MAEVA: A Framework for Security Risk Response Based on Attack-Motivation Analysis

Louai Maghrabi[1] & Eckhard Pfluegel[2]

May 30, 2021 - June 03, 2021

[1] Department of Cybersecurity
School of Engineering, Computing & Informatics
Dar Al-Hekma University
Jeddah, Saudi Arabia
LMaghrabi@DAH.edu.sa

[2] School of Computer Science & Mathematics
Faculty of Science, Engineering & Computing
Kingston University
London, United Kingdom
E.Pfluegel@Kingston.ac.uk

Presenting Author – About

Eckhard Pfluegel (PhD, SFHEA) is a Senior Lecturer in Network & Information Security at the School of Computer Science and Mathematics, Faculty of Science, Engineering and Computing at Kingston University, London, UK. He is leading the Cyber and Energy Security (CYENS) Research Group and his current research interests are applications of game theory for security, Blockchain security and security protocols.

Kingston University London

IARIA

OUTLINE

- Motivation
- The Challenges of Risk Computation
- The MAEVA Framework
- Application to Game Theoretic Risk Assessment
- Conclusion

MOTIVATION

- Organisations are increasingly facing cyber attacks, targeting their systems and data
- Security assessment and risk analysis are popular techniques for informing budget spending in relation to security controls
- They mainly focus on analysing the expected impact of an attack on the organisation’s assets
- However, this is a difficult task and tricky to get accurate estimates.
- Could there be new methodologies, focusing on ”the other side”, i.e. the motivation that an external attack might have on launching attacks?

Research Contributions

- This paper presents two contributions.
  - The first contribution is a novel framework for risk assessment of cyber security attacks on an organisation.
  - The second contribution is an application of this framework to game-theoretic risk assessment.
- The main difference to previous work is:
  - The novel framework, entitled MAEVA, focuses on the attackers perspective (rather than the defender, i.e. the security assessor)
  - We develop a scheme, entitled the Attack Incentive Matrix (AIM), which can be contrasted with the standard Risk Response Matrix
  - Benefits arise when using this framework in combination with traditional approaches, as it might increase accuracy of risk estimates

The Challenges of Risk Computation

- Using formal notation, the risk R can be expressed as an expected impact I.
- This can be computed using the following equation:

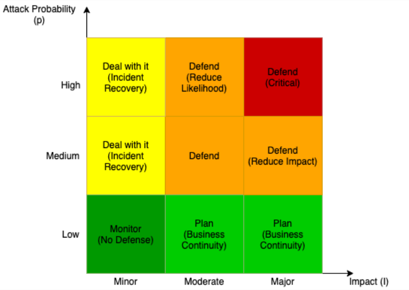
$$R = p \cdot I.$$

- Here p is the probability of an attack occurring, often referred to as *attack likelihood*.
- From this equation, one can see that the problem now is to quantify and compute p and I and the difficulty is to perform a realistic estimate of these variables.

Risk Assessment Based on Risk Response Matrix

- It is now assumed that one is able to determine the attack likelihood p.
- This leads to a table containing risk response actions, such as defending critical assets, recovering from an attack, planning for defense or choosing not to respond at all.
- An appropriate response action is then determined by indexing the table rows with attack probabilities using qualitative metrics (low, medium or high) and its columns with a measure for the impact (minor, moderate or major) of the attack.
- This table is referred to as *Risk Response Matrix* (RRM) in this talk.

Risk Response Matrix



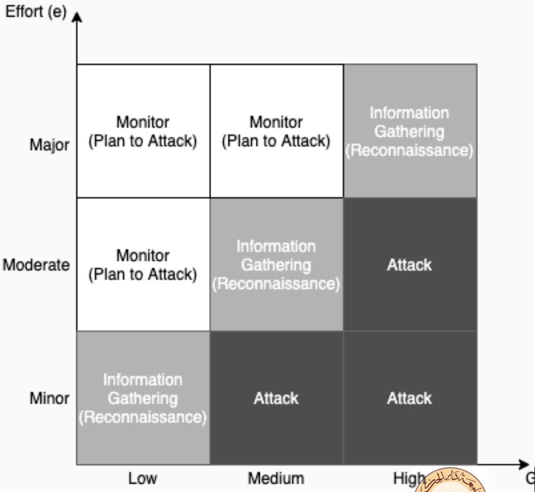
Attack Probability (p)				
High	Deal with it (Incident Recovery)	Defend (Reduce Likelihood)	Defend (Critical)	
Medium	Deal with it (Incident Recovery)	Defend	Defend (Reduce Impact)	
Low	Monitor (No Defense)	Plan (Business Continuity)	Plan (Business Continuity)	
	Minor	Moderate	Major	Impact (I)

Figure 1: Risk Response Matrix (RRM) [NIST]

THE MAEVA FRAMEWORK (EXPLANATION)

- **M**otive: the underlying reason for attacking the victim. This could be for the purposes of financial gains, or personal satisfaction.
- **A**bility: the capability of the attacker to invest in resources for implementing the attack, as well as her/his technical knowledge
- **E**xploitability: the ease by which the system can be penetrated, through exploiting a vulnerability.
- **V**isibility of target: how prominent is the target – e.g. does it have a popular website or brand name, or a large user base?
- **A**ttractiveness of target: from the point of view of the attacker, how attractive is the target?

The MAEVA Framework (Attack Incentive Matrix)



Effort (e)	Low	Medium	High
Major	Monitor (Plan to Attack)	Monitor (Plan to Attack)	Information Gathering (Reconnaissance)
Moderate	Monitor (Plan to Attack)	Information Gathering (Reconnaissance)	Attack
Minor	Information Gathering (Reconnaissance)	Attack	Attack

Figure 2: Attack Incentive Matrix (AIM)

Application to Game Theoretic Risk Assessment

- Under the assumption of complete information about the strategies available to both players, the use of game theory improves the traditional risk assessment.
- The security game $\mathcal{G}$ between the attacker and defender in strategic normal form:

Table 1: Payoff Matrix for $\mathcal{G}(\mathcal{D}, \mathcal{A})$

$\mathcal{D} \downarrow \mathcal{A} \rightarrow$	s_a	s_{-a}
s_d	$-c_{\mathcal{D}}, -c_{\mathcal{A}}$	$-c_{\mathcal{D}}, 0$
s_{-d}	$-I$, $G - c_{\mathcal{A}}$	0, 0

Using MAEVA to Inform Game Payoff Functions

- Before the game can be solved, it needs to be specified in terms of the precise values for the payoff functions, and Table 1 reveals that the MAEVA framework can be used to determine (an estimate for) G.
- The parameter $c_{\mathcal{D}}$ is effectively the *defense budget* of the organisation and $c_{\mathcal{A}}$ can be related to the attacker's effort e.
- Hence, in a natural way, both the RRM and AIM methodologies provide the input parameters for the game.
- The analysis of the game based on computing the Nash equilibrium will then result in the desired risk value.

Kingston University London

IARIA

SUMMARY

- The MAEVA framework is based on analysing the incentive an adversary may have to attack the organisation when weighing up the potential gain from the attack and the effort it takes to breach the system.
- We argue that this point of view, which is fundamentally different to that taken in traditional risk assessment, can complement and enhance the standard approach based on estimating risk as a function of attack likelihood and impact on the organisation.
- Our framework is very convenient when wishing to inform the design of complete information games, modelling attacker-defender scenarios.
- It is a natural first step an organisation can take to prepare a game-theoretic risk assessment.

Kingston University London

IARIA

Conclusion

- To our knowledge, our framework constitutes a novel approach and we recommend using it as a practical methodology for any organisation wishing to assess risk, perhaps in combination with other mainstream methods.
- The next step for this research would be an implementation of a real scenario, and a detailed evaluative comparison with existing approaches.
- For example, an organisation could review their information assets, apply both the RRM and AIM, and compare the resulting parameters.
- It would be interesting to relate this to historical information about cyber security incidents that happened in the past at this organisation, or in its sector.

Kingston University London

IARIA

QUESTIONS?

Thank you for listening!