Security Risk Assessment: Towards a Justification for the Security Risk Factor Table Model

Beverly Rivera[1], Francisco Zapata[2], and Vladik Kreinovich[1]
[1]Computational Science Program
[2]Department of Industrial, Manufacturing, and
Systems Engineering
University of Texas at El Paso
El Paso, TX 79968, USA
barivera@miners.utep.edu, fazg74@gmail.com, vladik@utep.edu

Abstract

One of the widely used methods to gauge risk is the Security Risk Factor Table (SRFT) model. While this model has been empirically successful, its use is limited by the fact that its formulas do not have a theoretical explanation – and thus, there is no guarantee that these formulas will work in other situations as well. In this paper, we provide a theoretical explanation for the SFRT formulas.

1 Formulation of the Problem

Security Risk Factor Table (SRFT) model: a brief description. Many systems face security risks. To properly protect these systems, it is important to gauge relative security risk of different systems, so that more resources will be used to protect systems with higher risk.

One of the widely used techniques for gauging risk is the Security Risk Factor Table (SRFT) model; see, e.g., [1, 2, 3, 4]. In this model, important factors affecting risk are listed, such as location, visibility, inventory, etc. For each factor, experts estimate the risk corresponding to this factor by selecting a number from 0 to 5, 0 meaning lowest risk and 5 meaning highest risk. Numbers corresponding to different factors are then added into a single *risk score*. Based on the value of the risk score, the system's risk is then classified into low, moderate, high, and extreme.

For example, for 15 factors:

- scores below 15 indicate low risk;
- scores from 16 to 30 indicate moderate risk;
- scores from 31 to 45 indicate high risk, and

- scores above 45 indicate extreme risk.

Problem. The SRFT model has been empirically successful – as judged, e.g., by the fact that it is widely used. The fact that it is successful seems to indicate that this model indeed reflects the actual risks. So, a natural question is: why is the above simple model properly reflecting actual risks?

Specifically, why adding the scores makes sense? Why equally spaces thresholds (15, 30, 45) make sense?

What we do in this paper. In this paper, we analyze the risk situation, and we show that this analysis indeed explains the two main features of the SRFT model: addition of scores and equal spacing of thresholds.

2 Why Adding Scores Make Sense: Our Explanation

A natural way to gauge risk. A natural way to gauge risk for a system is to estimate the expected value of the loss due to a possible attack on this system. In general, the expected loss E is equal to the product $E = P \cdot L$ of the probability P of a successful attack and a loss L caused by this attack.

The success of an attack depends on several independent factors: for the attack to be successful, the location must be vulnerable to an attack, the system must be highly visible, perimeter protection must be weak, etc. Since these factors are independent, the probability P of a successful attack is equal to the product $P = P_1 \cdot \ldots \cdot P_n$ of the probabilities $P_1, \ldots, P_n$ corresponding to these factors.

Thus, we conclude that the expected loss E is equal to the product

$$E = P_1 \cdot \ldots \cdot P_n \cdot L, \tag{1}$$

where the values P_i and E describe different factors affecting risk.

Analyzing the resulting formula. Let us show that the formula (1) enables us to explain the addition of scores.

Before we start our explanation, let us note that while from the purely mathematical viewpoint, the value E depends in a similar way on all $n + 1$ factors $P_1, \ldots, P_n$, and L, the ranges of possible values of these factors are different:

- most of the factors are probabilities, i.e., numbers whose possible values are between 0 and 1, while
- the numerical value of the loss L is usually much larger than 1.

To make the formula more symmetric, let us replace the actual loss in dollars L with a relative loss $\ell \stackrel{\text{def}}{=} \dfrac{L}{L_{\max}}$, where $L_{\max}$ is the largest possible loss. The resulting product

$$p \stackrel{\text{def}}{=} P_1 \cdot \ldots \cdot P_n \cdot \ell \tag{2}$$

describes the expected value of the relative loss.

The comparison of risk of different systems does not depend on the units used to describe loss:

- a system with the higher value of E will have the higher value of $\ell = \dfrac{E}{L_{\max}}$;
- similarly, a system with the lower value of E will have the lower value of ℓ.

Thus, we can use the formula (2) to gauge risks.

Now that all the factors $P_1, \ldots, P_n$, and ℓ are from the interval $[0, 1]$, we can denote ℓ by P_{n+1} and get a simplified formula

$$p = \prod_{i=1}^{n+1} P_i. \tag{3}$$

From the usual formula for risk to score addition. In the usual risk formula, the risk measure is equal to the *product* of risk measures corresponding to different factors. We would like to justify the SRFT technique in which we compute the *sum* of the values corresponding to different factors. There is a natural way to go from a product to a sum: by taking the logarithm – since the logarithm of the product is equal to the sum of the logarithms.

The larger p, the larger its logarithm $\ln(p)$. So, to decide which schemes leads to a smaller risk, instead of comparing the values p corresponding to different schemes, we can alternatively compare the logarithms $\ln(p)$.

For the logarithms, the formula (3) leads to

$$\ln(p) = \sum_{i=1}^{n} \ln(P_i). \tag{4}$$

If we use this formula, then, to estimate the overall risk $\ln(p)$ of a system, we add the scores $\ln(P_i)$ corresponding to different factors – and this is exactly what is done in the the SRFT technique.

We have therefore explained why the addition of scores makes sense when assessing the overall risk.

Comment. While we explained why the SRFT idea of adding scores makes sense, the scores $\ln(P_i)$ that we use in our explanation are different from the scores used by SRFT: indeed, the SRFT scores are always non-negative (and usually positive), while the logarithms $\ln(P_i)$ are always non-positive (and usually negative).

To come up with non-negative scores, we can use the fact that the comparison between two quantities x_1 and x_2 does not change if we use a different scale for measuring both quantities, i.e., a different starting point and a different measuring unit. For example, a temperature which is large in the Fahrenheit scale is also larger in the Celsius scale. In general, if we use the new scale $y = a \cdot x + b$ with $a > 0$, then $x_1 > x_2$ if and only if $y_1 > y_2$, where $y_i \stackrel{\text{def}}{=} a \cdot x_i + b$.

So, instead of the logarithms $\ln(P_i)$, we can use expressions $S_i = a \cdot \ln(P_i) + b$. Here, $\sum S_i = a \cdot \sum_{i=1}^{n+1} \ln(P_i) + (n+1) \cdot b$, so minimizing this sum is equivalent to minimizing the expression (4). Let us select the values a and b in such a way that the resulting scores match the scale used in the SRFT mode.

In SRFT, for each factor i, the worst risk has a score $S_i = 5$, while the smallest risk corresponds to $S_i = 0$. In terms of the corresponding probability P_i, the worst case is when $P_i = 1$, and the best case is when P_i is equal to some pre-defined small value p_0. (In real life, there is always some risk, so we cannot reach $P_i = 0$.) Thus, we should have $a \cdot \ln(1) + b = 5$ and $a \cdot \ln(p_0) + b = 0$. The first equality implies $b = 5$, and thus, the second leads to $a \cdot \ln(p_0) = -b = -5$ and $a = \dfrac{5}{|\ln(p_0)|}$.

3 Why Thresholds Are Equally Spaced: Our Explanation

Main idea: let us take into account that risks can be only estimated with some uncertainty. Based on the scores $S_i = a \cdot \ln(P_i) + b$ corresponding to different factors i, we form the summary score

$$S = \sum_{i=1}^{n+1} s_i = a \cdot \ln(p) + (n+1) \cdot b. \tag{5}$$

Since the probabilities P_i (and thus, the scores $s_i = a \cdot \ln(P_i) + b$) are only approximately known, the resulting score is estimated with some estimation error. If the difference between the scores of two different arrangements is smaller than this estimation error, we may not be able to notice this difference based on the estimates corresponding to these arrangements.

Instead of the numerical values of the risk scores – whose exact values are affected by estimation errors – it thus makes sense to consider groups of distinguishable risks.

From the main idea to the actual classification of risks. Based on our estimates for the probabilities P_i, we can estimate the resulting risk p only with some uncertainty. Let us denote the relative accuracy of estimating p by k.

This means that when we know the estimate $\widetilde{p}$ for the relative loss, the actual (unknown) value p of this relative loss can be anywhere within the interval $[\widetilde{p} - k \cdot \widetilde{p}, \widetilde{p} + k \cdot \widetilde{p}]$, i.e., within the interval $[\widetilde{p} \cdot (1-k), \widetilde{p} \cdot (1+k)]$.

When the two estimates $\widetilde{p} < \widetilde{q}$ are close to each other, the corresponding intervals $[\widetilde{p} \cdot (1-k), \widetilde{p} \cdot (1+k)]$ and $[\widetilde{q} \cdot (1-k), \widetilde{q} \cdot (1+k)]$ have a non-empty intersection, which means that it is possible that both estimates correspond to the same value of risk p.

The estimates are guaranteed to correspond to different values of risk if the corresponding intervals do not intersect, i.e., when $\widetilde{p} \cdot (1+k) < \widetilde{q} \cdot (1-k)$, or,

equivalently, when $\widetilde{q} > \widetilde{p} \cdot \dfrac{1+k}{1-k}$.

For a given $\widetilde{p}$, the minimum of the values $\widetilde{q}$ which satisfy this inequality – i.e., which correspond to a definitely higher actual risk – is equal to $\widetilde{q} = \widetilde{p} \cdot \dfrac{1+k}{1-k}$. Thus, if we select $\widetilde{p}$ as a representative of a certain level of risk, then the next higher level of risk starts at $\widetilde{q} = \widetilde{p} \cdot \dfrac{1+k}{1-k}$.

So, if we start with the value $\widetilde{p}_0$ corresponding to the smallest value of risk, then the next representative risk values are $\widetilde{p}_1 = \widetilde{p}_0 \cdot \dfrac{1+k}{1-k}$, $\widetilde{p}_2 = \widetilde{p}_1 \cdot \dfrac{1+k}{1-k} = \widetilde{p}_0 \cdot \left(\dfrac{1+k}{1-k}\right)^2$, and, in general, $\widetilde{p}_j = \widetilde{p}_0 \cdot \left(\dfrac{1+k}{1-k}\right)^j$.

Resulting explanation. For these values $\widetilde{p}_j$ of relative loss, the corresponding values of risk $\widetilde{S}_j = a \cdot \ln(\widetilde{p}_j) + (n-1) \cdot b$ take the form

$$\widetilde{S}_j = a \cdot \ln(\widetilde{p}_0) + j \cdot a \cdot \ln\left(\frac{1+k}{1-k}\right) + (n-1) \cdot b. \tag{6}$$

We can see that these values linearly depend on j, i.e., that they are indeed equally spaced: the difference $\widetilde{S}_{j+1} - \widetilde{S}_j$ between the two consecutive thresholds $\widetilde{s}_j$ is a constant $a \cdot \ln\left(\dfrac{1+k}{1-k}\right)$.

We have therefore explained why in the SRFT model, thresholds are equally spaced.

Acknowledgments. This work was supported in part by the El Paso Regional Cyber and Energy Security Center RCES and by National Science Foundation grants HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence) and DUE-0926721.

References

[1] Advanced Chemical Safety, Assessing Risk, available at http://chemical-safety.com/documents/pdf/SECURITY

[2] American Petroleum Institute (API), *Secirity Guidelines for the Petroleum Industry*, Washington, DC, 2003, available at http://new.api.org/policy/otherissues/upload/Security.pdf

[3] S. Baijal and J. P. Gupta, "Site security for chemical process industries", *Journal of Loss Prevention in the Process Industries*, 2005, Vol. 18, pp. 301–309.

[4] S. Baijal and J. P. Gupta, "Securing oil and gas infrastructure", *Journal of Petroleum Science and Engineering*, 2007, Vol. 55, pp. 174–186.