2014

Measuring Security: A Challenge for the Generation

Janusz Zalewski
Florida Gulf Coast University, zalewski@erau.edu

Steven Drager
Air Force Research Lab, steven.drager@us.af.mil

William McKeever
Air Force Research Lab

Andrew J. Kornecki
Embry-Riddle Aeronautical University, kornecka@erau.edu

Position papers of the 2014 Federated Conference on Computer Science and Information Systems pp. 131–140
DOI: 10.15439/2014F490
ACSIS, Vol. 3

Measuring Security: A Challenge for the Generation

Janusz Zalewski
Dept. of Software Engineering
Florida Gulf Coast University
Ft. Myers, FL 33965, USA
zalewski@fgcu.edu

Steven Drager
William McKeever
Air Force Research Lab
Rome, NY 13441, USA
Steven.Drager@us.af.mil
William.McKeever.1@us.af.mil

Andrew J. Kornecki
ECSSE Department
Embry-Riddle Aeronautical Univ.
Daytona Beach, FL 32114, USA
kornecka@erau.edu

***Abstract*—This paper presents an approach to measuring computer security understood as a system property, in the category of similar properties, such as safety, reliability, dependability, resilience, etc. First, a historical discussion of measurements is presented, beginning with views of Hermann von Helmholtz in his 19-th century work "Zählen und Messen". Then, contemporary approaches related to the principles of measuring software properties are discussed, with emphasis on statistical, physical and software models. A distinction between metrics and measures is made to clarify the concepts. A brief overview of inadequacies of methods and techniques to evaluate computer security is presented, followed by a proposal and discussion of a practical model to conduct experimental security measurements.**

I. Introduction

WHEN Henry I, the King of England, decreed in the first half of the XII-th century that a yard shall be "the distance from the tip of the King's nose to the end of his outstretched thumb", neither he nor any of his subjects realized that the first standard of measuring length was introduced over the ages [1]. The standard of measuring length (distance) has significantly evolved, from the ancient Egyptian cubit to the one based on physical properties, as captured in a diagram presented in Figure 1.

The current definition of the standard unit of length, a *meter*, involves the speed of light and reads as follows [2]: "the length of the path travelled by light in vacuum during a time interval of 1/299,792,458 of a second." The historical evolution of the humankind's understanding of the unit of length, pictured in Figure 1, shows an amazing path, which led us from a very vague concept to an extremely precise definition based on the speed of light, we have now. It must be noticed, however, that it took us nearly 800 years to straighten the concept, which we now take for granted.

It is the conjecture of this paper that at current stage of understanding how to measure security as a system property, we are at the point comparable to the early days of attempting to measure length. All methods we have are as vague as the one applied by Henry I to defining the unit of length. In this view, the rest of the paper is devoted to clarification of basic concepts of measurement and how they can be applied to building a model of security as a system property that could be used to measuring security.

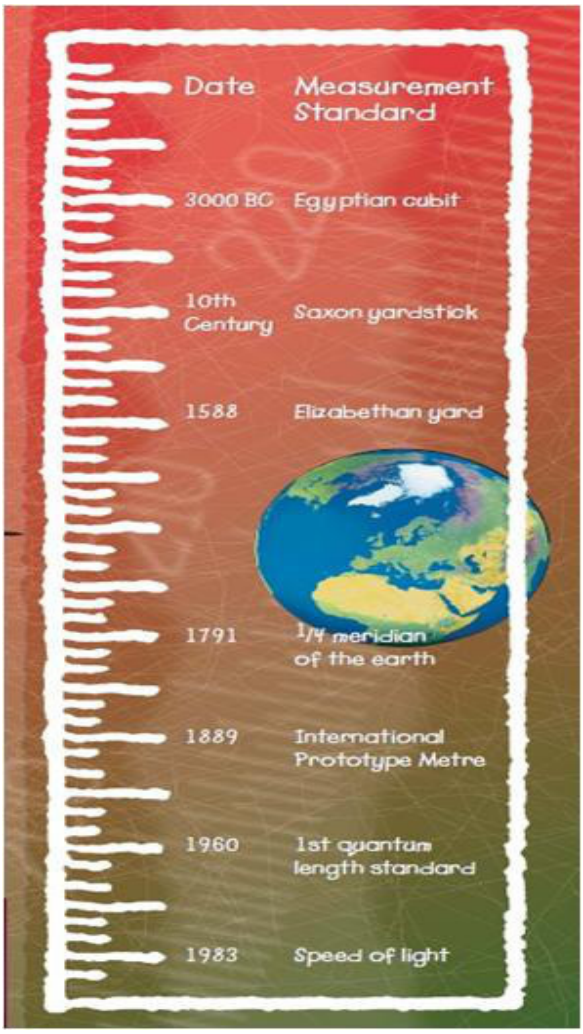

Fig. 1 Evolution of the concept of unit of length [1]

This work was supported in part by the 2014 Visiting Faculty Research Program at the Information Institute of the Air Force Research Labs, in Rome, New York. Distribution A: approved for public release.

II. What is a Measurement?

A. Hermann von Helmholtz Concept of Measurement

Although there are several concepts of measurement, they all seem to converge to the idea formulated in the 19-th century by Herman von Helmholtz, in his groundbreaking work "Zählen und Messen" [3], in which Helmholtz says:

> "The special relation which can exist between the attributes of two objects and which is designated by us by the name equality is characterized by […] Axiom I: If two magnitudes are equal to a third, they are equal to each other."

This statement, which may seem trivial from today's perspective, actually is very constructive and quite distinctly sets the stage for conducting measurements in a way that it determines the following:

- a *property* (called an attribute) of a object to be measured;
- a *standard*, that is, in Helmholtz' words, the third magnitude, to which others are compared; and
- an existence of a *procedure* used to make the comparisons between magnitudes.

This procedure is further characterized by von Helmholtz in the same work, as follows:

> "The procedure by which we put the two objects under proper conditions in order to observe the stated result and to be able to establish its occurrence or its non-occurrence, we shall designate as the method of comparison."

Defining measurement procedure as a method of comparison, von Helmholtz gives several examples of physical quantities that can be measured, by comparison with a standard, including distance, time, brightness, pitch of tone and weight, measured with the use of scales, for which he explains the measurement principle further:

> "… the bodies the weights of which we compare can consist of the most different materials and can be of different form and volume. The weight which we call equal is only an attribute of these bodies discriminated by abstraction."

To summarize, the contribution of von Helmholtz was to make a clear distinction between three factors necessary for a measurement to make sense: a property to be measured, a standard against which comparisons are made, and a procedure to determine how exactly make the comparisons. In modern terms, the standard can be viewed as a *metric*, and measurement procedure relates to a *measure*, that is, measuring instrument.

Overall, von Helmholtz' contribution to measurement theory is much broader than that, and as one of the investigators of his work states, "Zählen und Messen" is "commonly regarded as a turning point between an older concept of measurement in which quantity precedes number and the present concept in which quantity and number are defined separately" [4].

B. Statistical Approach to Measurements

The contribution of von Helmholtz is significant, in terms of the logic of measurement and the associated theory. However, without questioning his work, newer theories treat the measurement processes as statistical in nature. The principal assumption of the statistical approach to measurements is that due to the inherent uncertainties in the measurement process, the result of a measurement always consists of two numbers: the value of the measured quantity and the estimation of the measurement uncertainty with which this value has been obtained (error).

With this view, it is easy to recognize that even the most common notion of measuring time results in two values. When we ask "What time is it?", we obtain a single value, say, 5:30pm, which just happens to be indicated on a watch, but with an implicit understanding that the accuracy of this time value is one minute.

To illustrate the significance of the implications of this concept, one can show an apparently trivial example of measuring the resistance of a DC battery [5]. With a simple battery model consisting of an ideal battery (with zero resistance) and an ideal resistor connected to it in series, the actual measurement circuit will need to have several sources of noise, representing uncertainty. In particular, given some simplifying assumptions, such as linear and time-invariant circuits and neglecting temperature effects, among the factors that cannot be ignored are the following:

- noise caused by battery voltage fluctuations and thermal effects from the resistor
- noise from the voltmeter used in the measurement and its calibration error
- load resistance, including input impedance of the voltmeter.

Combining all these factors leads to a rather significant complication in calculating the battery resistance, making it a non-linear computation of what looked like a simple application of Ohm's Law. Consequently, taking into account uncertainties in the measurement process turns out to be crucial in providing the quality of measurement values.

C. Lessons from Measurements in Physics

To help realize the challenge of measuring properties, one can look closer at the extreme of measuring strictly physical properties (quantities). In addition to length, mentioned above, among physical properties we are most familiar with are time and mass.

The current definition of a second, a metric (unit) of time, involves atomic radiation and reads as follows [2]: "the duration of 9 192 631 770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium 133 atom." It must be noticed that this definition, just like the one of a unit of length, quoted in Section I, evolved historically from much less precise definitions and understanding of respective quantities. A historical background can be found at [2].

The metric of mass (its unit), a kilogram, is currently the only physical unit that officially remains defined based on a physical artifact, an international prototype stored in the International Bureau of Weights and Measures, near Paris. However, there is a substantial push towards defining it more precisely, using the number of atoms in a silicon 28 crystal [6]. Developing this new definition has not been fully successful, yet, but (in the context of considering definition of security) it is worth mentioning, why this is so: "The measurement uncertainty is 1.5 higher than that targeted for a kilogram redefinition […]. The measurement accuracy seems to be limited by the working apparatuses." Clearly, any measurement of security must involve the use of measuring devices and assessment of their accuracy.

It may be further argued that security is not a physical property and cannot be measured directly, so even considering such measurements would make little or no sense. In physics, however, there are examples of quantities, which do not measure directly certain properties of matter. One such prominent example is temperature, which is essentially a quantity corresponding to and measuring kinetic energy.

It is clear from these lessons that several points have to be taken into consideration, if one is to develop scientifically based security measurements:

- the process of designing a validated metric of security may take years, if not decades;
- any measures of security must be treated as (physical or mental) measurement devices (instruments), to which regular statistical measurement theory applies
- security is likely to be measured only indirectly, possibly via its inherent components.

D. Software Measurements

With all that has been said in the subsections above, software measurements cause a particular challenge. First of all, software is not a physical quantity, so the question arises can we really distinguish some meaningful software attributes that would have significance regarding the estimation of software quality? In other words, "Analogous to physics, there is the idea whether we can compare a software quality attribute to a norm" [7].

This dilemma has been resolved in two ways. First, we apply a concept of a latent variable, to represent a property that cannot be measured directly but can be estimated using observable attributes (or respective variables representing them) [7]. Second, being aware of our imperfection in approaching the measurements of software, similarly to the evolution of a concept of measuring length and time, we relax the requirement about ultimate quality of software measurements by adopting the rule: "For software then, like time, we want measures that are practical and that we expect will evolve over time to meet the need of the day" [8].

The first publication adopting concepts of measurement theory to software measurements, and comparing them, appears to be [9]. Among the major factors that attention should be paid to in software measurements, the authors list *uncertainty* of the measurement, stating that "improvements in the maturity of software engineering as a truly engineering discipline require for software measurements to include the evaluation of measurements uncertainty whenever measurement results are expressed" [9]. However, they further apply measurement concepts to the function-point analysis, which is a method estimating development effort not the quality of software itself.

III. Can Security Be Measured?

A. Overview

There have been numerous publications in the last decade on security assessment, including books [10-11], research and engineering papers [12-13], government reports [14-16], and Internet sources [17-18], all of them discussing security metrics. However, a vast majority of them deal with metrics at the management level and have very little to do with measurement in a scientific sense of the term, as developed in measurement theory [5,7-8].

What is meant by security metrics in these publications is primarily adherence to standards, whether established industry standards [19-21] or internal company standards [22-23], leading to the assessment of how security policies are executed, for example, by implementing respective processes and auditing them. As one paper defines it [24], security metrics mean "the measurement of the effectiveness of the organization's security efforts over time." While this way of security assessment is beneficial and productive, measuring security as a property of a computing system or software is not particularly well developed.

What is of specific interest in the current paper is not security at the enterprise or the organization level, but rather how security as a computer system property or software property can contribute to protecting information and other resources during system's operation. In this regard, security can be viewed as one specific aspect of system's dependability, the other two aspects being safety and reliability, with one of the earliest papers addressing this issue published over twenty years ago [25].

Such focus on quantitative assessment of operational aspects of security has become more popular in recent years. A thorough survey has been published in 2009 [26], covering quantitative representation and analysis of operational security since 1981, and addressing the question whether "security can correctly be represented with quantitative information?" The major finding of this study was that "there exists significant work for quantified security, but there is little solid evidence that the methods represent security in operational settings." This brings us to the question "Is security measurable?" Before that, it would be even more important to answer a more fundamental question: "Why do we measure?"

B. Why Do We Measure?

There is an often quoted and famous statement by Lord Kelvin [27] that "when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind". Similar motivations guided generations of physicists who gave us all the discoveries thanks to which we are now able to define the basic metrics of physical quantities so precisely. Despite a different nature of software, which is not a material entity, this view of measurement can be also pursued.

Software engineering, being a young discipline, does not have its Lord Kelvin, yet, but one name is certainly worth mentioning. Watts Humphrey deserves quoting, having said [28] that "quality management is impossible without quality measures and quality data. As long as software people try to improve quality without measuring and managing quality, they will make little or no progress." This is the main premise why measurements are critical for any software controlled system. Introduction of rigorous processes based on measurements allows software organizations improve their products, reaching higher capability maturity levels.

For a complete picture, it is worthwhile including a comment from an electrical engineer, published in a systems engineering magazine [29]. After outlining significant deficiencies in current approaches to security and pointing to successes of engineering disciplines, which base their designs on scientific measurements, Fred Cohen writes:

> "As systems engineers, it would be nice to be able to use the same sorts of notions of design for information security as we use for other sorts of design. It would be nice to be able to have standard units of measurement against which we could test things. It would be nice to be able to develop tools for measurement that could be calibrated against the standards, to have a theoretical basis for developing a mathematics and testing it, and then to be able to build up a systems engineering approach to information security like we do in other engineering fields. But first, we need to be able to make meaningful measurements."

With these three sample views, coming from a physicist, a software engineer and an electrical/systems engineer, it becomes quite obvious that the measurements are necessary to improve decision making. In engineering, we have to say it even more strongly, that we measure properties to receive adequate information to determine system's behavior and be able to better control system's parameters. Thus, what has been also expressed in the most recent security research quite clearly [16,30-31], we want to measure security to predict system's behavior and better respond to potential threats or, at least, estimate the associated risks. As one author stated it rather bluntly [32]: "And until we can measure security, we can't improve it."

C. Measurable or Not?

As the quoted author stated in [32], and several other publications expressed as well [33-36], there are significant concerns about the feasibility of security assessment, with some authors even arguing that security as a system property is not measurable [37-38]. In particular, [38] presents a view that any security metric must be a *computable function* mapping a set of features of systems, subject to security concerns, into the real numbers. Under this assumption, introducing a system model with an owner, its adversaries, and an observer, it is claimed that security is non-measurable for the combination of the following three reasons:

- the set of unmitigated weaknesses (vulnerabilities) is not measurable by anyone, including the owner of the system;
- the set of weaknesses (vulnerabilities) known to the observer is not known by the owner of the system and thus is not measurable by the owner; and
- no system owner can know the totality of his adversaries.

Other authors are less skeptical, advocating respective developments [39] and even outlining a number of reasons why measuring security is hard but feasible, including [40]:

- impossibility of testing all security requirements
- interactions between measurements and security
- changes in the environment imposed by adversaries
- subjectivity of the evaluators.

In addition, the same authors also offer some guidance, which are mainly considerations on what should be included in security measurement to make it "more accurate and useful." Among those suggestions several are worth mentioning [40]: (a) building adequate models; (b) using a set of metrics as opposed to a single metric; (b) use different metrics for different purposes; (c) embrace uncertainty.

In the editorial introduction to the special issue of IEEE Security and Privacy Magazine, on the Science of Security [41], the guest editors also express skepticism about measurability of security properties, and anticipate a rough road to reaching this goal, saying that: "We're a long way from establishing a science of security comparable to the traditional physical sciences, and even from knowing whether such goal is even achievable."

The same authors, in another article for this issue of IEEE Security and Privacy [42], referring to "Lord Kelvin's oft-repeated maxim," argue that the essential issue in making progress in security measurement is the existence and usefulness of respective tools. They offer a tip to pursue security metrics saying that two types of metrics can and need to be pursued: "either analytical or experimental."

As pointed out in the aforementioned editorial, we should aim at making the security measurement process comparable to those used in physical sciences. Let's look, then, into the ways the values of security can be assessed using scientific methods, similar to those of measuring physical quantities.

IV. Model for Security Assessment

A. Scientific Approaches to Measurement

Following the observation from [42], for assessment of value of a system property, where there is no science or theory developed, one could try conducting measurement experiments. Nevertheless, if experimental assessment of a system property quantitatively is impossible or difficult, one can also apply simulation. As Glimm and Sharp, for example, point out [43]: "It is an old saw that science has three pillars: theory, experiment, and simulation." This principle is broadly applied in physics, the mother of modern sciences, but it has been also adopted in various ways in computing [44-45].

A closer look at selected computing disciplines reveals that, knowingly or not, this principle has merit, for example, in computer networks. Analytical modeling of network traffic is usually done using queuing theory, measuring network parameters, such as throughput and latency, is done via experiments, and computer simulations use combined computational models to accomplish what cannot be done with theory or live experiments.

However, before any theory, experiment or simulation is developed, putting cards on the table is necessary by developing an initial model of the phenomena whose properties are to be measured. This is the critical first step to conduct the measurement.

B. General Modeling Objectives

Summarizing the discussion thus far, the critical elements in measurements of any property are the following:

1) Clearly identify the *property* to be measured. It is at this point where building a model of the phenomenon is necessary. We use the term "property", although in measurement theory [46], it is called *measurand*.
2) Establish a *metric* to quantitatively characterize the property. Ideally, this would be a unit of measurement, but for vaguely defined properties it can be just a standard against which measurements are applied, or a scale against which the property can be evaluated.
3) Develop a *measure*, which would apply the metric to related objects under investigation. Ideally, this is just a measuring instrument, but for vaguely defined metrics it can be a formula or any other mental device to apply a metric. One important characteristic of a measure should be its linearity, that is, any two identical changes in the property value should be reflected as two identical changes in the measure.
4) Design the *measurement* process to deliver results. An important part of this process is calibration[1] of the measuring device [46], an activity almost never thought of in soft sciences. Another crucial component of this process is the collection and availability of data.
5) Make sure that each instance of a measurement delivers a result composed of the *value* of the measurement and the estimate of its accuracy (an *error*). Alternatively, and consistently with current views in measurement theory, it could be a rage of values designating one value as "measured quantity value" [46].

So knowing all this, now the question is, are we able to develop a model for security measurement? It should embrace all important factors regarding this phenomenon.

C. Architectural Model for Security Assessment

Various types of mathematical models exist to depict physical and mental phenomena, all forming the basis of modern science and engineering. Some of them are continuous, for example, differential equations, but most of those used in computing are discrete, such as queuing theory, finite state machines, network and graph models (Bayesian networks, Petri nets, Markov chains), rule-based systems, etc., including what is called formal methods.

An interesting approach to modeling measurement processes is presented in [9] and involves the IDEF0 process notation specified in the Federal Information Processing Standard [47]. This model is shown in Figure 2 and includes the phenomenon being measured, shown as a *process*, and the *control* unit representing an entity receiving *measurement* results and taking respective *actions*. A number of additional inputs to both the process and the control unit are considered as well.

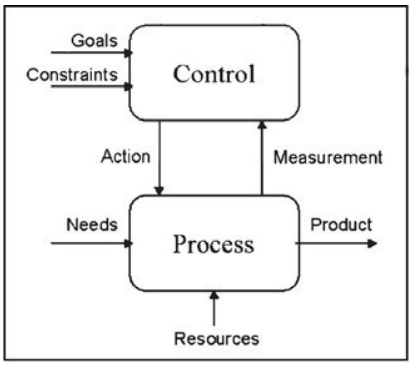

Fig. 2 Modeling of measurement activities according to [9]

We propose the adaptation of this model, making it closer to those used in control theory, which can reflect an impact of external circumstances on computer system's security. Taking the analogy with control engineering, one would only keep interfaces relevant to security during system's operation and, as a result, derive a model of an embedded

[1] The International Vocabulary of Metrology [46] defines *calibration* as "operation that, under specified conditions, in a first step, establishes a relation between the quantity values with measurement uncertainties provided by measurement standards and corresponding indications with associated measurement uncertainties and, in a second step, uses this information to establish a relation for obtaining a measurement result from an indication."

controller (or more broadly, a cyberphysical system) subject to security threats as shown in Figure 3.

The diagram shows that multiple controller interfaces to the process, the operator, the network, and the database, are all subject to security threats, forming the attack surface. More importantly, to take the analogy further, just like control theory assumes that the controlled process (a plant) is subject to disturbances, security theory, if one is developed for this model, could assume that known or unknown *threats* play the role of disturbances to the controller. While the control theory can make usually realistic assumptions about the statistical nature of disturbances (e.g., Gaussian noise), it would be challenging – but not impossible – to try and develop a statistical model for threats.

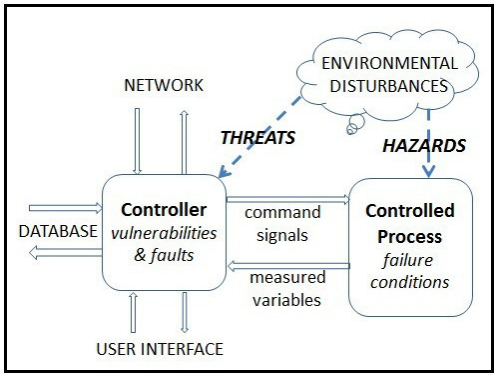

Fig. 3 Generic view of an embedded controller with security threats

In this model, *vulnerabilities* affecting the controller are understood as an "asset or group of assets that can be exploited by one or more threats" [48] or as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" [49], while a *threat* can be defined as "a state of the system or system environment which can lead to adverse effects" [50]. Consequently, the disturbances in Figure 3 are an abstraction incorporating all threats relevant to security and play a role in assessing security.

This is our generic model of a cyberphysical system subject to security threats. It has internal vulnerabilities and an attack surface composed of four interfaces. It is a precondition to meet objective (1) from Section IV-B. Now the question is how to define its security property?

D. Definition of the Term

From what has been written in general literature on security measurements, cited earlier in this paper, it is not a simple and unique property, which could be easily identified and defined. Literature on cyberphysical systems is already big and exponentially growing, but is relatively silent on the issue of security measurement [51-52]. We are, therefore, proposing our own approach, which is based on a multifaceted view of security and its measurement.

Looking at definitions of security in established standard glossaries, such as [49] or [53], it becomes immediately clear that in none of these documents security is defined as a system property. For example, one of several definitions in [53] reads as follows: "Protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them" and a corresponding one in [49]: "A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems."

These are both good definitions, but not for our purposes, because they both refer to security as a *state*, as opposed to *ability*. A definition of security as a system property must imply that one wants to measure it. In this regard, just like for several other properties, the definition should include a phrase "the extent to which" or "the degree to which." Consequently, we propose adopting the definition of security from [53], to read as follows:

> *security*. The extent to which information and data are protected so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them.

What is additionally important and captured well in [53] is the fact that the secure system must be not only protected against threats but also accessible to those authorized.

Having the definition in place, one needs to figure how to assess "the extent" or "the degree" to which the conditions spelled out in the definition are met? The community has adopted several ways to do it. One view, which gained especially wide popularity, is called C-I-A triad, where the acronym comes from the first letters of, what are called, Confidentiality, Integrity, and Availability [54]. The assessment of the degree to which a system is secure is based on meeting the three criteria of the C-I-A triad.

Another broadly adopted view to assess security is based on the STRIDE threat model, which determines the security of the system based on how well it is protected against the following six specific threats: Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [55].

We tend to agree with these multifaceted views of assessing security. To use a trivial comparison, measuring security is like assessing patient's health. It is necessary for a doctor to look at more than one parameter to determine a proper diagnosis or to discover a potential disease. Analogically, from the security perspective, we are looking for system health involving multiple indicators, not just one. Additionally, we must take into account that security situation changes over time [56], so the system is dynamical and the security assessment must be continuous.

This merely concludes meeting objective (1) outlined in Section IV-B and gives a background to meet objective (2).

V. Practical Considerations

A. Outline of Establishing a Security Measurement Process

Thus far, we have determined the model for security assessment for one particular class of systems, cyberphysical systems, and defined security as a term. What is necessary in the next step is developing the measurement process (with metrics and measures) for measuring security in the proposed context. This is, of course, an open question and a tremendous challenge.

The model of Figure 3 forms the basis for building a case study for security assessment, by analyzing threats and vulnerabilities. The traditional way of determining and investigating threats is done using attack trees, supported with methods like STRIDE or DREAD as tools for general security analysis [57-58]. In this paper, because of the need for more quantitative approach, an alternative method is suggested, based on assessing the vulnerabilities as per the Common Vulnerability Scoring System (CVSS) [59-60].

To recap what we are looking for, let's repeat that items (2)-(4) from Section IV-B have to be addressed: a *metric*, which for CVSS is a continuous numerical scale; a *measure*, which for CVSS is a set of integrated formulas; and the *measurement* process, which in this case relies on applying the measures to continuously collected data. With these assumptions, the data can be obtained by online checking of the subject entity (embedded device, server, cyberphysical system, etc., for which security is being measured) for known vulnerabilities, as per the Common Vulnerability Exposure (CVE) database [61]. Then calculating the security score based on the CVSS can be accomplished. Several authors have proposed similar methodologies to use CVE/CVSS data [62-63] for security measurement purposes, although without actual theoretical underpinning.

The challenge is the unpredictable nature of threats. Even if one can design countermeasures for existing threats and assess those, there is high likelihood that new, unknown, threats will appear, so one has to design the security system for the unknown, as well as include this type of unpredictability in the computational model for security assessment. The lack of sufficient information for calculating security values suggests building a model based on one of the theories, which deal with uncertainty, for example Bayesian belief networks [64], Dempster-Shafer theory [65], fuzzy sets [66] or rough sets [67].

B. Overview of a Case Study in Aviation

The aircraft internal networks tied with air traffic management and airline operations bring security to the forefront, because they may adversely affect flight safety. This would fit in the model presented in Figure 3. However, the existing aircraft system safety guidance does not address airborne networks and data security issues.

Even though the RTCA committee on Aeronautical Systems Security, SC-216, completed Airworthiness Security Process Specification guidance, DO-326/ED202, in 2010 [68], its work focuses on processes, methods and considerations, staying away from engineering and scientific approach based on measurements and analyses. Often the terminology used in the documents contradicts that used by scientific community. As an example, the aviation community uses term "measures" to represent the procedures, approaches, and tools used to mitigate the security threat (which in common language are "mitigation measures" or "countermeasures").

There is an evident challenge to quantitatively characterize the security properties. Nevertheless, there is a significant practice, established in the safety domain, to use a metric based on ranking applied on an ordinal scale. Clear and unambiguous determination of the metric's scale categories (with assigned ranks) would allow developing effective measures leading to modeling of security for specific assets. However, the measurements would need to be based on the developers' experience and collection of well scrutinized historical data. The resulting measurement (rank or category) would be representing the value, while the accuracy is defined by the category boundaries. Just like in the case described in previous subsection, due to the subjective nature of assessment and lack of sufficient information, it might be useful to explore the application of theories dealing with uncertainty [64-67].

Security property is often assessed indirectly, in terms of risk. Similar to the safety domain, where risk is defined as a combination of probability of hazard and severity of the potential consequences, the security domain also uses this concept. The metrics used for assessing such security aspects as attacker profile, vulnerabilities, operational conditions, or threat conditions, are defined in terms of likelihood (or probabilities). Again, these metrics are more ordinal than numerical. Metrics such as likelihood of attack, impact of a successful attack, level of exposure (vulnerability), are very subjective, ill-defined, and collecting data for them is an obvious challenge. The typical categorization of the attack likelihood is presented below:

- Frequent – anticipated to occur routinely in the life of each asset.
- Probable – unlikely to occur during a routine operation but may occur a few times in the life of an asset.
- Remote – unlikely to occur during its total life but may occur several times in the total life of an entire group of this type of assets.
- Extremely Remote – occurrence not anticipated during its total life but may occur a few times in the total life of entire group of this type of assets.
- Extremely Improbable – occurrence not anticipated during the entire operational life of all assets of this type.

The obvious question is what does it mean "routinely", "unlikely", "not anticipated"? How much is "few" or "several"? There is no agreement on specific numerical

values and assessment of these likelihoods is difficult. Similarly, typical categorization of a successful attack's impact or consequence is:

- Catastrophic – loss of system (occurrence of multiple fatalities).
- Hazardous – large reduction in safety margins or functional capabilities (potential serious or fatal injury).
- Major – significant reduction in safety margins or functional capabilities.
- Minor – slight reduction in safety margins or functional capabilities.
- No Safety Effect – no impact on the operational capability of the system.

Again, the questions are: what is "slight", "significant" or "large"?

Using similar categories we can classify vulnerability level of the asset (e.g., highly vulnerable, vulnerable, marginally vulnerable, not vulnerable) and the effectiveness of the applied countermeasures (e.g., highly effective, effective, marginally effective, not effective).

The current trend in aviation security [68] is to use the term "characteristics" to denote "property" used in this paper. The aviation community agrees on the following set of parameters defining security property (*S*) under specific operational conditions (indicated as *O*):

- *A* - likelihood of attack
- *V* - level of asset vulnerability
- *E* - effectiveness of applied countermeasures
- *I* - level of impact upon successful attack.

There has been little discussion on how these parameters should be measured, less even what models are reflecting their interrelations. Considering the discrete and ordinal nature of the above parameters, there is a possibility to create mathematical model of security *S* in a form of a discrete function:

$$S = f(A, V, E, I, O)$$

Evidently, higher ranks of parameters *A*, *V*, and *I* would have a negative impact and thus decrease the security value, while higher rank of parameter *E* would have positive impact on security as the system property. Based on historical data and actual assessment of security an attempt can be made to identify the *f()* function.

VI. Conclusion

This paper presents a view on addressing an enormous challenge of measuring computer security as a system property. Guided by principles of measurements introduced in the 19-th century by Hermann von Helmholtz, as well as by the statistical nature of measurements, and facing some fundamental questions whether security is a measurable property, a high-level model for security assessment is proposed. This model is built exploiting an analogy with a control system, treating threats as disturbances to the controller. The proposed model requires identifying measured property, establish appropriate metric, developing measure and the measurement process, and finally present the results in form of a value with an associated accuracy.

This model can be only as good as the data set to which it can be applied. With a chronic lack of reliable data related to security threats and vulnerabilities, it is proposed to use the National Vulnerability Database [61] and apply to it the Common Vulnerability Scoring Systems (CVSS) [59-60], to derive security assessment using computational methods dealing with uncertainty. Comparing the process of security assessment to the development of measurement standards and processes for physical quantities, such as length or time, it is anticipated that refining and adjusting the concepts of computer security assessment may take decades and in fact is a challenge for the entire generation.

References

[1] National Physical Laboratory, *History of Length Measurement*. Teddington, Middlesex, United Kingdom. URL: http://www.npl.co.uk/educate-explore/posters/history-of-length-measurement/

[2] National Institute of Standards and Technology, *Definitions of the SI Base Units*, Gaithersburg, Maryland, USA. URL: http://physics.nist.gov/cuu/Units/current.html

[3] H. von Helmholtz, Zählen und Messen: erkentnisstheoretisch betrachtet. In: *Philosophische Aufsätze: Eduard Zeller zu seinem fünfzigjährigen Doctorjubiläum gewidmet*. Leipzig, Germany: Fues Verlag, 1887, s. 17-52. English translation: *Counting and Measuring*, New York: Van Nostrand, 1980.

[4] O. Darrigol, "Number and measure: Hermann von Helmholtz at the crossroads of mathematics, physics, and psychology," *Studies in History and Philosophy of Science*, vol. 34, pp. 515–573, 2003.

[5] R.W. Potter, *The Art of Measurement: Theory and Practice*. Upper Saddle River, NJ: Prentice Hall PTR, 2000.

[6] B. Andreas et al., "Counting the Atoms in a ^{28}Si Crystal for a New Kilogram Definition," *Metrologia*, vol. 48, pp. S1-S13, 2011.

[7] H. Zuse, *A Framework of Software Measurement*. Berlin and New York: Walter de Gruyter, 1998.

[8] L.M. Laird and M.C. Brennan, *Software Measurement and Estimation: A Practical Approach*, Hoboken, NJ: Wiley & Sons, 2006.

[9] P. Carbone et al., "A Comparison between Foundations of Metrology and Software Measurement," *IEEE Trans. Instrumentation and Measurement*, vol. 57, no. 2, pp. 235-241, February 2008.

[10] D.S. Herrmann, *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI*. London: Auerbach Publications, 2011.

[11] W.K. Brotby and G. Hinson, *Pragmatic Security Metrics: Applying Metametrics to Information Security*, Boca Raton, FL: CRC Press, 2013.

[12] A. Atzeni and A. Lioy, "Why to Adopt a Security Metric? A Brief Survey." *Quality of Protection: Security Measurements and Metrics*, D. Gollmann, F. Massacci and A. Yautsiukhin, Eds. New York: Springer-Verlag, 2006, pp. 1-12.

[13] J. Bayuk and A. Mostashari, "Measuring Systems Security," *Systems Engineering*, vol. 16, no. 1, pp. 1-14, 2013.

[14] E. Chew et al., *Performance Measurement Guide for Information Security*. NIST Special Publication 800-55 Rev. 1. National Institute of Standards and Technology, Gaithersburg, Maryland, 2008.
[15] W. Jansen, *Directions in Security Metrics Research*, Report NISTIR 7564, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2009.
[16] R. Barabanov, S. Kowalski and L. Yngström, *Information Security Metrics: State of the Art*. Swedish Civil Contingencies Agency, DSV Report No. 11-007, March 2011.
[17] *A Community Website for Security Practitioners*. URL: http://www.securitymetrics.org
[18] G. Hinson, *Seven Myths about Security Metric*. 2006. URL: http://www.noticebored.com/html/metrics.html
[19] *Department of Defense Trusted Computer Systems Evaluation Criteria* (aka *Orange Book*), DoD 5200.28-STD, Washington, DC, December l985.
[20] *Common Criteria for Information Technology Security Evaluation, Parts 1-3*. Documents No. CCMB-2012-09-001, 002 and 003, September 2012. URL: http://www.commoncriteriaportal.org/cc/
[21] ISO/IEC 15408 Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Models, Geneva, 2009.
[22] N. Bartol et al., *Measuring Cyber Security and Information Assurance. State of the Art Report*. Information Assurance Technology Analysis Center (IATAC), Herndon, VA, 2009.
[23] *Software Security Assessment Tools Review*. Booz Allen Hamilton, McLean, VA, 2009.
[24] D.A Chapin and S. Akridge, "How Can Security Be Measured?" *Information Systems Control Journal*, vol. 2, 2005.
[25] Littlewood, B. et al., "Towards Operational Measures of Computer Security," *Journal of Computer Security*, vol. 2, no. 2-3, pp. 211-229, June 1993.
[26] V. Verendel. "Quantified Security Is a Weak Hypothesis." *Proc. NSPW'09 New Security Paradigms Workshop*, Oxford, UK, 8-11 September, 2009. New York: ACM, New York, 2009, pp. 37-50.
[27] W. Thompson – Lord Kelvin, "Electrical Units of Measurement," Lecture at the Institution of Civil Engineers, London, 3 May 1883, *Popular Lectures and Addresses*, vol. 1, pp. 73-136, 1889.
[28] W.S. Humphrey, *The Watts New? Collection: Columns by the SEI's Watts Humphrey*, Special Report CMU/SEI-2009-SR-024, Software Engineering Institute, Pittsburgh, Penn., November 2009.
[29] F. Cohen, "How Do We Measure Security?" *INCOSE Insight*, vol. 14, no. 2, pp. 30-32, July 2011.
[30] R.M. Savola, "Quality of Security Metrics and Measurements," *Computers & Security*, vol. 37, pp. 78-90, 2013.
[31] J.L. Bayuk, "Security as a Theoretical Attribute Construct," *Computers & Security*, vol. 37, pp. 155-175, 2013.
[32] S.M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," *IEEE Security and Privacy*, vol. 4, no. 4, p. 96, July/August 2006.
[33] M.D. Aime, A Atzeni and P.C. Pomi. "The Risks with Security Metrics." *Proc. QoP'08, 4th ACM Workshop on Quality of Protection*, Alexandria, VA, October 27, 2008. New York: ACM, 2008, pp. 65-69.
[34] J. Rosenblatt. "Security Metrics: A Solution in Search of a Problem." *EDUCAUSE Quarterly*, vol. 31, no. 3, pp. 8-11, July 2008.
[35] W. Jansen, W., *Directions in Security Metrics Research*. Report NISTIR 7564. National Institute of Standards and Technology, Gaithersburg, Maryland, 2009.
[36] T. Sree Ram Kumar, A. Sumithra and K. Alagarsamy. "The Applicability of Existing Metrics for Software Security," *Intern. Journal of Computer Applications*, vol. 8, no. 2, pp. 29-33, October 2010.
[37] R. Savola, "On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems," *Intern. Journal of Computer Science and Network Security*, vol. 10, no. 1, pp. 230-239, January 2010.
[38] M.D. Torgersen, "Security Metrics for Communication Systems," *Proc. ICCRTS'07, Intern. Command and Control Research and Technology Symposium*, Newport, RI, June 19-21, 2007.
[39] W.H. Sanders, "Quantitative Security Metrics: Unattainable Holy Grail or a Vital Breakthrough within Our Rich?" *IEEE Security and Privacy*, vol. 12, no. 2, pp. 67-69, March/April 2014.
[40] S.L. Pfleeger and R.K. Cunningham, "Why Measuring Security is Hard?" *IEEE Security and Privacy*, vol. 8, no. 4, pp. 46-54, July/August 2010.
[41] S. Stolfo, S.M. Bellovin and D. Evans, "Measuring Security." *IEEE Security and Privacy*, vol. 9, no. 3, pp. 60-65, May/June 2011.
[42] D. Evans and S. Stolfo, "The Science of Security," *IEEE Security and Privacy*, vol. 9, no. 3, pp. 16-17, May/June 2011.
[43] J. Glimm and D.H. Sharp. "Complex Fluid Mixing Flows: Simulation vs. Theory vs. Experiment." *SIAM News*, vol. 39, no. 5, June 12, 2006.
[44] G. Dodig-Crnkovic, "Scientific Methods in Computer Science." In *Proc. PROMOTE IT 2002, 2nd Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden*, Skövde, Sweden, April 22-24, 2002, pp. 126-130.
[45] R.W. Longman, "On the Interaction Between Theory, Experiments, and Simulation in Developing Practical Learning Control Algorithms." *Intern. Journal of Appl. Math. Comput. Sci.*, vol. 13, no. 1, pp. 101-111, January 2003.
[46] *International Vocabulary of Metrology – Basic and General Concepts and Associated terms (VIM)*. 3rd Edition, Joint Committee for Guides in Metrology, 2012.
[47] *Integration Definition for Function Modeling (IDEF0)*, Draft FIPS Publication 183, National Institute of Standards and Technology, Gaithersburg, MD, December 1993.
[48] *ISO/IEC 27005:2011 Information Technology - Security Techniques - Information Security Risk Management*. International Organization for Standardization, Geneva, 2011.
[49] *National Information Assurance (IA) Glossary*. CNSS Instruction No. 4009. Committee on National Security Systems, 26 April 2010.
[50] *ISO/IEC/IEEE 24765a:2011 Systems and Software Engineering -- Vocabulary*. International Organization for Standardization, Geneva, 2011.
[51] *Foundations for Innovation in Cyber-Physical Systems*. Report of the Workshop held in Rosemont, Ill., March 13-14, 2012. Energetics Inc., Columbia, MD, January 2013.
[52] Steering Committee for Foundations in Cyber-physical Systems. *Foundations for Innovation: Strategic R&D Opportunities for 21st Century Cyber-physical Systems*. National Institute of Standards and Technology, Gaitherburg, MD, January 2013.

[53] *IEEE Software and Systems Engineering Vocabulary*. IEEE Computer Society, Washington, DC, URL: http://computer.org/sevocab

[54] *Standards for Security Categorization of Federal Information and Information Systems*. FIPS Publication 199, National Institute of Standards and Technology, Gaithersburg, MD, February 2004.

[55] M. Howard, D.C. LeBlanc, *Writing Secure Code. Second Edition*, Microsoft Press, Redmond, Wash., 2003.

[56] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, San Francisco, Calif., 2013.

[57] J.A. Ingalsbe, L. Kunimatsu, T. Baten, and N.R. Mead, "Threat Modeling: Diving into the Deep End." *IEEE Software*, vol. 25, no. 1, pp. 28-34, January/February 2008.

[58] D. Dhilon, "Developer-Driven Threat Modeling: Lessons Learned in the Trenches." *IEEE Security and Privacy*, vol. 9, no. 4, pp. 41-47, July/August 2011.

[59] P. Mell, K. Scarfone, and S. Romanosky (Eds.) *CVSS – A Complete Guide to the Common Vulnerability Scoring System. Version 2.0*. 2007. National Institute of Standards and Technology, Gaithersburg, Maryland. URL: http://www.first.org/cvss/cvss-guide

[60] *Common Vulnerability Scoring System Support V2*. National Institute of Standards and Technology, Gaithersburg, Maryland. URL: http://nvd.nist.gov/cvss.cfm/

[61] *National Vulnerability Database Version 2.2*. National Institute of Standards and Technology, Gaithersburg, Maryland. URL: http://nvd.nist.gov/

[62] J.A. Wang et al., Security Metrics for Software Systems, *Proc. ACM-SE '09, 47th Annual Southeast Regional Conference*, Clemson, SC, March 19-21, 2009, Article No. 47.

[63] A. Tripathi and U.K. Singh, On Prioritization of Vulnerability Categories Based on CVSS Scores, *Proc. ICCIT, 6th Intern. Conference on Computer Sciences and Convergence Information Technology*, Seogwipo, South Korea, November 29 - December 1 2011, pp. 692-697.

[64] F.V. Jensen, *An Introduction to Bayesian Networks*, London, UK: UCL Press, 1996.

[65] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ: Princeton University Press, 1976.

[66] L. Zadeh and J. Kacprzyk (Eds.), *Fuzzy Logic for the Management of Uncertainty*, New York: Wiley & Sons, 1992.

[67] Z. Pawlak, *Rough Sets: Theoretical Aspects of Reasoning about Data*. Dordrecht: Kluwer Academic Publishers, 1991.

[68] RTCA DO-326 Airworthiness Security Process Specification, December 2010.