Mitigando Ataques DDoS em SGIs por Reorganizações em Agrupamentos de IdP

Apresentação: André Luiz Marasca

Fonte principal: Macedo et al. (2013)

Ataques DDoS

- Um ataque de negação de serviço é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores.
- Num ataque distribuído de negação de serviço, um computador mestre pode ter sob seu comando até milhares de computadores ("Zombies"). Neste caso, as tarefas de ataque de negação de serviço são distribuídas a um "exército" de máquinas escravizadas.

Sistema de Gerenciamento de Identidade

- Um Sistema de Gerenciamento de Identidade (SGI), é um sistema capaz de automatizar os processos de acrescentar, modificar, revogar, excluir e gerenciar direitos de acesso e senhas de usuários.

- Com o objetivo de oferecer maior segurança e facilidade, O SGI permite que o responsável legal pelo órgão ou entidade jurisdicionada delegue competência para que um servidor administre os direitos de acesso, distribuindo, organizando e configurando o acesso de cada usuário.

Provedores de identidade (IDP)

- Provedores de identidade são responsáveis pelo fornecimento de identificadores para os usuários que procuram interagir com um sistema, e assegurar a esse sistema o identificador apresentado para o usuário é conhecido pelo fornecedor, e fornecendo outras informações sobre o usuário que é conhecido para o provedor.

Relação entre SGIs e IdPs

- Os Sistemas de Gerenciamento de Identidades (SGI) vêm recebendo atenção devido ao seu potencial em integrar diferentes domínios administrativos, preservando tecnologias e políticas locais. A principal vantagem destes sistemas consiste em empregar autoridades de autenticação (IdP) como guardiões das informações críticas dos usuários, separando o provimento de recursos do gerenciamento dos dados críticos dos usuários

O problema

- IdPs são disponibilizados na Internet, tornando-se propensos à ataques de negação de serviço distribuídos (DDoS).
- Em SGIs, os ataques DDoS podem resultar na indisponibilidade das operações de autenticação de usuários legítimos e congestionar o tráfego de dados para IdPs, impactando indiretamente no provimento de serviços.

Proposta pelo autor

- Mitigar os efeitos de ataques DDoS em SGIs através da reorganização de agrupamentos de IdPs
- As reorganizações proporcionam a otimização do uso dos recursos computacionais do sistema dos IdPs, minimizando os efeitos do ataque e prolongando o tempo de vida do SGI

Como é feito

- As reorganizações de agrupamentos de IdPs são realizadas através de três procedimentos: Agrupamento, Pré-Configuração, Otimização
- Agrupamento: recrutar o maior número de agrupamentos de IdPs capazes de suportar a sobrecarga gerada pelo ataque DDoS através de um algoritmo genético

Como é feito

- As reorganizações de agrupamentos de IdPs são realizadas através de três procedimentos: Agrupamento, Pré-Configuração, Otimização
- Pré-Configuração : Computa todos os benefícios possíveis em balancear a carga das identidades e SPs entre os IdPs de cada agrupamento

Como é feito

- As reorganizações de agrupamentos de IdPs são realizadas através de três procedimentos: Agrupamento, Pré-Configuração, Otimização
- Otimização: Utiliza técnicas de otimização para encontrar o benefício máximo de balanceamento de carga

Detalhes de implementação

- Assume-se que os IdPs utilizam um canal seguro de comunicação para se comunicarem
- o SGI é considerado como um ambiente cooperativo onde IdPs realizam operações de controle e monitoramento sobre as identidades

Detalhes de implementação

- SGI é representado por um grafo G = (V,E)
- V é composto por vértices provenientes do particionamento de três conjuntos de vértices sendo este conjuntos as identidades, os provedores de identidade (IdPs) e os prestadores de serviço (SPs) do sistema. Ou seja, todos os elementos do sistema estão modelados no grafo.

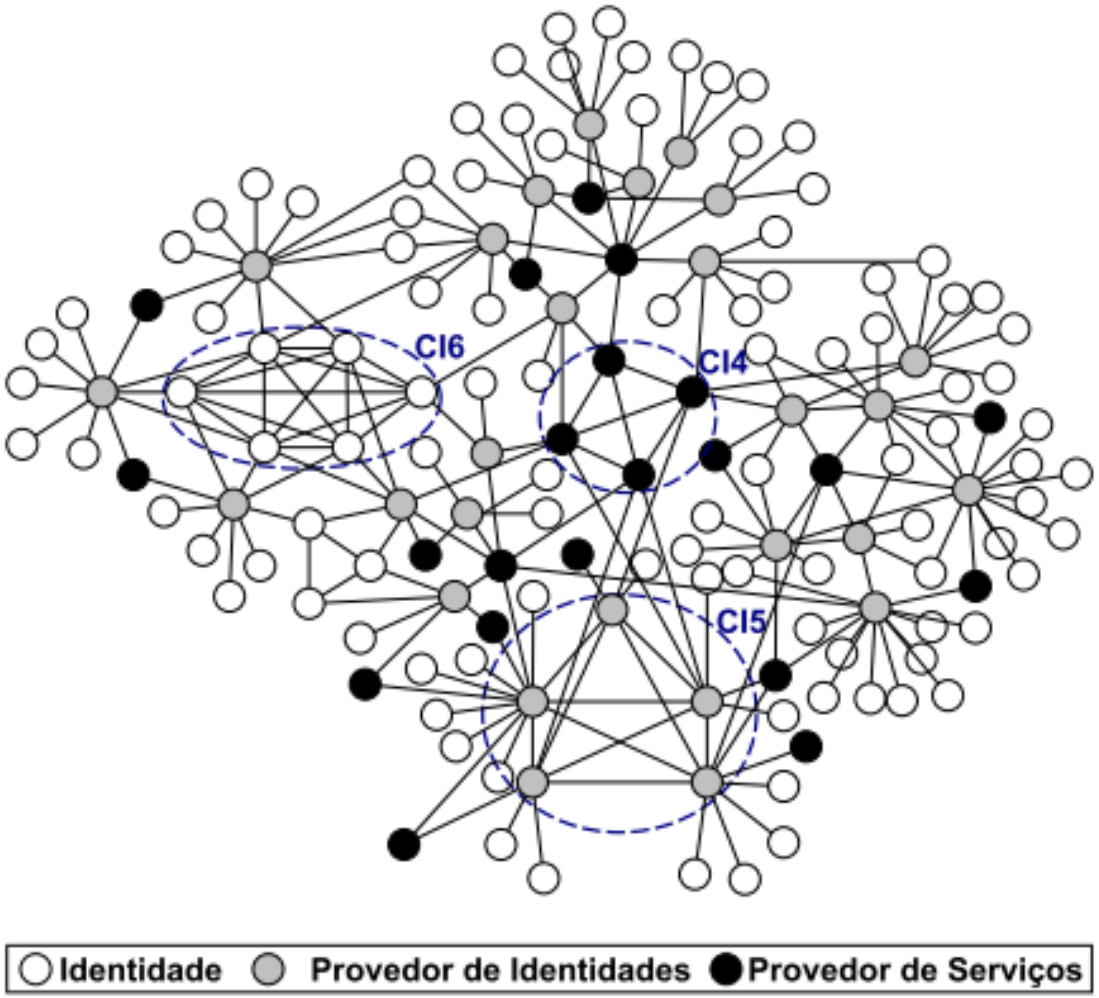
Detalhes de implementação

- Existem arestas entre as identidades e os provedores de identidade, representando quais IdPs uma identidade pode usar para se autenticar.
- Existem arestas entre os provedores de identidade e entre os provedores de serviço, descrevendo quais SPs confiam nas autenticações de um IdP.

Detalhes de implementação

- Existem arestas dentro do mesmo conjunto.
- identidade – identidade: retrata a composição de identidades parciais de um usuário
- Idps – Idps: expõe os IdPs afetados por ataques DDoS
- SPs – Sps: representa a composição de SPs, ou seja, situações onde serviços podem ser consumidos por outros serviços, tal como ocorre em arquiteturas orientadas a serviço

Detalhes de implementação



Agrupamentos

- Encontrar o número máximo de agrupamentos capazes de suportar uma sobrecarga consiste em um problema de otimização multiobjetivo: minimizar o número de membros de um agrupamento e maximizar o número total de agrupamentos
- Os algoritmos genéticos (AGs) surgem como uma solução heurística capaz de prover boas soluções para problemas de otimização em tempo aceitável

Pré-Configuração

- A Pré-Configuração computa os benefícios possíveis para balancear a carga dos agrupamentos. Cada membro do agrupamento pode apresentar diferentes capacidades de processamento, memória ou fluxo de rede para os outros membros
- Esse procedimento possibilita a atribuição de pesos de importância aos requisitos de rede, processamento de carga ou memória dos IdPs, permitindo aos administradores do SGI empregarem sua expertise para guiar a reorganização

Otimização

- Este procedimento emprega técnicas de otimização para reorganizar a carga do SGI dentro de um agrupamento, tendo como base os benefícios atribuídos pelo procedimento de Pré-organização
- O objetivo é encontrar uma solução para reorganizar o SGI com o maior benefício existente de modo que todos os nós do agrupamento de IdPs sejam utilizados para atender todas as identidades e SPs

Conclusão

- Os resultados obtidos mostram indícios da viabilidade desta proposta, possibilitando a mitigação dos efeitos do ataque primeiramente nos agrupamentos e abordando o SGI de modo recursivo
- O esquema proposto também possibilita aos administradores do SGI utilizarem sua expertise sobre os requisitos do sistema para guiar as reorganizações para priorizar o melhor fluxo da rede, processamento, ou memória dos IdPs

Referencias

- MACEDO, R.; MELNISKI, L.; SANTOS, A.; GHAMRI-DOUDANE, Y.; NOGUEIRA, M. Mitigando Ataques DDoS em SGIs por Reorganizações em Agrupamentos de IdP. , 2013.
- http://www.qualisoft.com.br/Artigo200708-01.asp
- http://www.tce.mg.gov.br/portalsgi/
- https://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o