FINSTIX: A Cyber-Physical Data Model for Financial Critical Infrastructures

Giorgia Gazzarata\textsuperscript{1,2(✉)}, Ernesto Troiano\textsuperscript{3}, Luca Verderame\textsuperscript{1,2}, Maurizio Aiello\textsuperscript{1,2,3,4}, Ivan Vaccari\textsuperscript{1,4}, Enrico Cambiaso\textsuperscript{4}, and Alessio Merlo\textsuperscript{1}

\textsuperscript{1} Department of Informatics, Bioengineering, Robotics and System Engineering, University of Genoa, Genoa, Italy
\textsuperscript{2} Consorzio Interuniversitario Nazionale per l’Informatica, Catania, Italy
\{giorgia.gazzarata,luca.verderame\}@dibris.unige.it
\textsuperscript{3} GFT Italia S.r.l., Genoa, Italy
ernesto.troiano@gft.com
\textsuperscript{4} Consiglio Nazionale delle Ricerche, IEIIT Institute (CNR-IEIIT), Genoa, Italy
\{ivan.vaccari,enrico.cambiaso\}@ieiit.cnr.it

Abstract. Cyber-physical security of financial institutions is a critical and sensitive topic. In this context, the FINSEC project aims to design and build a reference architecture for the integrated physical and cyber security of financial institutions. To make feasible, the interactions among the different services of the FINSEC platform, a proper data model defining the exchanged information semantic is fundamental. One of the objectives of the FINSEC project is to integrate cyber and physical security measures in the financial services industry. To do so, the data model must consider both cyber and physical systems. In this paper, the authors present FINSTIX, namely the data model adopted in the FINSEC platform. In particular, they extended the Structured Threat Information eXpression (STIX) standard creating custom objects to describe the financial organization’s infrastructure and then to integrate cyber and physical security measures. The paper also reports an example of the use of FINSTIX in a relevant use case scenario.

Keywords: Data model · FINSEC · STIX · Cyber-Physical Threat Intelligence

1 Introduction

In the last few years, the number of cybersecurity incidents against financial institutions has been kept growing. According to the CLUSIT (the Italian association for cybersecurity) 2019 report, the number of financial attacks has increased by 33% from 2017 to 2018\textsuperscript{1}, thereby underlining how financial institutions are a primary target for cyber-attacks nowadays. This is mainly due to the growing sophistication of the IT technologies and the complex processes involving

\textsuperscript{1} The report is available at the following link: https://clusit.it/pubblicazioni/.

© Springer Nature Switzerland AG 2021
H. Abie et al. (Eds.): CPS4CIP 2020, LNCS 12618, pp. 48–63, 2021.
https://doi.org/10.1007/978-3-030-69781-5_4
multiple organizations. It is clear that financial institutions must increase their robustness against attack vectors. To deal with such a problem, the European Commission funded the Integrated Framework for Predictive and Collaborative Security of Financial Sector (FINSEC)\(^2\) as an H2020 project. FINSEC aims to design and build a reference architecture for integrating physical and cyber security of financial institutions: in fact, in the financial services industry, cyber and physical security measures usually act in isolation, thus entailing inaccurate vulnerability assessment and risk analysis and, in general, poor-quality security guarantees.

Beyond architecture design, the definition of the semantic used to represent the information inside the FINSEC platform was one of the most demanding tasks. A proper data model is fundamental to:

- Enable the interactions between the FINSEC platform and third parties;
- Enable the interactions among the different services within the FINSEC platform;
- Provide the FINSEC services with a sufficiently fine-grained information granularity: in fact, too coarse-grained data may not be sufficient to support the activities of the services, while too fine-grained data may reveal to be unmanageable in actual cases;
- Enable the integration of cyber and physical security measures.

In this paper, the authors present the data model used by the FINSEC platform.

2 Background

2.1 FINSEC Reference Architecture

As shown in Fig. 1, the FINSEC core platform consists of different services divided into three distinct tiers:

- Edge Tier: it receives input data from the external probes and carries out activities on the probes, upon request from the upper layers. The probes are systems that collect and produce security information and events related to the organizations physical and cyber assets. Example of probes are logs, Security Information and Event Management (SIEM) systems, Closed Circuit Television (CCTV) systems and Simple Network Management Protocol (SNMP) agents;
- Data Tier: it stores information coming from the other tiers of the FINSEC platform or from external Cyber Threat Intelligence (CTI) sources;
- Service Tier: it contains the kernel applications and exposes the FINSEC functionalities to external parts. It consumes the information stored in the Data Tier.

\(^2\) https://www.finsec-project.eu.
More details about the Reference Architecture are available in Deliverable 2.5 - “FINSEC Reference Architecture - II”\(^3\). In Sect. 3.1, the authors will present a practical example of the use of FINSTIX on a real use case scenario. There, the following architectural components will be considered:

- **Probes**: devices adopted in the financial field to collect cyber-physical information (e.g., CCTV probe, syslog probe, SIEM probe);
- **Data Collector**: collects data generated by the probes. Before storing them in the Data Layer, the Data Collector sanitizes data to remove eventual pieces of information violating the GDPR (personal references, etc.);
- **Anomaly Detection**: service that monitors events produced by the FINSEC probes in order to correlate them according to the models of attacks stored in the Data Layer as FINSTIX “x-attack”;
- **Mitigation Service**: service aimed to generate information that will be used to mitigate the attack detected by the Anomaly Detection;
- **Mitigation Enabler**: service acting on the field level to send notifications and to provide the probes with mitigation actions: some situations will require an active response of the platform onto the assets, such as locking a rack under attack, or shutting down a server that is threatened by a cyber attack.

\(^3\) [https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ce3a941d&appId=PPGMS.](https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ce3a941d&appId=PPGMS)
2.2 STIX - Structured Threat Information eXpression

The Structured Threat Information eXpression (STIX) standard is a language and serialization format used to exchange CTI [4]. In particular, it was designed to support four use cases:

- Analyzing Cyber Threats;
- Specifying Indicator Patterns for Cyber Threats;
- Managing Cyber Threat Response Activities;
- Sharing Cyber Threat Information.

STIX is a trademark of the MITRE Corporation, but it has been transitioned to OASIS, aiming to foster both the development of STIX and its adoption. STIX defines two kinds of objects: the STIX Domain Objects (SDOs) and the STIX Relationship Objects (SROs)\(^5\). The SDO corresponds to domain concepts commonly used in CTI, while the SROs are the relationships between the SDOs. From a graph standpoint, the SDOs are the nodes, while the SROs are the edges, as shown in Fig. 2.

![Fig. 2. SDOs and RDOs can be seen respectively as nodes and edges of a graph.](image)

In STIX 2, SDOs and SROs are represented in JSON. More information on SDOs and SROs are available in the specification STIX™ Version 2.0. Part 2: STIX Objects\(^6\). The STIX standard enables customization by two different means: custom properties and custom objects. The first one consists in adding properties not defined by the specification to existing SDOs, while the second one consists in creating brand new objects. Independently from the customizations, STIX defines a set of requirements that must be enforced to preserve the conformity with the standard. For a description of such requirements, we refer the interested reader to the STIX™ Version 2.0. Part 1: STIX Core Concepts specification\(^7\).

---

\(^4\) STIX Use Cases web page, [http://stixproject.github.io/usecases/](http://stixproject.github.io/usecases/).

\(^5\) STIX web page, [https://oasis-open.github.io/cti-documentation/stix/intro](https://oasis-open.github.io/cti-documentation/stix/intro).

\(^6\) STIX™ Version 2.0. Part 2: STIX Objects, [http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html](http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html).

\(^7\) STIX™ Version 2.0. Part 1: STIX Core Concepts, [http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html](http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html).
2.3 State of the Art on the Use of STIX

CTI is a holistic approach to the automated sharing of threat intelligence [5]. Nowadays, it is considered one of the most promising strategies in the cybersecurity topic [10]. In the CTI context, [32] propose a classification and distinction among existing threat intelligence types. [16,23] instead summarize and compare the most prevalent information-sharing models adopted. Similarly, [24,27] propose a survey of the current platforms and formats available for threat information sharing. There are indeed different CTI formats available, like OpenIOC [15], Trusted Automated eXchange of Indicator Information (TAXII) [10,16], Real-Time Inter-network Defense (RID) [13,16], Incident Object Description Exchange Format (IODEF) [5,25]. Among the available CTI formats, Structured Threat Information Expression (STIX) [10] is considered the most commonly used CTI standard [29], although CyBOX and TAXII are considered good alternative solutions [7]. STIX provides a modular format that can also efficiently incorporate other standards [5].

STIX is adopted in different contexts of different nature. In this context, [18] adopts STIX as an input format for analyzing data for machine learning algorithms to increase new threat detection ability and responsiveness. In addition, [28] presents an innovative approach to automatically generate Cyber-Threat Intelligence data as STIX documents, starting from raw threat data. [19] adopts STIX to share threats and security information in IoT contexts, while [6,22] make use of a blockchain-based system to share CTI data using STIX format. [1] proposes an industrial adoption of STIX to exchange information between Integrated Management System (IMS) and Security Information and Event Management systems (SIEM). [20] presents an alternative use of STIX, to describe the actual state of the reference system, instead of exchange attack information. [34] presents a collaborative platform to share cyber threat information using STIX by focusing on anonymity exploitation. [26] makes use of STIX for threat information inputs, combining it with other similar information sources to develop a collaborative cognitive system, able to detect threats by combining different collaborative agents, covering both host and network information. Also, [11] combines STIX concepts with Markov chains ones, for cyber threats modeling. [9] proposes a cyber threat protection solution based on a Threat Intelligence Platform (TIP), based on both STIX and TAXII. Instead, [8] proposes MANTIS, a threat intelligence platform that makes use of different standards for threat data correlation, accomplished through a novel similarity algorithm. [17] proposes CyTIME, a framework that integrates CTI data like STIX under a global JSON format and automatically generates network security rules from the incorporated data seamlessly. Another innovative framework is proposed in [35], making use of STIX to exchange information about detected incidents, generated alerts, and applied mitigations. [14] introduces STIXGEN, a framework based on STIX able to generate meaningful, properly placed and error-free structured data. Although it is widely used, STIX presents different limitations: [3] analyses STIX by detailing the advantages and limitations of the format. STIX is indeed considered very complex to implement [16] and its
limits include the lack of support to reasoning [31]. In virtue of this, different extensions of STIX are proposed: UCO: A Unified Cybersecurity Ontology is a semantic-based alternative of STIX [31]. Also, [7] proposes some extensions of STIX, while [33] extends it to support the inclusion of relevant attack details on sophisticated attacks through the description of complex patterns. Similarly, while [30] extends STIX to support network and security events, [36] proposes a STIX extension to integrate and support additional cyber threats. Such extension is used in ChainSmith, a system able to extract Indicators of Compromise (IOC) by analyzing technical articles and industry reports.

The proposed work represents an extension of STIX in the fintech context. FINSTIX represents an innovative extension of STIX that considers both the cyber and the physical domain, thus modeling the entire financial infrastructure. Indeed, FINSTIX describes information like organization assets, how they are inter-connected, or monitoring probes and event types.

3 FINSTIX Cyber-Physical Data Model

Thanks to its expressiveness, flexibility, and extensibility, STIX is surely one of the most famous industrial standards used to represent and share Cyber Threat Intelligence. By the way, it has two weaknesses that prevent to use it as it is for the FINSEC purposes:

- It does not provide for an accurate representation of the financial institution infrastructure;
- It does not envisage physical systems; it is just limited to the cyber ones.

For those reasons, an extension to STIX was inevitable. The FINSEC extension to STIX 2 was driven by the FINSEC project use cases, which caused the introduction of some custom objects, among them:

- **Organization**: FDO used to represent an organization;
- **Area of Interest**: logical or physical area, such as a server room. An area of interest can be part of an organization or can be a sub-area of another area of interest;
- **Asset**: an organization valuable asset, such as a PC, an ATM, an application, or whatever is crucial for the organization. It can also be part of another asset;
- **Probe**: monitoring infrastructure that generates events and/or observed data. It can be related to one or more sensors, CCTVs, etc. A probe monitors one or more areas of interest;
- **Event**: event produced by a probe. Events, observed data, assets model and external CTI are used by the Analytics/Predictive modules to produce Cyber-Physical Threat Intelligence;
- **Attack**: cyber-physical attack. Differently from the Attack Pattern SDO, it also considers physical attacks, thus enabling an integration among cyber and physical scopes. An attack can be a sequence or a concurrency of events;
– **Cyber-Physical Threat Intelligence (CPTI)**: the result of the analytic tools. One or more CPTI objects are used to generate the output of the intelligence process, which is a report about ongoing or possible future attacks on one or more assets belonging to the infrastructure. This object is still a work-in-progress.

The resulting data model was named FINSTIX (from **FINSEC-STIX**). All the domain objects defined in FINSTIX, including those already introduced in STIX, take the name of FINSTIX Domain Objects (FDOs). The introduction of the FDOs **Organization**, **Area of Interest**, **Asset**, and **Probe** is due to the poor granularity of the **Identity** SDO. Instead, FINSTIX presents an ontology for a hierarchical representation of the organization infrastructure. As a consequence, any part of the infrastructure can be referenced during the Cyber-Physical Threat Intelligence process performed by the FINSEC platform. The introduction of **Event**, **Attack**, and **CPTI** is motivated by the need to cope with both the cyber and the physical domains. In fact, STIX is adequate for Cyber Threat Intelligence, but not for Cyber-Physical Threat Intelligence. The details of every custom object are not discussed here for reasons of space; however, the description of the FDOs is available in Deliverable 3.9 - “Security Knowledge Base”\(^8\).

Every custom object introduced in FINSTIX contains all the mandatory keys defined by STIX. In addition, FINSTIX defines the following mandatory keys for all the custom objects:

- **domain**: it can be “Cyber”, “Physical”, or “Hybrid”;
- **datatype**: it can be “Model” or “Instance”. When **datatype** is “Model”, then the object is used to define a concept, such as an event, an attack, a countermeasure, etc. Instead, if **datatype** is “Instance”, the object is used to represent something that actually happened/is happening;
- **x_organization**: contains the identifier of the organization that owns the information. This key was introduced for multi-tenant applications, in order to avoid data disclosure. **x_organization** is also a custom parameter for the objects already defined by STIX;
- **reference**: is the identifier of the parent object. It is used to generate a hierarchy of objects;
- **model_ref**: when **datatype** is “Instance”, **model_ref** contains the identifier of the object used to define the specific concept. The latter has the same **type**, but its **datatype** is “Model”.

Most of the custom objects introduced by FINSTIX are used to describe the financial organization infrastructure. Figure 3 shows a graph representing the infrastructure of an imaginary bank, SuperBank. The latter has an indoor area, which includes the entrance area and the ATM area. The indoor, entrance, and ATM areas are modeled through **Area of Interest** FDOs. In the ATM area,

\(^8\) https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8e14437&appId=PPGMS.
there is an ATM, which is composed by a vault and a computer. The ATM, the vault, and the computer are modeled through Asset FDOs. Finally, there is the monitoring infrastructure, which consists of four probes:

- Entrance CCTV: monitors the entrance area;
- ATM CCTV: monitors the ATM;
- Screen CCTV: monitors the person in front of the screen of the ATM;
- Network probe: monitors the ATM computer.

Each probe is also conceived as an asset. For this reason, it is modelled through both a Probe and an Asset FDOs. In particular, the Probe FDO refers to the Asset FDO, which in turns refers to an Area of Interest or to another Asset. For example, the Probe ATM CCTV refers to the Asset ATM CCTV, which refers to the Asset ATM. A concrete example of the use of FINSTIX inside the FINSEC Platform is presented in Sect. 3.1.

![Diagram of FINSTIX Domain Objects](image)

**Fig. 3.** Hierarchy of FINSTIX Domain Objects describing the infrastructure of a financial institution.

Events and observed data produced by the organization probes are pushed into the FINSEC platform, which correlates and aggregates information gathered from asset models and external CTI through the machine learning analytics and prediction algorithms. The result of this process is the Cyber-Physical Threat Intelligence, which integrates important information coming from both the cyber
and the physical world. The CPTI produced in the FinTech sector is the added-value information produced by the FINSEC platform that could be exchanged (in-out) between financial organizations and security organizations (CERT/C-SIRT like). The integration between cyber and physical security aspects introduced by FINSTIX is an innovation attributable to the FINSEC project.

3.1 Data Flow

This section shows the use of FINSTIX in a concrete use case scenario, in which the FINSEC platform detects a jackpotting attack to the organization SuperBank, whose infrastructure is described in Sect. 3. In particular, the use case describes how FINSTIX Domain Objects are used to exchange data between:

- The probes and the FINSEC Platform:
  - From the probes to the Data Collector;
  - From the Mitigation Enabler to the probes;
- The different services composing the FINSEC platform;
- The FINSEC platform and the Dashboard.

**Step 1 and Step 2.** In Step 1, the Network probe represented by the Probe FDO having id “x-probe--network” generates the instance of Event presented in Listing 1.1. The Event has “x-event--cyber_instance” as id and “x-event--cyber_model” as model_ref. The Probe, as well as all the FDOs used in this example, is owned by SuperBank, whose id is “x-organization--superbank”. The probe sends the Event to the Data Collector through the FINSEC Data Collection API. In Step 2, the Data Collector stores the Event in the Security Database through the FINSEC Data Access API.

Listing 1.1. Cyber Event generated by the Network probe

```json
"type": "x-event",
"domain": "Cyber",
"id": "x-event--cyber_instance",
"created": "2020-06-22T20:02:45.028Z",
"modified": "2020-06-22T20:02:45.028Z",
"datatype": "Instance",
"name": "Cyber event",
"description": "Cyber event detected by network probe",
"x_organization": "x-organization--superbank",
"reference": "x-root--generic_root",
"model_ref": "x-event--cyber_model",
"coordinates": [41.899163, 12.473074],
"probe_ref": "x-probe--network",
"observed_refs": ["observed-data--netflow"],
"asset_refs": ["x-asset--ATM"]
```
**Step 3 and Step 4.** In Step 3, the CCTV probe generates an instance of Event having “x-event--tampering_instance” as id and “x-event--tampering_model” as model_ref, as shown in Listing 1.2. The probe sends the Event to the Data Collector through the FINSEC Data Collection API. In Step 4, the Data Collector stores the second Event in the Security Database through the FINSEC Data Access API.

Listing 1.2. Tampering Event generated by the ATM CCTV probe

```json
{
    "type": "x-event",
    "id": "x-event--tampering_instance",
    "datatype": "Instance",
    "name": "Tampering",
    "description": "CCTV camera tampering",
    "model_ref": "x-event--tampering_model",
    ...
}
```

**Step 5 and Step 6.** In Step 5, through the FINSEC Data Access API, the Anomaly Detection retrieves from the Security Database the instances of Event FDOs owned by “x-organization--superbank” and generated in a certain time window. As a result, in Step 6, the Event FDOs sent by the probes to the FINSEC platform in Step 1 and Step 3 are returned to the Anomaly Detection.

**Step 7 and Step 8.** In Step 7, the Anomaly Detection retrieves from the Security Database the models of attack owned by the organization identified by the id “x-organization--superbank”. As a result, in Step 8, the Attack FDOs matching the query are provided to the Anomaly Detection. The Anomaly Detection finds out that the Attack identified by the id “x-attack--model” has “x-event--cyber_model”, “x-event--tampering_model” as event.refs, as shown in Listing 1.3. These Event FDOs correspond to the models of the Event FDOs “x-event--cyber_instance” and “x-event--tampering_instance” respectively.

Listing 1.3. Model of Attack for the Jackpotting attack

```json
{
    "type": "x-attack",
    "id": "x-attack--model",
    "datatype": "Model",
    "name": "Jackpotting",
    "description": "Cyber-physical attack to send consecutive money dispense command to ATM device to empty the Cassette",
    "event_refs": ["x-event--cyber_model", "x-event--tampering_model"],
    "rules": [{...}, ...],
    ...
}
```
Step 9 and Step 10. Consequently to Step 8, in Step 9, the Anomaly Detection analyses the Observed Data referenced by the observed.refs of the Event “x-event--cyber.instance” (namely “observed-data-netflow”). By using the rules described in the Attack rules, the Anomaly Detection detects something malicious. As a consequence, it generates the instance of Attack “x-attack--instance” presented in Listing 1.4, having “x-attack--model” as model_ref and “x-event--cyber.instance” and “x-event--tampering.instance” as event.refs. The Attack is then stored in the Security Database. The Mitigation Service listens to insertions of Attack FDOs and consequently receives the Attack “x-attack--instance” in Step 10.

Listing 1.4. Instance of Attack generated by the Anomaly Detection

```json
{
    "type": "x-attack",
    "id": "x-attack--instance",
    "datatype": "Instance",
    "name": "Jackpotting",
    "description": "Cyber-physical attack to send consecutive money dispense command to ATM device to empty the Cassettes",
    "model_ref": "x-attack--model",
    "event_refs": ["x-event--cyber.instance", "x-event--tampering.instance"],
    ...
}
```

Step 11 and Step 12. The Mitigation Service needs to find a countermeasure for any attack modelled by “x-attack--model”. This information is contained in the Cyber Physical Threat Intelligence (CPTI) FDO. In Step 11, the Mitigation Service retrieves the CPTI characterized by “x-attack--model” as attack_ref from the Security Knowledge Base, through the FINSEC Data Access API. Then, in Step 12, the CPTI “x-cpti--model” presented in Listing 1.5 is returned to the Mitigation Service. From the CPTI, the Mitigation Service can find the id of the Course of Action necessary to mitigate the attack, namely “course-of-action--model”.

Listing 1.5. Model of Cyber-Physical Threat Intelligence for the Jackpotting attack

```json
{
    "type": "x-cpti",
    "id": "x-cpti--model",
    "datatype": "Model",
    "name": "CPTI for jackpotting",
    "description": "CPTI for jackpotting attacks",
    "attack_ref": "x-attack--model",
    "coa_refs": ["course-of-action--model"],
    ...
}
```
Step 13 and Step 14. In Step 13, the Mitigation Service uses the id of the Course of Action learned in Step 12 ("course-of-action--model") to request the FDO in Listing 1.6 to the Security Knowledge Base. In Step 14, the Course of Action "course-of-action--model" is returned to the Mitigation Service. The Course of Action is characterized by x_subtype set to to_mail: then the Mitigation Service knows that the mitigation consists in sending a mail notification. x_actions contains all the information regarding the mail to send, in particular the recipient address (to), the mail subject (subject) and the message (body). In the body, there are two markers, that must be replaced with information on the occurring attack, in particular the id of the asset involved in the attack and the timestamp of the attack. markers contains all the information needed by the Mitigation Service to perform this task.

Listing 1.6. Model of Course of Action used to mitigate the Jackpotting attack

```
{
  "type": "course-of-action",
  "x_subtype": "to_mail",
  "id": "course-of-action--model",
  "x_datatype": "Model",
  "name": "CoA for jackpotting",
  "description": "CoA to mitigate jackpotting attacks",
  "x_actions": [{
    "to": [{
      "type": "fixed",
      "address": "finsec@superbank.eu"
    }],
    "subject": "Jackpotting attack detected",
    "body": "FINSEC system detected an activity attributable to a possible jackpotting attack on the ATM identified by %%asset_id%%. The activity has been detected at %%time%%."
    "markers": [{
      "marker": "%%asset_id%%",
      ...
    }, {
      "marker": "%%time%%",
      ...
    }]
  }]
}
```

Step 15 and Step 16. The Mitigation Service has to generate an instance of Course of Action to mitigate the attack "x-attack--instance". To do so, it needs to retrieve the instance of Event involved in the attack and modelled by "x-event-cyber_model", to obtain the id of the asset involved. The Mitigation Service learned from the Attack "x-attack--instance" retrieved in Step 10 that the Event FDOs involved in the attack are identified by "x-event-cyber_instance" and
“x-event--tampering_instance”. As a consequence, in Step 15, the Mitigation Service retrieves from the Security Database the Event having “x-event--cyber_instance” or “x-event--tampering_instance” as id and “x-event--cyber_model” as model_ref. The Security Database returns the Event “x-event--cyber_instance” to the Mitigation Service in Step 16.

**Step 17 and Step 18.** In Step 17, the Mitigation Service generates the instance of Course of Action “course-of-action--instance”, whose x_actions contains the information needed to send the mail notification. The FDO is shown in Listing 1.7. Notice that the Mitigation Service replaced the markers contained in body with the id of the asset involved in the attack and the timestamp of the attack. The Mitigation Service inserts the FDO into the Security Database. In Step 18, the Mitigation Enabler, who listens to the insertion of instances of Course of Action FDOs into the Security Database, receives the FDO.

**Listing 1.7.** Instance of Course of Action used to mitigate the Jackpotting attack

```json
{
  "type": "course-of-action",
  "x_subtype": "to_mail",
  "id": "course-of-action--instance",
  "x_datatype": "Instance",
  "name": "CoA for jackpotting",
  "description": "CoA to mitigate jackpotting attacks",
  "x_model_ref": "course-of-action--model",
  "x_organization": "x-organization--superbank",
  "x_actions": [{
    "to": ["finsec@superbank.eu"],
    "subject": "Jackpotting attack detected",
    "body": "FINSEC system detected an activity attributable to a possible jackpotting attack on the ATM identified by x-asset--ATM. The activity has been detected at 2020-06-22T20:03:05.142Z."
  }],
  ...
}
```

**Step 19 and Step 20.** Since in the Course of Action “course-of-action--instance” x_subtype is to_mail, the Mitigation Enabler knows that the mitigation consists in a mail notification. It then extracts to, subject, and body contained in x_actions and performs a request to the Mailserver. The latter finally sends the mail notification in Step 20.

4 Conclusions and Discussions

This paper presents the design of the FINSTIX data model as an extension of the Structured Threat Information eXpression standard version 2. In particular, FINSTIX introduces many custom objects to describe the financial organization’s infrastructure and integrates both cyber and physical security domains.
Moreover, the paper reports an example of the use of FINSTIX in a relevant use case scenario. The use case refers to the FINSEC platform. Albeit explicitly designed for the Finsec domain, the FINSTIX model could be easily extended to other critical infrastructures that require to model both cyber and physical security threats, e.g., cellular networks [21], industrial plants [2] or other financial services [12]. To the best of our knowledge, FINSTIX is the first data model coping with both cyber and physical domains and can thus be considered an innovation introduced by the FINSEC project.

Acknowledgements. This work has been supported by the following research project: Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures (FINSEC) project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant agreement no. 786727.

References

1. Abe, S., Uchida, Y., Hori, M., Hiraoka, Y., Horata, S.: Cyber threat information sharing system for industrial control system (ICS). In: 2018 57th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), pp. 374–379. IEEE (2018)
2. Ackerman, P.: Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems. Packt Publishing Ltd., Birmingham (2017)
3. Aviad, A., Wecel, K.: Cyber threat intelligence modeling. In: Abramowicz, W., Corchuelo, R. (eds.) BIS 2019. LNBIP, vol. 353, pp. 361–370. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-20485-3
4. Barnum, S.: Standardizing cyber threat intelligence information with the structured threat information expression (STIX). MITRE Corporation
5. Burger, E.W., Goodman, M.D., Kampanakis, P., Zhu, K.A.: Taxonomy model for cyber threat intelligence information exchange technologies. In: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, pp. 51–60. ACM (2014)
6. Chia, V., et al.: Rethinking blockchain security: position paper. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1273–1280. IEEE (2018)
7. Fransen, F., Smulders, A., Kerkdijk, R.: Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik 132(2), 106–112 (2015)
8. Gascon, H., Grobauer, B., Schreck, T., Rist, L., Arp, D., Rieck, K.: Mining attributed graphs for threat intelligence. In: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, pp. 15–22. ACM (2017)
9. Ginn, R.J., Ionescu, I.: Cyber threat analysis (2017)
10. Gong, N.: Barriers to adopting interoperability standards for cyber threat intelligence sharing: an exploratory study. In: Arai, K., Kapoor, S., Bhatia, R. (eds.) SAI 2018. AISC, vol. 857, pp. 666–684. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-01177-2_49
11. Gore, R., Padilla, J., Diallo, S.: Markov chain modeling of cyber threats. J. Defense Model. Simul. 14(3), 233–244 (2017)
12. Guerar, M., Merlo, A., Migliardi, M., Palmieri, F., Verderame, L.: A fraud-resilient blockchain-based solution for invoice financing. IEEE Trans. Eng. Manage. 67, 1086–1098 (2020)
13. Hazeyama, H., Kadobayashi, Y., Miyamoto, D., Oe, M.: An autonomous architecture for inter-domain traceback across the borders of network operation. In: 11th IEEE Symposium on Computers and Communications (ISCC 2006), pp. 378–385. IEEE (2006)
14. Iqbal, Z., Anwar, Z., Muntaz, R.: STIXGEN-a novel framework for automatic generation of structured cyber threat information. In: 2018 International Conference on Frontiers of Information Technology (FIT), pp. 241–246. IEEE (2018)
15. Jaeger, D., Ussath, M., Cheng, F., Meinel, C.: Multi-step attack pattern detection on normalized event logs. In: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 390–398. IEEE (2015)
16. Kampanakis, P.: Security automation and threat information-sharing options. IEEE Secur. Priv. 12(5), 42–51 (2014)
17. Kim, E., Kim, K., Shin, D., Jin, B., Kim, H.: CyTIME: cyber threat intelligence management framework for automatically generating security rules. In: Proceedings of the 13th International Conference on Future Internet Technologies, p. 7. ACM (2018)
18. Kim, K., An, J.H., Yoo, J.: A design of IL-CyTIS for automated cyber threat detection. In: 2018 International Conference on Information Networking (ICOIN), pp. 689–693. IEEE (2018)
19. Ko, E., Kim, T., Kim, H.: Management platform of threats information in IoT environment. J. Ambient Intell. Humaniz. Comput. 9(4), 1167–1176 (2018)
20. Leichtnam, L., Totel, E., Prigent, N., Mé, L.: STARLORD: linked security data exploration in a 3D graph. In: 2017 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–4. IEEE (2017)
21. Lewis, T.G.: Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley, Hoboken (2019)
22. Li, J., Xue, Z.: Distributed threat intelligence sharing system: a new sight of P2P botnet detection. In: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–6. IEEE (2019)
23. Liu, M., Xue, Z., He, X., Chen, J.: Cyberthreat-intelligence information sharing: enhancing collaborative security. IEEE Consum. Electron. Mag. 8(3), 17–22 (2019)
24. Lutf, M.: Threat intelligence sharing: a survey. J. Appl. Sci. Comput. 8(11), 1811–1815 (2018)
25. Martinelli, F., Osliak, O., Saracino, A.: Towards general scheme for data sharing agreements empowering privacy-preserving data analysis of structured CTI. In: Katsikas, S.K. (ed.) SECPRE/CyberICPS -2018. LNCS, vol. 11387, pp. 192–212. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12786-2_12
26. Narayanan, S.N., Ganesan, A., Joshi, K., Oates, T., Joshi, A., Finin, T.: Early detection of cybersecurity threats using collaborative cognition. In: 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 354–363. IEEE (2018)
27. Rattan, A., Kaur, N., Chamotra, S., Bhushan, S.: Attack data usability and challenges in its capturing and sharing
28. Sadique, F., Cheung, S., Vakilian, I., Badsha, S., Sengupta, S.: Automated structured threat information expression (STIX) document generation with privacy preservation. In: 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (IEEE UEMCON 2018) (2018)
29. Shackleford, D.: Who’s using cyberthreat intelligence and how? SANS Institute (2015)
30. Steinke, M., Hommel, W.: A data model for federated network and security management information exchange in inter-organizational IT service infrastructures. In: NOMS 2018–2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–2. IEEE (2018)
31. Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A.: UCO: a unified cybersecurity ontology. In: Workshops at the Thirtieth AAAI Conference on Artificial Intelligence (2016)
32. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. 72, 212–233 (2018)
33. Ussath, M., Jaeger, D., Cheng, F., Meinel, C.: Pushing the limits of cyber threat intelligence: extending STIX to support complex patterns. Information Technology: New Generations. AISC, vol. 448, pp. 213–225. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-32467-8_20
34. Wagner, T.D., Palomar, E., Mahbub, K., Abdallah, A.E.: Towards an anonymity supported platform for shared cyber threat intelligence. In: Cuppens, N., Cuppens, F., Lanet, J.-L., Legay, A., Garcia-Alfaro, J. (eds.) CRiSIS 2017. LNCS, vol. 10694, pp. 175–183. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76687-4_12
35. Zarca, A.M., et al.: Security management architecture for NFV/SDN-aware IoT systems. IEEE Internet Things J. 6, 8005–8020 (2019)
36. Zhu, Z., Dumitras, T.: ChainSmith: automatically learning the semantics of malicious campaigns by mining threat intelligence reports. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&lP), pp. 458–472. IEEE (2018)