Protocols for exchange of cyber security information

Ing. Július Baráth, PhD.

julius.barath@aos.sk

Department of informatics
Armed Forces Academy
Liptovský Mikuláš, Slovakia

doc. Ing. Marcel Harakaľ, PhD.

marcel.harakal@aos.sk

Department of informatics
Armed Forces Academy
Liptovský Mikuláš, Slovakia

Abstract

Traditional approaches to share cyber security information about vulnerabilities, weaknesses, attackers, methods and types of attacks are mostly based on secure email exchanges, verbal communication, and posts to the security related web sites. Modern approaches, however, require standardized and automated exchange and processing of such information using well defined terms, protocols (and the legislation in the case of cross-border exchanges) to achieve the fast understanding of attacker's intent and quick and effective response.

The proposed paper reviews main protocols and formats for intruder and incident description and information exchange. Main section of this paper focuses on STIX. STIX is the Structured Threat Information Expression language used for the specification, capture, characterization and communication of cyber threat information and TAXII stands for the Trusted Automated Exchange of Indicator Information, which is the protocol enabling the detection, prevention and mitigation of threats in near-real time. Primary components, the structure of messages, relation to other protocols, and possible use of STIX are shown in the following paragraphs. We conclude with Cyber Security Management System with STIX formatted information exchange between participating entities.

Keywords: STIX, cyber security

1 Introduction

Proper, timely, and effective reaction to cyber-attacks requires overall situational awareness and the correct information in the right place and at the right time. Information acquired from sensors, operating systems, security network devices on the one side and security professionals and organizations on the other one may suffer from insufficient cyber security information exchange. Common, standardized, community and industry accepted protocols are required to accomplish vision of automated, real time, secure, and trustworthy information exchange.

Cyber security is a challenging area where a standalone organization does not have all the knowledge to form the global situational awareness. The only solution of the problem is to share cyber security information with the trusted partners and communities. Such information exchange is beneficial for all the participants because they can better analyse actual situation, correlate ongoing malicious activities, and make effective counteractions to stop the threat. Even if the organization is not currently under attack, possibility of attack is still present and cyber security information exchange helps address the threat in early (preparation) stages.

2 Background

If we look at the standardization organizations and their influence in the cyber security phenomena, message transport standards are de facto IETF TCP/IP, message format standards used are ISO/W3C XML, message protection standards are W3C XML-sig / -enc, and message content standards are de facto adopted from MITRE CVE, CPE, CCE, CWE …

Now let us look at the activities of main standardization bodies in more detail. Internet Engineering Task Force – IETF published RFC 5070 – The Incident Object Description Exchange Format in addition to message transport protocol (TCP/IP in both versions V.4 and V.6). The purpose of IODEF is to define a common data format for the description, archiving, and exchange of information about incidents between CSIRTs (Computer Security Incident Response Teams) (including alert, incident in investigation, archiving, statistics, reporting, etc.) (2) extended by RFC 5901, RFC 6684, RFC 6685. Second relevant activity is RFC 6545 – Real-time Inter-network Defence (RID), which outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident-handling solution. Combination of these capabilities in a communication system provides the way to achieve higher security levels on networks. Policy guidelines for incidents handling are recommended and can be agreed upon by a consortium using the security recommendations and considerations (3). The application-layer protocol for RID based upon the passing of RID messages over HTTP/TLS is defined in RFC 6546 (4).

Joint Technical Committee ISO /IEC JTC 1 Information technology, Subcommittee SC 27 for IT Security techniques relevant facts are mainly covered in ISO/IEC 27k series. ISO/IEC 27000:2012 describes the overview and the vocabulary of information security management systems, which forms the subject of the ISMS family of standards and defines related terms and definitions (5). ISO/IEC 27010:2012 provides control and guidance specifically related to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications for large and medium-sized organizations. ISO/IEC 27035:2011 provides a structured and planned approach with the aim to:

- detect, report, and assess information security incidents,
- respond to and manage information security incidents,
- detect, assess, and manage information security vulnerabilities, and
- continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) cyber security relevant work is under X-series of standards; to name some of them[1] – ITU-T X.1205 Overview of cyber security (6), ITU-T X.1500 – Overview of cyber security information Exchange (7). There are

[1] Recommendations and Supplements under responsibility of this Question as of December 1st, 2012: X.1205, X.1206, X.1207, X.1209, X.1303, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1528, X.1528.1, X.1528.2, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1570, X.1580, X.1581, X.Suppl.8, X.Suppl.9, and X.Suppl.10.

also new activities[2] such as X.cee – Common event expression and X.sisnego – Framework of security information sharing negotiation under TAP (Traditional Approval Process). Recommendation on common event expression (CEE) standardizes the way computer events are described, logged, and exchanged. By using CEE's common language and syntax, enterprise-wide log management, correlation, aggregation, auditing, and incident handling can be performed more efficiently and produce better results. The primary goal is to standardize the representation and exchange of logs from electronic systems. CEE breaks the recording and exchanging of logs into four (4) components: the event taxonomy, log syntax, log transport, and logging recommendations. X.sisnego – Framework of security information sharing negotiation provides a framework for security information sharing negotiation on security information sharing between cyber security entities such as information requesters and information providers. This recommendation defines functional requirements and a reference model for security information sharing negotiation, conceptual data modelling of security information sharing agreement (SSA), security information sharing policy (SSP) and SSA negotiation process.

The MITRE Corporation (8) – a not-for-profit (US) organization creates de facto cyber security message content standards such as:

- Common Vulnerabilities and Exposures (CVE®), Common Platform Enumeration (CPE®), Common Configuration Enumeration (CCE™), Common Attack Pattern Enumeration and Classification (CAPEC™), Common Weakness Enumeration (CWE™),
- Open Vulnerability and Assessment Language (OVAL®), Trusted Automated eXchange of Indicator Information (TAXII™), Structured Threat Information eXpression (STIX™), Cyber Observable Expression (CybOX™), Malware Attribute Enumeration and Characterization (MAEC™), Common Event Expression (CEE™), Common Weakness Scoring System (CWSS™) Common Weakness Risk Analysis Framework (CWRAF™).

To conclude, list of organizations participating in security and cyber security related research and standardization will not be complete without mentioning CEN – European Committee for Standardization, CENELEC – European Committee for Electrotechnical Standardization, ECMA – European Computer Manufacturers Association, ETSI – European Telecommunications Standards Institute, IEEE – Institute of Electrical and Electronics Engineers, IET – Institute of Engineering and Technology, ITU – International Telecommunications Union, OASIS – Organization for the Advancement of Structured Information Standards and many other individual researchers at universities.

In such complex space of activities around the globe with common intent to face cyber treats, attacks, or even cyber war, there are different approaches to choose from. We need common platform to describe and share cyber security-related information and, in the reality, adopters – vendors and customers will choose which standard will or will not be commonly accepted. Rest of the paper will focus on STIX and TAXII, new initiative of MITRE to attract US and possibly international community of adopters in the cyber security message content area.

3 STIX

Currently automated management and exchange of cyber threat information is typically tied to the specific security product lines, service offerings, or community-specific solutions. STIX (currently in draft version) will enable the sharing of comprehensive, rich, “high-fidelity” cyber threat information across organizational, community, and product/service boundaries.

[2] Texts under development: X.1526 (X.oval), X.1544 (X.capec), X.abnot, X.bots, X.cce, X.cee, X.cee.1, X.cee.2, X.cee.3, X.cee.4, X.cee.5, X.csi, X.csmc, X.cwss, X.cybex-beep, X.cybex-tp, X.eipwa, X.maec, X.oval, X.sisnego, and X.trm.

STIX, however, aims to extend indicator sharing to enable the management and exchange of significantly more expressive sets of indicators as well as other full-spectrum of cyber threat information.

STIX is a language being developed in collaboration with any and all concerned parties for specification, capture, characterization and communication of standardized cyber threat information. It does so in a structured fashion to support more effective cyber threat management processes and application of automation (9).

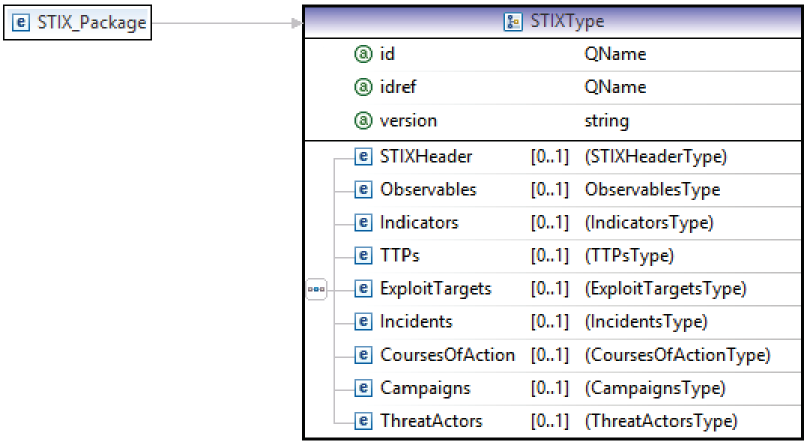
STIX addresses structured cyber threat information across and among full range of use cases improving consistency, efficiency, interoperability and overall situational awareness. In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information:

- Cyber Observables,
- Indicators,
- Incidents,
- Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, targeting, etc.),
- Exploit Targets (e.g., vulnerabilities and weaknesses),
- Courses of Action (e.g., incident response or vulnerability/weakness remedies),
- Cyber Attack Campaigns,
- Cyber Threat Actors (9).

To achieve efficiency of proposed STIX structure, the language leverages XML definitions from existing standardized languages. If we look at the proposed STIX schema, almost every element is optional and it creates simple messages using only relevant portions of STIX.

3.1 STIX Architecture

The STIX XML schema in the Figure 1 will be used for description of core cyber threat concepts using independent and reusable elements (Observables, Indicators, TTPs, ExpoloitTargets, Incidents, CoursesOfAction, Campaigns, and ThreatActors). These elements reuse appropriate structures already known from CybOX, Maec, Capec and Iodef specifications and define new structures where necessary. All the elements in the sequence are optional allowing either simple or complex messages to be created and exchanged.



e STIX_Package → STIXType

ⓐ id		QName
ⓐ idref		QName
ⓐ version		string
e STIXHeader	[0..1]	(STIXHeaderType)
e Observables	[0..1]	ObservablesType
e Indicators	[0..1]	(IndicatorsType)
e TTPs	[0..1]	(TTPsType)
e ExploitTargets	[0..1]	(ExploitTargetsType)
e Incidents	[0..1]	(IncidentsType)
e CoursesOfAction	[0..1]	(CoursesOfActionType)
e Campaigns	[0..1]	(CampaignsType)
e ThreatActors	[0..1]	(ThreatActorsType)

Figure 1: STIX architecture.

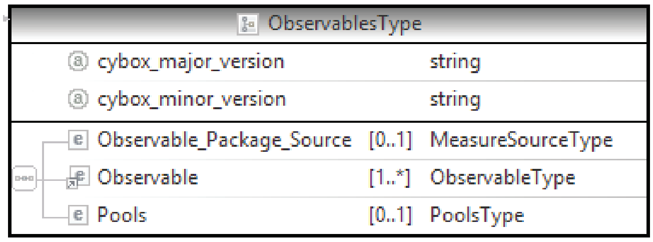
3.1.1 Observables structure

Observables are base elements of STIX structure (Figure 2). They utilize the CybOX language and represent status and activities observed in computer systems and network devices. Observables include three elements for identification of measured source, description of observable and relation to other elements via pools.

The first type is Measure source. To identify source of measure – Contributors, Time, Tools, Platform, System and Instance elements are used.

Second, the Observable type, is used to specify structured description of the observable with the help of Title, Description, Keywords, Observable source – for specification of how it was identified and specified, next behaviour which can be Stateful measure if observable is statically stateful in nature, Event if observable is dynamic in nature or composition if observable is made up of logical constructions of atomic observables. Noisiness specify how likely it is to generate false positives, Easy of Obfuscation indicates how easy it would be for an attacker to obfuscate the observability of this observable; and finally Obfuscation Techniques to specify potential techniques an attacker can use for obfuscation.

Third is Pools type, where Event, Action, Object and Attribute pool elements are defined. Each element enables the description of CybOX structure in a space-efficient pooled manner reducing redundancy caused when identical events occur multiple times.



ObservablesType		
cybox_major_version		string
cybox_minor_version		string
Observable_Package_Source	[0..1]	MeasureSourceType
Observable	[1..*]	ObservableType
Pools	[0..1]	PoolsType

Figure 2: Observables structure.

3.1.2 Indicators structure

STIX specification of indicators aims to extend automated machine to machine and human readable indicator sharing of more expressive sets of indicators about cyber threats. Indicators combine one or more observables with additional contextual information to represent behaviour and/or building blocks of particular cyber security context. Indicator type can be constant name string or a reference to an external value in a controlled vocabulary for better categorization supported with (optional) alternativeID-Alias and information about source of this entry in the Producer element.

Kill Chain Phases, IndicatedTTP (tactics, techniques, and procedures), Handling and Suggested COAs (Course of Action) give an idea about the phase of attack the observable belongs to, what actions are taken by the attacker, and how to handle and react to the threat.

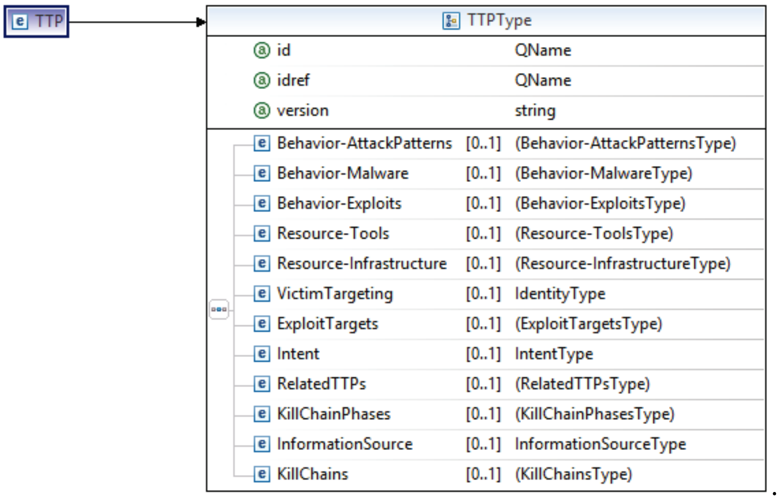
Confidence specifies a level of confidence held in the accuracy of the indicator's observable to TTP relationship assertion and Sightings and Extended Information provide reports and additional supporting information as specified by the content producer.

3.1.3 TTPs structure

Cyber intelligence seeks to understand and characterize things like: what sort of attack actions have occurred and are likely to occur; how can these actions be detected and recognized; how can they be mitigated; who are the relevant threat actors; what are they trying to achieve; what are their capabilities in the form of tactics, techniques, and procedures (TTP) they have leveraged over time and are likely to leverage in the future; what sort of vulnerabilities, misconfigurations, or weaknesses they are likely to target; what actions have they taken; etc. (9).

Tactics, Techniques, and Procedures describe activities of attackers. What is their target, Intent for a specified Kill Chain Phase, type of code they use (Malware, Exploits), what tools and resources are leveraged by this TTP. Relation to other TTPs and Information Source is also covered.

The victim Targeting element characterizes people, organizations, information, or access being targeted; Exploit Targeting characterizes potential vulnerability, weakness, or configuration targets for exploitation by this TTP and Kill Chain Phase is the activity left or right of hack (left of hack is Reconnaissance, Weaponization, Delivery, and partially Exploitation; right of hack starts with Exploitation followed by Installation, Command and Control, and Actions on Objectives).



TTPType		
id		QName
idref		QName
version		string
Behavior-AttackPatterns	[0..1]	(Behavior-AttackPatternsType)
Behavior-Malware	[0..1]	(Behavior-MalwareType)
Behavior-Exploits	[0..1]	(Behavior-ExploitsType)
Resource-Tools	[0..1]	(Resource-ToolsType)
Resource-Infrastructure	[0..1]	(Resource-InfrastructureType)
VictimTargeting	[0..1]	IdentityType
ExploitTargets	[0..1]	(ExploitTargetsType)
Intent	[0..1]	IntentType
RelatedTTPs	[0..1]	(RelatedTTPsType)
KillChainPhases	[0..1]	(KillChainPhasesType)
InformationSource	[0..1]	InformationSourceType
KillChains	[0..1]	(KillChainsType)

Figure 3: TTPs structure.

The phrase „kill chain" describes the structure of the intrusion and the corresponding model guides analysis to inform actionable security intelligence. Through this model defenders can develop resilient mitigations against intruders and intelligently prioritize investments in new technology or processes. Kill chain analysis illustrates that the adversary must progress successfully through each stage of the chain before he/she can achieve its desired objective; just one mitigation disrupts the chain and the adversary (1).

3.1.4 ExploitTargets structure

Exploit Targets elements address vulnerabilities of assets that are attacked by “ThreatActors” using appropriate TTPs. To address the target, its vulnerability, weakness, configuration, and already known PotentialCOAs and InformationSource are used. Structures used for ExploitTargets are not redefined, existing standards are used instead.

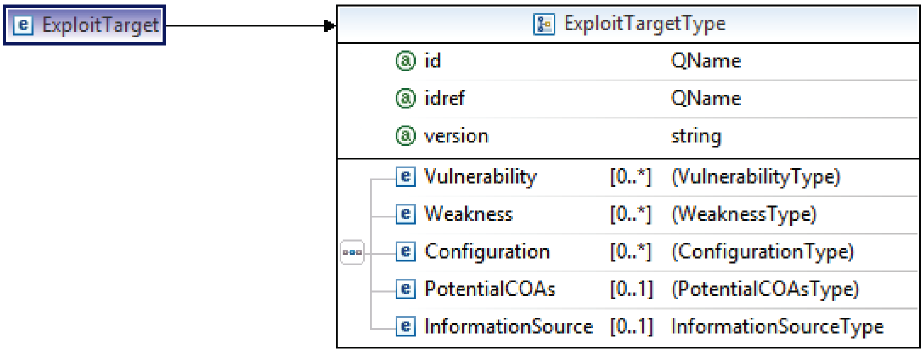

ExploitTarget
ExploitTargetType
id QName
idref QName
version string
Vulnerability [0..*] (VulnerabilityType)
Weakness [0..*] (WeaknessType)
Configuration [0..*] (ConfigurationType)
PotentialCOAs [0..1] (PotentialCOAsType)
InformationSource [0..1] InformationSourceType

Figure 4: ExploitTargets structure.

The Common Vulnerabilities and Exposures (CVE®) and the Open Source Vulnerability Database (OSVDB) are utilized for identification of publicly disclosed vulnerabilities. The Common Vulnerability Reporting Framework (CVRF) format is utilized for structured characterization of vulnerabilities not identified in CVE or OSVDB including the potential for characterizing 0-day vulnerabilities. The Common Weakness Enumeration (CWE™) is utilized for identification of weaknesses. The Common Configuration Enumeration (CCE™) is utilized for identification of configuration issues (9).

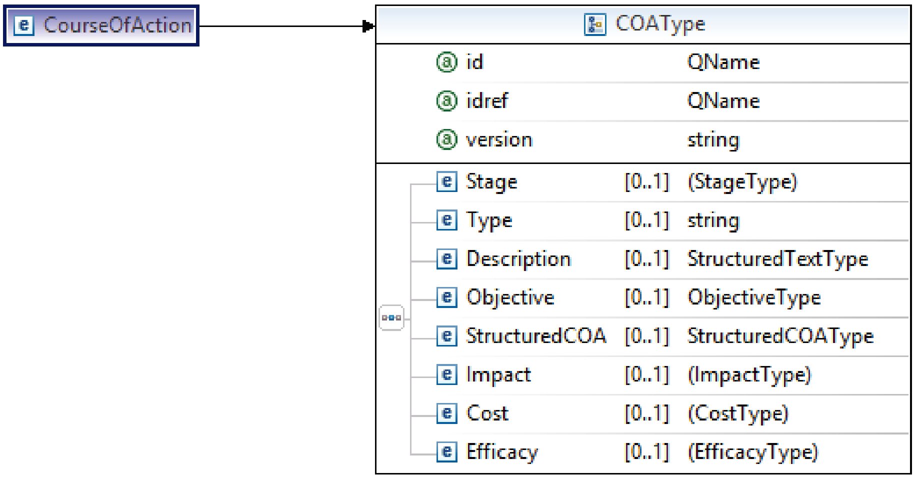
3.1.5 Incidents structure

Incidents consist of Time, Description, Reporter, Responder, Coordinator, Victim, Affected Assets, Impact Assessment, Related Indicators, Leveraged TTPs, Related TreatActors, Intent, Discovery Method, Related Incidents, COA Requested, COA Taken, Confidence, Contact and History types.

The goal of the Incident structure is to provide a platform for exchange of complex information about what is the target of the attack, who is an attacker and how the attack is conducted, who and how discovered and responded to the incident wrapped with the supporting information about time, description, contact and history of the incident.

3.1.6 CoursesOfAction structure

The CoursesOfAction structure describes proactive or retroactive actions to mitigate impacts of incidents. The Stage field specifies what stage in the cyber threat management lifecycle this CourseOfAction is relevant to (e.g. Remedy or Response), Description enables a generalized but structured description of COA, Objective, Impact and Cost are self-explanatory and the Efficacy field characterizes the effectiveness of this CourseOfAction in achieving its targeted Objective – Figure 5.



CourseOfAction

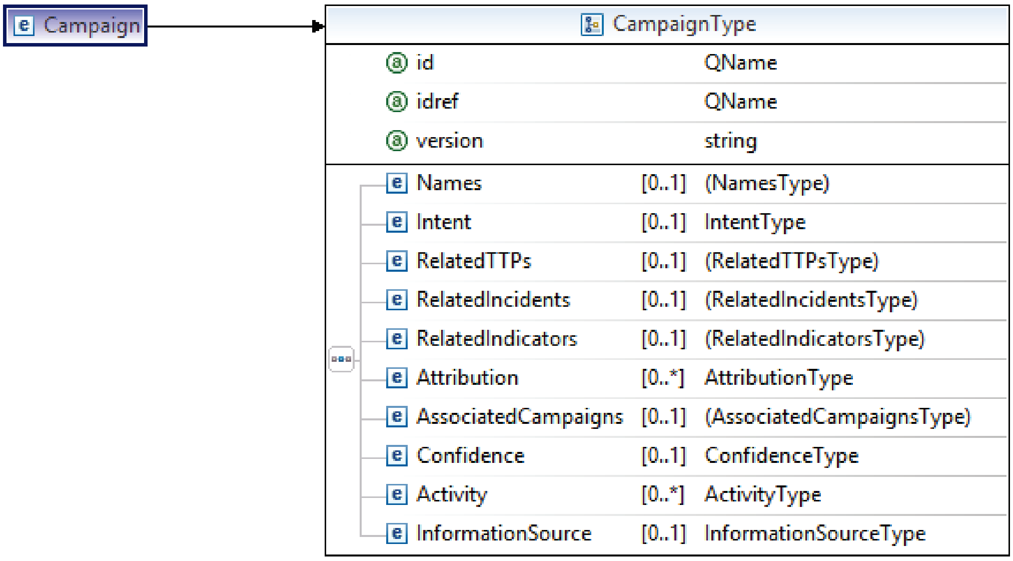
COAType

id		QName
idref		QName
version		string
Stage	[0..1]	(StageType)
Type	[0..1]	string
Description	[0..1]	StructuredTextType
Objective	[0..1]	ObjectiveType
StructuredCOA	[0..1]	StructuredCOAType
Impact	[0..1]	(ImpactType)
Cost	[0..1]	(CostType)
Efficacy	[0..1]	(EfficacyType)

Figure 5: CoursesOfAction structure.

3.1.7 Campaigns structure

The Campaign structure consists of Names, Intent, Related TTPs, Related Incidents, Related Indicators, Attribution, Associated Campaigns, Confidence, Activity and Information Source elements. In addition to already described elements there is the Attribution field, which specifies assertions of attributed Threat Actors for this cyber threat Campaign, the Confidence field, which characterizes the level of confidence held in the characterization of this Campaign and the Activity field characterizes actions taken in regards to this ThreatActor. This field is defined as one of the type ActivityType which is an abstract type enabling the extension and inclusion of various formats of Activity characterization (Figure 6).



Campaign

CampaignType

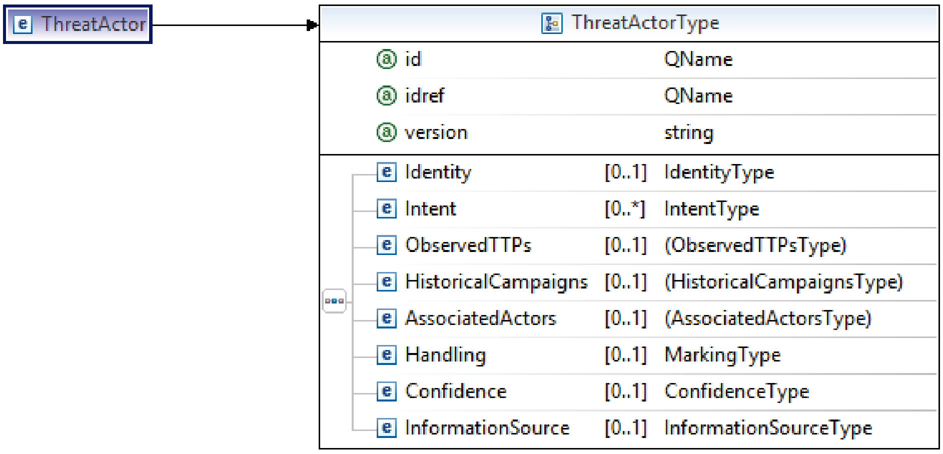
id		QName
idref		QName
version		string
Names	[0..1]	(NamesType)
Intent	[0..1]	IntentType
RelatedTTPs	[0..1]	(RelatedTTPsType)
RelatedIncidents	[0..1]	(RelatedIncidentsType)
RelatedIndicators	[0..1]	(RelatedIndicatorsType)
Attribution	[0..*]	AttributionType
AssociatedCampaigns	[0..1]	(AssociatedCampaignsType)
Confidence	[0..1]	ConfidenceType
Activity	[0..*]	ActivityType
InformationSource	[0..1]	InformationSourceType

Figure 6: Campaign structure.

Campaigns are structures potentially overlapping boundaries of one institution, usually characterised via common intent and same or very similar TTPs and set of incidents and indicators. Current standardised protocols do not handle campaign description needs properly so STIX tries to define required entities.

3.1.8 ThreatActors structure

Threat Actors represent cyber criminals or hackers responsible for cyber-attacks associated with current and past campaigns. Treat Actors entities describe Identity, Intent, TTPs, historical activity, co-actors and supporting documentation fields in Figure 7.



ThreatActor → ThreatActorType

id		QName
idref		QName
version		string
Identity	[0..1]	IdentityType
Intent	[0..*]	IntentType
ObservedTTPs	[0..1]	(ObservedTTPsType)
HistoricalCampaigns	[0..1]	(HistoricalCampaignsType)
AssociatedActors	[0..1]	(AssociatedActorsType)
Handling	[0..1]	MarkingType
Confidence	[0..1]	ConfidenceType
InformationSource	[0..1]	InformationSourceType

Figure 7: ThreatActors structure.

4 Example of use

Cyber security management system with STIX formatted information exchange between participating entities is described in the following example – Figure 8. The area of interest consists of a group of protected localities interconnected via the public internet. The public internet connects potential attackers and potential victims located in protected and unprotected localities and it is also a place for a variety of security detectors and analysers.

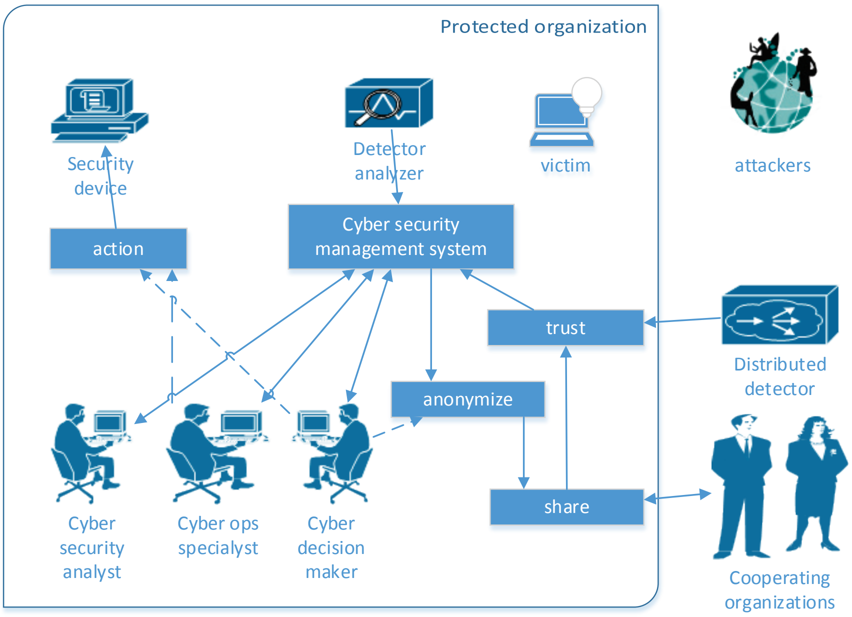
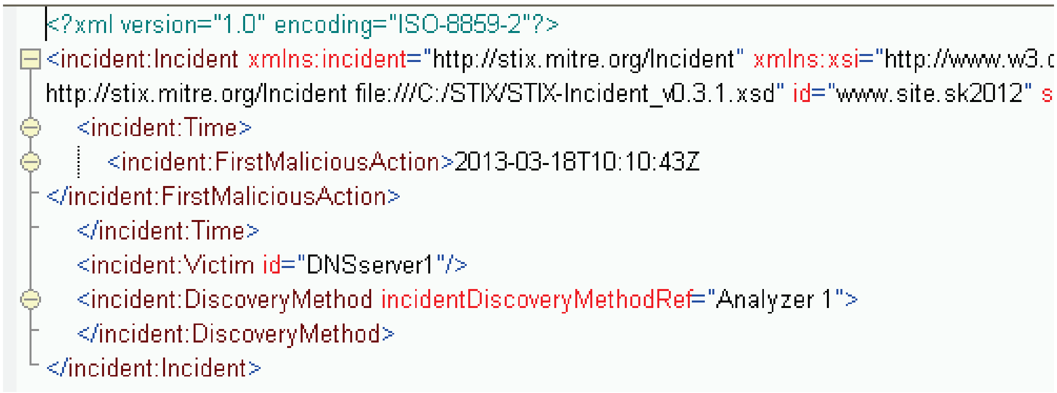


Figure 8: Example scenario.

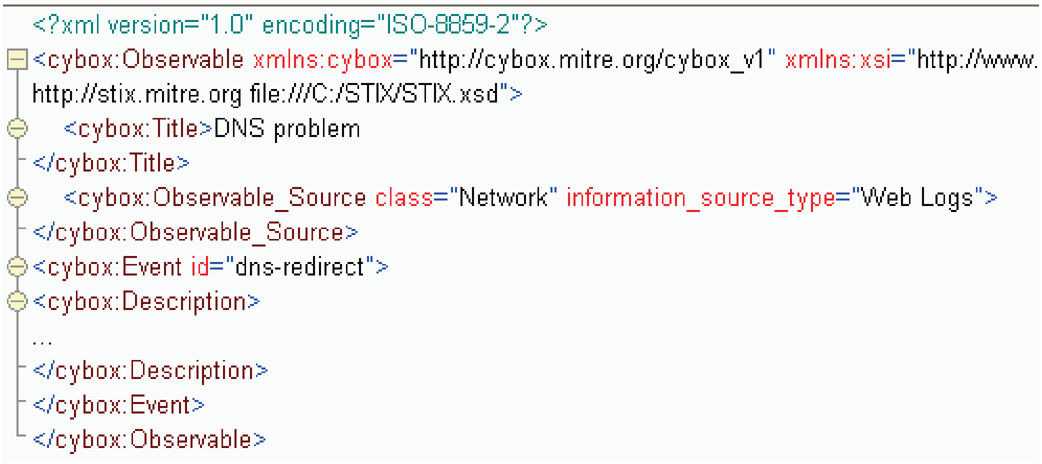
Cyber security detectors and analysers monitor data traffic travelling via important gateways and generate STIX formatted Incidents (3.1.5) if needed. Such logs are automatically stored and processed in Cyber security management system together with logs from other sources (shared with cooperating organizations). Figure 9 is one simplified example of Incident message sent from Analyzer 1 – log data are excluded due to their actual size.



```
<?xml version="1.0" encoding="ISO-8859-2"?>
<incident:Incident xmlns:incident="http://stix.mitre.org/Incident" xmlns:xsi="http://www.w3.c
http://stix.mitre.org/Incident file:///C:/STIX/STIX-Incident_v0.3.1.xsd" id="www.site.sk2012" s
    <incident:Time>
        <incident:FirstMaliciousAction>2013-03-18T10:10:43Z
</incident:FirstMaliciousAction>
    </incident:Time>
    <incident:Victim id="DNSserver1"/>
    <incident:DiscoveryMethod incidentDiscoveryMethodRef="Analyzer 1">
    </incident:DiscoveryMethod>
</incident:Incident>
```

Figure 9: Simplified Incident message.

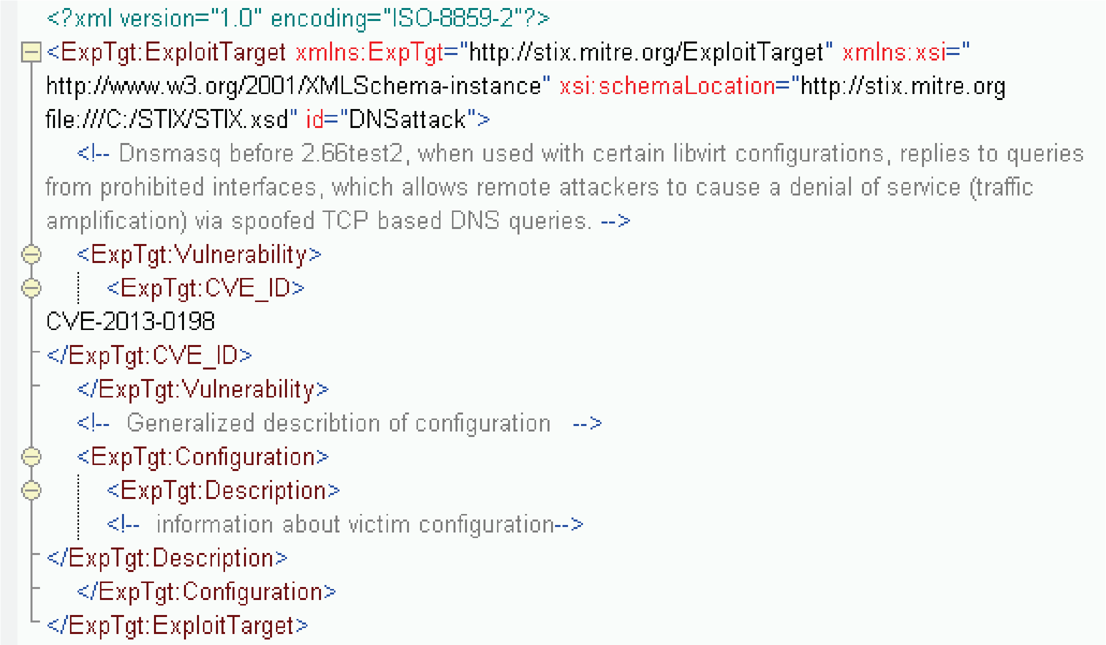
Cyber security management system is used for automatic information exchange between remote cooperating organizations, communities, and individuals and local cyber security analysts, cyber ops specialists and cyber decision makers. Couple of other participating organizations reported same type of attack to their primary DNS servers and shared their Observable reports – Figure 10.



```
<?xml version="1.0" encoding="ISO-8859-2"?>
<cybox:Observable xmlns:cybox="http://cybox.mitre.org/cybox_v1" xmlns:xsi="http://www.
http://stix.mitre.org file:///C:/STIX/STIX.xsd">
    <cybox:Title>DNS problem
</cybox:Title>
    <cybox:Observable_Source class="Network" information_source_type="Web Logs">
</cybox:Observable_Source>
<cybox:Event id="dns-redirect">
<cybox:Description>
...
</cybox:Description>
</cybox:Event>
</cybox:Observable>
```

Figure 10: Simplified Observation message.

Local cyber security analysts process and interpret Incidents, identify their nature and correlate them with other cyber activities to form Observables and Indicators. They refine descriptions of Incidents and together with cyber ops specialists analyze and identify ExploitTarget (Figure 11) and ThreatActors.



```
<?xml version="1.0" encoding="ISO-8859-2"?>
<ExpTgt:ExploitTarget xmlns:ExpTgt="http://stix.mitre.org/ExploitTarget" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://stix.mitre.org
file:///C:/STIX/STIX.xsd" id="DNSattack">
   <!-- Dnsmasq before 2.66test2, when used with certain libvirt configurations, replies to queries
from prohibited interfaces, which allows remote attackers to cause a denial of service (traffic
amplification) via spoofed TCP based DNS queries. -->
   <ExpTgt:Vulnerability>
      <ExpTgt:CVE_ID>
CVE-2013-0198
</ExpTgt:CVE_ID>
   </ExpTgt:Vulnerability>
   <!--  Generalized describtion of configuration   -->
   <ExpTgt:Configuration>
      <ExpTgt:Description>
      <!--  information about victim configuration-->
</ExpTgt:Description>
   </ExpTgt:Configuration>
</ExpTgt:ExploitTarget>
```

Figure 11: Simplified ExploitTarget message.

Later they analyze TTPs and define boundaries of separate Campains. For this scenario, cyber ops specialists concluded that the site face to DoS DNS attack for specific installation of DNS servers.

Decision makers take advantage of shared awareness about current cyber security situation and propose optimal CoAs. For this incident they recommended to fix DNS bug and decrease allowed DNS requests per host per minute. They also define rules of sharing for cyber information. Released information is anonymised and shared using chosen transport protocol or service.

5 Conclusion

As it is mentioned in the ITU-T SG17 motivation section "Cyber attacks continue to be widespread; they cause a complex range of problems to users, service providers, operators and networks. Countering cyber attacks by technical means requires development of frameworks and requirements for: detecting and protecting against cyber attacks; mitigating and recovering from their effects; and exchanging cyber security information."

STIX is an XML-based language developed for exchanging cyber security information. The first whitepaper draft of STIX was published in December 2012 utilizing the XML schema as structured and portable mechanism for discussion, evaluation, and refinement among the communities involved. STIX as a structured threat information expression language helps exchange information between components of information security management systems worldwide in a formalized manner.

The structure of the language allows formalizing outputs (reports, notifications, and alarms) of security-related programs and appliances, correlate them with other outputs, and then process them by security specialists. Specialists will be able to quickly reuse historical information about past incidents, campaigns, threat actors, TTPs used and more properly define attacker's intents and propose COAs and estimate the costs of actions.

A common format of cyber security information will also help share cyber security knowledge between organizations allowing them to proactively mitigate or eliminate cyber security threats and use past data for learning, training, or simulation of future cyber campaigns.

References

[1] HUTCHINS, E., M. CLOPPERT AND R. AMIN Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Proceedings of the International Conference on Information Warfare & Security, 2011, 113.

[2] IETF. The Incident Object Description Exchange Format. In RFC 5070. 2007.

[3] IETF. Real-time Inter-network Defense (RID). In RFC 6545. 2012.

[4] IETF. Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS. In RFC 6546. 2012.

[5] ISO/IEC. Information technology — Security techniques — Information security management systems — Overview and vocabulary. In ISO/IEC 27000:2012(E). Genova, 2012.

[6] ITU-T. SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security. In Overview of cyber security. 2008.

[7] ITU-T. SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyber security information exchange – overview of cyber security. In Overview of cyber security information exchange. 2011.

[8] cyber security[online]. [cited january 2013]. Available from:<http://www.mitre.org/work/cyber security/cyber_standards.html>.

[9] Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)[online]. 2012 [cited january 2013]. Available from: <http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0_(Draft).pdf>.