Association for Information Systems
AIS Electronic Library (AISeL)

Proceedings of the XI Brazilian Symposium on Information Systems (SBSI 2015)

Brazilian Symposium on Information Systems (SBIS)

5-2015

An Investigation About the Absence of Validation on Security Quantification Methods

Rodrigo Sanches Miani
Universidade Federal de Uberlândia (UFU), miani@ufu.br

Bruno Bogaz Zarpelão
Londrina State University, brunozarpelao@uel.br

Leonardo de Souza Mendes
Universidade Estadual de Campinas (UNICAMP), lmendes@decom.fee.unicamp.br

Investigação sobre a Ausência de Validação nos Métodos Empregados para Quantificar Segurança da Informação

Alternative Title: An Investigation About the Absence of Validation on Security Quantification Methods

Rodrigo Sanches Miani
Faculdade de Computação
Universidade Federal de Uberlândia (UFU)
Uberlândia, MG, Brasil
miani@ufu.br

Bruno Bogaz Zarpelão
Departamento de Computação
Universidade Estadual de Londrina (UEL)
Londrina, PR, Brasil
brunozarpelao@uel.br

Leonardo de Souza Mendes
Faculdade de Engenharia Elétrica e Computação
Universidade Estadual de Campinas (UNICAMP)
Campinas, SP, Brasil
lmendes@decom.fee.unicamp.br

RESUMO

A área conhecida como quantificação de segurança é fundamental para construção de modelos e métricas relevantes para apoiar as decisões que devem ser tomadas para a proteção de sistemas e redes. A investigação proposta nesse trabalho consiste em identificar as razões que envolvem a ausência de validação nos métodos empregados para a quantificação da segurança. Os resultados encontrados ao longo da análise crítica e classificação de 57 trabalhos científicos revelam que grande parte dos modelos para quantificar segurança buscam medir alvos genéricos e complexos, como por exemplo medir a segurança da rede ou a segurança da organização, contudo, as tentativas de validações aparecem com maior frequência nos trabalhos que propõem a quantificação de alvos locais e específicos.

Palavras-Chave

Modelos de quantificação de segurança, Métricas de segurança, Validação

ABSTRACT

To understand the actions that lead to successful attacks and also how they can be mitigated, researchers should identify and measure the factors that influence both attackers and victims. Quantifying security is particularly important to construct relevant metrics that support the decisions that need to be made to protect systems and networks. In this work, we aimed at investigating the lack of validation in security quantification methods. Different approaches to security quantification were examined and 57 papers are classified. The results show that most of papers seek to measure generic and complex targets like measuring network security or the security of an entire organization, however, the incidence of validation attempts is higher in works that propose the quantification of specific targets.

SBSI 2015, May 26th-29th, 2015, Goiânia, Goiás, Brazil

Categories and Subject Descriptors

K.6.5 [[**Management of Computing and Information Systems**]: Security and Protection; H.1 [**Information Systems**]: Models and Principles; C.4 [**Performance of Systems**]: Modeling Techniques

General Terms

Measurement, Reliability, Security, Verification

Keywords

Quantitative security models, Security metrics, Validation

1. INTRODUÇÃO

Os desafios enfrentados pelas organizações com relação ao tratamento e prevenção às ameaças de segurança são grandes e exigem muitos cuidados. Alguns exemplos incluem os ataques de negação de serviço direcionados a instituições financeiras e governamentais realizados pelo grupo *Anonymous*, a descoberta de códigos maliciosos capazes de espionar e controlar sistemas industriais como o *Stuxnet* e o vazamento de informações sigilosas liderado pelo grupo *Wikileaks*. Com esse intuito, diversos meios para analisar e representar a segurança de sistemas computacionais são propostos. O emprego da abordagem quantitativa, em particular, é objeto de discussões dos pesquisadores da área ao longo das últimas duas décadas [17], [8].

A ideia de quantificação aplicada a segurança da informação envolve desde o desenvolvimento de métricas de segurança até estudos sobre impactos econômicos, avaliação de risco e modelos para medir segurança [17]. Esforços conjuntos entre academia e organizações de padronizações afirmam que o tratamento quantitativo de segurança não somente é possível como também é benéfico e em alguns casos necessário para um bom gerenciamento da segurança de sistemas. Isso sugere que a quantificação correta da segurança

depende de certos requisitos. Um deles envolve a verificação da validade dos métodos de quantificação. Contudo, conforme notado por [17], as métricas e os modelos propostos, na maioria dos casos, não são confiáveis devido a falta de validação.

A ausência de dados sobre segurança pode ser visto como um potencial problema ligado a validação dos métodos para medir segurança. O compartilhamento e disponibilidade desse tipo de informação ainda é visto com desconfiança pelos envolvidos [5]. Muitas organizações acreditam que a exposição de informações sobre segurança, mesmo anonimamente, pode eventualmente prejudicar os negócios [9]. Outro problema está ligado à própria natureza da segurança da informação. Medir segurança é uma tarefa complexa, diferente e muitas vezes mais difícil do que outros tipos de medida. [13] investigaram nove possíveis razões para esse fato. Uma das razões citadas pelos autores é a de que a segurança é multidimensional, ou seja, é composta por diversos atributos. Mesmo decompondo a segurança em diversos atributos, a combinação ou composição das medidas em um único número que represente a segurança de todo o sistema não é uma tarefa trivial. Outra razão citada é a de que o próprio adversário (atacante) modifica o ambiente. Os adversários alteram o ambiente utilizando novas estratégias e criando novas classes de ataques, levando a um aumento da complexidade e da quantidade de variáveis envolvidas no processo de medir segurança.

A compreensão das razões que cercam essa ausência de validação pode ser o ponto de partida para o desenvolvimento de métodos quantitativos mais robustos e eficientes para a comunidade de segurança. Dessa forma, o presente trabalho propõe a investigação dos fatores ligados à falta de validação nos métodos empregados para a quantificação da segurança. A abordagem consiste em avaliar os diversos modelos propostos na literatura de acordo com conceitos básicos de quantificação de informação. Com esse intuito, 57 trabalhos científicos na área de quantificação de segurança da informação foram estudados e classificados de acordo com os seguintes critérios [16]: o alvo da medida, ou seja, o sistema de interesse, a metodologia de obtenção da medida e os dados utilizados.

O restante do artigo está organizado da seguinte forma: a Seção 2 descreve os trabalhos relacionados. A Seção 3 relata a metodologia adotada para a criação da pesquisa e do questionário. A Seção 4 apresenta os principais resultados da aplicação do questionário em uma determinada população. Por fim, as conclusões e sugestões de trabalhos futuros são apresentadas na Seção 5.

2. TERMINOLOGIA E DEFINIÇÕES BÁSICAS

Esta seção descreve os termos e conceitos básicos usados ao longo do artigo.

2.1 Medidas, Métricas e Modelos

Medidas, métricas e modelos de segurança estão relacionados entre si da seguinte forma [17]. Uma *medida* é feita a partir da observação de um evento, usando métodos apropriados para transformar o resultado em um dado. Uma *métrica* atribui a esse dado algum tipo de escala quantitativa para representar determinado atributo de segurança que está sob observação. A ideia de um *modelo* de segurança é fornecer uma representação formal (uma série de equações, por exemplo) o mais próxima possível da realidade para a segurança dos sistemas que estão sendo analisados.

A necessidade de desenvolver modelos de quantificação de segurança é verificada quando não existe uma relação trivial entre as medidas e o atributo a ser quantificado. A validação determina se, de acordo com as suposições assumidas, o modelo retrata com sucesso o sistema investigado. Portanto, a construção e validação de modelos quantitativos tornam-se essenciais para a descrição correta da segurança de sistemas computacionais.

2.2 Validação de modelos

Validação pode ser definida como o ato de verificar se o modelo, dentro de seu domínio de aplicação, se comporta de maneira satisfatória de acordo com os objetivos do estudo [1]. Em outras palavras, a validação consiste em verificar se o modelo construído é o correto para a situação.

Dois tipos de fontes de informações são comumente usadas para auxiliar a validação de modelos [1]: especialistas no assunto e dados. As técnicas de validação que envolvem especialistas no assunto são diretamente relacionadas ao uso de entrevistas diretas ou indiretas (questionários). No caso da disponibilidade de dados, a validação é feita com o auxílio de métodos estatísticos.

3. TRABALHOS ANTERIORES

O trabalho desenvolvido por [18] foi uma das primeiras pesquisas voltada para a análise de métodos de quantificação de segurança, em particular, sobre métricas de segurança. O principal objetivo dos autores é a criação de uma série de características para permitir a classificação de métricas de segurança. Primeiramente os autores apresentam uma classificação com base nos seguintes itens: objetivo de segurança, área de controle, dimensão temporal e público alvo.

A partir desta classificação, os autores propõem um conjunto de seis características para uma determinada métrica. As três primeiras características são propriedades básicas de qualquer métrica (objetividade-subjetividade, direta-indireta, tempo de execução-estática). Já as três características restantes determinam se uma métrica foi ou não validada, o tipo de validação usada (teórica ou empírica) e se a métrica possui alguma ferramenta para automação de seu processo de coleta.

Os resultados encontrados na análise de 57 métricas em 8 trabalhos diferentes mostram que a maioria das métricas são diretas, formadas por somente um atributo. As métricas indiretas geralmente fornecem mais informação e representam a etapa inicial para a construção de indicadores de segurança. Outro resultado interessante é a ausência de validação (teórica e empírica) e automação nas métricas analisadas. Nenhuma métrica investigada foi validada de maneira teórica e somente uma foi validada de maneira empírica. Com relação a automação, somente uma métrica possui algum tipo de suporte para essa atividade. Esse resultado evidencia que o cenário das métricas de segurança em 2004 envolvia o desenvolvimento de pesquisa em validação teórica, empírica e suporte a automação.

[17] apresentou um levantamento bibliográfico sobre a análise e representação quantitativa de segurança. O trabalho é uma extensão do trabalho anterior, desenvolvido por [18], pois trata de vários tipos de modelos de quantificação de

segurança, não somente o uso de métricas. A hipótese discutida pelo autor é se a segurança pode ser representada corretamente utilizando métodos quantitativos.

Para avaliar essa hipótese, o autor analisou 90 trabalhos entre os anos de 1981 e 2008 e os classificou com relação as perspectivas de segurança, alvos de quantificação, suposições básicas e os tipos de validações. Com base na análise dos trabalhos, o autor propõe a seguinte classificação: *perspectiva*, *alvo*, *suposições* e *validação*.

São quatro as *perspectivas* definidas: CIA (confidencialidade, integridade e autenticidade), econômica, baseada em teorias de confiabilidade e outras. Os cinco possíveis *alvos* para os métodos de quantificação são, econômico, *frameworks* sobre como desenvolver e selecionar métodos de quantificação, componentes e sua estrutura no sistema em consideração, ameaças e a existência de vulnerabilidades. As *suposições* são relacionadas a independência de eventos, quando assumimos que o sistema em questão é invariante ao longo do tempo ou entre diferentes ambientes e quando a decomposição do sistema é feita de maneira simples, utilizando somente a descrição de seus componentes. Os quatro meios de *validação* são o uso de hipóteses, validação empírica, simulações e validação teórica.

O primeiro resultado significativo obtido pelos autores trata das suposições que foram consideradas nos trabalhos. A maioria dos métodos emprega suposições não coerentes com o sistema avaliado e também sem base empírica. Utilizar tais suposições sem a validação necessária pode comprometer a aplicação dos modelos.

Outro resultado, similar ao já encontrado em [18], comprova que a minoria dos trabalhos emprega o método empírico de validação. Além disso, o foco desses métodos reside em demonstrar como eles podem ser aplicados ao invés de validar como a segurança é representada pelos atributos de interesse. De acordo com os autores, os trabalhos relacionados à modelagem de vulnerabilidades foram os únicos que apresentaram resultados empíricos convincentes. A ausência de comparação entre os métodos que usam o mesmo tipo de metodologia ou experimentos com os mesmos dados também foi destacado pelo autor.

Com base nos resultados, Verendel faz diversas sugestões para melhorar a compreensão dos métodos quantitativos aplicados à segurança da informação: comparar os métodos usando os mesmos conjuntos de dados, melhorar a colaboração entre os diversos tópicos de pesquisa, exigir melhores requisitos de validação e estabilizar a coleta e disponibilidade de diferentes conjuntos de dados.

Outro trabalho que investiga a literatura sobre métodos de quantificação de segurança é apresentado em [14]. Os autores analisam o 43 trabalhos da área, com o objetivo de caracterizar as estratégias de quantificação, o nível de maturidade das métricas e os obstáculos técnicos ou conceitais que eventualmente prejudicam o progresso da área.

A pesquisa estende a classificação definida em [17], incluindo atributos como escopo de quantificação, procedimento de quantificação, ciclo de vida e suporte a ferramentas. Diferentemente do trabalho de Verendel que é restrito a trabalhos relacionados a segurança de sistemas em ambientes reais, em [14] os autores incluem áreas como o desenvolvimento de software seguro nos critérios de busca de artigo.

A partir da análise dos trabalhos selecionados, os autores desenvolveram uma classificação para métricas de segurança com base em cinco atributos: custo, probabilidade, eficiência, conformidade e cobertura do alvo.

Esta classificação permitiu aos autores algumas conclusões importantes sobre os trabalhos investigados. Novamente foi possível mostrar que não há resultados empíricos que confirmem a correlação entre as métricas de segurança e os alvos da medida, ou seja, a maioria das métricas propostas não foi aplicada, testada ou sequer aceita na prática. Assim, trabalhos que discutem a significância das métricas em ambientes reais são importantes pontos de partida em direção a esse objetivo. Outros resultados encontrados incluem: a ausência de métricas com suporte às ferramentas de automação de coleta de dados e a maioria das métricas não trata de maneira adequada a oscilação dos objetivos de segurança definidos pelas organizações e também as variações das ameaças de segurança, de acordo com vários fatores, como o tempo ou motivações para o ataque.

É possível notar que os trabalhos apresentam conclusões similares sobre os métodos de quantificação de segurança. O grande problema ainda é a ausência de validação dos métodos propostos usando dados empíricos. O objetivo deste trabalho consiste em analisar de maneira crítica os métodos para quantificar segurança e fornecer subsídios para compreender porque tais métodos não são validados.

4. METODOLOGIA DA PESQUISA

Conforme dito anteriormente, o objetivo desse estudo é investigar as razões que envolvem a ausência de validação dos métodos para quantificar segurança. A abordagem consiste em avaliar os diversos modelos propostos na literatura de acordo com conceitos básicos do processo de quantificação de informação. Esse processo possui certas características e está intimamente ligado as regras de extração de informações relativas a processos ou sistemas [16].

A Figura 1 ilustra parte da metodologia para extração e quantificação de informação de processos ou sistemas. O sistema ou processo de interesse se encontra no centro e é a partir dele que as informações serão geradas. A observação do processo envolve, sob o ponto de vista do pesquisador, questionamentos sobre o funcionamento, regras, organização ou comportamento do sistema em questão. Esta observação faz parte da primeira fase de extração de informações. A segunda fase consiste em como obter os dados que serão utilizados para gerar as informações. Nessa fase, é importante que a metodologia seja estável, bem definida e reprodutível, de modo que, quando repetida em circunstâncias semelhantes, os dados coletados sejam coerentes entre si. Por fim, a fase de obtenção da informação é baseada na reelaboração dos dados brutos para a visualização da informação (por exemplo, reordenando-os de diversos modos, efetuando algum tipo de cálculo ou aplicando alguma análise estatística), interpretação e compreensão da informação obtida e, em alguns casos, o refinamento em uma ou mais das etapas anteriores.

Desta forma, três critérios devem ser devidamente definidos: o alvo da medida, que representa o sistema ou processo de interesse, a metodologia de obtenção da medida, representado pelos procedimentos padronizados e os dados utilizados.

Suponha que o processo de interesse seja os ataques direcionados à organização. Uma possível metodologia de obtenção dos dados seria o cálculo do número de ataques detectados pela organização. Os dados utilizados poderiam ser obti-

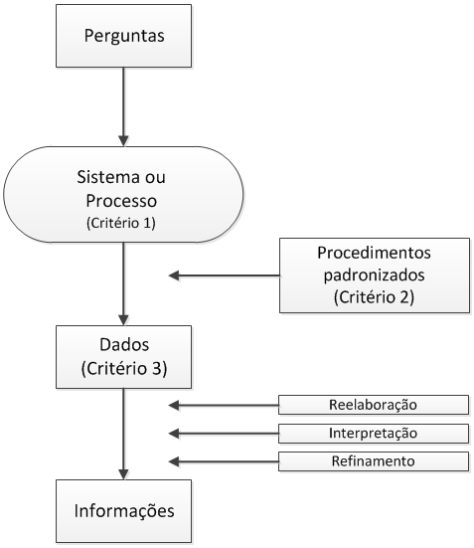

Figura 1: Diagrama para extração de informações relativas a processos ou sistemas de qualquer natureza. Adaptado de [16]

dos através dos registros do sistema de detecção de intrusão da organização. Note que o exemplo ilustra a clareza e coerência dos critérios definidos. Porém, isso não garante que as informações obtidas são correlacionadas com o processo ou ainda são suficientes para medi-lo. Validações devem ser feitas para investigar tais fatos. Dessa forma, a grande vantagem em analisar os modelos de segurança usando os três critérios básicos de quantificação de informação é a possibilidade de detectar se as características mínimas de um determinado método de quantificação foram respeitadas.

No decorrer deste trabalho, as seguintes questões serão investigadas: a) relação entre as metodologias empregadas para quantificar segurança e o sistema em questão, b) relação entre os dados utilizados e o sistema em questão e c) relação entre as metodologias empregadas para quantificar segurança e os dados utilizados.

4.1 Seleção dos trabalhos

O material inicial consistia de 92 documentos publicados em revistas científicas, anais de congressos internacionais e nacionais, livros e relatórios técnicos. Esse material era composto pelas referências bibliográficas utilizadas ao longo dos primeiros anos de estudo sobre o tema. O principal critério utilizado para guiar as modificações na base de dados inicial foi o seguinte: "Analisar os trabalhos que propõem métricas para avaliar a segurança de uma organização ou que ao menos estimem parte da segurança organizacional utilizando métodos quantitativos".

Com base nesse critério foi feita uma inspeção no resumo, palavras-chave e conclusão de cada um dos 92 documentos iniciais. Além disso, foram realizadas pesquisas nos principais portais acadêmicos (*IEEE Xplore*, *ACM Digital Library*, *SpringerLink*, *Science Direct*, *Wiley* e *Google Scholar*) usando várias combinações de palavras-chave ligadas ao critério de busca inicial, como "("Security Metrics"OR "Information Security Metrics"OR "Cyber Security Metrics") AND ("Enterprise Security Metrics"OR "Enterprise Level Security Metrics"OR "Indicators"OR "Estimators"OR "Score") AND ("System security"OR "Security evaluation"OR "Security level")" .

Assim como no levantamento realizado por [17], somente trabalhos relacionados a segurança operacional [1] foram incluídos. Além disso, como o critério central envolve a seleção de trabalhos que apresentam métricas para avaliar a segurança de uma organização ou que no mínimo descrevam parte da segurança organizacional empregando uma abordagem quantitativa, excluímos documentos relacionados a quantificação do impacto econômico, métricas de segurança de software e artigos redundantes. Também foram excluídos documentos sobre modelos de descoberta de vulnerabilidades, pois, conforme observado por [17], a validação e comparação usando diferentes conjuntos de dados é uma prática comum neste tipo de trabalho.

Finalmente, após os refinamentos citados e cuidadosa inspeção manual, 57 documentos, publicados entre 2001 e 2012, foram selecionados para a investigação. Conforme discutido em [17], esse tipo de seleção de material, apesar de ser baseada em diversos critérios, depende também do julgamento do responsável em selecionar os trabalhos, assim como dos limites de esforço dos envolvidos na busca. Logo, acreditamos que os principais trabalhos da área foram selecionados para a pesquisa. A tabela com todos os trabalhos investigados pode ser encontrada no Apêndice.

4.2 Classificação proposta

Os trabalhos foram classificados de acordo com os seguintes critérios: alvo da medida, que representa, o sistema ou processo de interesse, a metodologia de obtenção da medida e os dados utilizados. Após a análise dos trabalhos, foi criada uma taxonomia para cada um dos critérios. É importante frisar que devido a multidisciplinaridade que envolve a segurança da informação, os trabalhos podem pertencer a mais de uma categoria dentro da mesma classificação.

A classificação do sistema ou processo de interesse é dada por:

- **Segurança da rede (NET):** inclui trabalhos que avaliam a segurança da rede como um todo. Tipicamente mais de um componente é analisado.
- **Segurança da organização ou sistema (ORG):** similarmente, inclui trabalhos que avaliam não só a rede, mas a segurança da organização em geral.
- **Risco (RSK):** trabalhos que avaliam certos tipos de risco associados à segurança. Por exemplo, um processo de interesse pode ser o risco associado ao valor esperado das perdas (financeiras ou de outros tipos) relacionadas aos ataques à organização.
- **Eficiência (EFF):** quando o processo de interesse está relacionado a quantificação da eficiência de controles de segurança. Por exemplo, a avaliação da eficiência de medidas comuns de segurança, como atualizações, virtualização e remoção de softwares não utilizados.
- **Outros (SPE):** sistemas ou processos específicos, mas diferente dos anteriores, como o comprometimento de contas de usuários.

[1]Segurança de sistemas que funcionam em ambientes reais, como por exemplo a Internet, a infraestrutura de uma organização ou qualquer outra interação realística com ameaças não triviais.

A classificação da metodologia inclui:

- **Modelos probabilísticos (PRO):** modelagem da segurança através de processos estocásticos para estudar a propagação de ataques, modelar as falhas de um sistema ao longo do tempo, estimar o tempo que um atacante com um determinado nível de habilidade leva para atacar com sucesso um sistema entre outros.
- **Estatística (STA):** análise e interpretação de dados usando técnicas estatísticas, como modelos de regressão linear, correlação e séries temporais.
- **Métricas simples (MET):** utilização de métricas de segurança que envolvem cálculos simples, como por exemplo, porcentagem de incidentes de segurança investigados e número de usuários com privilégios de administrador por máquina.
- **Grafos (GRA):** aplicação de grafos de ataque e variações para modelar como as vulnerabilidades de um determinado nó da rede podem ser combinadas para a realização de um ataque.
- **Técnicas estruturadas - (STR):** decomposição hierárquica ou estruturada de fatores, como o AHP.
- **Outros - (OTH):** Outros métodos matemáticos, como por exemplo o uso de cálculo diferencial e integral e álgebra linear.

A classificação dos dados é composta por:

- **Exemplos fictícios (EXE):** exemplos criados com o propósito de ilustrar a viabilidade da proposta.
- **Sistemas em funcionamento (REA):** dados extraídos de ambientes reais, como *honeypots*, registros de incidentes de Universidades e etc.
- **Vulnerabilidades (VUL):** bases de dados de vulnerabilidades de segurança, como por exemplo o NVD.
- **Opiniões de especialistas / Questionários - (QUE):** dados coletados de questionários ou da opinião de especialistas na área.
- **Teóricos (THE):** modelos teóricos que não usam quaisquer tipos de dados.

5. RESULTADOS E DISCUSSÃO

Para avaliar se a ausência de validação dos métodos para medir segurança está relacionada aos três critérios básicos da quantificação de informação, é necessário analisar, em cada um dos trabalhos, o relacionamento dos critérios entre si.

A análise da relação entre as metodologias empregadas para quantificar segurança e o processo medido é o primeiro passo da investigação. A ideia principal consiste em compreender como os diferentes métodos são usados em cada um dos processos identificados. A relação entre os dados utilizados e o processo medido também deve ser estudada. A última análise desenvolvida contempla a relação entre as metodologias empregadas para quantificar segurança e os dados utilizados. Esse estudo pode esclarecer se determinadas metodologias tendem a usar certos tipos de dados.

O levantamento bibliográfico realizado fornece uma perspectiva simples sobre quais metodologias para quantificar segurança são aplicadas nos diferentes sistemas ou processos de interesse. A Tabela 1 mostra o relacionamento entre esses dois critérios.

Tabela 1: Como as diferentes metodologias para quantificar segurança são aplicadas nos sistemas ou processos

	PRO	STA	MET	GRA	STR	OTH	Total
NET	3	0	5	8	3	3	22
ORG	11	2	7	4	3	6	33
RSK	0	1	3	1	0	0	5
EFF	1	2	4	0	0	0	7
SPE	5	9	15	3	2	3	37

As abordagens relacionadas a risco (RSK) e eficiência (EFF) foram as menos representativas no estudo. Grande parte da literatura associada a análise de risco envolve o estudo de fatores econômicos como o cálculo de métricas como o *Return on Investment* (ROI) e *Return on Security Investment* (ROSI). Mesmo considerando a exclusão dos trabalhos com viés econômico do levantamento bibliográfico, ainda existe espaço para pesquisa quando o alvo é a quantificação de risco, mas sem considerar a perspectiva econômica. Dos três trabalhos investigados, um deles propõem um conjunto de métricas para minimizar os riscos de ataques à organização [3], o outro trabalho estima o risco baseado em melhorias no CVSS [2] e o outro propõe um modelo para auxiliar as tomadas de decisões relacionadas à TIC [4]. O objetivo da avaliação da eficiência de controles de segurança é fornecer recursos para um profissional de segurança comparar as diversas medidas propostas na literatura e assim decidir quais serão implementadas. Os resultados encontrados na Tabela 1, mostram que, apesar de importante, essa área ainda é pouco explorada pelos pesquisadores. Dois trabalhos, em especial, se destacam por apresentar estudos sobre a eficiência de medidas comuns de segurança como o uso de ferramentas de virtualização, senhas de administrador seguras, aplicação de atualização de segurança, entre outros [7] e métricas para caracterizar a eficiência de políticas de segurança da informação [6].

Dessa forma, com relação ao alvo da medida ou sistema de interesse, os trabalhos ficaram polarizados entre as seguintes áreas: segurança da rede (NET), segurança da organização (ORG) e alvos específicos (SPE).

De acordo com a Tabela 1, quase 60% dos trabalhos ligados a segurança de rede (NET), envolvem o uso de métricas simples ou grafos. Como o alvo da medida é a segurança da rede, muitos trabalhos usam grafos de ataque para modelar a rede e estudar como as vulnerabilidades de um determinado nó podem ser combinadas para a realização de um ataque. Com relação a segurança da organização (ORG), mais de 54% dos trabalhos usam modelos probabilísticos ou métricas simples. Quando o objetivo é medir a segurança da organização como um todo, o uso de somente grafos de ataque não é suficiente. Dessa forma, outros métodos são utilizados e em especial o uso de modelos probabilísticos para a avaliação da vulnerabilidade, confiabilidade, ameaças e consequências se destaca. Por fim, para os alvos específicos (SPE), mais de 64% dos trabalhos utilizam métodos estatísticos ou métricas

simples. Nenhum método estatístico foi usado nos trabalhos em que o alvo é a segurança da rede. Já para a segurança da organização, somente dois trabalhos usavam tais métodos. Esse número aumentou para nove nos trabalhos em que o sistema a ser medido é um alvo específico de segurança da informação. Isso pode ser considerado um bom sinal, já que a aplicação de métodos estatísticos, como regressão linear, séries temporais e testes de correlação indica um esforço dos pesquisadores no uso de dados empíricos para quantificação de segurança.

Conforme discutido anteriormente, a definição adequada do alvo da medida, da metodologia e dos dados utilizados é um passo importante para a construção de processos de quantificação. No levantamento realizado, os trabalhos sobre segurança da rede, compreendem, de maneira geral, a quantificação da segurança de uma rede como um todo. Essa abordagem envolve inúmeros aspectos desde os técnicos (equipamentos, políticas e controles de segurança), gerenciais (contratação de pessoal e orçamento) e o fator humano. Consequentemente, a criação de um modelo que visa quantificar a segurança da rede como um todo pode ser complexo demais e não refletir a segurança como deveria.

Vários trabalhos discutem e fundamentam essa questão:[8], [13] e [15]. De acordo com essa linha de pensamento, o mais sensato seria avaliar processos ou sistemas mais simples e específicos e deste ponto em diante tirar conclusões sobre a segurança da rede. 21 dos 57 trabalhos analisados são relacionados a quantificação de alvos específicos de segurança. A economia é quantificada dessa forma. Existem diversos indicadores econômicos e cada um deles descreve um determinado aspecto do todo [11]. Uma análise econômica é feita com o auxílio de diversos indicadores. Portanto, espera-se que a análise sobre a segurança de toda uma rede ou organização envolva também vários fatores. Os principais problemas consistiriam então em como identificar, validar e correlacionar estes fatores.

A Tabela 2, mostra o relacionamento entre os tipos de dados utilizados e o processo medido. Importantes observações podem ser feitas a partir da análise dessa tabela. Os trabalhos relacionados à quantificação da segurança da rede (NET) usam em sua grande maioria dados oriundos de exemplos fictícios (EXE) ou são completamente teóricos (THE). Nenhum trabalho utilizou dados reais (REA) ou de questionários (QUE). Isso pode indicar problemas na validação dos modelos propostos. Analogamente, os trabalhos sobre quantificação da segurança da organização (ORG) também usam na maioria das vezes (72%) dados de exemplos fictícios ou nenhum tipo de dado. Somente três trabalhos envolvem o uso de dados reais. Porém, dentre esses trabalhos, dois deles [19] e [12] não fornecem uma descrição clara dos conjuntos de dados usados, comprometendo a reprodução e comparação dos métodos.

Diferentemente dos trabalhos sobre segurança de rede e segurança da organização, os resultados presentes na Tabela 2 também apontam que os alvos de medida relacionados a eficiência, risco e alvos específicos possuem uma incidência maior de estudos com dados reais e questionários. A análise mostra uma tendência de utilização de dados reais nos trabalhos analisados quando os alvos da medida não incluem sistemas genéricos como segurança da rede ou segurança da organização. Esses resultados sugerem que a definição do processo ou sistema de segurança que será medido influencia nos tipos de dados utilizados. Uma definição abrangente ou imprecisa pode implicar na dificuldade de obtenção de dados, gerando trabalhos sem nenhum suporte a dados ou somente com exemplos fictícios. Conforme notado em [17], apesar da importância do desenvolvimento de trabalhos teóricos na área de quantificação de segurança, o uso de dados reais é crucial para permitir novos avanços nessa área.

Tabela 2: Relação entre os dados utilizados e o processo medido

	EXE	REA	VUL	QUE	THE	Total
NET	10	0	1	0	3	14
ORG	8	3	1	1	5	18
RSK	0	2	1	1	1	5
EFF	1	2	0	2	1	6
SPE	5	9	2	0	6	22

A Tabela 3, apresenta a relação entre os tipos de dados utilizados e a metodologia de quantificação empregada. É possível notar quais métodos estão relacionados a determinados tipos de dados, como ao uso de dados reais. De acordo com o levantamento feito neste trabalho, o uso de métricas simples (MET) e métodos estatísticos (STA) são os alvos de medida que possuem a maior incidência do uso de dados reais e questionários. Metodologias que envolvem o uso de grafos (GRA) e decomposição hierárquica de fatores (STR) não utilizaram dados reais em suas propostas. Além disso, modelos probabilísticos (PRO) e baseados em grafos costumam adotar somente exemplos fictícios em seus modelos de quantificação.

Ainda de acordo com a Tabela 3, apesar do baixo número, os dados relacionados a vulnerabilidades (VUL) aparecem ao menos uma vez em todas metodologias. As diversas bases de vulnerabilidades (*National Vulnerability Database* (NIST-NVD) e *Common Vulnerabilities and Exposures* (CVE)) disponibilizadas para o público, aliado ao uso do CVSS certamente contribuiu para esse resultado. Assim, o baixo número de trabalhos encontrados em nosso estudo e a alta disponibilidade de informações relacionadas a vulnerabilidade de segurança mostram que as pesquisas nessa área ainda podem ser expandidas. Trabalhos puramente teóricos (THE), sem nenhum uso de dados, também aparecem ao menos uma vez em todas as metodologias. Em especial, métodos probabilísticos, métricas simples e grafos não usam quaisquer tipos de dados na maioria das vezes.

Tabela 3: Relação entre os dados utilizados e a metodologia

	EXE	REA	VUL	QUE	THE	Total
PRO	11	2	1	0	6	20
STA	0	10	2	1	1	14
MET	9	12	4	2	8	35
GRA	9	0	1	0	6	16
STR	6	0	1	0	1	8
OTH	7	1	2	0	2	12

6. CONSIDERAÇÕES FINAIS

O principal objetivo do levantamento e análise crítica desses trabalhos é estudar as razões que envolvem a ausência de validação dos métodos para quantificar segurança. A compreensão dessas razões pode indicar os próximos caminhos de pesquisa na área de quantificação de segurança. Os resultados encontrados ao longo da análise mostram que grande parte dos modelos investigados para quantificar segurança buscam medir alvos genéricos e complexos, como medir a segurança da rede ou a segurança da organização. Na maioria das vezes, os modelos que buscam medir a segurança da rede ou a segurança da organização estão vinculados a metodologias que não utilizam dados reais (modelos probabilísticos, grafos e técnicas estruturadas) em sua construção.

Dentre os modelos estudados, a aplicação de métodos estatísticos e uso de dados reais aparece com maior frequência nos trabalhos que propõem a quantificação de alvos específicos. Porém, a pesquisa nessa área ainda está no começo, visto que muitos trabalhos ainda utilizam exemplos fictícios ou propõem novos modelos sem verificar se ele se comporta de maneira satisfatória usando critérios claros de validação. Além disso, poucos trabalhos investigados usam dados das bases públicas de vulnerabilidades de segurança. A maioria dos trabalhos que usam esses dados são voltados para predição de vulnerabilidades em software ou comportamentos relacionados a divulgação de vulnerabilidades. Outra área pouco explorada foi a avaliação da eficiência de controles de segurança. Trabalhos como [7] e [6] que propõem a investigação da eficiência de medidas comuns de segurança poderiam ser estendidos e validados por outros pesquisadores. Ainda com relação ao uso de dados, maioria dos dados reais encontrados ao longo da pesquisa são provenientes de universidades e *honeypots*. Poucos trabalhos usaram conjuntos de dados de maneira compartilhada ou realizaram comparações. O estudo conduzido por [20], no qual dados de contas de usuários corrompidas em duas universidades norte-americanas são investigados, é uma exceção.

Outro resultado destacado é que em diversos casos, a escolha de um certo alvo de medida seguida de uma determinada metodologia, pode resultar em modelo com sérias restrições para obtenção de dados e consequentemente com problemas de validações. Por exemplo, o modelo definido em [10], sugere medir a segurança da organização usando um modelo probabilístico composto por diversos atributos do sistema e do ambiente em que a organização está inserida. Contudo, a quantidade e complexidade de atributos dificulta a aplicação do modelo em ambientes reais.

Por fim, as inúmeras tentativas de quantificar a segurança de toda uma rede ou organização possuem virtudes que podem ser aproveitadas, contudo, tais abordagens ainda não foram extensivamente validadas pela comunidade científica. A pesquisa apresentada mostrou evidências de que a quantificação de segurança é melhor aproveitada quando são tratados problemas menores e específicos. São esses os modelos que devem ser validados e comparados entre si usando diferentes tipos de dados.

7. REFERÊNCIAS

[1] O. Balci. Verification, validation, and accreditation. In *Proceedings of the 30th conference on Winter simulation*, 1998.

[2] S. Bhatt, W. Horne, and P. Rao. On Computing Enterprise IT Risk Metrics. pages 271–280, 2011.

[3] W. Boyer and M. McQueen. Ideal based cyber security technical metrics for control systems. In *Critical Information Infrastructures Security*, pages 246–260, 2008.

[4] D. Chrun. *Model-Based Support for Information Technology Security Decision Making*. PhD thesis, University of Maryland, 2011.

[5] D. Geer, K. Hoo, and A. Jaquith. Information security: Why the future belongs to the quants. *Security & Privacy, IEEE*, 1(4):24–32, 2003.

[6] S. Goel and I. N. Chengalur-Smith. Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4):281–295, Dec. 2010.

[7] K. Harrison and G. White. An Empirical Study on the Effectiveness of Common Security Measures. In *2010 43rd Hawaii International Conference on System Sciences*, pages 1–7, 2010.

[8] W. Jansen. Directions in security metrics research. Technical report, National Institute of Standards and Technology (NIST), 2010.

[9] A. Jaquith. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Professional, 2007.

[10] E. Jonsson and L. Pirzadeh. A Framework for Security Metrics Based on Operational System Attributes. In *2011 Third International Workshop on Security Measurements and Metrics*, pages 58–65, Sept. 2011.

[11] G. Kaminsky, S. Lizondo, and C. Reinhart. Leading indicators of currency crises. *Staff Papers -I nternational Monetary Fund*, 45(1):1–48, 1998.

[12] M. A. Khan and M. Hussain. Cyber security quantification model. In *Proceedings of the 3rd international conference on Security of information and networks - SIN '10*, page 142, New York, New York, USA, 2010. ACM Press.

[13] S. L. Pfleeger and R. K. Cunningham. Why measuring security is hard. *Security & Privacy, IEEE*, 8(4):46–54, 2010.

[14] M. Rudolph and R. Schwarz. A Critical Survey of Security Indicator Approaches. *2012 Seventh International Conference on Availability, Reliability and Security*, pages 291–300, Aug. 2012.

[15] S. Stolfo, S. Bellovin, and D. Evans. Measuring Security. *IEEE Security and Privacy*, 9(June):60–65, 2011.

[16] P. Trzesniak. Indicadores quantitativos : reflexões que antecedem seu estabelecimento. *Ciência da Informação*, 27(2):159–164, 1998.

[17] V. Verendel. Quantified security is a weak hypothesis. In *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*, pages 37–49, 2009.

[18] C. Villarrubia, E. Fern, and M. Piattini. Towards a Classification of Security Metrics. In *Proceedings of the 2nd international workshop on security in information systems (WOSIS 2004)*, pages 342—-350, 2004.

[19] O. Weissmann. A comprehensive and comparative metric for information security. In *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM 2005)*, 2005.

[20] J. Zhang, R. Berthier, W. Rhee, and M. Bailey.

Learning from early attempts to measure information security performance. In *Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test*, pages 1–10, Bellevue, WA, 2012. USENIX Association.

APÊNDICE

A. TRABALHOS ANALISADOS

Título	Processo de interesse	Metodologia	Dados
Learning from early attempts to measure information security performance	SPE	STA	REA
Useful Cybersecurity Metrics	SPE	MET, STA	THE
Ideal based cyber security technical metrics for control systems	RSK	MET	REA
Managing information systems security: critical success factors and indicators to measure effectiveness	ORG	MET	THE
Cyber security quantification model	ORG	PRO	REA
Measuring Cyber Security in Intelligent Urban Infrastructure Systems	SPE	MET	THE
Model-Based Support for Information Technology Security Decision Making	ORG, RSK, EFF	STA, MET	REA, QUE
An Empirical Study on the Effectiveness of Common Security Measures	EFF	MET, STA	REA
Measuring Effectiveness of Information Security Management	EFF	MET	THE
Performance metrics for information security risk management	EFF	PRO	EXE
Metrics for characterizing the form of security policies	EFF	MET	QUE
Turing Assessor: A New Tool for Cyber Security Quantification	NET	PRO	EXE
Impact of vulnerability disclosure and patch availability-an empirical analysis	SPE	MET, STA	REA
Does information security attack frequency increase with vulnerability disclosure? An empirical analysis	SPE	MET, STA	REA, VUL
Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment	SPE	PRO	THE
Security metrics models and application with SVM in information security management	ORG	PRO	THE
Efficient Security Measurements and Metrics for Risk Assessment	ORG	STR, MET	EXE
A Comparison between Internal and External Malicious Traffic	SPE	MET, STA	REA
Measuring and ranking attacks based on vulnerability analysis	SPE	STR, MET, GRA	VUL
Prioritizing vulnerability remediation by determining attacker-targeted vulnerabilities	SPE	STA, MET	REA
A Novel Quantitative Approach For Measuring Network Security	NET	PRO, OTH	VUL, EXE
An attack graph-based probabilistic security metric	NET	GRA	THE
Evaluation Model for Computer Network Information Security Based on Analytic Hierarchy Process	NET	STR, MET	EXE
Evaluating Network Security With Two-Layer Attack Graphs	NET	GRA, OTH	EXE
Security Level Quantification and Benchmarking in Complex Networks	NET	STR, MET, GRA	EXE
Automatic security analysis using security metrics	NET	MET, STR	EXE
Attack graph based evaluation of network security	NET	GRA, MET	EXE
Information systems security criticality and assurance evaluation	ORG	PRO, MET	EXE
Measuring Network Security Using Bayesian Network-Based Attack Graphs	NET	GRA	THE
Measuring the overall security of network configurations using attack graphs	NET	GRA	EXE
A framework for security quantification of networked machines	NET	PRO, OTH	EXE
Finding corrupted computers using imperfect intrusion prevention system event data	SPE	MET, STA	REA
A Comprehensive Objective Network Security Metric Framework for Proactive Security Configuration	SPE	GRA, PRO, MET	THE
An Experimental Evaluation to Determine if Port Scans are Precursors to an Attack	SPE	STA, MET	REA
Relationships Between Information Security Metrics: An Empirical Study	SPE	MET, STA	REA
Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value	ORG	PRO	THE
On Computing Enterprise IT Risk Metrics	RSK	GRA, MET	THE, VUL
Measuring IT security - a method based on common criteria's security functional requirements	SPE	PRO, MET	EXE
An algorithm design to evaluate the security level of an information system	ORG	STR, GRA, MET	EXE
On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks	NET	GRA, MET	THE
A Framework for Security Metrics Based on Operational System Attributes	ORG	PRO, OTH	THE
A comprehensive and comparative metric for information security	ORG	PRO, MET	REA
Metrics for mitigating cybersecurity threats to networks	ORG	STA, MET, OTH	VUL
A Flexible Approach to Measuring Network Security Using Attack Graphs	SPE	GRA	EXE
An Empirical Model for Quantifying Security Based on Services	SPE	MET, OTH	REA
Quantitative Assessment of Enterprise Security System	ORG	GRA, PRO, OTH	EXE
Towards Quantification of Information System Security	ORG	STR, PRO	EXE
Appraisal and reporting of security assurance at operational systems level	ORG	PRO, OTH	EXE
A weakest-adversary security metric for network configuration security analysis	NET	GRA	EXE
iMeasure Security (iMS): A Novel Framework for Security Quantification	ORG	GRA, PRO	THE
Quantifying Security Threats for E-learning Systems	SPE	PRO	EXE
Dependability and Security Metrics in Controlling Infrastructure	SPE	MET	EXE
Quantifying security threats and their potential impacts: a case study	ORG	PRO, OTH	EXE
Security Assurance Aggregation for IT Infrastructures	ORG	OTH, GRA	EXE
Estimating a System's Mean Time-to-Compromise	SPE	PRO, OTH	EXE
Untrustworthiness: A Trust-Based Security Metric	SPE	OTH	THE
A framework for measuring the vulnerability of hosts	SPE	STR, MET	THE