A Protection Profile for Secure Information Sharing Among Critical Infrastructures

SRC'10
5th edition of the European Security Research Conference

Matthieu Aubigny[1] , Carlo Harpes [1].

1: [aubigny, harpes]@itrust.lu

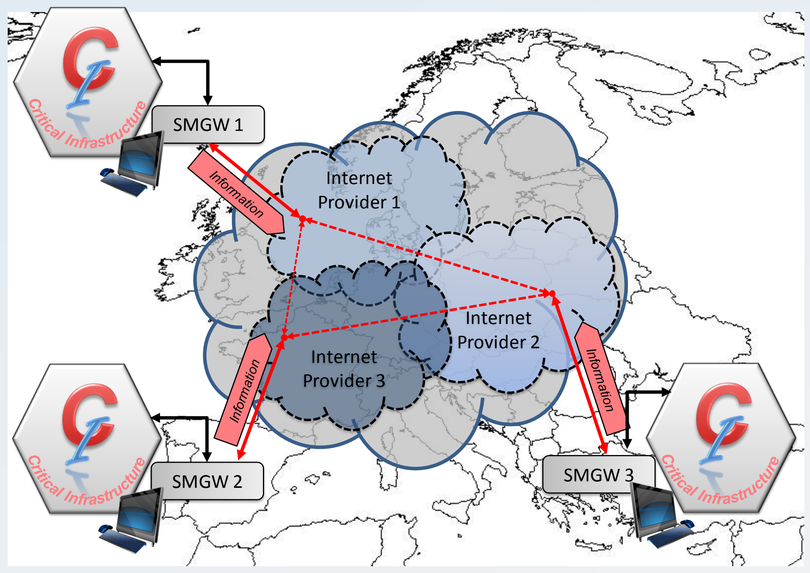
Context

Critical Infrastructures (CIs) have to ensure the highest possible security levels despites multiple dependencies, from technology or related, inter sector or cross sector CI. They need to be prepared to continue their duty in case of failures. To reach this objective, CIs should exchange relevant information on their own risk in order to avoid risk cascading. This has led to the main goal of the FP7 ICT-SEC project **MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures**): the design and implementation of a real-time CI risk level prediction and alerting system. To allow relevant information to be shared, the MICIE project has defined a specific interface, called Secure Mediation Gateway (SMGW).
This poster presents security requirements on the SMGW, designed according to the ISO/IEC 15408, and open issues for practical implementation.

Information Sharing in MICIE project

Aims of MICIE:

- Deployment of risk related information sharing among European CIs to predict risk level of CIs and avoid risk cascading phenomena
- Use of a specific interface called Secure Mediation GateWay (SMGW);
- Use of untrusted networks to provide communication channel between CIs (e.g. Internet);
- High level of confidentiality, integrity, availability, and reliability.

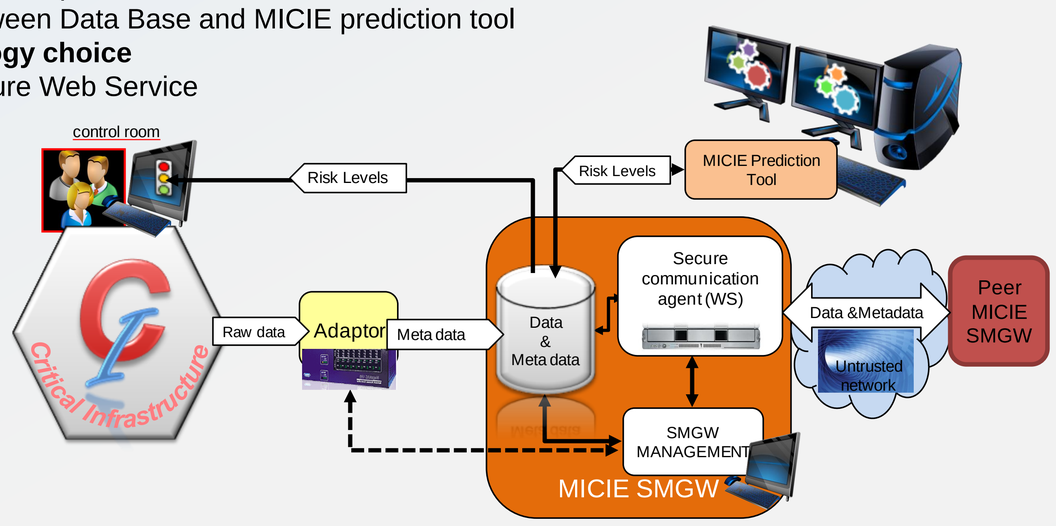


Interfaces:

- Between CI and Data Base
- Between peer SMGW
- Between Data Base and MICIE prediction tool

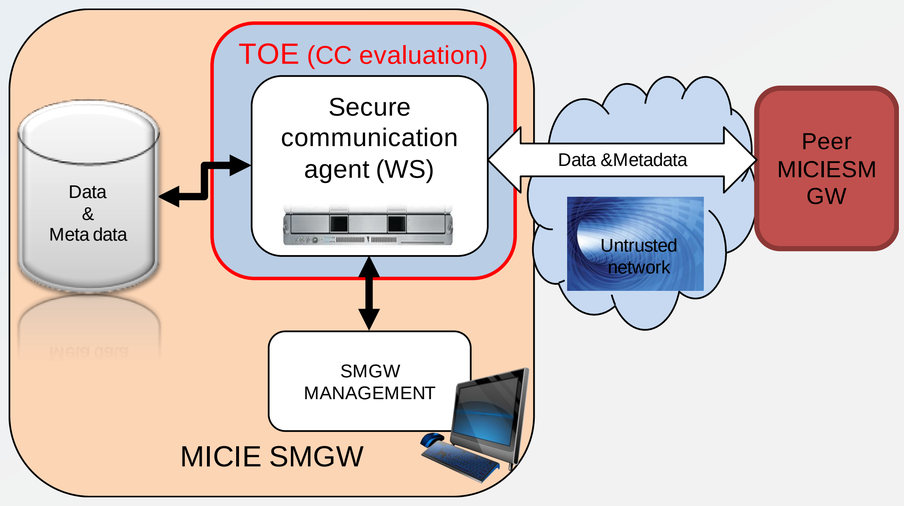
Technology choice

- Secure Web Service



Target of Evaluation Overview

The target of evaluation is the interface with the external environment of the operator: the Secure Communication Agent (SCA) based on Web services



Usage and major security features of the TOE:

- Collect risk related information from, and broadcast to peer CI operator via open networks.
- Ensure confidentiality, integrity, availability or risk related information.

Protection Profile

TOE Description: The SCA based on Web services and its interfaces:

1. with the unsecured network (internet) to communicate with peer SMGW;
2. with the Data Base used by the prediction tool and the CIs data adaptor;
3. with the SMGW management system (policy, audit, supervision…).

Assets - Two classes

- Shared information, like risk related data to share and general information about the CI topology.
- The ToE and its configuration itself.

Assumptions – only two:

- Administrator non hostile,
- protected physical access to TOE

Threats – 8 in three types

- Threats on communication, i.e. interception of admin. command or of messages.
- Threats on keys management
- Threats on security policies and their security contexts

Security Objectives [SO] – 17 SO in three types

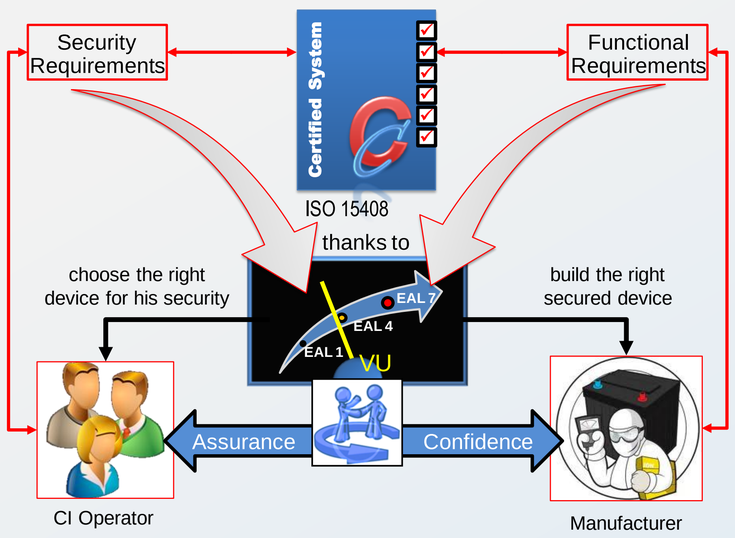
- **SO for services** delivered by the TOE: Management of the TOE, Confidentiality and integrity of data exchanges and of data topology
- **SO for the TOE**: identification and authentication of users or administrators, management of security policy, detect replay messages, use appropriate cryptography and protect keys.
- **SO for the operational environment**: trusted administrator, secure environment administration, protection of physical access., secure keys generation.

40 Functional Requirements: to reach the identified SO:
Security Alarms, Audit data generation, User identity association, Potential violation analysis, Enforced proof of origin, Enforced proof of receipt, Cryptographic key generation, Cryptographic key distribution, Cryptographic key destruction, Cryptographic operation, Complete access control, Security attribute based access control, Basic Data Authentication, Complete information flow control, Simple security attributes, Import of user data with security attributes, Basic internal transfer protection, Full residual information protection, Basic data exchange confidentiality, Data exchange integrity, Authentication failure handling, User attribute definition, User authentication before any action, User identification before any action, Management of security functions behaviour, Management of security attributes, Secure security attributes, Static attribute initialisation, Management of TSF data, Specification of Management functions, Security roles, Anonymity, Failure with preservation of secure state, Inter-TSF confidentiality during transmission, Inter-TSF detection of modification, Notification of physical attack, Replay detection, Reliable time stamp, TSF Testing, Inter-TSF trusted channel, Trusted path

Benefits of ISO 15408

The standardised approach allows:

- Choosing security objectives and assumption to cover identified treats.
- Designing Security Functional Requirements to cover objectives.
- Certifying that the SMGW is secure if operated in the conditions it has been designed for.
- Providing confidence to manufactures that the device is secure enough.
- Allows operators to trust in the security of a given device.



Conclusion

Our work describes a preliminary research results of the FP7 ICT-SEC MICIE project. MICIE intends to develop a real-time risk related information sharing and alerting system.

A system architecture based on a Secure Mediation Gateway has been presented. This SMGW allows heterogeneous CI to securely and timely communicate relevant data to predict in advance how local failures, threats, malfunction, adverse events can affect the operative level of interconnected CIs.

To define security requirements of the SMGW and prepare implementation, a protection profile has been defined for the communication agent. This PP defines 40 Security Functional Requirements.

We suggest pursuing the determination of security functional requirements for the other vulnerable parts of the MICIE system, i.e. the adaptor and the prediction tool according to ISO 15408 or ISO 19791 (used for operational system). These are the next steps to realise a certified system of risk information sharing for European CIP.

Acknowledgement
The research leading to these results has received funding from the European Community's Seventh Framework Programme FP7/2007-2013 under grant agreement n° 225353 also referred as MICIE.

For more information:
http://www.itrust.lu/
http://www.micie.eu

European Commission
Information Society and Media