Funded by the European Commission
Seventh Framework Programme

CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Information Exchange

Author(s): Olga Segou (NCSRD), Isidoros Monogioudis (HMOD)

CC RG-51 - Secure Signed Documents
CT RG-52 - Secure Signed Documents
CC RG-52 - Secure and Interoperable EDI
CT RG-82 – How to engage operators/exchangers in information exchange
CC RG-34 and CT RG-34 - Data mining for fraud detection
CT RG-53 - Data analysis and Intelligence in customs brokerage
CT RG-54 - Early detection of supply chain attacks

ABSTRACT

Electronic Data Interchange (EDI) is the process of electronic communication of formatted, structured data (documents, invoices, etc.). Through EDI, document and information exchange can be more secure and easy to monitor. Use of EDI can thus help combat crime such as fraud, tax evasion etc. Furthermore, there is an increased need for interoperable EDI that is certified to handle classified or sensitive material, often needed for information between law enforcement agencies, government, etc.

Although there is a multitude of Electronic Data Interchange solutions available in the market, they are based on a variety of different standards leading to a lot of fragmentation and thus creating barriers in the adoption of this technology. A multitude of businesses or organisations that require paper document handling fail to adopt EDI or are unwilling to change business processes. Furthermore, the cost of the initial setup of EDI solutions, the multitude of different standards and the cost of training employees to a new process also hinder the adoption of EDI. Thus, there is a pressing need for interoperable, easy to use and easy to deploy EDI solutions, for a variety of different stakeholders ranging from small business owners to government to military etc.

RESEARCH ACTION #1

Harmonization of information exchange including sensitive and classified across public, military, private and academic sector.

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: 2 **STREP + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **42 months**
ACTORS: **government, law enforcement, customs, border guard, military, IT security industry, high-tech industry, research/academia**

Information exchange is a critical factor for effective cyber security. Actionable information can be used by organizations to enhance their security measures, update their controls and protect by threats that have been recognized and identified elsewhere.

This saves time and effort and contributes to the improvement of the overall security posture. However, it is quite usual that such information falls under classification or sensitiveness rules that prevent further sharing with relevant stakeholders.

Specific operational requirements and communication channels have to be established in order to facilitate the information exchange process, overcome unnecessary approval constraints, and at the same protect any unintentional disclosure.

An official framework should be developed describing the specific content and context of cyber security information that needs to be shared across all relevant national and international stakeholders.

RESEARCH ACTION #2

Combating fraud and theft in freight transport and customs brokerage

DISTANCE TO THE MARKET: **TRL 5-7**
COST OF THE TOPIC: **2 STREP + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **government, law enforcement, customs, border guard, IT security industry, freight forwarders, customs brokers, research/academia**

Freight transport within and across borders is a vital part of modern economy. The high value of transported cargo makes freight forwarders an attractive target for cybercriminals who use illicit techniques and tools to enable crimes such as cargo theft, customs fraud, excise or VAT fraud, smuggling etc.
Furthermore, transporting cargo through international borders requires clearing through customs. The massive amount of documents and data that are processed through customs can lead to errors in handling and loss of revenue for importers/exporters who are fully exposed to this risk. Monitoring the vast amount of documents to detect suspected cases of fraud or smuggling, is a very difficult task and not sufficiently automated.

Thus, customs are vulnerable to ransomware and DDOS attacks that can disrupt normal operations and require intelligent, secure and interoperable solutions to handle and authenticate massive amounts of documents. Freight forwarders are often the victims of identity theft leading to cargo high-jacking, fuel fraud etc.

This action aims to combat cybercrime in freight transport by:

- Providing tools to prevent and detect identity theft,
- Providing tools to prevent and detect document forgery,
- Providing interoperable and mobile Electronic Data Interchange solutions and promoting their adoption,
- Enabling Real-time cargo tracking across different transport modalities,
- Introducing improved data analysis and intelligence in customs brokerage, and
- Ensuring that information flow is safe, secure and uninterruptible.