aspects for Information Sharing Environments*.

As explained in this report, the former research area is devoted to investigate modeling aspects of the Semantic Room collaborative environment, developed in the context of the CoMiFin project, exploiting the strong expertise of the Sandia people in modeling such complex environments. The principal objective of this modeling work is to gain qualitative and quantitative insights of the CoMiFin system that allows us to foster a wider use of collaborative environments for cyber attacks detection in the financial domain. In this sense, the outcomes of this line of research of the working session highlighted that two main aspects can be modeled:

- the adoption of the CoMiFin collaborative model
- the generalization of the CoMiFin approach to the global cyber security scenario in critical infrastructures.

The latter research area is devoted to investigate organizational, social and technological aspects of the information sharing employed by the Semantic Room abstraction of CoMiFin. In particular, the working session outcomes highlighted that in such a context two fundamental aspects are to be considered:

- the analysis of the interconnections between the different actors of the financial ecosystem.
- the possibility to use novel adaptation mechanisms in order to detect emerging sophisticated threats. The strong expertise of Sandia people built in engineering Complex Adaptive Systems of Systems (CASoS) can be exploited in this case.

All the previous research lines have been discussed and analyzed during the working session under four important angles, introduced in the slides we include in this deliverable:

- the technical motivations for tackle the identified issues;
- the principal motivations concerning the urgency to address the identified issues;
- the role and importance of the international cooperation between CoMiFin and Sandia;
- the initial approach that can be followed in order to tackle the identified issues.

This deliverable includes a number of slides that summarize the principal outcomes obtained by the CoMiFin and Sandia research groups during the working session. In particular, Section 1 includes the slides we have produced for the analysis of the first previously mentioned research area. The slides report the initial approach the two research groups decided to undertake. Section 2 includes those slides we have produced as result of the analysis of the second mentioned research area. Once again, the slides report the initial approach that is going to be undertaken in order to achieve the expected results. Finally, section 3 concludes this report highlighting possible issues to be faced and discussed in future working sessions.

Table of Contents

1. Collaboration models for large scale critical infrastructures: research challenges and applications *8*
1.1 Principal outcomes with respect to the CoMiFin-ICA objectives **8**
2. Organizational, social, technological aspects for information sharing environments *17*
2.1 Principal outcomes with respect to the CoMiFin-ICA objectives **17**
3. Conclusions *26*
3.1 Possible issues to be faced in future CoMiFin-ICA working sessions **26**

List of Figures

List of Tables

1. COLLABORATION MODELS FOR LARGE SCALE CRITICAL INFRASTRUCTURES: RESEARCH CHALLENGES AND APPLICATIONS

A number of objectives have been identified in the proposal of CoMiFin-ICA that highlight the added value of the international cooperation between CoMiFin and Sandia Laboratories.
In this section, we include the slides the two research groups have produced during the working session and that summarize the main points of the discussion concerning the first research area introduced in the executive summary of this report, i.e., collaboration models for large scale critical infrastructures: research challenges and applications. As it can be noted by the slides below, the following initial CoMiFin-ICA objectives are addressed in the brainstorming of the working session within this research line; namely *the evaluation of the improvements that each financial institution can achieve through the cooperation with other financial institutions, with respect to risk assessment, preparedness, detection and suggestion for reaction*, and *the evaluation of the specific risks that a FI has to face and how the project can address them*.

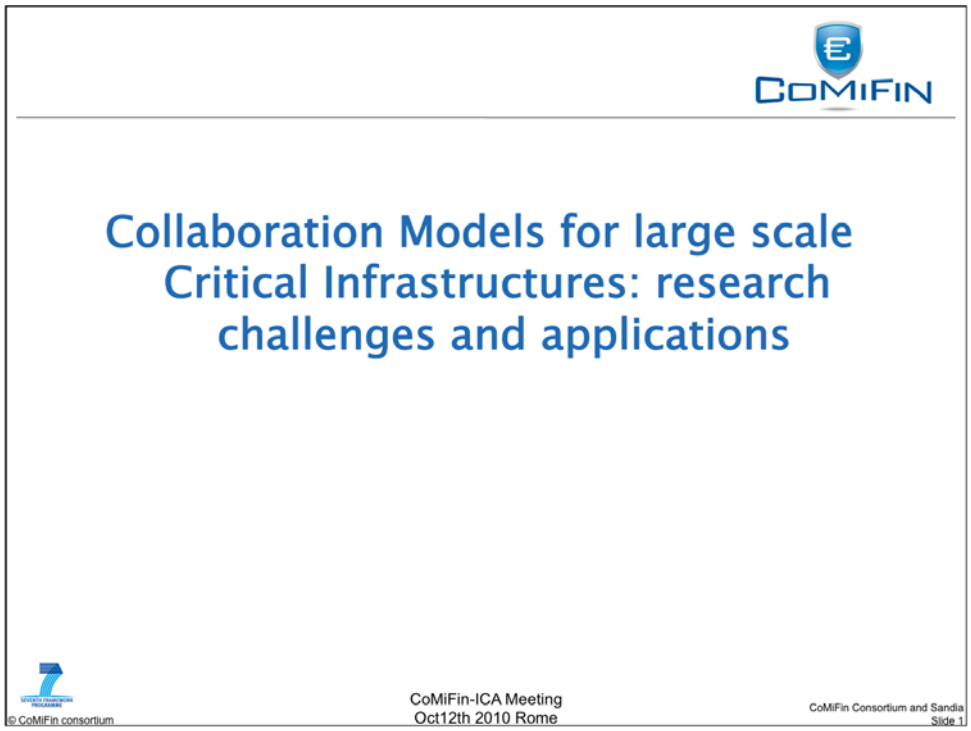
In particular, two aspects have been analyzed: the *adoption* of the Semantic Room based approach by financial stakeholders and the possibility to extend the CoMiFin architecture in order to deal with *cyber security* in general.

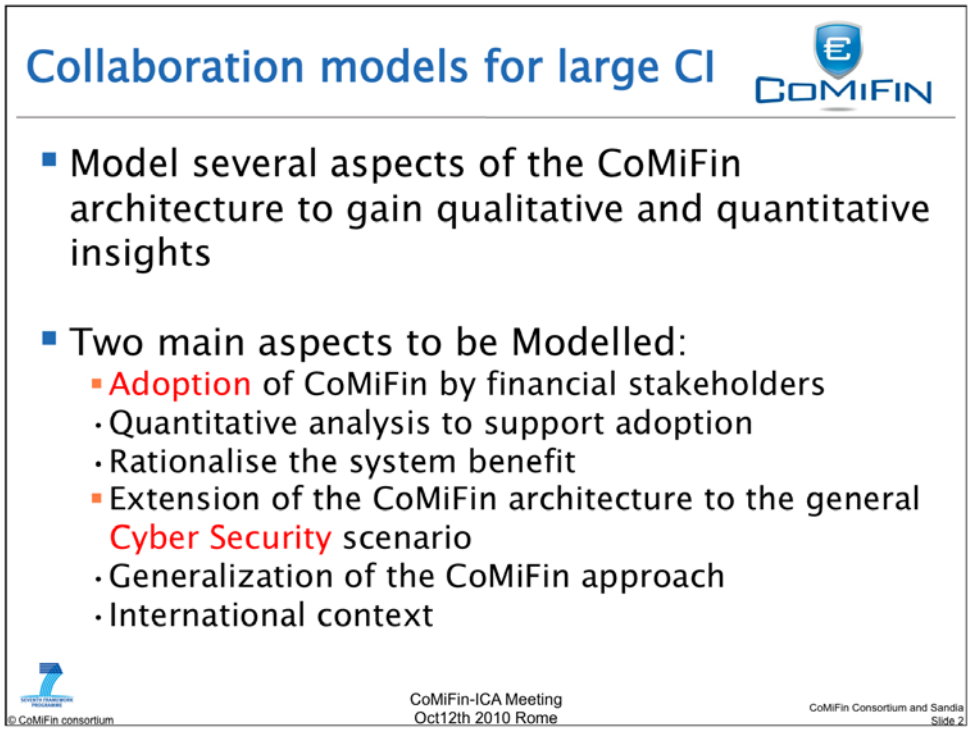
1.1 Principal outcomes with respect to the CoMiFin-ICA objectives

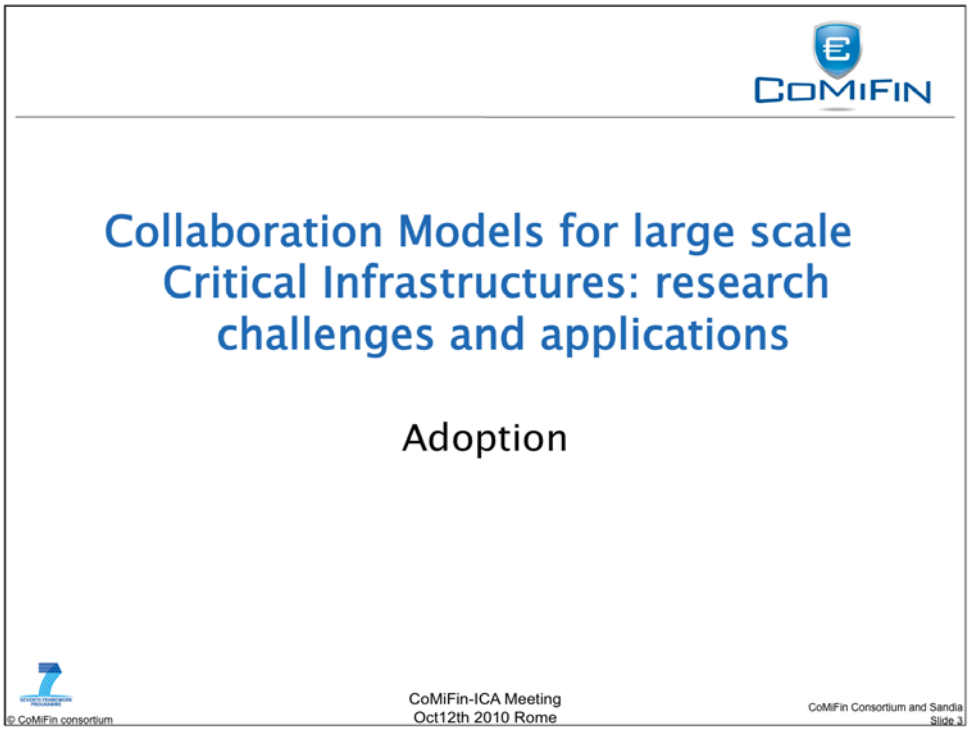
The main *outcomes* produced during of the working session can be summarized in the following:

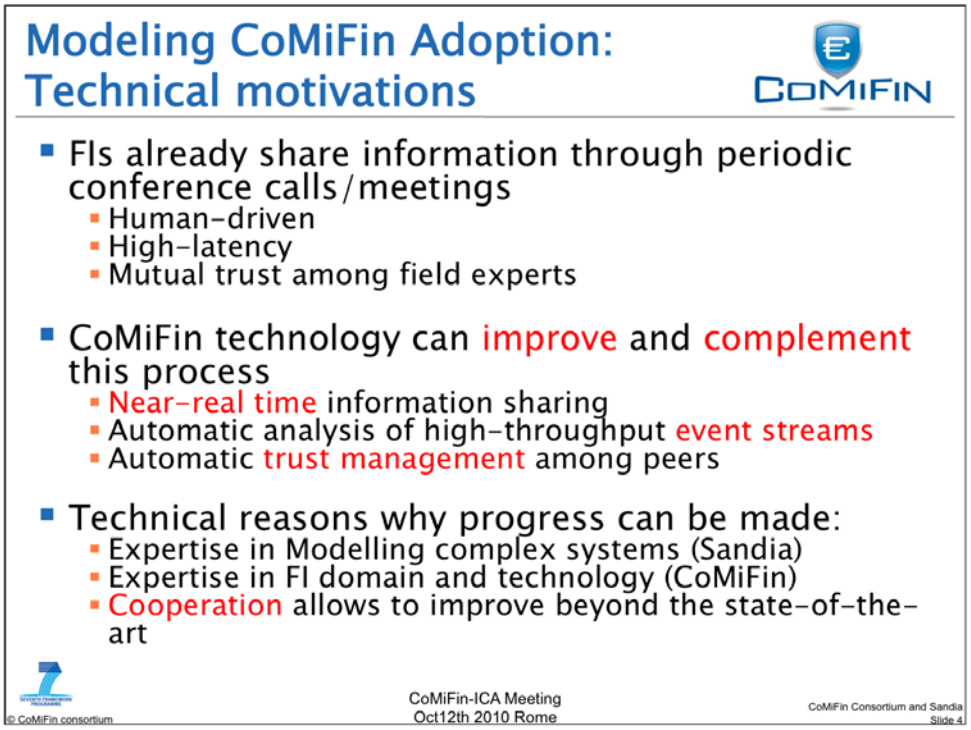
1 properly modelling the adoption of the collaborative approach enabled by the Semantic Room abstraction is beneficial in order to "visualize" the potential of CoMiFin in the financial ecosystem. This can be achieved thanks to the qualitative and quantitative insights the model can highlight. In essence, modelling the adoption of CoMiFin allows us to evaluate the improvements that financial institutions can obtain through the collaborative approach and the related risks, with the final aim to foster the adoption of our model also in the conservative financial domain;

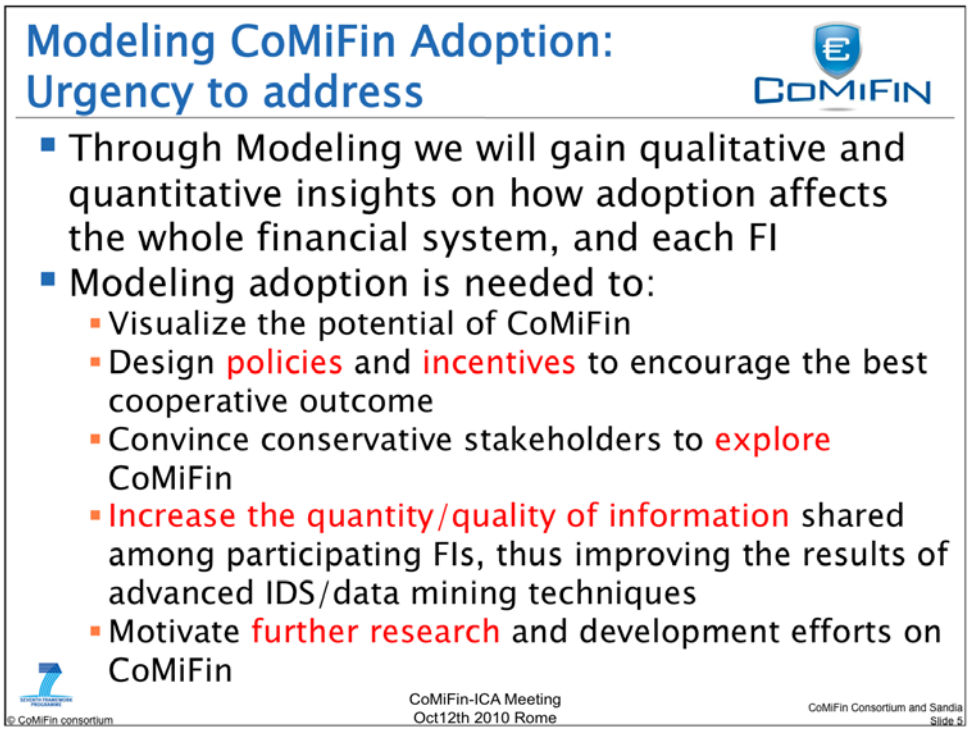
2 generalizing the CoMiFin approach to critical infrastructures and to a wider variety of cyber attacks allows us to bring together diverse utilities and improve the detection of modern cyber attacks that do not respect national and organizational boundaries.

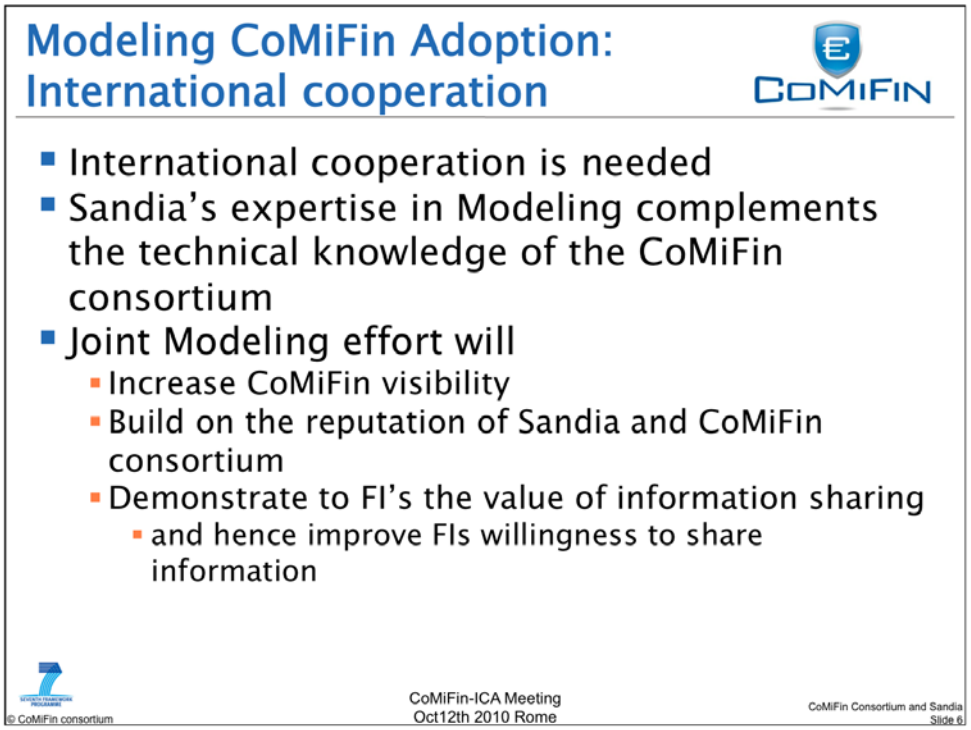

Collaboration Models for large scale Critical Infrastructures: research challenges and applications
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 1

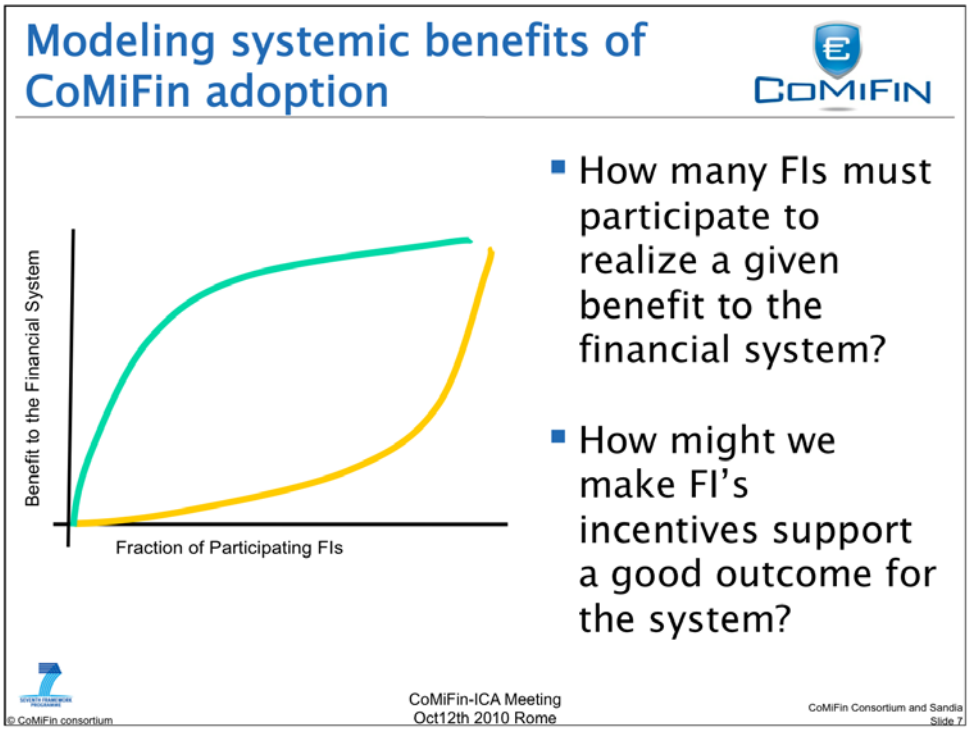

Collaboration models for large CI
Model several aspects of the CoMiFin architecture to gain qualitative and quantitative insights
Two main aspects to be Modelled:
Adoption of CoMiFin by financial stakeholders
Quantitative analysis to support adoption
Rationalise the system benefit
Extension of the CoMiFin architecture to the general Cyber Security scenario
Generalization of the CoMiFin approach
International context
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 2

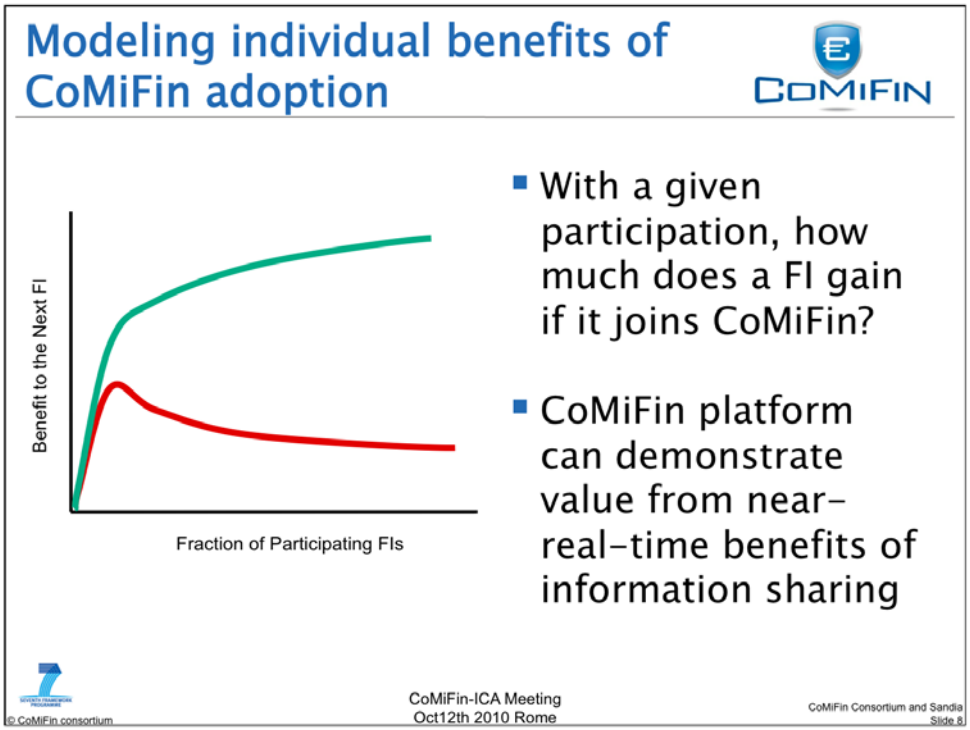

CoMiFin
Collaboration Models for large scale Critical Infrastructures: research challenges and applications
Adoption
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 3

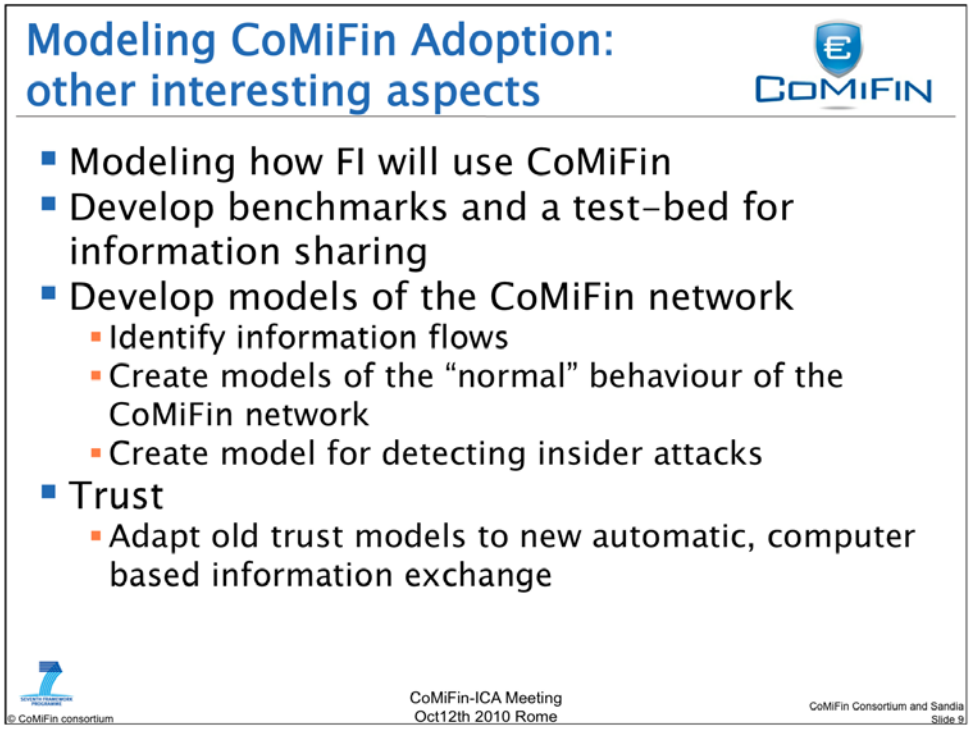

Modeling CoMiFin Adoption: Technical motivations
CoMiFin
FIs already share information through periodic conference calls/meetings
Human-driven
High-latency
Mutual trust among field experts
CoMiFin technology can improve and complement this process
Near-real time information sharing
Automatic analysis of high-throughput event streams
Automatic trust management among peers
Technical reasons why progress can be made:
Expertise in Modelling complex systems (Sandia)
Expertise in FI domain and technology (CoMiFin)
Cooperation allows to improve beyond the state-of-the-art
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 4

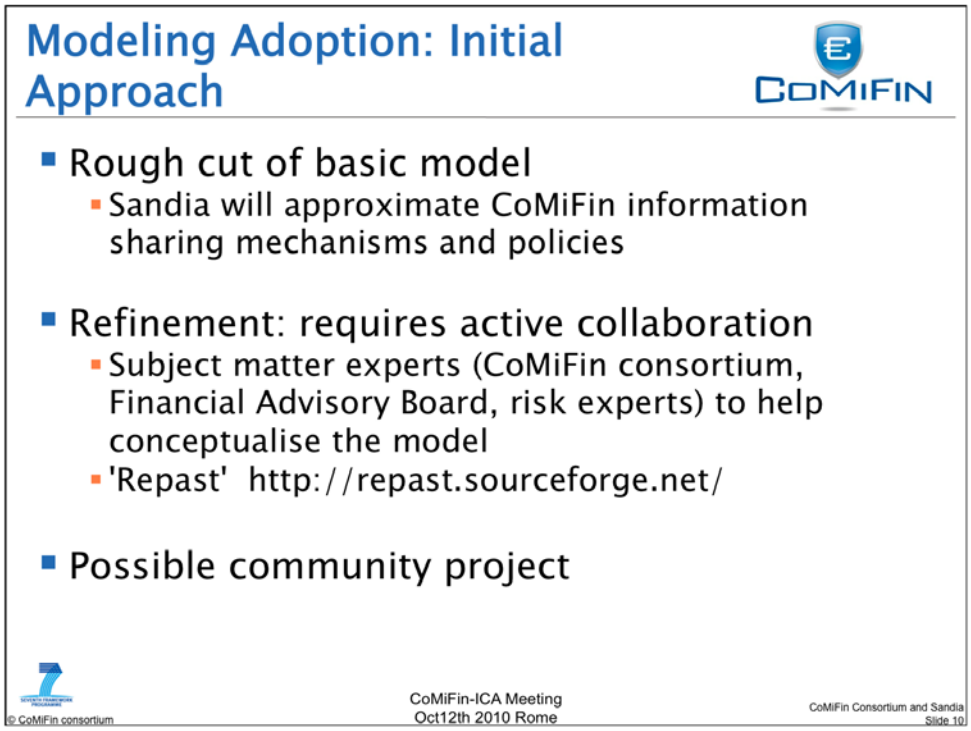

Modeling CoMiFin Adoption:
Urgency to address
CoMiFin
Through Modeling we will gain qualitative and quantitative insights on how adoption affects the whole financial system, and each FI
Modeling adoption is needed to:
Visualize the potential of CoMiFin
Design policies and incentives to encourage the best cooperative outcome
Convince conservative stakeholders to explore CoMiFin
Increase the quantity/quality of information shared among participating FIs, thus improving the results of advanced IDS/data mining techniques
Motivate further research and development efforts on CoMiFin
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 5

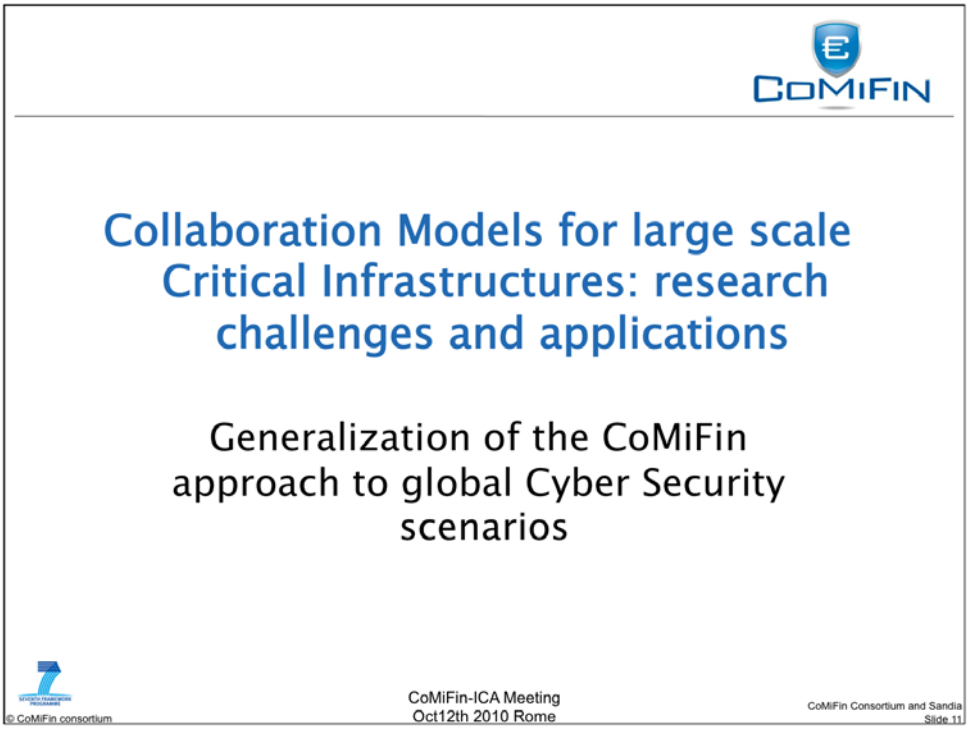

Modeling CoMiFin Adoption:
International cooperation
CoMiFin
International cooperation is needed
Sandia's expertise in Modeling complements the technical knowledge of the CoMiFin consortium
Joint Modeling effort will
Increase CoMiFin visibility
Build on the reputation of Sandia and CoMiFin consortium
Demonstrate to FI's the value of information sharing
and hence improve FIs willingness to share information
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 6

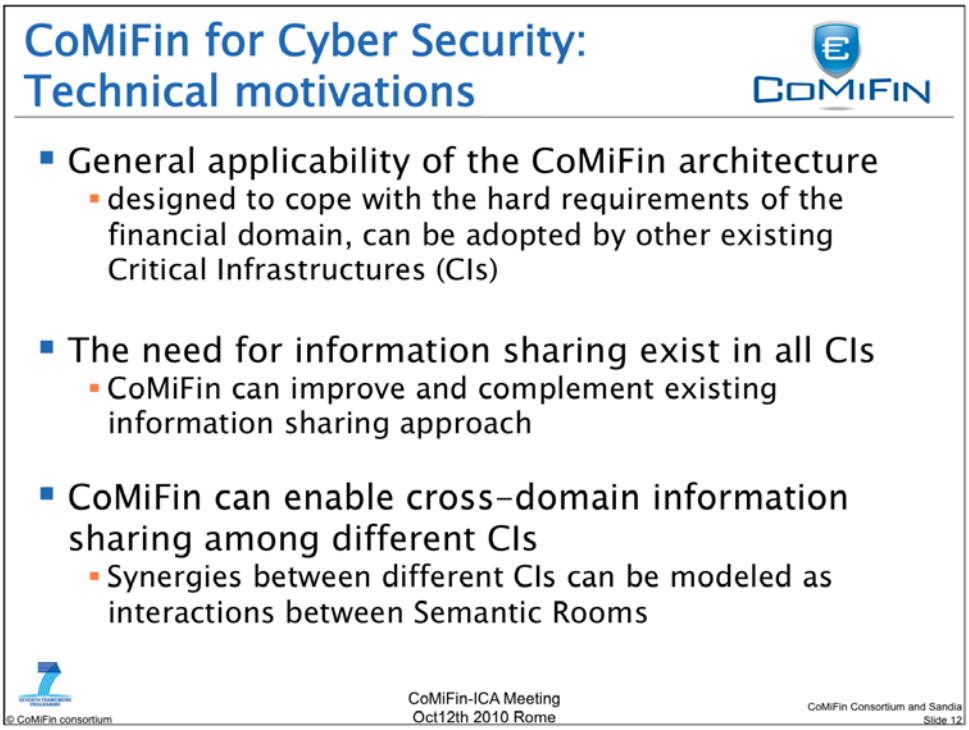

Modeling systemic benefits of CoMiFin adoption
CoMiFin
Benefit to the Financial System
Fraction of Participating FIs
How many FIs must participate to realize a given benefit to the financial system?
How might we make FI's incentives support a good outcome for the system?
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 7

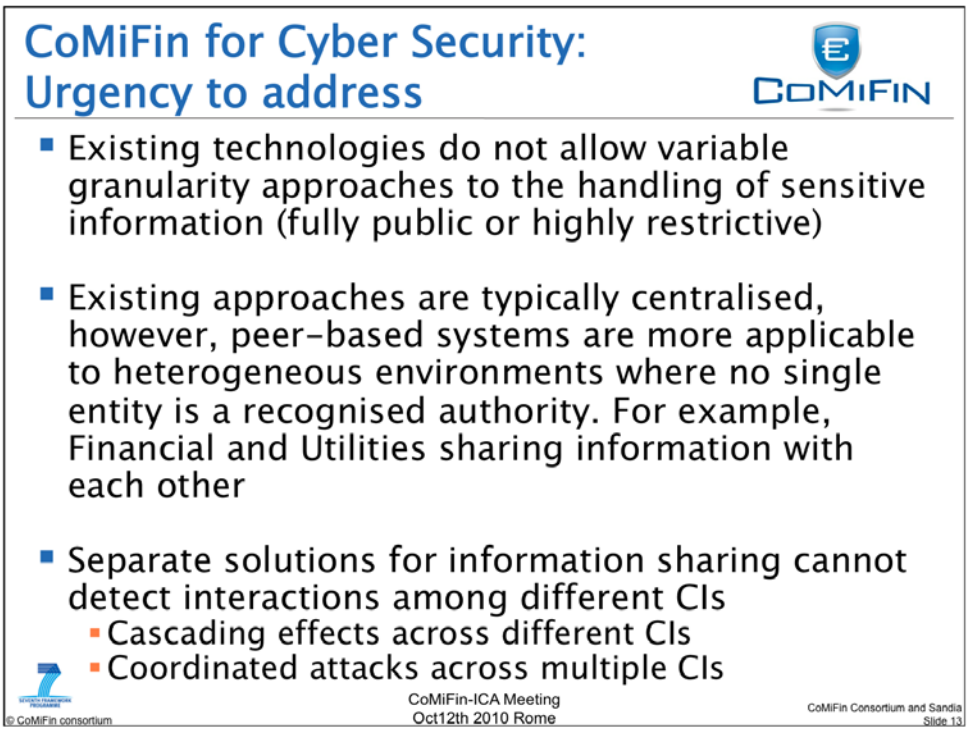

Modeling individual benefits of CoMiFin adoption
CoMiFin
Benefit to the Next FI
Fraction of Participating FIs
With a given participation, how much does a FI gain if it joins CoMiFin?
CoMiFin platform can demonstrate value from near-real-time benefits of information sharing
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 8


Modeling CoMiFin Adoption: other interesting aspects
CoMiFin
Modeling how FI will use CoMiFin
Develop benchmarks and a test-bed for information sharing
Develop models of the CoMiFin network
Identify information flows
Create models of the "normal" behaviour of the CoMiFin network
Create model for detecting insider attacks
Trust
Adapt old trust models to new automatic, computer based information exchange
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 9

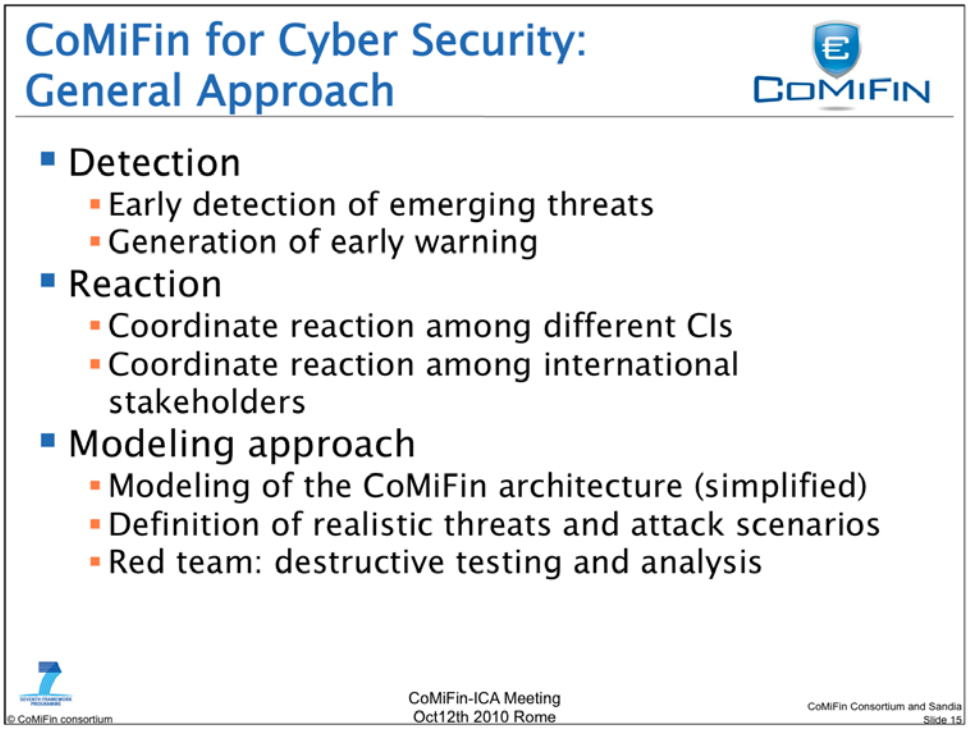

Modeling Adoption: Initial Approach
CoMiFin
Rough cut of basic model
Sandia will approximate CoMiFin information sharing mechanisms and policies
Refinement: requires active collaboration
Subject matter experts (CoMiFin consortium, Financial Advisory Board, risk experts) to help conceptualise the model
'Repast' http://repast.sourceforge.net/
Possible community project
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 10


Collaboration Models for large scale Critical Infrastructures: research challenges and applications
Generalization of the CoMiFin approach to global Cyber Security scenarios
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 11


CoMiFin for Cyber Security: Technical motivations
General applicability of the CoMiFin architecture
designed to cope with the hard requirements of the financial domain, can be adopted by other existing Critical Infrastructures (CIs)
The need for information sharing exist in all CIs
CoMiFin can improve and complement existing information sharing approach
CoMiFin can enable cross-domain information sharing among different CIs
Synergies between different CIs can be modeled as interactions between Semantic Rooms
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 12


CoMiFin for Cyber Security:
Urgency to address
CoMiFin
Existing technologies do not allow variable granularity approaches to the handling of sensitive information (fully public or highly restrictive)
Existing approaches are typically centralised, however, peer-based systems are more applicable to heterogeneous environments where no single entity is a recognised authority. For example, Financial and Utilities sharing information with each other
Separate solutions for information sharing cannot detect interactions among different CIs
Cascading effects across different CIs
Coordinated attacks across multiple CIs
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 13


CoMiFin for Cyber Security:
International cooperation
CoMiFin
International cooperation is needed
Cyber security is one of the three main thrusts in Sandia
Joint modeling effort will:
Exploit the ability to bring together diverse stakeholders, for example, different utilities
Allow for effective detection of modern cyber-threats, that do not respect national boundaries
Allow to model the effects of coordinated and international reaction
Joint modeling experience of SANDIA and COMIFIN people could be used to create a model based description of attacks
Helpful in an increased attack detection rate
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 14


CoMiFin for Cyber Security:
General Approach
CoMiFin
Detection
Early detection of emerging threats
Generation of early warning
Reaction
Coordinate reaction among different CIs
Coordinate reaction among international stakeholders
Modeling approach
Modeling of the CoMiFin architecture (simplified)
Definition of realistic threats and attack scenarios
Red team: destructive testing and analysis
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 15

2. ORGANIZATIONAL, SOCIAL, TECHNOLOGICAL ASPECTS FOR INFORMATION SHARING ENVIRONMENTS

In this section, we include the slides CoMiFin and Sandia research groups have produced during the working session and that summarize the main points of the discussion concerning the second research area introduced in the executive summary of this report, i.e., organizational, social, technological aspects for information sharing environments. As it can be noted by the slides below, the following initial CoMiFin-ICA objectives are addressed in the brainstorming of the working session within this research line; namely *provide a description of the behavior of single Financial Institution (FI) nodes and the result of interaction among the nodes, simulate the behavior of the interconnected FIs to face extraordinary situations,*

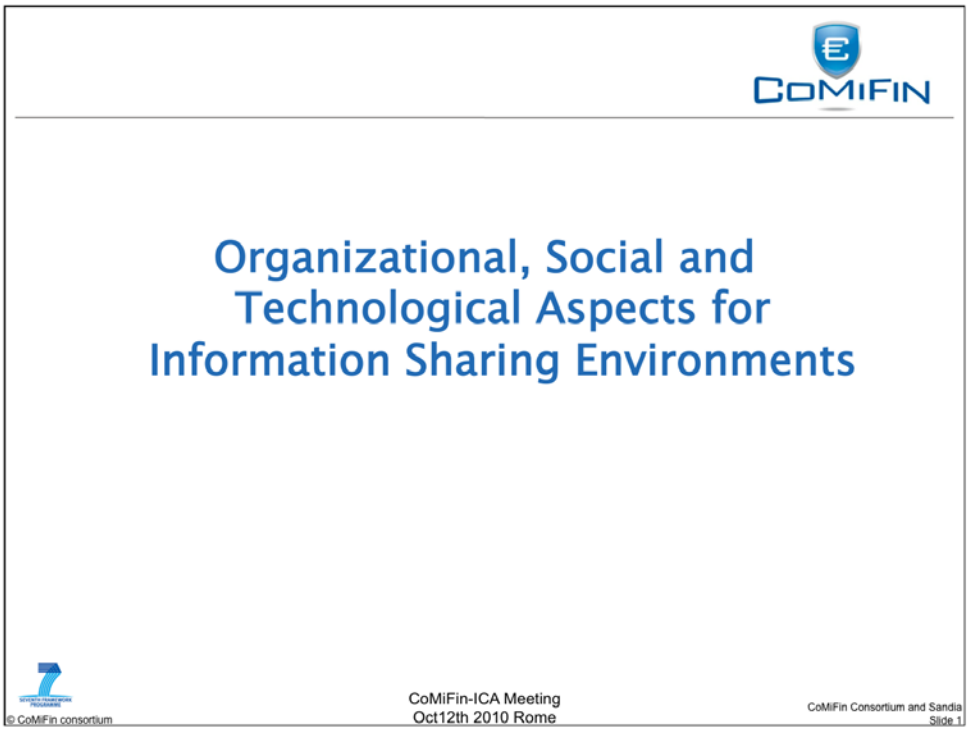
To this end, the discussion focused on the *network analysis* of financial ecosystem (i.e., understand who are all the actors of the system and who is talking to whom) and the *level of adaptation* of the CoMiFin system in order to face new emerging and more complex threats in the financial domain.

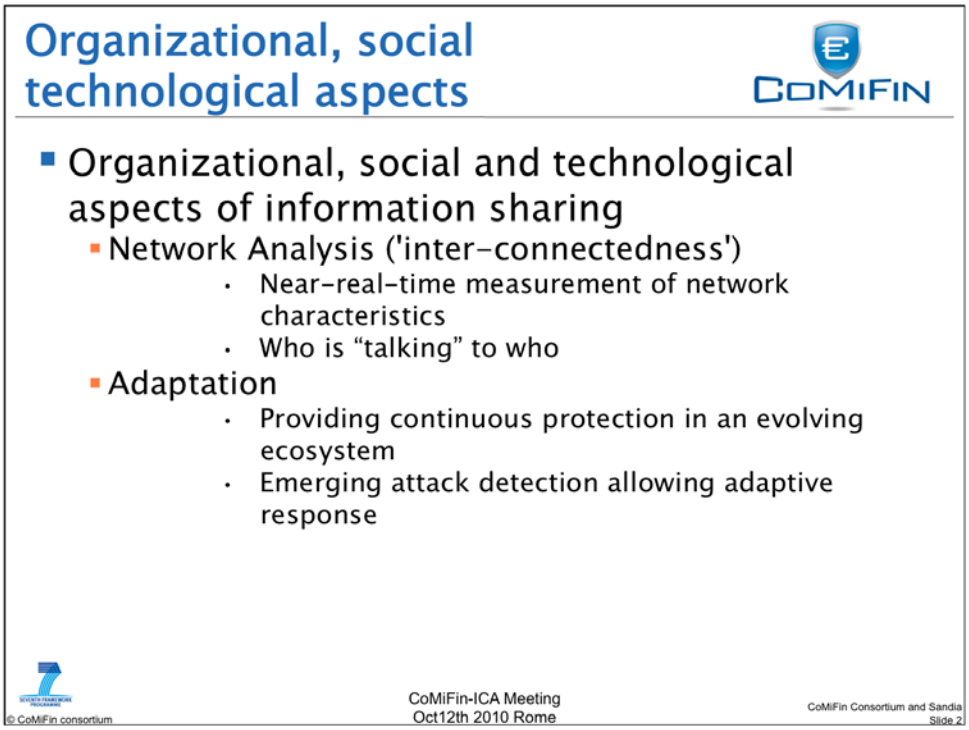
2.1 Principal outcomes with respect to the CoMiFin-ICA objectives

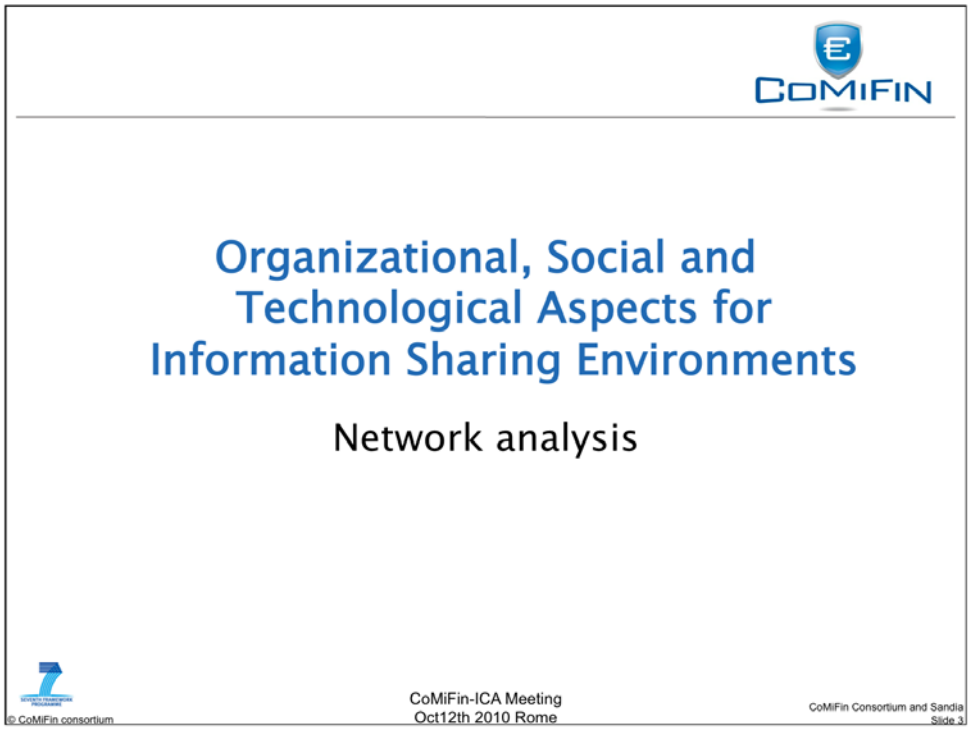
The main *outcomes* produced during of the working session can be summarized in the following:

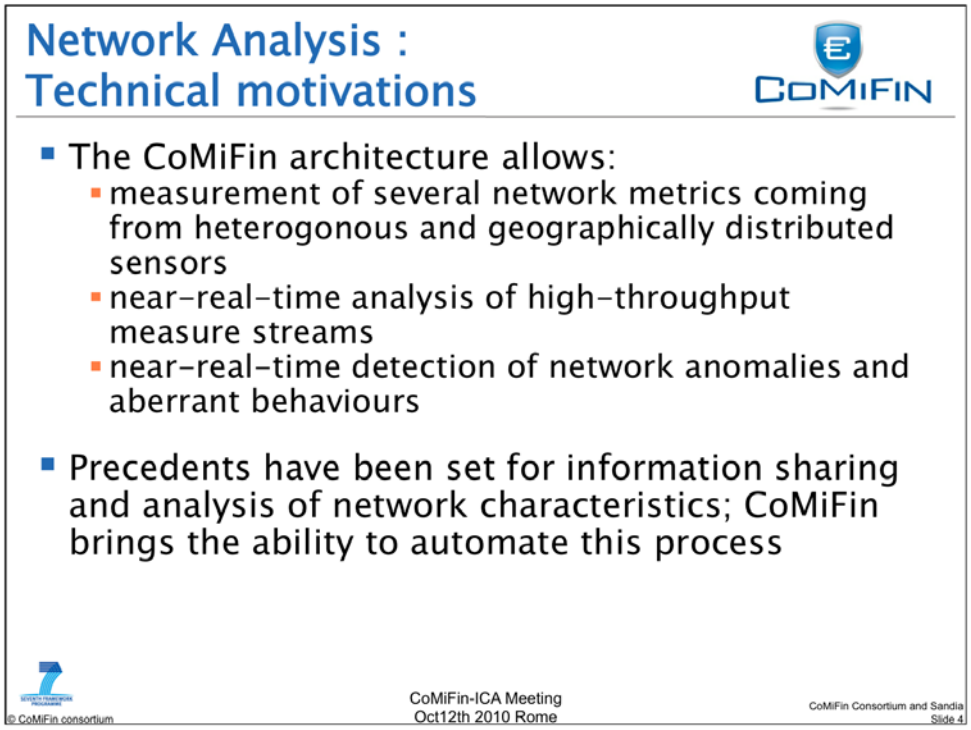
1 analyzing the network of the actors in the financial ecosystem allows us to enrich the information provided to the system, thus potentially augmenting (i) the accuracy of the detection of the attacks, (ii) the possibility to detect new threats, and (iii) the flexibility of CoMiFin's trust score model currently available in the fist prototype;

2 advanced adaptation mechanisms in addition to the basic ones already provided by the CoMiFin system can be particularly beneficial in order to face extraordinary situations in which more complex threats occur and need to be promptly detected in order to mitigate the damages they can cause.


CoMiFin
Organizational, Social and Technological Aspects for Information Sharing Environments
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 1


Organizational, social technological aspects
CoMiFin
Organizational, social and technological aspects of information sharing
Network Analysis ('inter-connectedness')
Near-real-time measurement of network characteristics
Who is "talking" to who
Adaptation
Providing continuous protection in an evolving ecosystem
Emerging attack detection allowing adaptive response
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 2


CoMiFin
Organizational, Social and Technological Aspects for Information Sharing Environments
Network analysis
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 3


Network Analysis : Technical motivations
CoMiFin
The CoMiFin architecture allows:
measurement of several network metrics coming from heterogonous and geographically distributed sensors
near-real-time analysis of high-throughput measure streams
near-real-time detection of network anomalies and aberrant behaviours
Precedents have been set for information sharing and analysis of network characteristics; CoMiFin brings the ability to automate this process
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 4

Network Analysis : Urgency to address

- Network analysis provides out-of-band intelligence that can be used to enrich information provided explicitly to the system
  - Increases detection accuracy
  - Enables detection of new threats
- Intelligence gathering and analysis of network characteristics can provide insights into impact of attacks on CI and the potential for cascade scenarios to emerge

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 5

Network Analysis : International cooperation

- International cooperation is needed
- The Internet is a global architecture
- The financial "social" network is global
- CERTs only provide monitoring and response at a national level
  - This information needs to be shared among shareholders
  - Currently, there is no central authority for the management of this information
  - A peer-based approach (such as CoMiFin) would be more acceptable

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 6

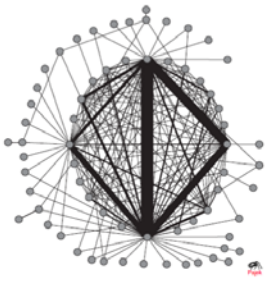
Main benefits of Network Analysis

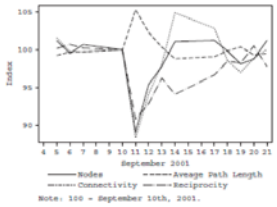
- Inferring traffic patterns for non-members of CoMiFin
  - By aggregating the views of CoMiFin members
  - Learning from them and feeding that information into CoMiFin
  - Automatic adjustment of trust levels
  - Automatic tuning of thresholds
- Detect strong perturbations (abnormal patterns) with respect to the normal network behaviour
  - Early detection of aberrant behaviour
  - Correlation of anomalies may allow root-cause analysis
- If the system is adopted, over time you can start looking for precursors

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 7

Network Analysis Example

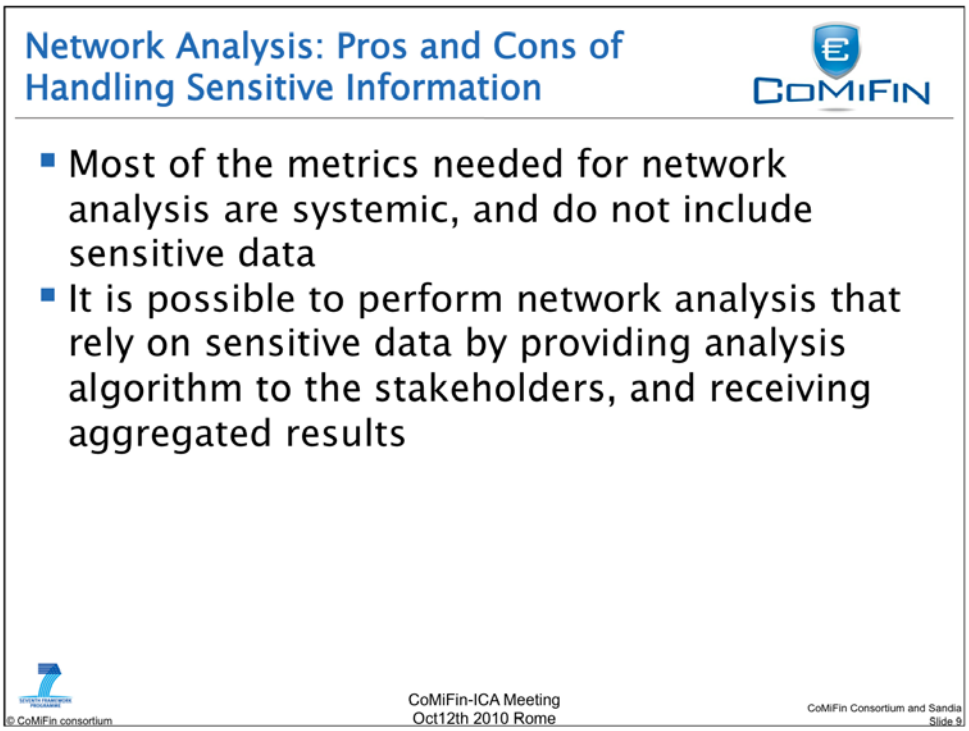
- Example network analysis: payment systems
  - network of payment system transactions shows a fully connected and strongly interdependent kernel
  - Network measures in time over perturbation 9-11 show strong response

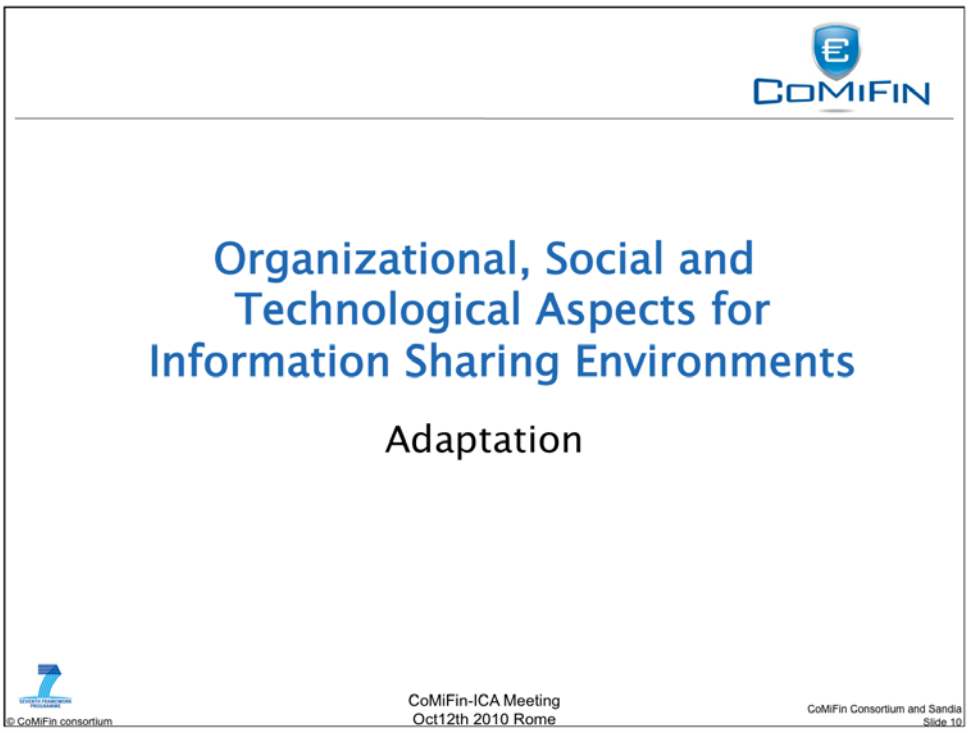




Soramaki et al., Physica A, 379 (2007) 317-333

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 8


Network Analysis: Pros and Cons of Handling Sensitive Information
CoMiFin
Most of the metrics needed for network analysis are systemic, and do not include sensitive data
It is possible to perform network analysis that rely on sensitive data by providing analysis algorithm to the stakeholders, and receiving aggregated results
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 9


CoMiFin
Organizational, Social and Technological Aspects for Information Sharing Environments
Adaptation
© CoMiFin consortium
CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 10

Adaptation : Technical motivations

- The CoMiFin architecture is designed to allow basic adaptation
- Unique expertise of combined Sandia-CoMiFin personnel allows for exploration of novel approaches to adaptation for the detection of emerging threats

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 11

Adaptation : Urgency to address

- Threat development and evolution is outpacing existing mitigation strategies (arms race)
- More complicated attacks are predicted to emerge using composite exploits and vectors (the attackers are winning)
- Adaptive systems are required to keep pace

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 12

Adaptation : International cooperation

- International cooperation is needed
- Advanced Persistent Threats (APTs) are a global issue
- Such a difficult problem requires an international effort to address (defense against cyber terrorism)
- Unique Sandia expertise in modeling CASoS (Complex Adaptive Systems of Systems)

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 13

Initial adaptation approach in CoMiFin

- Fine tuning parameters of detection algorithm implemented by the Semantic Room
  - Detection thresholds
  - Trust levels
- Changing characteristics of gateway level configuration
  - Levels of aggregation filtering
  - Anonymization (within constraints of SR contract)

CoMiFin-ICA Meeting
Oct12th 2010 Rome
CoMiFin Consortium and Sandia
Slide 14

Genetic adaptation approach in CoMiFin

- AI approach to evolving CoMiFin system: Genetic Algorithms can be used for this purpose
  - It can be considered as a future research challenge
- The SLA characteristics define the 'genetic pattern' of an SR
- Machine assisted learning to identifying and refining successful 'genes'; an SR is the sum of its parts
- Automated generation of SRs will allow near-real-time response to emerging threats
  - Weak SRs are allowed to die
  - Healthy SRs thrive and form the basis of the next generation

CoMiFin-ICA Meeting
Oct12th 2010 Rome

Slide 15

CoMiFin as a CASoS

- Need for modeling of the adaptive features in CoMiFin
- Effect of CoMiFin (sub?)-system on the entire system
- Feeds back to 'Adoption' of system; an adaptive response to evolving threats leads to promoting resilience
- Complex adaptive systems: Complexity vs Robustness
  - Carlson and Doyle "Highly Optimised Tolerance" (HOT)
  - Investigate CoMiFin robustness in case of faults/ attacks that were not considered when designing its own fault-tolerance methods

CoMiFin-ICA Meeting
Oct12th 2010 Rome

Slide 16

3. CONCLUSIONS

The next CoMiFin-ICA workshop and working session will be held in US at the Sandia Laboratories premises. The outcomes obtained by the international collaboration on the research aspects explained in the slides of the previous sections will be discussed in that occasion and described in the upcoming CoMiFin-ICA deliverables.

3.1 Possible issues to be faced in future CoMiFin-ICA working sessions

The two research groups have also identified possible issues in dealing with the research aspects previously summarized. From this analysis it turned out the following: although introducing more complex adaptation mechanisms in the CoMiFin system, based on a genetic approach, can be highly effective in terms of capabilities of the CoMiFin system to timely react to new emerging threats, it can be very challenging to develop in the remaining part of the project. The lack of full expertise in such a research area of the CoMifin group and the tight time remaining till the end of the project brought the two groups to consider these aspects as possible future extensions of the CoMiFin project itself. However, it is worth noting that these aspects, and their applicability to the current CoMiFin system, will be further discussed and analyzed in the upcoming CoMiFin-ICA working session.