INTERNET-DRAFT
Internet Engineering Task Force (IETF)
Request for Comments: 6684
Category: Informational
ISSN: 2070-1721
Expires: July 11, 2014

M. Murillo
IEEE
January 2014

IODEF extension for Reporting Cyber-Physical System Incidents
draft-murillo-mile-cps-00.txt

Abstract

This draft document will extend the Incident Object Description Exchange Format (IODEF) defined in [RFC5070] to support the reporting of incidents dealing with attacks to physical infrastructure through the utilization of IT means as a vehicle or as a tool. These systems might also be referred as Cyber-Physical Systems (CPS), Operational Technology Systems, Industrial Control Systems, Automatic Control Systems, or simply Control Systems. These names are used interchangeably in this document. In this context, an incident is generally the result of a cybersecurity issue whose main goal is to affect the operation of a CPS. It is considered that any unauthorized alteration of the operation is always malign. This extension will provide the capability of embedding structured information, such as identifier- and XML-based information. In its current state, this document provides important considerations for further work in implementing Cyber-Physical System incident reports, either by utilizing any already existing industry formats (XML-encoded) and/or by utilizing atomic data.

In addition, this document should provide appropriate material for helping making due considerations in making an appropriate decision on how a CPS reporting is done: 1) through a data format extension to the Incident Object Description Exchange Format [RFC5070], 2) forming part of an already existing IODEF-extension for structured cybersecurity information (currently draft draft-ietf-mile-sci-11.txt), or others. While the format and contents of the present document fit more the earlier option, these can also be incorporated to the later.

Citations and references

Some of the text in this document has been taken from other MILE documents, most notably draft-ietf-mile-sci-11.txt and RFC-5901. In addition, some of the text has been taken from the references at the end of the document. We have tried to adequately reference. Once this document turns into an "official draft", these issues will be taken care of and additional references added. For the sake of circulating the document so as to get feedback on its focus, we leave this task for the immediate future.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6684.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Cyber-Physical and related systems have taken a key role in all types of infrastructures for decades. These are now at a higher risk to be the target of attacks by motivated and highly-skilled attackers, these being individuals, groups, or nation-states [ACS]. Among the issues that catalyse this higher risk are: i) these systems are gradually becoming more interconnected, ii) legacy systems do not have proper cybersecurity protection, iii) the existence of highly-skilled individuals and motivations, iv) some these systems are generally considered critical, v) these are a natural extension of IT cyber-attacks, vi) the emergence of the Internet of Things (IOT), and vi) these attacks can be carried out remotely and quite inexpensively.

While over 90% of critical control system infrastructure is currently owned by private enterprises, these can have direct repercussions on national security [SFC]. Indeed, various of these systems are key parts of nuclear reactor facilities, missile systems, transportation systems, electric power distribution, oil and natural gas distribution, water and waste-water treatment, dam infrastructure, and others. They are also at the core of health-care devices and transportation management. The disruption of these control systems could have a significant impact on public health, safety, and lead to large economic losses.

Sections Section 2 and Section 3 of this document provide an overview of the terminology, architecture, and process of a cyber-physical event. Section Section 4 introduces the high-level report format and how to use it. Sections Section 5 and Section 6 will describe the data elements of the cyber-physical extensions. The appendices will include an XML schema for the extensions and a few examples Cyber-Physical Systems reports.

1.1. What are Cyber-Physical Systems?

Cyber-Physical Systems are computer- or microprocessor- or microcontroller-based systems that monitor and control physical processes [ACS]. A basic example of a control system is the heating system of a room. The system is composed of a regulation knob, regulating box, heating device, thermostat, and appropriate cabling that links these devices. A human sets the desired temperature and the control system continuously regulates the heating device in order to maintain the desired temperature throughout the day. The current temperature of the room, which naturally will be much influenced by outside conditions, is continuously read by the controller through one or many sensors. Such reading is fed back to the regulating box, which holds a control system algorithm that provides the rules on how this regulation will take place. More complex control systems are the core of industries such as oil, gas, water, nuclear, electric grid, and others. For example, the electricity industry utilizes industry control systems to control the nuclear processes for the delivery of electricity. In this case, the operators will be located in control rooms that continuously display the health of the systems and request asynchronous input from the operators.

"Industrial control system" is a general term that include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and others. One of the primary differences between the two is that DCS are usually located within a more confined factory or plant-centric area, when compared to geographically dispersed SCADA field sites [RKAL].

1.2. Components of a Cyber-Physical System

Figure 1 illustrates a general composition of an industrial control system [ACS], [SFC]. Devices located at the Corporation Workspace (a), network (b), and operation workstation (c) could be considered mainstream IT infrastructure; these workstations run special programs that display the status of processes and are connected to a Local Area Network, a Wide Area Network, and possibly the Internet.

From the control network (d) downwards, the infrastructure differs, with specialized protocols for control networks, specialized devices (PLCs and RTUs) that house automation algorithms (e), sensors and actuators that operate and measure physical variables (g), and specialized networking infrastructure and protocols (f). The Operator Workstation (b) provides supervisory commands which are generally given by humans. Partly as a result of the advent of the Internet and new powerful devices, control system infrastructure is increasingly inheriting some infrastructure from IT systems [SFC].

Sensors (g) are devices that can measure temperature, pressure, water level, nuclear centrifuge rotor speed, and others. Actuators (g) enable/disable/regulate heating elements, motor speed, water pumps, reservoir locks, and others. Programmable Logic Controllers (PLCs) (e) house special control system algorithms that read sensors and command the actuators based on these readings and a multitude of control schemes; such task is done automatically in real-time. PLCs are generally utilized to coordinate work in closed environments, while Remote Terminal Units (RTUs) are generally utilized to coordinate remote operations, task generally coordinated by control servers (c).

An important fact about ICS is that Control networks are often more complex than plain IT systems and require a different level of expertise: control networks are typically managed by control engineers, not IT personnel [SFC].

```
                    +-------------------------------------------+
                    |          Corporation  Workspace           |   (a)
                    +-------------------------------------------+
                               ^                      ^
       ------------------------|----------------------|------------------------
 Corporate
                               |                      |             (b)
 Network
                               v                      v
 (mainstream IT system)
                     +--------------------+  +--------------------+
                     |Operator Workstation|  |   Control Servers  | (c)
                     +--------------------+  +--------------------+
                               ^                      ^
                               |                      |
                               v                      v             (d)
       ------------------------------------------------------------------------
 Control
                   ^                      ^                      ^
 Network
                   |                      |                      |
 (wired/wireless)
                   v                      v                      v
           +-----------------+    +-----------------+    +-----------------+
           |  | RTU/PLC |    |    |  | RTU/PLC |    |    |  | RTU/PLC |    | (e)
           |  +---------+    |    |  +---------+    |    |  +---------+    |
           |    ^     |      |    |    ^     |      |    |    ^     |      | (f)
       ----|----|-----|------|----|----|-----|----------------|-----|----------
 Field
           |    |     v      |    |    |     v      |    |    |     v      |
 Area
           |------+ +--------|    |------+ +--------|    |------+ +--------|
 Network
           |Sensor| |Actuator|    |Sensor| |Actuator|    |Sensor| |Actuator| (g)
       +----------------------------------------------------------------------+
       |                                                                      |
       |           P H Y S I C A L   I N F R A S T R U C T U R E              |
(h)
       |                                                                      |
       +----------------------------------------------------------------------+
```

Figure 1: A general Cyber-Physical System infrastructure

1.3. Incidents in Cyber-Physical Systems

In the context of cyber-physical systems (i.e. industrial control systems), an incident can be a mainstream IT incident itself (a, b, c) or the misbehaviour of a cyber-physical system (d, e, f, g, h) as a result of an IT incident. See Figure 1. The IT incident might intentionally seek to infiltrate the very PLCs and RTUs with aim to monitor and, in extreme scenarios, alter the operation of these devices and thus influence the operation of physical infrastructure. Incidents are known to be originated because numerous reasons, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and natural sources such as system complexities, human errors and accidents, equipment failures, and natural disasters [SFC].

1.3.1. Mainstream IT computer security incident

As per IODEFs, an incident can be a:

a. Benign configuration issue

b. computer/network incident

c. infraction to a service level agreement (SLA)

d. system compromise

e. socially engineered phishing attack

f. denial-of-service (DoS) attack

g. others

1.3.2. Cyber-physical system incident

A Cyber-physical incident can imply the presence of all the above IT computer security incidents. However, given the extra tasks carried out at lower layers (i.e. d - h) and the presence of dynamic physical infrastructure, the following issues are added to the incident list:

a. Control room alarm as a result of a 1) IT system misbehaviour (i.e one or more of the above), or 2) as a result of a physical system misbehaviour due to and IT system compromise, which might or might not have been detected

b. Misbehaviour of a physical system as noticed at the physical infrastructure level: explosion, flooding, pressure loss, and others

c. Misconfiguration or degradation of control system performance, as noticed by an operator. Extremely sophisticated attacks carried out by control system experts might carry out these types of attacks (i.e. compromising/missconfiguring control system schemes such as feedback control, robust control, optimal control, fault detection and estimation, others)

d. The disruption of control systems operation due to the blocking of the flow of information through corporate or control networks (d, f), thus causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS) [SFC]

e. Illegal or unauthorized changes made to programmed instructions or variables in PLCs, RTUs, DCS, or SCADA controllers (alarm thresholds changed, unauthorized commands issued to control equipment). This change can be benign or malign, with goals of damaging or disabling equipment (if tolerances are exceeded), premature shutdown of processes (i.e. electricity or gas transmission lines), and physical damage (explosion, flooding, and others).

f. False information sent to control system operators or to corporate HQ either to disguise unauthorized changes or to initiate inappropriate actions by system operators or other stakeholders SFC [SFC]

g. The modification of control system software or configuration settings, producing unpredictable results

h. Malicious software (e.g., virus, worm, Trojan horse) introduced into the system

i. Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel

It is important to note that, regardless on how the attack in originated (Internet, portable storage, insider job), there will generally always be, at least, IT components involved. Whether critical infrastructure is connected to the Internet is not a determinant on whether such will be attacked.

1.4. Why the appropriate reporting of a control system is needed

Control system incidents can cause irreparable harm to the physical system being controlled and to individuals. The reporting of a control system incident could save lives. A main goal of a well designed CPS attack will generally be to be unperceived and bypass basic (or mainstream) IT security defences in order to affect the physical world. In these situations, a possible incident will be abnormal operation of a physical system, generally represented by a control room alarm, perceived odd behaviour, or, in extreme scenarios, explosions, flooding, or other forms of physical infrastructure misbehaviour.

In this context, holding to report a physical incident until an IT incident surfaces (in case of a zero-day-worm attack, for example) can be a matter of life and death, more when other similar facilities are operated in other points, or when these operate in conjunction with the others (i.e. electric grid, gas pipelines). This is the case of the STUXNET worm, whose first observed symptom were the misbehaviour of nuclear centrifuges, with no control room alarms. It was months until researchers were able to detect the IT worm. The reporting of control system incidents from different locations could have possibly lead to its earlier detection.

Thus, the reporting of a cyber-physical incident is extremely important. By using a common format, it becomes easier for organizations to engage in coordination as well as correlation of information from multiple data sources or products into a cohesive view. As the number of data sources increases, a common format becomes even more important, since otherwise multiple tools would be needed to interpret the different sources of data. An important advantage of a common format is the ability to automate many of the analysis tasks and significantly speed up the response activities.

1.5. Examples of physical system attacks/incidents (Eventual case studies for validation of the incident report)

a. Australia

b. US

c. Iran

d. Others

1.6. What types of incidents to report?

a. Physical system incident, as observed by a stakeholder outside the control room (i.e. flooding, explosion, etc)

b. All incidents of Section Section 1.3.2

c. Mainstream cybersecurity incident in a control system infrastructure context, as observed by mainstream IT tools and reported by IODEF and its structured cybersecurity extension

d. Incidents related of the Internet of Things, especially in the context of the automation of buildings, vehicles, and other infrastructure

e. A combination of the above

1.7. Why a special extension is needed

IODEF provides a means to describe a cyber-physical incident information, but it would need to include various non-structured types of incident-related data tailored to physical systems in order to convey more specific details about what is occurring. Similarly, the IODEF-extension for structured cybersecurity information, currently a draft (draft-ietf-mile-sci-11.txt), would increase the machine readability of CPS incidents; however it would still need to be considerably modified in order to provide appropriate contextual machine readability.

Further structure within IODEF through any means increases the machine-readability of the document thus providing a means for better automating certain cybersecurity operations. Furthermore, because Cyber-Physical Systems are real-time and are for the most part automated, machine friendly data is paramount for effective incident response and coordination. This is even more relevant when very frequent reports are needed in these real-time systems that can have complex dynamics. Naturally this is also applicable, at a degree, to information in control room and even in corporate headquarters.

For instance, a worm might use zero-day attack and a PLC rootkit to attack a nuclear reactor. Special anomaly detection technology and backup sensors might detect unusual centrifuge control system input and output patterns. The institution might have similar facilities in different points in the nation. Then, enriched IODEF incident reports would be sent to other plants and to a central database. Such exchange of information would increase the chances to know quicker the source of the problem and to provide remediation. In the context of several independent systems, incident reports would help control equipment vendors quickly pinpoint weaknesses or exploits that were taken advantage of and make adequate fixes. In the case that a physical system is damaged, prompt incident reporting would avoid the same happening in other points.

This reporting is not limited to public or mainstream private infrastructure (industry), but also to home automation systems and various environments that form part of the Internet of Things and could pose significant physical dangers if compromised.

1.8. Relation to the IODEF Data Model

Instead of defining a new report format, this document seeks to define an extension to [RFC5070]. The IODEF defines a flexible and extensible format and supports a granular level of specificity. These cyber-physical extensions will reuse subsets of the IODEF data model and specify new data elements. Leveraging an existing specification allows for more rapid adoption and reuse of existing tools in organizations. For clarity, and in order to eliminate duplication, only the additional structures necessary for describing the exchange of cyber-physical activity will be provided; however the context of the location (i.e. different levels) will be considered in making appropriate decisions.

2. Terminology Used in This Document

Since many people use different but similar terms to mean the same thing, we underline the use of the following terminology in this document.

a. Cyber-Physical System. Also referred in this document as Operational Technology Systems or Industry Control System or Automatic Control Systems. Portions of a cyber-physical system can be considered a subset of Information Technology.

b. Cyber-physical event. The compromise of the Control Network, Field Area Network, Physical Infrastructure, or the compromise of any resource that influences the operation of the those entities

c. Physical infrastructure. Any physical infrastructure and premises that is part of a Cyber-physical system. Among many others, this categorization includes: nuclear reactors, oil and gas pipelines, water and electricity distribution systems, electricity generation systems, chemical plants, oil refineries, weapons systems, railway systems, traffic control systems, health-related systems, and critical infrastructure that form part of the Internet of Things.

d. Control room. Part of a control system infrastructure where humans monitor the overall status of the processes and make appropriate changes. These changes can be: set-points for processes (i.e. the power/level at which nuclear centrifuges will function), shutting down processes under a failure, and others..

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. The Elements of a physical system attack

A cyber-physical attacks are normally comprised of the following components. Data related to these elements or actors is key to capture in order make the event analysis and correlation with other events more useful:

a. The main attacker or party perpetrating the sabotaging activity. Most times this party is not readily identifiable.

b. The command and control centre. Generally compromised servers are at different locations. These can be used for sending instructions and for acquiring data, among others.

c. The ultimately targeted physical infrastructure (nuclear centrifuges, boilers, pressure chambers, pipelines, liquid control systems, dams, room heating, traffic lights, railway systems etc). Note that IT cybersecurity events might not have as a goal to target physical infrastructure, however might cause adverse consequences to these, as a result of a DoS attack, for example.

d. The devices that control the physical infrastructure: Control Network node(s), Field Area Network devices, Control Severs, and the wired and wireless networks and special protocols that connect them

e. Sensors and/or actuators that measure and manipulate physical infrastructure

f. The wired and/or wireless control network or field area network

g. The special control system algorithms that reside in PLCs, Control Servers, or sensor networks. These algorithms are based on control theory that determines the type of control to use (basic feedback control, robust control, optimal control, and others) and its gain parameters (proportional, integral, derivative, etc) [SFC]

h. Special supervisory and fault detection and estimation agents that monitor processes.[MMJS]

i. Sensor networks, generally locally distributed sets of wireless devices that measure and actuate physical devices. These are gradually being part of critical infrastructure.

j. The Internet or a removable device through which the malware infects the cyber-physical system

k. A human being, whom, willingly or unwillingly transports (and in some cases, injects) malware

l. A control room operator (or operators) that regulate set-points, react to alarms, and carry out supervisory duties

m. Detection information and Analysis output

n. Input/Output logs.

3.1. Cyber-Physical System Extensions to the IODEF-Document

Cyber-Physical System events are reported in a Cyber-physical activity report, which is an instance of an XML IODEF-Document Incident element with added EventData and AdditionalData elements. The additional fields in the EventData specific to cyber-physical incidents are enclosed in a CyberPhysicalReport XML element.

As a Cyber-Physical System attack may generate multiple reports to an incident team, multiple CyberPhysicalReports may be combined into one EventData structure, and multiple EventData structures may be combined into one incident report. One IODEF incident report may record one or more individual Cyber-physical events and may include multiple EventData elements.

This document will define new extension elements for the EventData IODEF XML elements and identifies those required in a CyberPhysicalReport. The appendices will contain sample activity reports and a complete schema. This Cyber-physical extension reuses subsets of the IODEF data model and, where appropriate, utilizes other extensions or specifies new data elements.

The IODEF Extensions defined in this document comply with Section 4, "Extending the IODEF Format" in [RFC5070].

4. Cyber-physical Reporting via IODEF-Documents

4.1. Report Types

As described in the following subsections, reporting cyber-physical events has three primary components: choosing a report type, a format for the data, and how to check the correctness of the format.

Similarly, there are three actions relating to reporting CPS events. First, a reporter or an automated system may *create* and exchange a new report on a new event. Secondly, a reporter may *update* a previously exchanged report to indicate new information. Lastly, a reporter may have realized that the report is in error or contains significant incorrect data and that the prudent reaction is to *delete* the report.

The three types of reports are denoted through the use of the ext-purpose attribute of an Incident element. A new report contains an empty or a "create" ext-purpose value; an updated report contains an ext-value value of "update"; a request for deletion contains a "delete" ext-purpose value. Note that this is actually an advisory for the report originator or recipients; operations might decide to file a new report with updated information. The nature of industry control systems will generally favour the later one, with exception of erroneously human-generated serious incidents.

Furthermore, administrators might decide to utilize this reporting in order to coordinate operations among different facilities, including SCADA networks. The machine friendliness of the report favour such, especially when automated reports are needed and when new infrastructure arises. Utilized in an automated way, it can be a tool to determine the health of most of the CPS infrastructure and conveniently inform various stakeholders in an standardized and straightforward manner. Other applications within CPS systems can vary, including its incorporation as a mainstream communication scheme.

4.2. CyberPhysicalReport Report XML (possible/alternative) Representations

The IODEF Incident element ([RFC5070], Section 3.2) is summarized below. It and the rest of the data model presented in Section Section 5 is expressed in Unified Modeling Language (UML) syntax as used in the IODEF specification. The UML representation is for illustrative purposes only; elements are specified in XML as defined in Appendix A.

```
   +--------------------+
   | Incident           |
   +--------------------+
   | ENUM purpose       |<>----------[ IncidentID ]
   | STRING ext-purpose |<>--{0..1}--[ AlternativeID ]
   | ENUM lang          |<>--{0..1}--[ RelatedActivity ]
   | ENUM restriction   |<>--{0..1}--[ DetectTime ]
   |                    |<>--{0..1}--[ StartTime ]
   |                    |<>--{0..1}--[ EndTime ]
   |                    |<>----------[ ReportTime ]
   |                    |<>--{0..*}--[ Description ]
   |                    |<>--{1..*}--[ Assessment ]
   |                    |<>--{0..*}--[ Method ]
   |                    |<>--{1..*}--[ Contact ]
   |                    |<>--{0..*}--[ EventData ]
   |                    |              |<>--[ AdditionalData ]
   |                    |                     |<>--[ CyberPhysicalReport ]
   |                    |<>--{0..1}--[ History ]
   |                    |<>--{0..*}--[ AdditionalData ]
   +--------------------+
   (i) No re-utilization of other extensions


        +---------------+
        | Incident      |
        +---------------+
        | ENUM purpose  |<>---------[IncidentID]
        | STRING        |<>--{0..1}-[AlternativeID]
        |   ext-purpose |<>--{0..1}-[RelatedActivity]
        | ENUM lang     |<>--{0..1}-[DetectTime]
        | ENUM          |<>--{0..1}-[StartTime]
        |   restriction |<>--{0..1}-[EndTime]
        |               |<>---------[ReportTime]
        |               |<>--{0..*}-[Description]
        |               |<>--{1..*}-[Assessment]
        |               |<>--{0..*}-[Method]
        |               |            |<>--{0..*}-[AdditionalData]
        |               |                  |<>--{0..*}-[AttackPattern]
        |               |                  |<>--{0..*}-[Vulnerability]
        |               |                  |<>--{0..*}-[Weakness]
        |               |<>--{1..*}-[Contact]
        |               |<>--{0..*}-[EventData]
        |               |            |<>--{0..*}-[ AdditionalData ]
        |               |            |             |<>--[ CyberPhysicalReport ]
        |               |            |<>--{0..*}-[Flow]
        |               |            |     |<>--{1..*}-[System]
        |               |            |           |<>--{0..*}-[AdditionalData]
        |               |            |                 |<>--{0..*}-[Platform]
        |               |            |<>--{0..*}-[Expectation]
        |               |            |<>--{0..1}-[Record]
        |               |                  |<>--{1..*}-[RecordData]
        |               |                        |<>--{1..*}-[RecordItem]
        |               |                              |<>--{0..*}-[EventReport]
        |               |<>--{0..1}-[History]
        |               |<>--{0..*}-[AdditionalData]
        |               |            |<>--{0..*}-[Verification]
        |               |            |<>--{0..*}-[Remediation]
        +---------------+
        (ii) Utilization of IODEF-extension for structured cybersecurity informa
tion
```

Figure 2: The IODEF XML Incident Element - Options

A cyber-physical report is composed of one iodef:Incident element that contains one or more related CyberPhysicalReport elements embedded in the iodef:AdditionalData element of iodef:EventData. The CyberPhysicalReport element is added to the IODEF using its defined extension procedure documented in Section 5 of [RFC5070].

One IODEF-Document may contain information on multiple incidents with information for each incident contained within an iodef:Incident element ([RFC5070], Section 3.12).

4.3. Syntactical Correctness of Cyber-Physical Reports

The cyber-physical report MUST pass XML validation using the schema defined in [RFC5070] and the extensions that will be defined in Appendix A of this document.

5. SCyberPhysicalReport Element Definitions

A CyberPhysicalReport consists of an extension to the Incident.EventData.AdditionalData element with a dtype of "xml". The elements of the CyberPhysicalReport will specify information about the components of activity identified in Section Section 5. Additional forensic information and commentary can be added by the reporter as necessary to show relation to other events, to show the output of an investigation, or for archival purposes. The inclusion of already existing reporting standards is possible through an appropriate element.

5.1. CyberPhysicalReport Structure

A CyberPhysicalReport element is structured as follows. The components of a CyberPhysicalReport are introduced in functional grouping, as some parameters are related and some elements may not make sense individually.

```
      +------------------+
      |CyberPhysicalRepor|
      +------------------+
      | STRING Version   |<>--{0..1}--[IncidentTitle]
      | ENUM IncdntType  |<>--{0..1}--[ReportingParty]
      | STRING ext-value |<>--{0..1}--[ReportReliability]
      |                  |<>--{0..1}--[IncidentType]
      |                  |<>--{0..1}--[Industry]
      |                  |<>--{0..1}--[TargetSystems]
      |                  |<>--{0..1}--[CyberPhysicalDepth]
      |                  |<>--{0..1}--[TransportMedium]
      |                  |<>--{0..1}--[Exploit]
      |                  |<>--{0..1}--[EntryPoint]
      |                  |<>--{1..*}--[PerpetratingParty]
      |                  |<>--{0..*}--[DetectionMethod]
      |                  |<>--{0..*}--[CommandAndControlCenters]
      |                  |<>--{0..*}--[CompromisedPhysicalInfrastrucute]
      |                  |<>--{0..*}--[ConstrolSystem]
      |                  |<>--{0..1}--[OrganizationalImpact]
      |                  |<>--{0..1}--[RecurrencePreventionMeasures]
      |                  |<>--{0..1}--[BriefDescriptionOfIncident]
      |                  |<>--{0..1}--[ProtocolType]
      |                  |<>--{0..1}--[NetworkType]
      |                  |<>--{0..1}--[Logs]
      |                  |<>--{0..1}--[References]
      +------------------+
```

Figure 3: The CyberPhysicalReport Element

5.2. Reuse of IODEF-Defined Elements

Elements, attributes, and parameters defined in the base IODEF specification are to be used whenever possible in the definition of the CyberPhysicalReport XML element.

5.3. Element and Attribute Specification Format

1. A terse XML-type identifier for the element or attribute.

2. An indication of whether the element or attribute is REQUIRED or optional. Mandatory items are noted as REQUIRED. If not specified, elements are optional. Note that when optional elements are included, they may REQUIRE specific sub-elements.

3. A description of the element or attribute and its intended use.

Elements that contain sub-elements or enumerated values are further sub-sectioned. Note that there is no "trickle-up" effect in elements. That is, the required elements of a sub-element are only populated if the sub-element is used.

5.4. Version Attribute

REQUIRED. STRING. The version shall be the value ___, to be compliant with this document.

5.5. IncdntType Attribute

REQUIRED. One ENUM. The IncdntType attribute describes the type of incident activity described in this CyberPhysicalReport. The IncidentType element indicates whether the incident is accidental, on purpose, or the result of other actions.

5.6. The IncidentTitle element

Briefly states the nature of the incident. This is mostly to convey understanding to humans.

5.7. The ReportingParty element

Describes the stakeholder that files the report

5.8. The ReportReliability element

Determines the degree of confidence of that the report information is accurate

5.9. The IncidentType element

Indicates whether the incident is accidental, on purpose, or the result of other actions

5.10. The Industry element

Determines the type of industry where the incident took/is taking place (petroleum, automotive, etc)

5.11. The TargetSystems element

Describes the main target: network, IT systems, control systems, etc.

5.12. The CyberPhysicalDepth element

Identifies the depth and all of the levels involved in the attack: control network, field area network, etc. See Diagram 1.

5.13. The TransportMedium element

Identifies how the worm or other tool penetrated the facilities: Internet, removable media, wireless, or others.

5.14. The Exploit element

Describes the characteristics of the exploit that was used for making the attack.

5.15. The EntryPoint element

Describes the device (router, PC, etc.) through which a worm or other threat entered the system. Note that the exploit does not necessary reside at the EntryPoint.

5.16. The PerpetratingParty element

Identifies the originator of the attack, this being a human being, nation state or others.

5.17. The DetectionMethod element

Describes how the detection was carried out, including the use of tools and the existence of irregularities in any device

5.18. The CommandAndControlCenters element

Describes the remote or local systems that are in control of the attack

5.19. The CompromisedPhysicalInfrastrucute element

Describes the elements of a physical infrastructure that was compromised

5.20. The ConstrolSystem element

Describes the parameters that were altered in the control system algorithm (proportional, integral, derivative, etc)

5.21. The OrganizationalImpact

Describes the economic and other aspect impact that the incident had on the institution

5.22. The RecurrencePreventionMeasures element

Describes the measures that must be taken for the incident not to repeat.

5.23. The BriefDescriptionOfIncident element

Describes a human friendly description of the incident. While the previousreporting elements should be enough to characterize an incident, this might provide additional information.

5.24. The Logs element

Takes the raw control system input/output, supervisory and other logs.

5.25. The References element

Provides with any resources that were used in the detection and amelioration of the incident.

5.26. The ProtocolType element

Describes the (field) protocol type. Allen Bradley; DF1,DH and DH+; GE Fanuc; Siemens Sinaut; Mitsubishi; Modbus RTU / ASCII; Omron; Toshiba; Westinghouse; Other Vendor Protocols

5.27. The NetworkType element

Provides with more idea of the network. Wide area networks: Analog point to point and multi-point modem networks, frame relay/Cell relay type point to point and multi-point networks, wireless Radio/ Satellite networks, fibre optic based networks

6. Mandatory IODEF and CyberPhysicalReport Elements

A report Cyber-Physical System report requires certain identifying information that is contained within the standard IODEF Incident data structure and the CyberPhysicalReport extensions. The required attributes are a combination of those required by the base IODEF element and those eventually required by this document. Attributes identified as required SHALL be populated in conforming Cyber-Physical System reports.

In case this draft extension will eventually embed structured cybersecurity information defined by other specifications, the implementation of this draft MUST be capable of sending and receiving the XML conforming to the specification listed in an initial IANA table without error. The receiver MUST be capable of validating received XML documents that are embedded inside that against their schemata. Note that the receiver can look up the namespace in an IANA table to understand what specifications the embedded XML documents follows.

6.1. An Example XML

To be populated

6.2. An XML Schema for the Extension

To be populated

7. Security Considerations

This document specifies a format for encoding a particular class of security incidents appropriate for exchange across organizations. As merely a data representation, it does not directly introduce security issues. However, given the comprehensiveness a report might have and the frequency of reports, third parties might be able to generate infrastructure characteristics, dynamics, and other parameters that, in extreme scenarios, might constitute industrial espionage. For this reason, the underlying message format and transport protocol used MUST ensure the appropriate degree of confidentiality, integrity, and authenticity for the specific environment. Organizations that exchange data using this document are URGED to develop operating procedures that document the following areas of concern.

7.1. Transport-Specific Concerns

The critical security concerns are that cyber-physical incident reports may be falsified or the CyberPhysicalReport may become corrupt during transit. In areas where transmission security or secrecy is questionable, the application of a digital signature and/or message encryption on each report will counteract both of these concerns. We expect that each exchanging organization will determine the need, and mechanism, for transport protection.

7.2. Using the iodef:restriction Attribute

In some instances, data values in particular elements may contain data deemed sensitive by the reporter. Although there are no general-purpose rules on when to mark certain values as "private" or "need-to-know" via the iodef:restriction attribute, the reporter is cautioned not to apply element-level sensitivity markings unless they believe the receiving party (i.e., the party they are exchanging the event report data with) has a mechanism to adequately safeguard and process the data as marked. Information that is considered sensitive can be marked as such using the restriction parameter of each data element.

8. IANA Considerations

This document uses URNs to describe XML namespaces and XML schemata [XMLschemaPart1] [XMLschemaPart2] conforming to a registry mechanism described in [RFC3688].

It is still to be determined whether this memo will create a registry for IANA to manage.

9. Manageability Considerations

If any of the operational and/or management considerations listed in Appendix A of [RFC5706] apply to this extension, they will be addressed in this section. If no such considerations apply, this section can be omitted.

10. Appendix A: XML Schema Definition for Extension

The XML Schema describing the elements defined in the Extension Definition section will be given here. Each of the examples in Section 11 will be verified to validate against this schema by automated tools.

11. Appendix B: Examples

This section will contain example IODEF Documents illustrating the extension. If example situations are outlined in the applicability section, documents for those examples should be provided in the same order as in the applicability section. Example documents will be tested to validate against the schema given in the appendix.

12. References

12.1. Normative References

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.

12.2. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3067] Arvidsson, J., Cormack, A., Demchenko, Y., and J. Meijer, "TERENA’S Incident Object Description and Exchange Format Requirements", RFC 3067, February 2001.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5706] Harrington, D., "Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions", RFC 5706, November 2009.

[RFC6545] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6545, April 2012.

[ACS] Amin, S., Cardenas, A., and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks", 2009.

[SFC] Stouffer, K., Falco, J., and K. Scarfonw, "Guide to Industrial Control Systems (ICS) Security", Organization US National Institute of Standards and Technology, June 2011.

[RKAL] Kalapatapu, R., "SCADA protocols and communication trends", Organization ISA, 2004.

[MMJS] Murillo, M. and J. Slipp, "Application of WINTeR Industrial Testbed to the Analysis of Closed-Loop Control Systems in Wireless Sensor Networks", Organization The 8th ACM/IEEE International Conference on Information Processing in Sensor Networks, 2009.

Author’s Address

Martin Murillo
Institute of Electrical and Electronics Engineers
1400 East Angela Blvd.
South Bend, Indiana
United States

Phone: +1 613 366 6003
EMail: murillo@ieee.org