Uma Proposta para Medição de Complexidade de Segurança em Procedimentos de Tecnologia da Informação

Giovane César Moreira Moura
Luciano Paschoal Gaspary

Instituto de Informática - Universidade Federal do Rio Grande do Sul

Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg '08)
3 de Setembro de 2008 – Gramado, RS

Roteiro

1. Introdução
2. Modelo de segurança de TI e métricas de complexidade
3. Security Complexity Analyzer
4. Avaliação experimental
5. Conclusões e trabalhos futuros

Informática UFRGS

Introdução

- Segurança de TI tornou-se nos últimos anos uma grande preocupação para as organizações
- Os requisitos de segurança são expressos por meio de SLAs e/ou políticas de segurança, materializados através de mecanismos de segurança
  - Ex: criptografia do tráfego de rede, filtragem de pacotes, ...
- Quanto mais mecanismos a serem implantados, mais complexos, longos e onerosos os respectivos procedimentos tendem a se tornar
  - Ex: mais parâmetros, mais passos a serem executados

Informática UFRGS

Introdução

- Apesar de não haver dúvidas quanto à percepção de que atividades de segurança impactam negativamente na complexidade, não se dispõe ainda de uma abordagem para caracterizar e quantificar esta percepção
- Determinar uma **medida de complexidade** de procedimentos é fundamental por uma série de razões:
  - provê uma diretriz para a equipe de TI acerca da escolha das ferramentas mais convenientes
  - permite identificar as ações relacionadas à segurança presentes nos procedimentos que apresentam os maiores valores de complexidade
  - os resultados podem ser utilizados para construir um modelo para realizar previsões de custos, a ser utilizado por diretores para revisar SLAs e políticas levando em consideração os custos preditos

Informática UFRGS

Objetivo do trabalho

- definir uma proposta sistemática para **isolar** e **mensurar a complexidade** associada à segurança – em diferentes dimensões – através de um modelo de complexidade de segurança

Informática UFRGS

Modelo de segurança de TI

- O primeiro passo para avaliar a complexidade consiste em obter um modelo que represente o sistema
- O modelo de segurança de TI permite expressar uma abstração da infra-estrutura de TI, incluindo os mecanismos de segurança
- O modelo é composto de duas partes:
  - o **modelo de infra-estrutura** representa os componentes de hardware e software
    - e o grau em que eles são relacionados à segurança
  - o **modelo de atividades** abstrai a seqüência de ações que devem ser executadas para atingir um objetivo em particular

Informática UFRGS

Modelo de segurança de TI

- Para ilustrar o modelo de segurança, apresenta-se um cenário de exemplo

Computador 1	
Mecanismo de Segurança	Ferramenta
Criptografia de Sistema de Arquivo	**dm-crypt e OpenSSL**
Criptografia da conexão com servidor de banco de dados	**MySQL e OpenSSL**

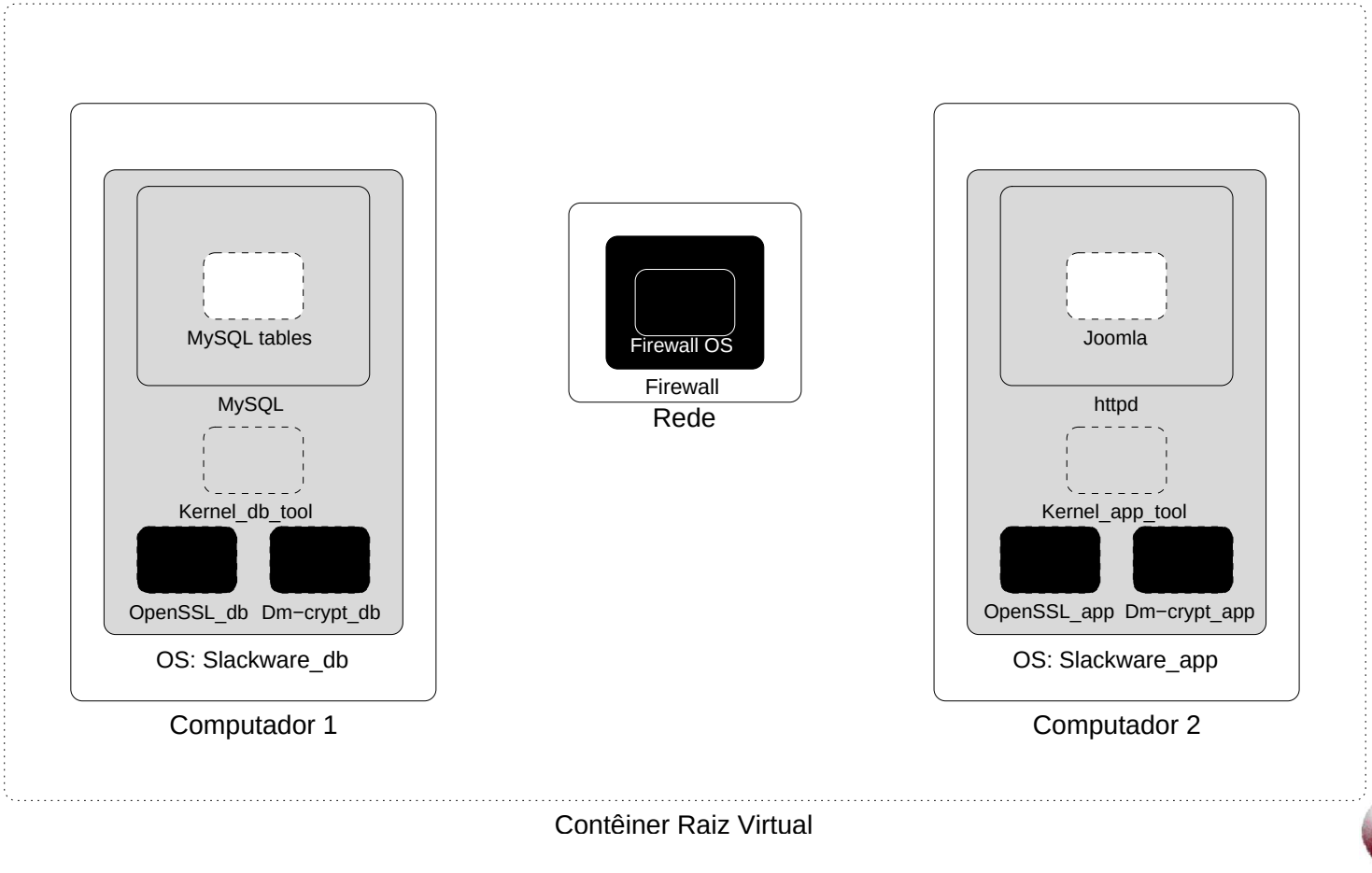
Computador 2	
Mecanismo de Segurança	Ferramenta
Criptografia de Sistema de Arquivo	**dm-crypt e OpenSSL**
Criptografia da conexão com servidor web	**httpd e OpenSSL**

Firewall	
Mecanismo de Segurança	Ferramenta
Packet Filter	**netfilter/iptables**

Informática UFRGS

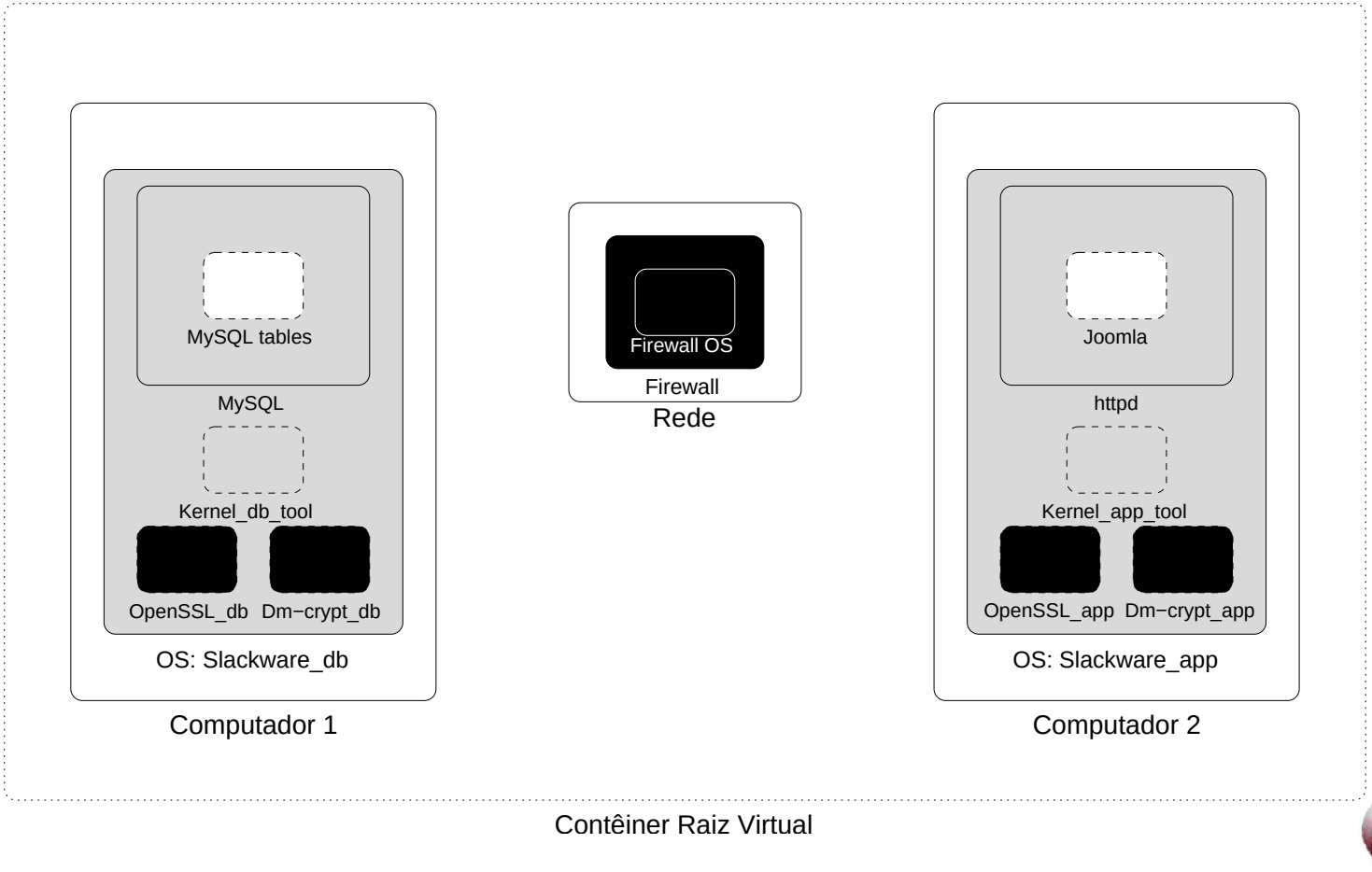
Modelo de infra-estrutura

- A infra-estrutura de TI pode ser modelada como um conjunto de contêineres



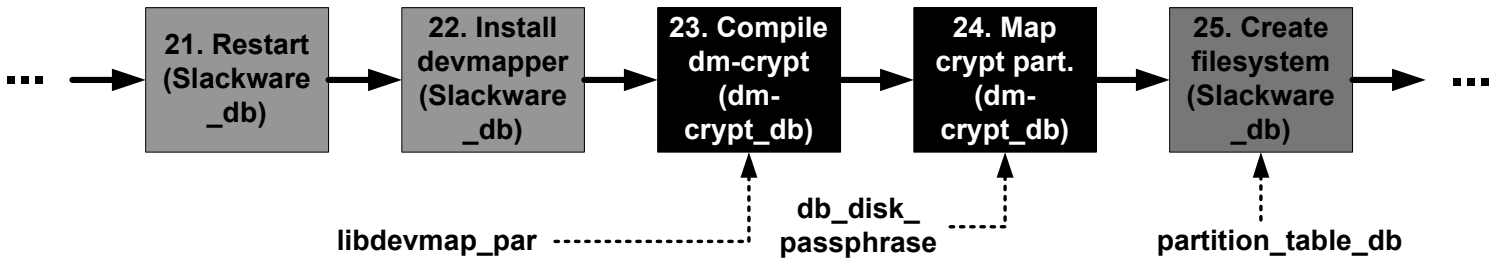
Modelo de infra-estrutura

- A cor dos contêineres reflete como eles se relacionam com segurança



Modelo de atividades

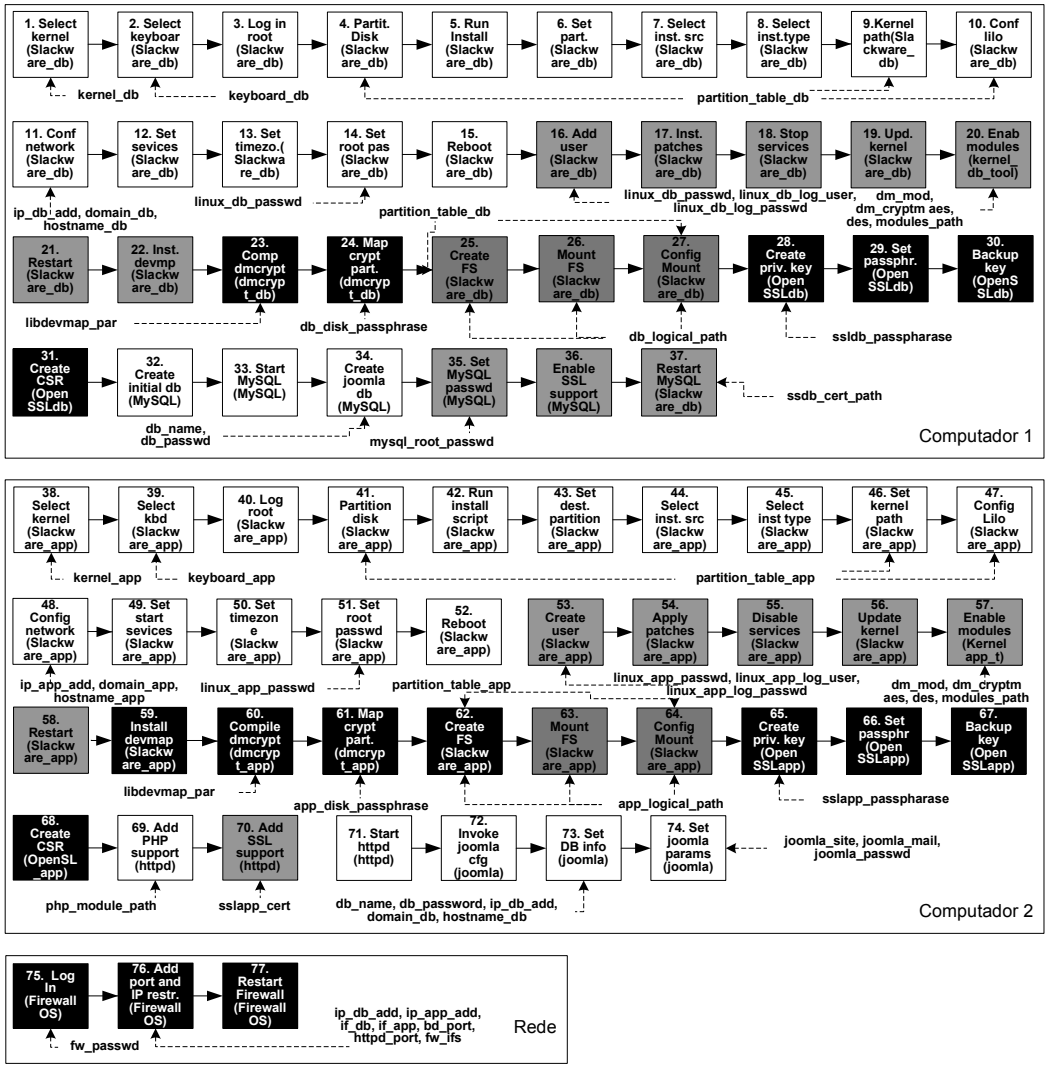
- O modelo de atividades provê uma abstração para a interação entre o administrador e o sistema
- O modelo é baseado em três pilares:
  - *Objetivo*: estado a ser atingido (ex: ativação de SSL para conexão com o servidor web)
  - *Procedimento*: seqüência de passos a serem seguidos para se atingir um objetivo específico
  - *Ações*: passo individual em um procedimento (como, por exemplo, a criação de uma chave privada)
- As cores representam a relação com segurança



Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

Procedimento do cenário exemplo:



Métricas de complexidade

- O modelo de segurança de TI provê uma base sobre a qual métricas são propostas e utilizadas para capturar a complexidade
- Estas métricas são organizadas em três grupos: **execução**, **parâmetro** e **memória**
- O cômputo pode ser realizado tanto no nível das ações quanto no nível de procedimentos

Complexidade de Execução
NumActions
ContextSwitchSum

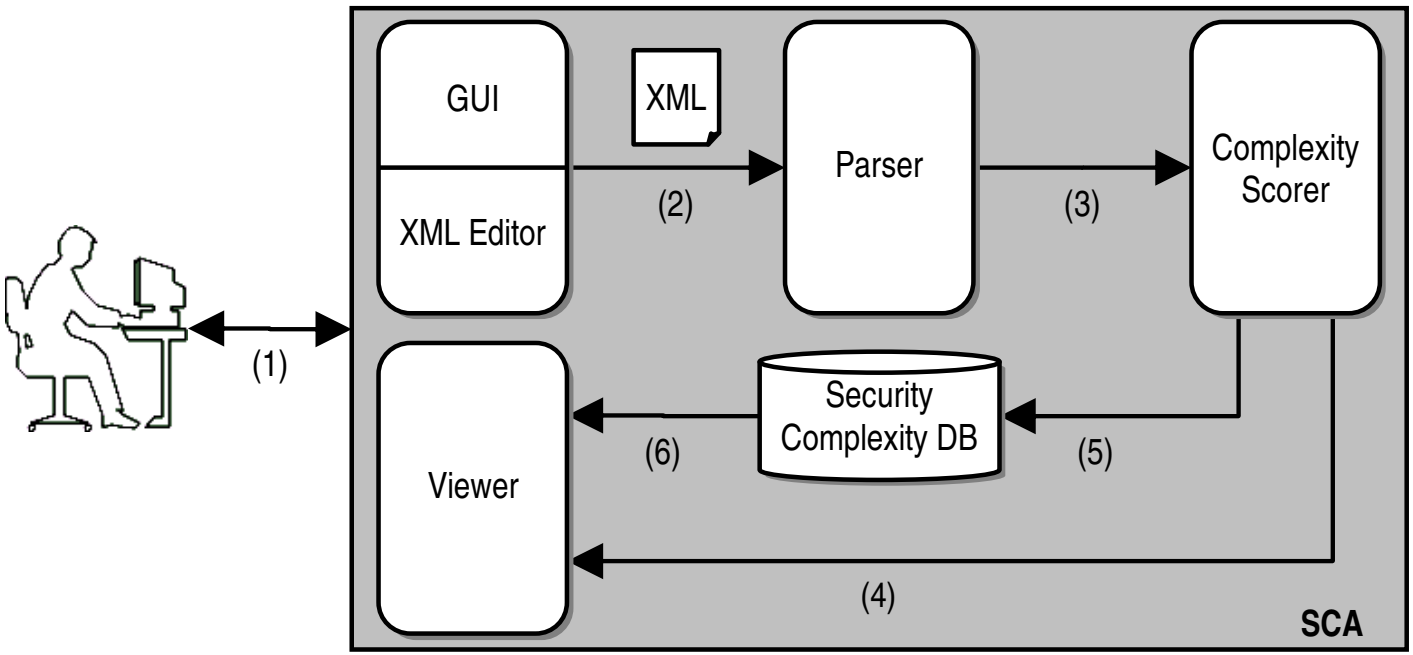
Complexidade de Parâmetros
ParamCount
ParamUseCount
ParamCrossContext
ParamAdaptCount
ParamSourceScore

Complexidade de Memória
MemSize
MemDepth
MemLat

Informática UFRGS

Security Complexity Analyzer

- Para automatizar o processo de medição e análise de complexidade, foi desenvolvida a SCA



Avaliação experimental

Foi conduzida uma série de experimentos para avaliar a complexidade de segurança em três dimensões:

1. quando mecanismos de segurança fazem parte de procedimentos mais gerais
2. quando mecanismos de segurança estão isolados
3. quando diferentes ferramentas implementam um mesmo mecanismo

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

- Segurança pode fazer parte de procedimentos mais gerais
- Em tais situações, é proposto utilizar uma abordagem **delta**:
  1. deve-se modelar um procedimento base (que não inclui quaisquer mecanismos de segurança) e proceder então com a avaliação de complexidade (x_1)
  2. então modela-se um novo procedimento com os mecanismos incluídos (x_2)
- A diferença entre as medidas (Δx) indica o complexidade adicional imposta pelos mecanismos de segurança

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

- Foram avaliados três cenários
- Eles compartilham o mesmo objetivo – instalar e configurar o Joomla e todo o software necessário – mas diferem quanto aos mecanismos de segurança implantados

Cenário A

Computador 1	
Mecanismo de Segurança	Ferramenta

Computador 2	
Mecanismo de Segurança	Ferramenta

Firewall	
Mecanismo de Segurança	Ferramenta

Complexidade agregada por mecanismos de segurança em procedimentos gerais

- Foram avaliados três cenários
- Eles compartilham o mesmo objetivo – instalar e configurar o Joomla e todo o software necessário – mas diferem quanto aos mecanismos de segurança implantados

Cenário B:

Computador 1	
Mecanismo de Segurança	Ferramenta

Computador 2	
Mecanismo de Segurança	Ferramenta
Criptografia de Sistema de Arquivo	**dm-crypt e OpenSSL**
Criptografia da conexão com servidor web	**httpd e OpenSSL**

Firewall	
Mecanismo de Segurança	Ferramenta

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

- Foram avaliados três cenários
- Eles compartilham o mesmo objetivo – instalar e configurar o Joomla e todo o software necessário – mas diferem quanto aos mecanismos de segurança implantados

Cenário C:

Computador 1	
Mecanismo de Segurança	Ferramenta
Criptografia de Sistema de Arquivo	dm-crypt e OpenSSL
Criptografia da conexão com servidor de banco de dados	MySQL e OpenSSL

Computador 2	
Mecanismo de Segurança	Ferramenta
Criptografia de Sistema de Arquivo	dm-crypt e OpenSSL
Criptografia da conexão com servidor web	httpd e OpenSSL

Firewall	
Mecanismo de Segurança	Ferramenta
Packet Filter	netfilter/iptables

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

Resultados (por métricas) obtidos para os cenários A, B e C:

Métrica	Cenário A	Cenário B	Cenário C
NumActions	38	55 (44,7%)	77 (102,6%)
ContextSwitchSum	6	11 (83,3%)	21 (250,0%)
ParamCount	20	32 (60,0%)	46 (130,0%)
ParamUseCount	31	45 (48,3%)	72 (132,2%)
ParamAdaptCount	0	0 (0%)	0 (0%)
ParamCrossContext	21	21 (0%)	45 (114,2%)
ParamSourceScore	45	74 (64,4%)	110 (144,4%)
MemSizeAvg	3,42	4,23 (23,6%)	7,38 (115,7%)
MemSizeMax	6	7 (16,6%)	14 (133,3%)
MemLatAvg	3,42	4,23 (23,6%)	7,38 (115,7%)
MemLatMax	116	201 (73,2%)	264 (127,5%)
MemDepthAvg	0,52	0,41 (-21,1%)	1,21 (132,6%)
MemDepthMax	15	15 (0%)	40 (166,6%)

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

Resultados (por métricas) obtidos para os cenários A, B e C:

Métrica	Cenário A	Cenário B	Cenário C
NumActions	**38**	55 (44,7%)	**77 (102,6%)**
ContextSwitchSum	**6**	11 (83,3%)	**21 (250,0%)**
ParamCount	**20**	32 (60,0%)	**46 (130,0%)**
ParamUseCount	**31**	45 (48,3%)	**72 (132,2%)**
ParamAdaptCount	**0**	0 (0%)	**0 (0%)**
ParamCrossContext	**21**	21 (0%)	**45 (114,2%)**
ParamSourceScore	**45**	74 (64,4%)	**110 (144,4%)**
MemSizeAvg	**3,42**	4,23 (23,6%)	**7,38 (115,7%)**
MemSizeMax	**6**	7 (16,6%)	**14 (133,3%)**
MemLatAvg	**3,42**	4,23 (23,6%)	**7,38 (115,7%)**
MemLatMax	**116**	201 (73,2%)	**264 (127,5%)**
MemDepthAvg	**0,52**	0,41 (-21,1%)	**1,21 (132,6%)**
MemDepthMax	**15**	15 (0%)	**40 (166,6%)**

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

Resultados (por métricas) obtidos para os cenários A, B e C:

Métrica	Cenário A	Cenário B	Cenário C
NumActions	38	55 (44,7%)	77 (102,6%)
ContextSwitchSum	6	11 (83,3%)	21 (250,0%)
ParamCount	20	32 (60,0%)	46 (130,0%)
ParamUseCount	31	45 (48,3%)	72 (132,2%)
ParamAdaptCount	0	0 (0%)	0 (0%)
ParamCrossContext	21	21 (0%)	45 (114,2%)
ParamSourceScore	45	74 (64,4%)	110 (144,4%)
MemSizeAvg	3,42	4,23 (23,6%)	7,38 (115,7%)
MemSizeMax	6	7 (16,6%)	14 (133,3%)
MemLatAvg	3,42	4,23 (23,6%)	7,38 (115,7%)
MemLatMax	116	201 (73,2%)	264 (127,5%)
MemDepthAvg	0,52	0,41 (-21,1%)	1,21 (132,6%)
MemDepthMax	15	15 (0%)	40 (166,6%)

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

Resultados (por métricas) obtidos para os cenários A, B e C:

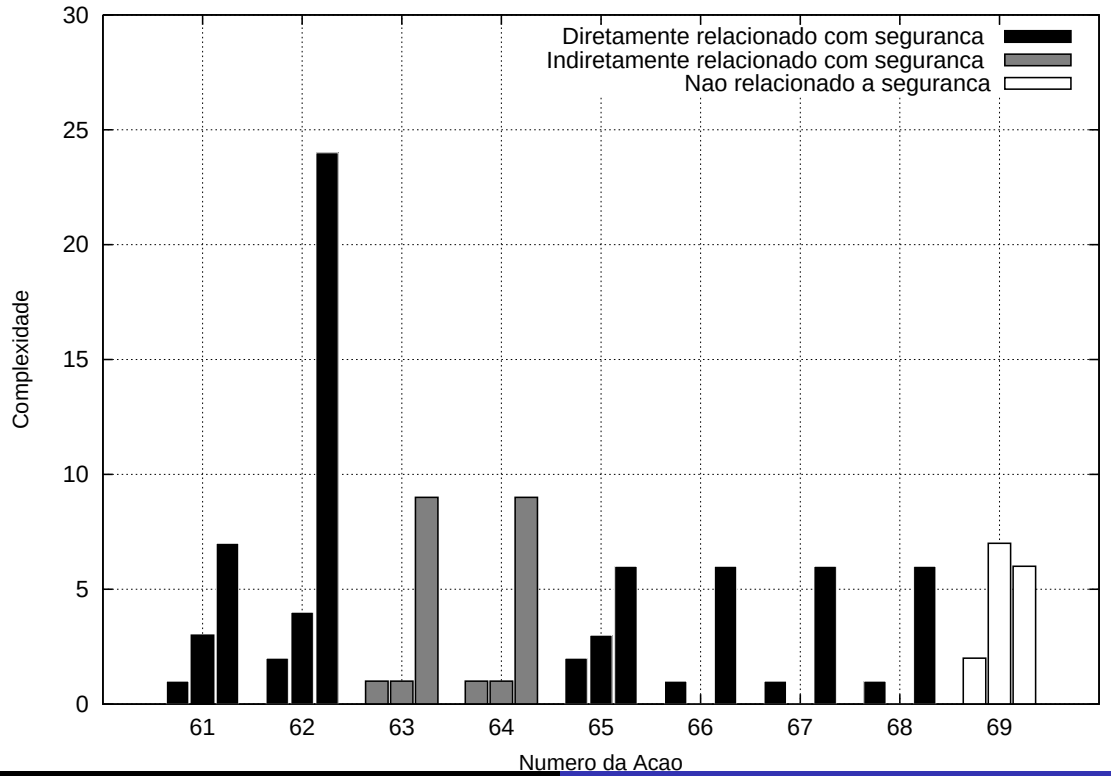
Métrica	Cenário A	Cenário B	Cenário C
NumActions	38	55 (44,7%)	77 (102,6%)
ContextSwitchSum	6	11 (83,3%)	21 (250,0%)
ParamCount	20	32 (60,0%)	46 (130,0%)
ParamUseCount	31	45 (48,3%)	72 (132,2%)
ParamAdaptCount	0	0 (0%)	0 (0%)
ParamCrossContext	21	21 (0%)	45 (114,2%)
ParamSourceScore	45	74 (64,4%)	110 (144,4%)
MemSizeAvg	3,42	4,23 (23,6%)	7,38 (115,7%)
MemSizeMax	**6**	**7 (16,6%)**	**14 (133,3%)**
MemLatAvg	3,42	4,23 (23,6%)	7,38 (115,7%)
MemLatMax	116	201 (73,2%)	264 (127,5%)
MemDepthAvg	0,52	0,41 (-21,1%)	1,21 (132,6%)
MemDepthMax	15	15 (0%)	40 (166,6%)

Informática UFRGS

Complexidade agregada por mecanismos de segurança em procedimentos gerais

Resultados (por tarefa, parciais) obtidos para o cenário C:

- tarefa 62 é diretamente relacionada com segurança (create fs)
- ela requer que o administrador se lembre e utilize um parâmetro consumido 15 ações antes



Medida de complexidade de procedimentos relacionados a mecanismos de segurança isolados

- Há situações em que mais de um mecanismo de segurança tem que ser instalado em uma infra-estrutura já implantada
  - ex: ativação de https num servidor web
- Para medir a complexidade de tais procedimentos, deve-se especificá-los isoladamente e então proceder com a avaliação de complexidade

Informática UFRGS

Medida de complexidade de procedimentos relacionados a mecanismos de segurança isolados

Foram avaliados diferentes procedimentos em um servidor Linux:

- Cenário D: uso de OpenSSL para permitir comunicação segura com o servidor web
- Cenário E: criptografia de sistema de arquivo com o dm-crypt
- Cenário F: configuração do netfilter/iptables
- Cenário G: todos os mecanismos em conjunto

Informática UFRGS

Medida de complexidade de procedimentos relacionados a mecanismos de segurança isolados

Métrica/Cenário	D	E	F	G
NumActions	7	10	3	17
ContextSwitchSum	2	4	1	7
ParamCount	3	10	8	19
ParamUseCount	3	13	8	22
ParamAdaptCount	0	0	0	0
ParamCrossContext	0	0	0	0
ParamSourceScore	9	31	16	52
MemSizeAvg	0	0.4	0	0.23
MemSizeMax	0	2	0	2
MemLatAvg	0	0.4	0	0.23
MemLatMax	0	3	0	3
MemDepthAvg	0	0.5	0	0.29
MemDepthMax	0	3	0	3

Informática UFRGS

Medida de complexidade de procedimentos relacionados a mecanismos de segurança isolados

Métrica/Cenário	D	E	F	G
NumActions	7	**10**	3	17
ContextSwitchSum	2	**4**	1	7
ParamCount	3	**10**	8	19
ParamUseCount	3	**13**	8	22
ParamAdaptCount	0	**0**	0	0
ParamCrossContext	0	**0**	0	0
ParamSourceScore	9	**31**	16	52
MemSizeAvg	0	**0.4**	0	0.23
MemSizeMax	0	**2**	0	2
MemLatAvg	0	**0.4**	0	0.23
MemLatMax	0	**3**	0	3
MemDepthAvg	0	**0.5**	0	0.29
MemDepthMax	0	**3**	0	3

Informática UFRGS

Medida de complexidade de procedimentos relacionados a mecanismos de segurança isolados

Métrica/Cenário	D	E	F	G
NumActions	**7**	**10**	**3**	**17**
ContextSwitchSum	2	4	1	7
ParamCount	3	10	8	19
ParamUseCount	3	13	8	22
ParamAdaptCount	0	0	0	0
ParamCrossContext	0	0	0	0
ParamSourceScore	9	31	16	52
MemSizeAvg	0	0.4	0	0.23
MemSizeMax	0	2	0	2
MemLatAvg	0	0.4	0	0.23
MemLatMax	0	3	0	3
MemDepthAvg	0	0.5	0	0.29
MemDepthMax	0	3	0	3

Informática UFRGS

Comparação de diferentes ferramentas que suportam os mesmos mecanismos de segurança

- Diferentes ferramentas podem atender a um mesmo mecanismos de segurança
- A comparação da medida de complexidade pode ajudar no processo de decisão
- Foram avaliados procedimentos associados a duas ferramentas que implementam VPNs:
  - OpenVPN
  - Openswan

Informática UFRGS

Comparação de diferentes ferramentas que suportam os mesmos mecanismos de segurança

- Openswan é significativamente mais complexo
- demanda 53% mais ações,180% mais trocas de contexto, and 58% mais parâmetros

Métrica	OpenVPN	Openswan
NumActions	13	20
ContextSwitchSum	5	14
ParamCount	24	38
ParamUseCount	40	69
ParamAdaptCount	0	0
ParamCrossContext	0	5
ParamSourceScore	66	94
MemSizeAvg	1.23	4.85
MemSizeMax	8	10
MemLatAvg	1.23	4.85
MemLatMax	8	43
MemDepthAvg	5.53	6.7
MemDepthMax	36	45

Informática UFRGS

Comparação de diferentes ferramentas que suportam os mesmos mecanismos de segurança

- OpenVPN fornece *scripts* para criar a CA (Openswan não)
- Openswan requer a instalação do GNU gmp e configuração explícita da placa de rede do *gateway*

Métrica	OpenVPN	Openswan
NumActions	13	20
ContextSwitchSum	5	14
ParamCount	24	38
ParamUseCount	40	69
ParamAdaptCount	0	0
ParamCrossContext	0	5
ParamSourceScore	66	94
MemSizeAvg	1.23	4.85
MemSizeMax	8	10
MemLatAvg	1.23	4.85
MemLatMax	8	43
MemDepthAvg	5.53	6.7
MemDepthMax	36	45

Informática UFRGS

Conclusões e trabalhos futuros

- Foi empregada um modelo de complexidade para medir o impacto de segurança nos procedimentos de TI
- A **principal** contribuição do trabalho reside em uma proposta sistemática para mensurar e isolar a complexidade de segurança, em diferentes dimensões:
  1. mecanismos de segurança são empregados em procedimentos de TI mais gerais
  2. mecanismos são manipulados isoladamente
  3. comparação de ferramentas diferentes que implementam um mesmo mecanismo

Informática UFRGS

Conclusões e trabalhos futuros

- Além disso, os resultados representam um passo importante em direção à determinação de uma metologia de *benchmarking* de complexidade de procedimentos relacionados à segurança
- Traduzir os valores observados de métricas de complexidade para métricas de nível de negócios (tempo e custo de execução) é um tópico em investigação

Informática UFRGS

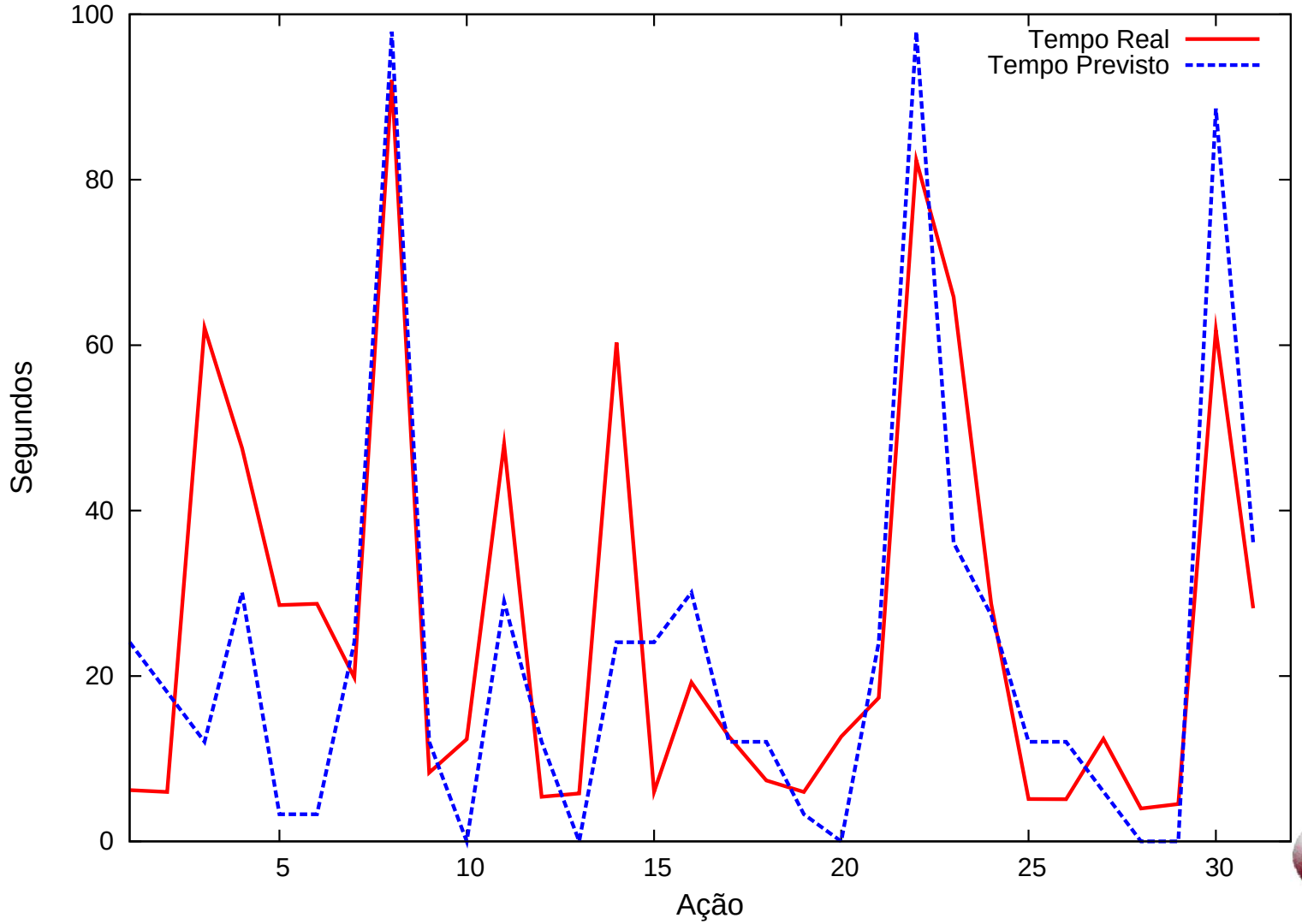
Conclusões e trabalhos futuros

Metodologia para criação de modelo de previsão de custos:

1. Definição e análise
   - cenários são definidos
   - análise de complexidade é executada
   - tempos são medidos
2. Criação do modelo
   - dados do cenário base são utilizados para criar o modelo
   - é realizada seleção de métricas
3. Extrapolação do modelo
   - modelo criado é utilizado para realizar previsões
   - qualidade da previsão é avaliada

Informática UFRGS

Previsão do tempo de execução dos procedimentos



Uma Proposta para Medição de Complexidade de Segurança em Procedimentos de Tecnologia da Informação

Giovane César Moreira Moura
Luciano Paschoal Gaspary

Instituto de Informática - Universidade Federal do Rio Grande do Sul

Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg '08)
3 de Setembro de 2008 – Gramado, RS