Advances in Threat and Risk Modeling

Gerald Beuchelt
Vijay Mehra
Problem Space

» Landscape of threats to information systems and corporate assets is changing
  • Multiple attack vectors, cyber, physical, environmental, others
  • Advanced threats utilize multiple vulnerabilities
  • Most current models do not include threats from natural disasters

» No comprehensive consistent semantic framework
  • Existing systems (such as corporate GRC solutions) allow insular treatment of threat/risk relationships
  • Comprehensive system would allow system-of-systems interoperability (private/private, public/private)
We have critical needs for analytics and information sharing.

Cyber
Crime
Terrorism
Critical Infrastructure
Natural Disasters

Sharing & Analytics
Sharing & Analytics
Sharing & Analytics
Sharing & Analytics
Sharing & Analytics

Risks and threats from threat actors and natural sources cross domains.
Yet the information sharing and analytics capabilities are stove piped.

Threat and risk
Identification, assessment, mitigation, situational awareness
The Challenge

» There are dozens of standards, exchange schemas and technologies for each domain
  • Each uses different terminology, structure and schema to represent the same or overlapping concepts
  • These only work together inside of proprietary products. No one product could ever cover the entire scope
  • Organizations with different or multiple products can’t integrate

» There are less shared semantics across threat domains

» Threat actors and natural disasters don’t respect our stovepipes, they exploit them

Impact: Our capacity for coordinated analysis and response is insufficient
Everything has a Cyber Component

» Cyber has introduced a critical new need for federation and coordination
» Many criminal and terrorist threats have a cyber component
» All response capabilities have a Cyber component
» We can’t consider Cyber as separate
Everything has a “Real World” Component

» As critical as Cyber is, it is how it impacts our physical world that is critical
» Attacks can contain coordinated physical and cyber components
» Incidents may have criminal and legal consequences
» Cyber and physical need to be understood together
The myth of separate domains

» While we like to compartmentalize for efficiency and management
  • No real separation between these domains
  • Concerns, processes and information cross all boundaries
  • Our protective forces must be aware of and be able to respond across any “domain”

Goal: Become Federated, integrated and coordinated
The N² Problem

» Every threat domain or community of interest has preferred threat information sharing standards

» Bridging between two standards creates a mapping

» Adding a new standard to become interoperable results in N new mappings resulting in an N² problem

  • The cost and time to execute is phenomenal
  • Emergency integration of a new schema is impractical
  • Different interpretations in each mapping make the end result error prone and unreliable

CC-BY-NC 2.5 © Randall Munroe
OMG Activity

» Object Management Group (OMG) started exploratory project in Dec 2013
  • Initial phase focused on semantic consistency between STIX and NIEM for threat modeling
  • Broadened to develop a conceptual model for risk and threat expression

» OMG Request for Proposal (RFP) issued at the June 2014 meeting
  • Submission date is scheduled for Feb 2015

» Support from multiple stakeholders (private, public, government)
Methodology
Precepts for OMG Project

» The purpose/organizational specific schema will not (should not) go away
» A “one size fits all” solution will not work
  • There will be no one technology
  • There will be no one terminology or language
  • There will be no one data structure for threats and risks

» Focus is **federation**
  • Understanding the concepts behind the existing schema
  • Mapping them to a common conceptual model
  • Enabling interoperability by bridging between the specific schema
  • Supporting integration and coordination of mitigation and response capabilities
**Goal: Break O(N²)**

» Existing N to N problem needs fixing
  - Not limited to cross-threat domain mappings and standards
  - Another layer of N to N problems exist within each domain

Refocus the discussion on solving the business/problem, instead of fighting format wars
Approach: Conceptual Model

» Develop conceptual model
  • Focused on semantics, not syntax
  • Informed by existing standards, research and best practices
  • Independent of specific data structures, technologies and terminologies

» Develop bridges that enable map from logical to conceptual layer and back

» Make models sufficiently precise to drive automated bridging between any mapped schema
“Pivoting” Through a Conceptual Model

» Data in source and target data representation is tangible
» The Conceptual Threat and Risk Model (formatted in UML) is a representation of “concepts”
» Concepts can be represented in different data structures
» Rules are used to define mapping from logical or physical models to the conceptual layer
Relationship to DIKW Model

Based on C. Zins definitions, DOI: 10.1002/asi.20508

Wisdom (Insight)
- Conceptual Models

Knowledge
- Logical models

Information
- Physical Models, schemas

Data
- Objects, instances

Predictive Capabilities

Descriptive Capabilities
Core Concept: Comprehending Planned and Unplanned Threats

» “All hazards” include man-made and natural disasters/system failures
  • There is not always an actor involved (e.g. hurricane, system malfunction)

» Adversarial/intentional actors are not the only threat actors
  • Non-malicious actors may constitute significant threat (e.g. spear-phishing victim, power plant operator)
  • Defenders (e.g. system admins, law enforcement, medical staff) may also act on offensive plans
  • Victims are actors as well
Core Concept: Attacker/Defender Symmetry

» Attack perspective:
  • Defender: Attackers/hazards are threats
  • Attacker: Targets are opportunities

» Defense perspective:
  • Attacker: Successful defense is a threat to the intentions/objectives
  • Defender: Maintaining effective defensive posture is an opportunity

Threat vs. Opportunity is in the eye of the emoji – it is not useful to create static classifications
Core Concept: Actor Capabilities

» Limiting actors to a static or single role in a specific scenarios is not helpful
  • Defensive actors may use offensive actions and plans to achieve defense objectives
  • Attackers may use defensive actions for ensuring OPSEC for the plan
  • Bystanders may support defensive or offensive plans or actions

» Capabilities are a better way to characterize actors
  • Capabilities may include offensive, defensive, and other abilities
  • Actors can leverage capabilities in executing plans
Example Use Case and Scenario
Flow of Events

Intent

Plan

Modus Operandi

Vulnerability

Risk

Threat

Potential Effect

Natural event or System failure

Real World Effect

Incident

Consequence

Impact on Objectives

Stakeholder

Threat Actor
Example Scenario: Coordinated Power Grid Attack

» Attack
  - Laptop with access credentials is stolen
  - Grid industrial control system is compromised in Cyber attack
  - Physical attack on substation disrupts power
  - Compromised system cascades failure
  - Physical infrastructure damaged

» Potential Mitigations
  - Compromise is recognized by Cyber defense, system is hardened
  - Law enforcement notified and arrests attackers
  - Preparation is identified and defense forces put in place
  - Real-time notification of systems going down initiates manual shutdown
Potential Information Flows

- Suspicious Activity Report
- NIEM Incident
- STIX Incident
- Intelligence Report
- Tactical Response Unit
- Manual Shutdown
- Public CAP Warning
- IT System Hardening
- Arrest Report
- Incident Report
- STIX Incident
- Intelligence Report
Example Use Case: Large Company

- Company with multiple data centers, office facilities, international business activity
- Large number of deployed security systems, sensors
  - Firewalls, IDS/IPS, SIEM, monitoring systems, notification/alerting, etc.
  - Uses FW/Snort rules, STIX/TAXII, IODef, alarms for fire and intrusions, etc.
  - Physical and information security staff, some 24/7
- Interoperable (but not uniform) threat monitoring and assessment
Example Scenario: Corporate SAR & Incident Management

Indicators of Compromise
Intelligence
Colocation Datacenter IDS

Corporate SOC

Email
Email/STIX
Email/IOS

User Reports
Corporate IDS
Corporate SIEM

Customer
Threat Sharing Community
Law Enforcement

Email
Syslog
NIEM
Email/RSS
Model Details
Model Scope Diagram

Wide & shallow conceptual model generically covering threats and risks

Other risks (Out of scope)

Operational Threat & Risk Concepts

High level Cyber-threat/risk concepts

NIEM Threat/Risk Model

Law Enforcement / Emergency Management Concepts

Physical. Spectrum, facilities, Probabilities, Forensic, Chemical, Biological, Medical, Nuclear, Military and Intelligence threats concepts

Other Inputs

Normative (Formal Specification)

In Scope with Limited Detail

Informative

STIX/TAXII/Cybox

IODEF

SACM

ISO

NIST

Others…

Other Risks

Systemic Risk

Credit Risk

Market Risk

Pension Risk

Reputation Risk

Liquidity Risk

Legal Risk

Project Management Risk

Legend

STIX/TAXII/Cybox

IODEF

SACM

ISO

NIST

Others…

Other Risks

Systemic Risk

Credit Risk

Market Risk

Pension Risk

Reputation Risk

Liquidity Risk

Legal Risk

Project Management Risk

In Scope with Limited Detail

Other Inputs

Other Risks

Systemic Risk

Credit Risk

Market Risk

Pension Risk

Reputation Risk

Liquidity Risk

Legal Risk

Project Management Risk

In Scope with Limited Detail

Other Inputs

Legend

STIX/TAXII/Cybox

IODEF

SACM

ISO

NIST

Others…

Other Inputs
Model Detail: Plans
Mapping Details: Indicator Mapping

Conceptual Model to NIEM

STIX to Conceptual Model

“Pivoting” through the Conceptual Model
Outlook
Expected Project Outcome

» Specification covering:
  • Conceptual threat and risk model as a semantic foundation for interoperability
  • Predefined mapping for NIEM, STIX, and potentially CAP - others per community interest
  • UML and XMI artifacts allowing automated generation of mappings

» Target applications
  • Security Operation Center applications including dashboards and advanced analytics
  • Governance, Risk Management, and Compliance systems
  • Integrated response planning
Additional Applications

» Enterprise Risk Modeling
  • Cross-domain accounting for threats, vulnerabilities, and risk
  • Tighter integration with public information sources

» Modeling for Response Strategies
  • Parameterization of threat and risk landscape
  • Monte-Carlo simulation and response testing

"Pi 3.0K" by Caitlin Jo - Own work. This mathematical image was created with Mathematica. Licensed under Creative Commons Attribution 3.0 via Wikimedia Commons.
Conclusions

» Current logical models are application domain specific or domain centric
  • Focus on emergency management, cyber/INFOSEC, law enforcement, etc.
  • Interoperability between different systems is hard and manual

» No comprehensive threat pictures that includes an “all-hazards” view

» Conceptual model can add this by providing semantic glue to allow effective mapping

Call to Action: Engage with “Team Threat & Risk”
Your Thoughts and Comments