Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 168 (2007) 207–220
www.elsevier.com/locate/entcs

Augmented Risk Analysis*

Giampaolo Bella[a,1] Stefano Bistarelli[b,c,2] Pamela Peretti[b,3]
Salvatore Riccobene[a,4]

[a] *Dipartimento di Matematica e Informatica, Università di Catania, Italy*
[b] *Dipartimento di Scienze, Università degli Studi "G. D'Annunzio", Pescara, Italy*
[c] *Istituto di Informatica e Telematica, CNR Pisa, Italy*

Abstract

Risk analysis has recently emerged as a structured and precise methodology to help modern companies understand their risks and plan the relative countermeasures well in advance. It is based on a number of *indicators*: parameters that quantify the key concepts on which an enterprise designs its security and safety investments. A *modificator* is a function that further modifies an existing indicator, and is itself an indicator. It is argued here that Risk Analysis can dramatically benefit from three novel modificators. One, the *Exposure Factor during Critical Time* (EFCT), expresses the percentage of loss or damage that an attack can infer to a time-critical asset. Another one, the *Exposure Factor under Retaliation* (EFR), formalises the mitigation to the loss or damage that an attack can infer to an asset when that loss or damage can be retaliated back onto the attacker. The third one, the *Mitigated Risk against Collusion* (MRC), formalises how a security measure can be effective against a single attacker but not necessarily against a large team of attackers working collaboratively for the same target. Our simulated results firmly support the benefits of such augmented Risk Analysis confirming the novel insights it can provide.

Keywords: exposure factor, mitigated risk, time-critical, retaliation, collusion

1 Introduction

There is increasing evidence that it is important to assure an adequate level of protection to the enterprise's assets from risks of loss or damage. A variety of risks exist: some are related to the political and social environment where the enterprise operates (*strategic risks*); others concern the money market and interest rate (*financial risks*); others still pertain to the enterprises's business processes (*operative risks*). Therefore, security has become one of the chief entries in the enterprise's investment plan.

* This paper is partially supported by the MIUR PRIN 2005-015491.
[1] Email: giamp@dmi.unict.it
[2] Email: bista@sci.unich.it
[3] Corresponding author. Email: peretti@sci.unich.it
[4] Email: sriccobene@dmi.unict.it

1571-0661 © 2007 Elsevier B.V. Open access under CC BY-NC-ND license.
doi:10.1016/j.entcs.2006.12.006

Risk Management is a structured process prescribing three phases: Risk Assessment, Risk Analysis, and Risk Mitigation. As it is intuitive, the possible vulnerabilities must be first identified and described. Then, they should be analysed using mathematical methods, and finally they ought to be mitigated. Mitigation consists in increasing the security managers' awareness of the risks and suggesting them a set of reasonable countermeasures capable of bringing the overall risk below an acceptable threshold.

This paper concentrates on Risk Analysis and precisely on Security Risk Analysis [12]. It is important to premise that a security threat is not necessarily successful in general, namely it will not accomplish its intended security breach with absolute certainty. However, Risk Analysis generally is an anticipated study of the consequences of successful threats. Therefore, the threats mentioned in the following are always assumed to succeed with total probability, and hence can be considered actual breaches.

Our contribution to Risk Analysis is the definition and demonstration of three unpublished modificators pertaining to three more and more stringent risks: *time-criticality*, *retaliation* and *collusion*.

A variety of assets are time-critical in the sense that exposing them to the risks of loss or damage may have different consequences depending on when they are exposed. For example, this is the case with the heating system or with the equipment for a public demonstration. There are times when a successful threat to such an asset will not raise much of the enterprise's concern. The Risk Analysis of time-critical assets exactly demands some account for time-criticality, which we will provide by the *Exposure Factor during Critical Time*.

The second modificator deals with the delicate issue of retaliation. No attack comes without consequences. Social engineering teaches us that a significant chance of retaliation raised by an attack may prevent the attack from happening in the first place. Any rational attacker will balance gains to risks. It follows that, if a damage can be retaliated, then it is not as problematic as it would have been without the chance of retaliation. In consequence, such a chance must be explicitly considered in a realistic Risk Analysis, as our *Exposure Factor under Retaliation* does.

The final modificator deals with the concept of collusion of attackers. Physical security of core assets in an enterprise cannot simplistically assume that the attacker is a single individual. Collusion of a group of attackers towards the same crime realistically is a higher threat against the target asset. It follows that a security measure effective against a single attacker does not necessarily remain as effective against a team of colluded attackers. Our modificator *Mitigated Risk against Collusion* will formally enter collusion into the Risk Analysis process.

The structure of this paper is simple: after the introduction of the basic terminology (§2), our original contribution is presented (§3) and some conclusions are derived (§4). The definitions are accompanied by simulations supporting the claim that the new indicators add relevant insights to the analysis that any generic enterprise may wish to conduct without excessive specificity.

2 Preliminaries

The *Risk Assessment* begins with the identification of the relevant assets. An asset can be seen as any tangible or intangible item that has some value for an enterprise and therefore needs protection. Once the assets are clearly defined, this phase produces a report describing *threats* and *vulnerabilities* that can harm a system, and advances putative *countermeasures*. Following [7,12,5], a *threat* is the potential for a threat-source to exercise (by accidental trigger or intentional exploit) a specific vulnerability; a *vulnerability* is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (by accidental trigger or intentional exploit) by an attack and result in a security breach or a violation of the systems security policy; a *countermeasure* is a control that should be implemented in order to reduce the ability for an attacker to leverage existing system vulnerabilities.

The *Risk Analysis* should determine the acceptable risk threshold and establish whether the actual total risk underlies that threshold. These are not simple tasks. There are no standard methodologies for the process, and often security managers have to decide among too many alternatives. Usually, two approaches can be taken: one is qualitative and the other one is quantitative. While the qualitative approach is based on a relative evaluation of risks, the quantitative approach [10] tries to give a precise and objective measure of risk. It adopts a number of *indicators* to mathematically calculate whether the enterprise's current risk is acceptable. Indicators are mathematical parameters formalizing the key concepts on which the enterprise intends to design its security and safety investments. The main indicators are introduced below.

The *Risk Mitigation* sees the senior management team prioritize, evaluate and implement the countermeasures recommended by the previous phases. Based on the risk level presented in the risk assessment report, the implementation actions are prioritized. Every alternative solution is analyzed calculating the indicators defined in the analysis phase, and then the most appropriate and cost-effective ones are selected for actual implementation. When the countermeasures are in place, they should be practically evaluated.

2.1 The Indicators in the Quantitative Approach to Risk Analysis

Several indicators can be used to help estimate the effectiveness of a security investment.

The Single Loss Exposure [9] gives a precise measure of how a single threat can affect or damage an asset. However, since not all threats are equally likely to occur, this value will be modified below by considering the frequency of the given threat.

Definition 2.1 (Single Loss Exposure) The *Single Loss Exposure* (SLE) represents a measure of an enterprise's loss from a single threat event and can be computed by using the following formula:

$$SLE = AV \times EF$$

where the *Asset Value* (AV) [9] is a synthetic measure of the cost of creation, development, support, replacement and ownership values of an asset, and the *Exposure Factor* (EF) [8] represents a measure of the magnitude of loss or impact on the value of an asset arising from a threat event, and is expressed as a percentage of the asset value.

The Annualized Loss Expectancy [9] attempts a financial measure of the total yearly loss or damage due to an asset.

Definition 2.2 (Annualized Loss Expectancy) The *Annualized Loss Expectancy* (ALE) is the annually expected financial loss of an enterprise that can be ascribed to a threat and can be computed by using the following formula:

$$ALE = SLE \times ARO$$

where the *Annualized Rate of Occurrence* (ARO) [9] is a number that represents the estimated number of annual occurrences of a threat.

It is important to notice that estimating the ARO could be very difficult. It is usually created upon the likelihood of the event and the number of attackers that could exploit the given vulnerability. For example, a meteorite damaging the data center could be estimated to occur only once every 100,000 years and will have an ARO of 0.000001. In contrast, 100 data entry operators attempting an unauthorized access attempt could be estimated to occur six times a year per operator and will have an ARO of 600.

Summarizing the above indicators, SLE (and EF) gives a measure of the damage of a single threat; the ARO gives the likelihood of a threat to occur in a year; ALE tries to consider both the likelihood and the damage of each threat. All of the indicators seen so far do not consider the fact that the enterprise can try to build some defense for reducing the probability of vulnerability exploitation by attackers (e.g. implementing some firewall filtering), or reducing the damage of an attack (e.g. applying some backup strategies).

The indicator that follows has the opposite property. It is exactly meant to consider the presence of countermeasures. The Return on security Investment [11] can be used to provide an economic evaluation of an enterprise's expenditure in security. It can help compare alternative investment strategies and evaluate whether an investment is financially justified.

Definition 2.3 (Return on Investment) The *Return on Investment* (ROI) indicator can be computed by using the following formula:

$$ROI = \frac{(ALE \times MR) - CSI}{CSI}$$

where MR is the *risk mitigated by a countermeasure* and represents the effectiveness of a countermeasure in mitigating the risk of loss deriving from exploiting a vulnerability (expressed as a numeric value in [0,1]), and CSI is the *cost of security investment* that an enterprise must face for implementing a given countermeasure.

If ROI is a positive number, the cost for the investment is financially justified.

Otherwise, if ROI is zero or a negative number, the investment is not profitable.

3 Three Novel Indicators

This section presents our contribution to Risk Analysis in the form of three unpublished indicators, which precisely are modificators of existing indicators. It is clear that innumerable indicators can be defined and exemplified. But they must be worthwhile in the sense that they are meant to bring forward details that are worth the while from modern companies' standpoints. For example, one may wish to define an indicator for the number of hinges that a specific threat will break. Although this might be meaningful for the Maintenance Office, it may not always be entirely worthwhile for the enterprise.

One may naively think that a valuable indicator must not address a microscopic detail such as the number of broken hinges, and that only macroscopic details are worthwhile. But this is not at all a theorem. A microscopic indicator may turn out to be relevant if specific analyses are being carried out, such as exactly on resistance of the hinges. The converse example says that the cost of installing stronger hinges is subsumed by the ROI, which may generically embody a variety of security measures. It follows that a valuable Risk Analysis tradeoffs detail and intelligibleness.

Our modificators address three major concerns that the industrial world is increasingly having to face day after day. One has to do with assets that are time-critical (§3.1). Exposing such an asset at specific, critical times will produce a different damage than at other times. So, the Exposure Factor must be upgraded. The second modificator deals with the delicate issue of retaliation (§3.2). In brief, if a damage can be retaliated, then it is not as problematic as it would have been without the chance of retaliation. The classic Exposure Factor is upgraded also in this case. The last parameter deals with attacks performed by a team of colluded attackers (§3.3). A security measure that is effective against a single attacker is not necessarily as effective against a team of attackers. The Mitigated Risk must be upgraded here. The definition of each modificator is followed by a table simulating its use.

Asset	AV	EF	ARO	SLE	ALE
Demo Machine	5000$	30%	55%	1500$	825$
Simulation Infrastructure	30000$	40%	60%	12000$	7200$
Researcher's Machine	3000$	15%	20%	450$	90$

Table 1
Demonstrating EFCT and related indicators.

3.1 The Exposure Factor during Critical Time

We have seen above that the EF is related to a threat and an asset. It expresses the percentage of damage that the threat causes on the asset. However, modern companies have to face asset exposures under various working circumstances, ranging from

public presentations to rushes before deadlines. Many assets can be time-critical in this very sense.

Innumerable examples are easy to advance here, but we only point out three working examples. A trojan-horse attack to a computer running the first public demonstration of the latest version of an Operating System certainly is more devastating than the same attack in private circumstances. The asset "demo machine" is time-critical. Along the same lines, an experiment that takes, say, months to complete would have worse consequences if compromised towards its end rather than towards its beginning. The worse attack might disrupt months of work. The asset here can be generically described as the "simulation infrastructure", which might be a single computer as well as a complex architecture of devices of various nature. It is easy to derive another example from the academic researchers' world: one would rather have his computer infected with malware the day after a deadline than the day before.

We feel that the EF is insufficient to treat time-critical assets, and advance an upgraded version that takes into account the criticality of the time instance that is being considered. This inspires the following definition.

Definition 3.1 (EFCT) The *Exposure Factor during Critical Time*, *EFCT* in brief, expresses the influence that the criticality of a specific time instance plays on the EF as follows:

$$EFCT = (EF + CTF) - (EF \times CTF)$$

CTF being the *Critical Time Factor* that expresses the percentage of criticality of a specific time instance.

The definition of EFCT is perhaps easier to interpret in terms of set theory. Let us think of $+$ as the set union operator, of $-$ as the set difference operator, and of $\times$ as the set intersection operator. The new indicator takes the two component sets EF and CTF, unions them and then subtracts their intersection. Intuitively, the resulting set will not be bigger than the union of two component sets, and will not be smaller than the bigger of the component sets carved of the smaller component.

It is also clear in numerical terms that the CTF can only increase the EFCT over the EF. Likewise, we have that the highest CTF raises the EFCT to its top regardless of the EF. These simple observations underly the following double proposition.

Proposition 3.2

- *If* $CTF = 0$*, then* $EFCT = EF$*.*
- *If* $CTF = 1$*, then* $EFCT = 1$*.*

The same statement can be trivially rephrased swapping CFT and EF, as in the following proposition. However, it may exceed intuition that the totality of CTF ends up into EFCT even if EF is null. It means that even a normally uninteresting asset becomes problematic if attacked during critical time. It seems more intuitive that the highest EF produces the highest EFCT regardless of the CTF.

Proposition 3.3

- *If* $EF = 0$, *then* $EFCT = CTF$.
- *If* $EF = 1$, *then* $EFCT = 1$.

The intermediate cases in which none of EF and CTF reach their limits may turn out to be more relevant. They are exemplified later on in Table 2. However, prior to the description of the Table, we must observe that all indicators classically calculated in terms of EF ought to be recalculated in terms of EFCT, producing versions that are sensitive to the Critical Time Factor.

Definition 3.4 (AROCT, SLECT, ALECT and ROICT)

- The *Annualized Rate of Occurrence during Critical Time*, *AROCT* in brief, is the rate of occurrence of an attack at a specific CTF per year.
- The *Single Loss Exposure during Critical Time*, *SLECT* in brief, is the cost of a single attack at a specific CTF:
$$SLECT = AV \times EFCT$$
- The *Annualized Loss Expectancy during Critical Time*, *ALECT* in brief, is the cost per year of an attack at a specific CTF:
$$ALECT = SLECT \times AROCT$$
- The *Return On Investment against Critical Time*, *ROICT* in brief, is the economic return of an enterprise's investment against an attack mounted at a specific CTF:
$$ROICT = \frac{(ALECT \times MR) - CSI}{CSI}$$

We can now move on to describing Table 2. It demonstrates EFCT versus EF and the consequences upon the related indicators. Our three working examples are considered for the sake of demonstration.

Let us consider the first asset. Its classical EF is some 30% as the demo machine is not particularly important during normal time periods. But its EFCT goes up to 96,5% because of the high CTF considered here, as it is for example at time of a public demonstration. In consequence, the SLECT is much higher than the SLE, nearly reaching the AV. It can also be seen that the AROCT is much lower than the ARO because it is assumed that a public demonstration can rely on the maximum precautions to make things work smoothly. Despite that, the ALECT is still approximately 50% higher than the ALE.

The second asset is the large simulation infrastructure typically used to conduct long experiments. The high CTF refers to a time when a very long experiment is about to terminate. Its influence on the SLECT is net. It is assumed that the infrastructure is subject to attacks with a rate of occurrence that is independent of the CTF. This proceeds from the assumption that always the same set of precautions is taken through time. This assumption has a major impact on the ALECT, which is some two and half times the ALE.

Analogous considerations apply to the last asset despite the smaller amounts. The analysis can be easily continued to study the ROICT with respect to the ROI.

Asset	CTF	EFCT	AROCT	SLECT	ALECT
Demo Machine	95%	96,5%	25%	4825$	1206,25$
Simulation Infrastructure	98%	98,8%	60%	29640$	17784$
Researcher's Machine	90%	91,5%	20%	2745$	549 $

Table 2
Demonstrating EFCT and related indicators.

3.2 The Exposure Factor under Retaliation

A recent analysis standpoint for security issues is that of retaliation [4]. Although it is certain to be socially rejected at present, retaliation may open new and interesting perspectives in terms of digital security.

The concept was originally spelled out in the context of security protocols [3]. Two decades of research efforts have been spent to analyse security protocols. Such analyses would either find protocol flaws or prove the protocols immune to attacks. A number of papers have been published to report on previously unknown protocol flaws and to often come to the same conclusion: the protocol must be redesigned because it is flawed.

Modern security economics [1] teaches us that is not always possible in practice to redesign a security system from scratch even after serious evidence that it is flawed. The system may already be widely deployed so that the costs of its global replacement would be prohibitive for any enterprise. An important contribute to the currently fervid debate is the chance to keep a flawed system in use without much concern if it is found that the attack can be retaliated.

An attack is always the outcome of a balanced decision between the risks of performing it and the consequent benefits. The chance of retaliation may influence the balance favourably — from the legal perspective. Who would infect a competitor's computer if the chances of consequently having a room of computers infected by that competitor were significant? Retaliation may in fact be taken as a strategy to keep a heterogeneous system stable, in a setting where ethical issues unfortunately seem weary.

Our contribution here is a generalization of the concept of retaliation from the specific setting of security protocols to the broad security setting. Industrial espionage, which is a well-known though hardly documented reality, arguably proceeds on this very paradigm: spy on competitors but never allow them to take advantage of this espionage. Hence, we feel that the classical EF must be upgraded to consider attacks on assets that can be retaliated. This inspires the following definition.

Definition 3.5 (EFR) The *Exposure Factor under Retaliation*, *EFR* in brief, expresses the influence that the chance of retaliating an attack to an asset plays on the EF as follows:

$$EFR = EF \times (1 - RF)$$

RF being the *Retaliation Factor* that expresses the percentage of retaliation that can be performed.

Also in this case an interpretation in terms of set theory may help the reader's

intuition. The $-$ and $\times$ operators can be interpreted routinely as set difference and set intersection.

It is interesting to notice in numerical terms that a null RF leaves the EFR unaltered as EF, whereas the highest RF brings down to null EFR regardless of EF. These simple observations underly the following double proposition.

Proposition 3.6

- *If* $RF = 0$, *then* $EFR = EF$.
- *If* $RF = 1$, *then* $EFR = 0$.

Focusing on EF, it is clear that a null EF causes a null EFR. while the highest EF leaves EFR entirely dependent on RF, as stated in the following proposition.

Proposition 3.7

- *If* $EF = 0$, *then* $EFR = 0$.
- *If* $EF = 1$, *then* $EFR = 1 - RF$.

The consequences of this proposition are not trivial. The first of its statements says that zero damage entails zero retaliation, as it is intuitive. The second highlights that the highest EF and the highest RF together bring the EFR down to null. Some pondering may convince that this is exactly in the spirit of retaliation. If we can totally retaliate, then we can get paid back of exactly what was stolen to us.

All indicators normally are conventional percentages and hence range between 0 and 1. However, we can imagine that the right end of the range of RF is open. It means that retaliation can even double or more the effects of the action that induced it in the first place. Interestingly enough, an EF of 1 and an RF of 2 will produce and EFR of -1 which in fact expresses a benefit for the entity that was originally attacked but then retaliated back.

As done in the previous section, all indicators relying on EF can be easily reformulated to rely on EFR, as stated in the following definition.

Definition 3.8 (AROR, SLER, ALER and ROIR)

- The *Annualized Rate of Occurrence with Retaliation*, *AROR* in brief, is the rate of occurrence per year of an attack that can be retaliated.
- The *Single Loss Exposure with Retaliation*, *SLER* in brief, is the cost of a single attack that can be retaliated:
$$SLER = AV \times EFR$$
- The *Annualized Loss Expectancy with Retaliation*, *ALER* in brief, is the cost per year of an attack that can be retaliated:
$$ALER = SLER \times AROR$$
- The *Return On Investment with Retaliation*, *ROIR* in brief, is the economic return of an enterprise's investment against an attack that can be retaliated:
$$ROIR = \frac{(ALER \times MR) - CSI}{CSI}$$

It can be seen that a very small ALER, namely a negative number actually expressing a benefit for the attacked enterprise, would produce a negative ROIR. Not only would this be an indication that a security investment is inconvenient, but it would also express the paradox that the enterprise rather benefits from being attacked and then retaliating. To the best of our knowledge, this is the first time that negative versus positive outcomes are accounted for in the context of Risk Analysis.

It is interesting to describe Table 3. It is assumed that an attack on the first asset has a small chance of retaliation, 25%. This moderately differentiates the EFR from the EF. A similar minor difference hence appears between the SLE and the SLER. The AROR, which is only 15%, is assumed to be much lower than the ARO because an attack that can be retaliated is better than one that cannot be and hence pessimistically considered rarer. This produces a much smaller ALER than the corresponding ALE. Such a conclusion might seem positive but in fact is not. It is merely due to the smaller AROR and not to the benefits of retaliation. These are better reflected by the SLER.

The second asset sees a similarly low retaliation factor but no variation between ARO and AROR. With this very static asset, it is reasonable to assume that attacks that can be retaliated occur at the same rate as attacks that cannot. This is in contrast with the first asset. The same considerations made for the first asset apply to the SLER and to the AROR here.

The third asset gains interest in this Table. It is assumed that when the single researcher's machine is attacked, the researcher has sufficient knowledge to learn and do the same back to its attacker. He might even most realistically improve the attack methodology, as the current statistics confirm. Here comes an RF of 130%, producing a negative EFR, precisely of $-4,5\%$. The negative SLER signifies that the researcher that was originally attacked will actually profit 135$ from attacking back! The negative ALER also reflects this setting. Because the MR and the CSI are never negative, the negative ALER produces a negative ROIR. It is a clear indication that any security investment to prevent the attack is technically inconvenient: the researcher benefits from being attacked and then attacking back.

Asset	RF	EFR	AROR	SLER	ALER
Demo Machine	25%	23%	15%	1150$	172,5$
Simulation Infrastructure	25%	30%	60%	9000$	5400$
Researcher's Machine	130%	-4,5%	20%	-135$	-27 $

Table 3
Demonstrating EFR and related indicators.

3.3 The Mitigated Risk against Collusion

Facing a single attacker is not generally the same as facing a team of attackers working for the same illegal purpose. Researchers in computer security have considered this issue determinant ever since the 1970s. A security measure may withstand an attacker but fail to resist another one. Therefore, any security statement is strongly

dependent on the kind of attacker that is assumed to operate.

A milestone in this area of research is the work of Dolev and Yao [6]. They advance a formal account for the threats against computer security and come to the brilliant conclusion that any set of colluding attackers is functionally equivalent to a single super-potent attacker. Equivalence here means that any illegal operation that the set of attackers can accomplish, also the single super-potent attacker can do.

Remarkably, this model of attacker has been adopted by researchers in computer security for some two decades. However, its age is starting to show [2], as collusion against computer security is not always necessary or desired at present. Offensive skills have become easy and cheap to acquire, so the present setting sees a large number attackers each working for his own sake. It is worth remarking that our treatment here is oriented to any security issues that an enterprise must face, and not to just those in computer security. If it is debateable that the Dolev-Yao threat model is rather unrealistic for computer security nowadays, it undoubtedly is entirely inappropriate for general security.

The best example might come from film fictions presenting attacks to banks or casinos performed by teams of colluded robbers. It is clear that a single attacker would have failed against such a demanding target. Not even surrounding a treasure with a number of robust steal-alloy doors operated by retina scanners will protect the treasure from an offending team with the same number of kamikazes plus a leader. If these examples confirm yet again the importance of setting a threat model, they also call for a detailed Risk Analysis able to account for the differences between one and many colluded attackers.

The Mitigated Risk [5] easily reflects the moderation percentage of a security attack following the adoption of a security measure. This indicator appears to be too static to both account for mitigation against a single attacker and a team of attackers. This concern inspires the following definition.

Definition 3.9 (MRC) The *Mitigated Risk against Collusion*, *MRC* in brief, expresses the influence that collusion of attackers plays on the MR as follows:

$$MRC = MR \times (MR - CF)$$

CF being the *Collusion Factor* that expresses the percentage of collusion of the attacker(s).

Identical propositions to 3.6 and 3.7 can be stated here replacing EFR with MRC, EF with MR, and RF with CF. Similar considerations apply. If CF is null, then MRC equals MR. Also, if a risk is totally mitigated, that is MR is 1, but CF is also 1, then MRC goes down to 0. The highest CF expresses a theoretical team of an infinite number of attackers, which can be imagined to subvert any security measure [5].

Following the MRC, also the ROI can be easily augmented as the following

[5] Notice that the percentage of collusion of the attackers, CF, depends to the type of applications, protocols and systems that we consider.

definition states.

Definition 3.10 (ROIC) The *Return On Investment against Collusion*, *ROIC* in brief, is the economic return of an enterprise's investment against an attack mounted by one or more colluding attackers:

$$ROIC = \frac{(ALE \times MRC) - CSI}{CSI}$$

Table 4 exemplifies the indicators defined in this section. It can be seen that the MRC of the first asset dramatically reduces the MR because of the high CF, which is realistic because of the importance of the machine. Therefore, while the ROI is moderately positive, the ROIC is significantly negative, expressing the large difference between adopting the related security measure against a single attacker or against a rather large team of colluded attackers (as indicated by CF=45%). This discrepancy precisely alerts the enterprise against attacks distributed on various, related fronts. The very security measure that is considered will not be effective against them.

As a transversal observation, let us consider the fourth column. It shows that the Cost of Security Investment is always lower than the ALE, as it is sensible. It is relatively low in case of the second asset. Here, the MRC also is much lower than the MR but the discrepancy is smaller than in the first case. In consequence, the ROI and ROIC are not as far apart as they were with the first asset, although they continue to signify that the security measure is only effective against a single attacker.

The third asset shows a high CSI compared to its ALE. The CF is low, as we are assuming an individual's networked machine. It can be seen that the MRC only moderately decreases the MR, and so does the ROIC with the ROI. The related security measure that is effective against a single attacker still is effective against a relatively small team of hackers.

Asset	CSI	CF	MR	MRC	ROI	ROIC
Demo Machine	600$	45%	85%	46,75%	16,87%	-35,71%
Simulation Infrastructure	4500$	35%	75%	45%	20%	-22%
Researcher's Machine	70$	10%	90%	81%	15,71%	4,14%

Table 4
Demonstrating MRC and related indicators.

4 Conclusion

Risk Analysis perhaps is the main phase of the Risk Management process, as it provides the mathematical methods to evaluate the risk and decide consequent security investments. It has gained importance in recent years and lately any medium or larger enterprise makes some investment in this process.

A variety of indicators are defined in the quantitative approach to Risk Analysis. An important one, the Exposure Factor, expresses the damage that a successful

threat on an asset causes to the enterprise. Another significant indicator, the Mitigated Risk, formalises the success of a security measure in withstanding a threat. This paper has advanced three novel indicators, two of which are modificators of the Exposure Factor, and the other one is a modificator of the Mitigated Risk.

Our Exposure Factor during Critical Time (EFCT) expresses the influence of time-criticality on EF. The Exposure Factor against Retaliation (EFR) indicates how the chance of retaliation can influence EF. The Mitigated Risk against Collusion (MRC) formalises the impact of a security measure against a team of colluded attackers. We have seen simulated results to demonstrate the novel insights that the three modificators can bring out.

All fundamental indicators defined in terms of EF, such as SLE and then ALE, or in terms of MR, such as ROI, have to be redefined in terms of EFCT, EFR and MRC, producing four sibling sets of indicators if we include the classical ones. In consequence, an enterprise may calculate the classical set first and then our three augmented sets. An evaluation of eventual discrepancies between related indicators, such as SLE and SLECT, or ALE and ALER, would confirm that attention must be paid to the very aspect that the augmented indicator considers, such as time-criticality or retaliation.

As future work we plan to investigate on acceptable thresholds for the new indicators we introduce also, we plan to use intervals of value (instead of only a single) for the indicator (ARO, EF, CFT, RF and CF). Using intervals we can take in account the uncertainty related to the estimation of the above indicators. Then we plan to study the effectiveness of our new indicators by testing them in same real cases.

Our present effort confirms that research in Risk Analysis is strongly motivated and steadily progressing.

References

[1] Anderson, R., "Security Engineering: A Guide to Building Dependable Distributed Systems," Wiley, 2001.

[2] Bella, G. and S. Bistarelli, *Soft constraint programming to analysing security protocols*, Theory Pract. Log. Program. **4** (2004), pp. 545–572.

[3] Bella, G., S. Bistarelli and F. Massacci, *A protocol's life after attacks*, in: *Proc. of the 11th Security Protocols Workshop (SPW'03)*, LNCS **3364** (2005), pp. 3–18.

[4] Bella, G., S. Bistarelli and F. Massacci, *Retaliation: Can We Live with Flaws?*, in: M. Essaidi and J. Thomas, editors, *Proc. of the NATO Advanced Research Workshop on Information Security Assurance and Security* (2005).

[5] Bistarelli, S., F. Fioravanti and P. Peretti, *Defense trees for economic evaluation of security investments*, in: *Proc. of the 1st Int. Conference on Availability, Reliability and Security (ARES'06), The International Dependability Conference: Bridging Theory and Practice* (2006), pp. 416–423.

[6] Dolev, D. and A. Yao, *On the security of public-key protocols*, IEEE Transactions on Information Theory **2** (1983), pp. 198–208.

[7] Jenkins, B. D., *Security Risk Analysis and Management*, white paper, Norman Data Defense Systems, Inc. (1998).

[8] Krause, M. and H. F. Tipton, "Handbook of Information Security Management," Auerbach Publications, 1999.

[9] Krutz, R. L., R. D. Vines and E. M. Stroz, "The CISSP Prep Guide: Mastering the Ten Domains of Computer Security," Wiley, 2001.

[10] Meritt, J. W., *A Method for Quantitative Risk Analysis*, in: *Proc. of the 22nd National Information Systems Security Conference*, 1999.

[11] Sonnenreich, W., J. Albanese and B. Stout, *Return On Security Investment (ROSI): A Practical Quantitative Model*, in: E. Fernández-Medina, J. C. Hernández and L. J. García, editors, *Security in Information Systems, Proc. of the 3rd Int. Workshop on Security in Information Systems (WOSIS'05), In conjunction with ICEIS'05* (2005), pp. 239–252.

[12] Stoneburner, G., A. Goguen and A. Feringa, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800–30, NIST (2002).