Risks Analysis

Djenana Campara
Chief Executive Officer
Member, Object Management Group Board of Directors
Chair, System Assurance Task Force
KDM Analytics - Who we are

• Leaders in automated cyber risk analysis
  – Formalized methodology
  – Book “System Assurance: Beyond Detecting Vulnerabilities”

• Standards Involvement
  – Object Management Group
    • Djenana Campara - Board of Directors of the Object Management Group (OMG)
    • Chairs of two OMG Task Forces:
      – System Assurance Task Force
      – Knowledge Discovery Meta-model (KDM) RT
    • Key contributors to upcoming Threat and Risk standards
  – ISO/IEC SC7/WG7
    • Priming 19506: Knowledge Discovery Meta-Model (KDM)
    • Contributing to 15206: System Engineering & System Assurance
KDM Analytics – What we do

We identify and measure security risks in cyber and cyber-physical systems
- Providing Tools, Technology & Methodology
- Risk and Vulnerability Analysis Services
- R&D Services in the area of automated security assurance

Some of our Clients
- US and Canadian Governments: DHS, DoD, NSA, USAF, AFRL, NIST, DND, DRDC, PWGSC
- Corporations: Lockheed Martin, EWA, EMC, Mentor Graphics, RTI

Awards
- 2014 Strategic Aerospace and Defence Initiative Program (SADI)
- 2013 Cameo Award for Modeling, Simulation & Analysis - MagicDraw Extension with Greatest Industry Impact
- Canadian Innovation Commercialization Program (CICP) 2012 award - Safety and Security
- "Best of Show" award at FOSE 2009 in the category "Software for Enterprise Systems"
Our Focus

• Systematic Threat Risk & Vulnerability Analysis (TRV)
  ☐ Unique, cost-effective approach
  ☐ Automated analysis
  ☐ Supported by integrated tools
Goal:
A Risk Assessment Methodology (within a Risk Management Framework) that is systematic, objective, allows automation, and can answer a tough question:
How do we know that all threats have been addressed?
Failing to understand ALL threats ...

- Not enough to trust credentials
- Firewall is no longer sufficient protection
- Ignorance MUST NOT be an option
  - Organized Crime
  - Smart hackers who share knowledge

Effective threat mitigation can only be achieved through identifying, analyzing, classifying and understanding the threat and related risk: Cause & Effect
The Challenge: Where are the Vulnerabilities?

- The point of entry to the system is the individual user
- The actual security perimeter is often much larger than anticipated
- Chief Security Officers cannot address risks that they are not aware of!
Undiscovered Vulnerabilities can Result in Massive Losses

- **STUXNET** - Sophisticated, multilevel targeted attack on SCADA system resulted in modification of system’s behavior
  - layered attack against three different systems initially exploiting four zero-day vulnerabilities within Windows systems and using it as spring board to install itself on PLC devices unnoticed with aim to periodically modify the frequency and thus affects the operation of the connected motors by changing their rotational speed and leading to destruction of centrifuges
Overcoming the Challenge

COMPREHENSIVE AND SYSTEMATIC RISK ANALYSIS
Examining Existing Risk Management Methodologies: Providing Assurance & Automation?

- ISO/IEC 13335
- ISO/IEC 15408
- ISO/IEC 15443
- ISO/IEC 27001
- CRAMM (UK)
- EBIOS (France)
- Mehari (France)
- Magerit (Spain)
- HTRA (Canada)
- NIST SP-800-30 (US)
- Octave (SEI CMU)
- RiskAn (Czech Rep)
- Microsoft Threat Analysis Methodology
- Open Group FAIR
- ...and others

Challenges

- No interoperability between those methods (an issue in an international coalition context – how do we know that a risk assessment conducted in the country from which a system was acquired is sufficient?)
- Few approaches deal with facts that are discernable in code or models -- hinders automation
- Few approaches are systematic enough to provide assurance
“Ingredients” of risk (ISO 15408)
Assurance through vulnerability detection
Assurance through asset protection
Assurance through standard controls
Each step can be a reasonable starting point...

... but all are needed for an end-to-end risk assessment
Goal: Justifiable Risk Management

Justifiable risk management = end-to-end risk mitigation assurance
Justifiable Risk Management:
KDM’s FORSA Methodology – Influenced by Standard Efforts

• Achieving justifiable risk management requires a methodology that
  – Is systematic (can enumerate all threats)
  – Deals with discernable concepts
  – Considers assurance (can provide confidence and justification)

• We selected most suitable methodologies, combined them and further enhanced to
  – Fully support assurance
  – Support import of structured Enterprise operational views (e.g. DoDAF/UAE)
  – Support automation of the methodology steps
    • Including multi-stage attack identification
Methodology describes the sequence of steps

- **Who cares?**
  - Owners and criteria
  - Sensitivity

- **Assets and Targets**
  - Value
  - Owners wish to minimise
  - To reduce
    - Countermeasures
      - That may be reduced by
      - That may possess
    - Vulnerabilities
      - May be aware of
      - Leading to risk
        - That exploit
          - That increase
            - Lead to threats
              - Give rise to assets
                - Wish to abuse and/or may damage

- **By who? and Why?**
  - Threat Sources

- **What to do about it?**
  - Controls, mitigation options

- **So what?**
  - Undesired events, Operational Impact
  - Severity

- **How?**
  - Attack scenarios
  - Likelihood

06/02/2017
(c) KDM Analytics Inc.
The corresponding FORSA steps

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

The sequence of steps is designed to increase confidence, and therefore increase assurance.

Enterprise Architecture

What?

Analysis of valuables, sensitivities and impacts
=> severity

How?

Analysis of targets, entries and attacks
=> likelihood

Risk

06/02/2017 (c) KDM Analytics Inc.
### Results of Justifiable Risk Analysis

- More systematic and comprehensive process leads to higher confidence in the risk calculation

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Severity</th>
<th>Likelihood</th>
<th>Level</th>
<th>Residual</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>R01</td>
<td>Hacker gains access to confidential assets by information gathering on stored files</td>
<td>high</td>
<td>high</td>
<td>high</td>
<td>low</td>
<td>80%</td>
</tr>
<tr>
<td>R02</td>
<td>Targeted virus or timebomb affects integrity or availability of network by attacking programmable node</td>
<td>high</td>
<td>high</td>
<td>high</td>
<td>low</td>
<td>80%</td>
</tr>
<tr>
<td>R03</td>
<td>Hacker subverts node by remote attack exploiting vulnerabilities in programmable node’s code</td>
<td>high</td>
<td>medium</td>
<td>high</td>
<td>low</td>
<td>80%</td>
</tr>
<tr>
<td>R04</td>
<td>Hacker subverts programmable node by remote attack exploiting vulnerabilities in system software on programmable node</td>
<td>high</td>
<td>medium</td>
<td>medium</td>
<td>low</td>
<td>80%</td>
</tr>
<tr>
<td>R05</td>
<td>Criminal learns about forensic activity by attacking software on programmable node</td>
<td>medium</td>
<td>high</td>
<td>medium</td>
<td>low</td>
<td>80%</td>
</tr>
<tr>
<td>R06</td>
<td>Targeted virus or timebomb affects availability of other assets by attacking software on programmable node</td>
<td>medium</td>
<td>high</td>
<td>medium</td>
<td>low</td>
<td>80%</td>
</tr>
<tr>
<td>R07</td>
<td>Malicious user subverts programmable node by locally attacking node’s code</td>
<td>medium</td>
<td>low</td>
<td>medium</td>
<td>low</td>
<td>70%</td>
</tr>
</tbody>
</table>
Risk Assessment Methodology Driven by the Assurance Case

- Integrating System Assurance into Risk Assessment Methodology
- Utilizing Assurance Case to deliver Risk Assessment
- Automating end-to-end process
Lockheed Martin Case Study

• Based on standards + framework + supported tools
  – Modeling tools, vulnerability scanning tools

• Lockheed Martin’s evaluations
  – Structured Assurance Models
    • Bring structured order to chaos
    • Relate Claims – Arguments – Evidence between various sources of evidence
  – System Risk Manager
    • Analysis of DoDAF model Operation, System, ... Views
    • Automated Gap Assessments in Models
    • Threat Risk Assessment capability on DoDAF models
  – Tools Output Integration Framework (TOIF) and Risk Analyzer tools
    • Significant improvement in Software Flaw and Vulnerability assessments
    • Lower labor costs
    • Significantly lower tool costs

Lockheed Martin found that KDM/OMG system assurance modeling tools can reduce security engineering lifecycle costs by 20 to 50%
Thank You

Djenana Campara
Chief Executive Officer
Office: (613) 627-1012
E-mail: djenana@kdmanalytics.com