Resenha de artigo: Analisando a viabilidade da implementação prática de sistemas tolerantes a intrusões

Leandro Machado Andrade. *e-mail*: leandro.andrade@ifba.edu.br
Luciano Pinheiro dos Santos. *e-mail*: lucianopinheiro@ifba.edu.br
Tiago Mesquita de Araujo Cunha. *e-mail*: tiagomac@gmail.com
Instituto Federal da Bahia - IFBA.
Grupo de Pesquisa em Sistemas Distribuídos, Otimização, Redes e Tempo Real.

***Resumo*—Nesse trabalho é realizada uma resenha do artigo "Analisando a viabilidade da implementação prática de sistemas tolerantes a intrusões".**

***Index Terms*—Tolerância a intrusão, diversidade.**

I. Introdução

O OBJETIVO desse trabalho é apresentar uma resenha comentando os principais aspectos abordados no artigo "Analisando a viabilidade da implementação prática de sistemas tolerantes a intrusões" [1], assim como discutir o assunto, apresentar o problema e a solução proposta pelos autores.

No artigo base para essa resenha os autores Rafael R. Obelheiro, Alysson Neves Bessani e Lau Cheuk Lung apresentam os problemas enfrentados por sistemas modernos para manter seu funcionamento íntegro.
Através de uma análise realizada nos pontos críticos de segurança em um sistema os autores levam ao conhecimento do leitor os principais pontos que podem gerar falhas ou acesso indevido a componentes e informações do sistema.

Os autores em questão abordam que os sistemas desenvolvidos devem partir do pressuposto que seus componentes podem falhar, uma abordagem apresentada questiona a intervenção de falhas através da replicação, mas logo essa abordagem é desfeita pelos autores pelo fato das réplicas serem igualmente suscetíveis a falhas por se tratarem de uma imagem fidedigna do sistema. Nesse caso, a falha que ocorreu em parte do sistema pode igualmente se repetir em outras réplicas sendo essa uma abordagem demostrada como não sendo segura. Os autores apresentam como vulnerabilidades passíveis aquelas de ataques como cavalo de tróia, *malware* e *worms*, dessas falhas o sistema tenta se prevenir usando mecanismos de segurança como, apresentados pelos autores:

- Autenticação;
- Controle de acesso.

Entretanto os autores pressupõem que mesmo esses mecanismos de segurança ainda não tornam o sistema inteiramente seguro a essas ameaças.

Uma proposta apresentada pelos autores a deficiência da utilização de réplicas para conter possíveis falhas os autores propõem a utilização da técnica de distribuição associada a diversidade. Por distribuição os autores apontam que um sistema não deve estar em um lugar apenas, mas distribuído e acessível entre lugares distintos, garantindo assim que se o componente de uma instância do sistema venha a falhar o sistema possa se recuperar através de outra instância que idealmente esteja alocada em outro local físico. Já por diversidade os autores explanam que o sistema deve prover de componentes distintos em suas instâncias, de modo que se uma falha comprometer o componente de uma instância X, essa mesma falha não comprometa o mesmo componente de outra instância Y por se tratar de componentes distintos, mas que, no entanto realizam a mesma função.

Além de apresentar o problema supracitado os autores discutem possíveis soluções para sistemas tolerantes a intrusões. Foi desenvolvida no artigo analisado uma proposta de desenvolvimento de um sistema web com características de resiliência e tolerância a falhas onde os autores demonstram uma solução teórica de um sistema tolerante a intrusão. Essa solução proposta também será analisada nesse trabalho.

Esse trabalho divide os comentários e análise do artigo nas seções seguintes apresentadas. Na seção II é discutido o problema apresentado pelos autores. Na seção III é apresentada a solução proposta pelos autores para o problema discutido e na seção IV é apresentada a conclusão da resenha do artigo analisado.

II. Problema apresentado

A. Tolerância a Intrusões

Os autores apontam que sistemas tolerantes a intrusões são, essencialmente, aqueles sistemas que podem prover um mecanismo de segurança de forma continuada em um número de componentes que fazem parte do sistema. Para tanto os autores ainda afirmam que o conceito de tolerância a intrusão aceita certo grau de perda em funcionalidade no sistema a fim de assegurar que sua segurança não seja violada.

Um fator de interesse abordado nessa seção pelos autores é que o sistema deve prezar com mais atenção para o isolamento dos pontos únicos de falha, apontando esses como aquelas falhas que caso ocorram podem comprometer todo o funcionamento do sistema. Como solução para problemas desse tipo os autores apontam que os protocolos de comunicação entre os componentes devem possuir algoritmos de tolerância a faltas bizantinas, desse modo sendo capazes de tolerar faltas arbitrárias desses componentes. As chaves criptográficas são apresentadas pelos autores como sendo um mecanismo de utilização mais comum no quesito de segurança e acesso nos sistemas modernos, mas, no entanto os autores exploram pontos que podem evidenciar problemas na sua utilização, tais como: confidencialidade e disponibilidade. Para tratar esses problemas apresentados com as chaves criptográficas os autores sugerem a adoção de mecanismo de segurança através de criptografia de limiar onde é sugerida a adoção dos métodos de compartilhamento de segredos, onde a chave é fracionada e as frações distribuídas pelo sistema e outra denominada computação multiparte segura, onde os componentes do sistema utilizam de um segredo que apenas ele possui para efetuar uma computação onde os resultados dessa computação são combinados através de uma determinada função para obter um resultado desejado.

B. Diversidade

Sobre diversidade os autores apontam que esse é um modo clássico para tratamento de faltas de *software*. O conceito de diversidade apresentado pelos autores aponta que um sistema ou subsistema deve conter projetos de implementações diferentes, teoricamente, conforme os autores esse mecanismo tornaria o sistema mais resiliente a intrusões, no entanto os autores não apresentam pesquisas que apontem a constatação.

Na seção em questão os autores também discutem os eixos de diversidade, apresentados no artigo como sendo possíveis pontos do sistema no projeto onde seja possível inferir a diversidade. Dentro dos eixos de diversidade os autores ainda dão o nome de grau de diversidade como o valor que representa o número de componentes com função igual, mas implementação distintas o sistema possui.

C. Implementação

Por implementação os autores entendem que um projeto que adote a diversidade aumenta a sua complexidade de implementação em torna de 70-80%, no entanto os autores não fornecem dados suficientes para o entendimento desse levantamento. Os argumentos utilizados pelos autores para que justifique esse aumento é o aproveitamento do levantamento de requisitos do projeto anterior, assim como o aproveitamento dos testes de caixa preta adotados no sistema já previamente implementado.

D. Sistema Operacional

Conforme destacado no artigo [1], o sistema operacional (SO) representa um ponto bastante delicado e altamente comprometedor de um sistema distribuído, caso este sofra uma invasão. Tendo em vista que o SO gerencia todos os recursos computacionais em uma máquina (*hardwares* e *softwares*), a aplicação que compõe o sistema distribuído pode ser totalmente comprometida em caso de falha no SO, por mais que essa aplicação tenha sido projetada da melhor forma possível, contemplando inclusive as melhores técnicas de segurança.

Haja vista que o controle de arquivos, processos, memória e demais recursos de um sistema distribuídos estão em uma camada superior ao SO, este último torna-se um ponto crítico na provisão de tolerância a falhas para um sistema distribuído.

Visando promover diversidade em nível de sistema operacional, pode-se utilizar recursos como as APIs – *Application Programming Interfaces* – que permite que a aplicação seja customizada e recompilada em sistemas operacionais diferentes. Com esta medida, caso um invasor busque atingir um SO “x”, as instruções geradas e acessíveis a nível de *shell* (interpretador do núcleo do SO) serão diferentes num SO “y”.

Garantir diversidade de sistemas operacionais para aplicações distribuídas torna-se custosa por requer uma administração mais especializada (profissionais especialistas). Uma vez que opte-se por utilizar diferentes sistemas operacionais com as configurações padrões, estes tornam-se meros COTS, o que não dificulta a sua invasão. Alguns SO como o *OpenBSD* (um *kernel* Linux customizado) possibilitam uma técnica de alocação de memória aleatória para os processos.

Convencionalmente, um SO tende a alocar os processos em posições de memória sequenciais, o que permite a um invasor antecipar-se e alocar um processo em uma posição de memória de seu interesse, tendo em vista que conhece a sequência de alocação daquele sistema. Com este tipo de manipulação, qualquer operação do sistema pode ser comprometida a critério desse invasor. Assim a técnica anteriormente destacada de aleatorização de memória no *OpenBSD*, configura-se um recurso a mais de segurança.

E. Métodos

Este eixo de diversidade propõe o uso de métodos distintos em um único item de segurança, de modo que este não seja violado, o que denota uma redundância de ações em prol da segurança do sistema.

Como exemplo, pode-se destacar o procedimento de autenticação do usuário em alguns sites. Chamando de m_1, o processo de inserção de *login* e senha do usuário, e de m_2, o processo de inserção do texto alfanumérico disposto em uma imagem que pode mudar a cada nova validação, o fato de haver erro ou acerto ao método m_2 não comprometerá o m_1. Neste exemplo, tem-se uma operação AND cujo valor lógico deve ser verdadeiro para satisfazer o item de segurança de autenticidade no *login*.

F. Hardware

Em virtude de pouca ou quase nenhuma ocorrência de falhas por conta de *hardware*, em virtude da maturidade no processo de construção deste ao longo do tempo, este eixo não representava um ponto crítico. Com o surgimento de falhas como o *bug* F00F em processadores Intel *Pentium*, que permitia ao invasor causar um *crash* no processador ou a falha no mecanismo de *hyperthreading* que permite a quebra de confidencialidade de chaves privadas RSA – com o acesso a *tokens* ou arquivos no computador – o *hardware* passa a ser um ponto crítico.

Outro ponto relevante para o eixo de diversidade relacionado a *hardware* está nos diferentes tipos de arquiteturas. *Exploits* – programas que agem em função de uma vulnerabilidade encontrada em um sistema – normalmente são desenvolvidos para arquiteturas específicas. Dificilmente um programa malicioso desenvolvido para a arquitetura (como i386) funcionará em uma AMD64. Isso porque o programa compilado em um arquitetura muito provavelmente não terá compatibilidade para executar em outra. *Malwares* – *softwares* maliciosos – desenvolvidos para dispositivos como *smartphones*, tendem a ter outra versão caso o objetivo seja atingir um computador pessoal, justamente por conta de instruções que precise executar que podem não estar disponíveis na outra arquitetura.

III. Solução proposta

Um estudo de caso foi elaborado por [1], considerando um projeto de um serviço Web crítico. Esse serviço tem como finalidade demonstrar algumas possibilidades de escolhas que podem ser feitas na construção dem um sistema distribuído real e tolerante a intrusões. Como objetivo, esse sistema deve permanecer o maior tempo possível disponível, considerando as diverças formas de falhas de desistema, ataques e intrusões.

O serviço foi espalhado em quatro áreas geográficas distintas. Essa arquitetura proposta define uma interface Web em cada um desses pontos espalhadas pelo mundo, que estão acessíveis via SOAP (*Simple Object Access Protocol*). Cada uma dessas réplicas sincronizam seus estados utilizando replicação ativa. Dessa forma, todas as réplicas respondem sempre às mesmas requisições, garantindo que elas permaneçam no mesmo estado, executando um protocolo de **difusão com ordem total**.

Os protocolos utilizados na replicação ativa na internet consideram que menos de 1/3 das réplicas do sistemas irão falhar em um determinado tempo. Como temos quatro serviços funcionando, esse sistema tolera que apenas 1 réplica venah a falhar. A diversidade na implementação desse sistema irá propiciar que ocorrências de falhas sejam mais raras, implementando em diferentes linguagens, bancos de dados, sobre diferentes sistemas operacionais, diferentes ambientes de execução, utilizando diferentes *hardwares* em cada réplica e distribuidos em diferentes localidades. A combinação desses cinco diferentes implementações são utilizadas nesse exemplo, chamadas de eixos de diversidade.

Em cada uma das quatro implementações será utilizada uma tecnologia diferente por eixo de diversidade. Essa configuração permite que falhas ou intrusões em um desses componentes de forma individual não comprometam as demais réplicas. A escolha de quatro réplicas com quatro configurações diferentes de implementações é intencional, isso ocorre porque protocolos tolerantes a falhas bizantinas são capazes de tolerar 'f' faltas se o número 'n' de réplicas do sistema for

$$n \leq 3f + 1$$

, sendo assim, o número mínimo de réplicas deve ser quatro.

IV. Conclusões

Os autores explicaram o problema abordado no artigo e apresentaram uma abordagem através dos eixos de diversidade como uma forma a ser seguida para atingir o objetivo de ter um sistema com alto grau de tolerância a intrusões. Acerca dos possíveis eixos de diversidade citados, pode-se inferir que quanto maior o nível de independência ao implementar componentes do sistema, maior são as possibilidades de diversidade. Como citam os autores [1], fatores como custo e disponibilidade também afetam o grau de diversidade de um eixo: havendo mais variações a um baixo custo de aquisição e manutenção, maior será o grau de diversidade do eixo em questão. Os autores abordaram os graus de diversidades possíveis a serem adotados no sistema e demonstraram através de um exemplo de um projeto de sistema como a diversidade de eixos e como o grau delas pode atuar no sistema de modo a torna-lo tolerante a intrusões. Uma abordagem não foi devidamente aprofundada diz respeito à questão do esforço necessário para a criação de sistemas com características de diversidade conforme a solução proposta, os autores limitaram a informação a um percentual apresentado, não informando devidamente os critérios adotados para esse levantamento.

Na solução proposta pelos autores foi apresentado um sistema com diversidade de grau quatro e complexidade de implementação plausível. Outro aspecto relevante apresentado é que a variedade versões de *software* proporcionam melhores testes e validações do *software*, possibilitando a descoberta prévia de erros.

Referências

[1] A. N. B. e. L. C. L. Rafael R. Obelheiro, "Analisando a viabilidade da implementação prática de sistemas tolerantes a intrusões," pp. 1–14, 2005. [Online]. Available: http://www.redes.unb.br/ceseg/anais/2005/artigos/13299.pdf