# Arquitetura de um Simulador em Larga em Escala de Ataques Distribuídos de Negação de Serviço

**Raphael Machado[1], Matheus Santos[1,3], Henrique Soares[1], Eduardo Ogasawara[2] Fabio David[3], Rafael Soares[1], Bruno Guimarães[3]**

[1] Clavis Segurança da Informação, Rio de Janeiro, Brasil
[2] Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, Rio de Janeiro, Brasil
[3] Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil

{raphael,matheus,henrique,rafael,bruno}@clavis.com.br,
eogasawara@cefet-rj.br, fabio@ufrj.br

***Abstract.*** *Distributed denial of service attacks are characterized by a coordinated action of a huge number of hosts that aims to overload a target system, compromising its availability. These attacks are neither based on software vulnerabilities nor on security architecture flaws. Instead, they are mainly based on the overload caused by an extremely large numbers of attackers. In this way, distributed denial of service attacks are among the hardest attacks to prevent, detect and respond. In the present work, we present a distributed denial of service attacks simulator that is able to reproduce a large variety of attack scenarios, which allows the characterization of networks and hosts resistance against such attacks.*

***Resumo.*** *Ataques distribuídos de negação de serviço caracterizam-se pela atuação coordenada de uma grande quantidade de máquinas agindo com o objetivo de sobrecarregar um sistema-alvo, comprometendo sua disponibilidade. Tais ataques não são baseados necessariamente em vulnerabilidades existentes em aplicativos de software ou em falhas na arquitetura de segurança. Na verdade, eles se baseiam principalmente na sobrecarga causada por um grande número de atacantes. Desta forma, os ataques distribuídos de negação de serviço estão entre os ataques de mais difícil prevenção, detecção e resposta. No presente trabalho, apresentamos um simulador de ataques distribuídos de negação de serviço capaz de reproduzir uma enorme variedade de cenários de ataque, permitindo caracterizar a resistência de redes e sistemas face a ataques DDoS.*

## 1. Introdução

A disponibilidade é um fator crítico para os atuais sistemas de informação. Vivemos em um mundo onde a dependência de usuários em relação aos sistemas computacionais é enorme, e a indisponibilidade destes sistemas, ainda que temporária, causa prejuízos enormes a clientes e responsáveis pelo serviço. Ataques denominados "ataques de negação de serviço" são exatamente aqueles que visam à indisponibilidade de um sistema de informação, o qual deixa de oferecer o serviço para o qual foi concebido - ou, ainda, passa a oferecê-lo de maneira precária. A partir do final da década de 1990

[1] O simulador apresentado no presente trabalho denomina-se SADI (Simulador de Ataques Distribuídos de Indisponibilidade) e tem desenvolvimento apoiado pelo CNPq, através da chamada RHAE (17/2012), e pela Finep, através da chamada TI-Maior (04/2013).

(Chara lampos Z. Patrikakis 2004, CNET News 1998, Mirkovic and Reiher 2004), percebeu-se que a indisponibilidade de sistemas poderia ser forçada a partir da sobrecarga de requisições causada pela atuação coordenada de um grande número de máquinas executando solicitações rotineiras a um sistema de informação. Devido à ação de diversas unidades computacionais atuando como um sistema distribuído, tais ataques passaram a ser denominados Ataques Distribuídos de Negação de Serviço, ou ataques DDoS (do inglês, *Distributed Denial of Service*). Por serem baseadas não apenas em falhas de software, mas no uso massivo dos recursos de um sistema-alvo, estes ataques estão entre aqueles de mais difícil prevenção, detecção e resposta. Ataques DDoS vêm consolidando-se como uma das armas mais letais contra sistemas computacionais.

Denominamos soluções anti-DDoS aos sistemas que visam defender uma rede ou sistema de informação contra ataques DDoS. Tipicamente, tais sistemas são compostos por mecanismos de prevenção, por ferramentas de detecção e classificação, e por controles de resposta a ataques. A grande variedade de técnicas de ataques DDoS, associada ao grande volume de tráfego gerado por uma enorme quantidade de usuários legítimos e potenciais atacantes, transforma as soluções anti-DDoS em sofisticados sistemas, fazendo uso de equipamentos de rede dedicados e técnicas avançadas de reconhecimento de padrões e inteligência computacional. Desta forma, determinar a efetividade das soluções anti-DDoS não é uma tarefa trivial. De fato, apenas por meio da execução de testes que reproduzam um amplo espectro de cenários de ataque é que se torna possível caracterizar a efetividade de uma solução anti-DDoS.

No presente trabalho, apresentamos um simulador de ataques DDoS denominado SADI (acrônimo para Simulador de Ataques Distribuídos de Indisponibilidade). Mostramos que o SADI atende a um conjunto de requisitos propostos como necessários a um simulador de ataques DDoS em larga escala, de modo a poder ser utilizado como elemento central na tarefa de caracterizar a efetividade de soluções anti-DDoS. O SADI tem uma arquitetura baseada em cartuchos (Birsan 2005) e é dotado de uma biblioteca de ataques que permite personalizar cada cenário de ataque de acordo com as necessidades do usuário, sendo capaz de efetuar medições precisas que permitem caracterizar completamente a efetividade de uma solução anti-DDoS. O SADI explora, ainda, uma série de técnicas que permitem otimizar o uso de recursos de rede, selecionando, a cada simulação, o conjunto de máquinas de ataque que permita alcançar os objetivos desejados com o menor uso de recursos possível.

O artigo está organizado da seguinte forma. A Seção 2 apresenta o estado da arte no que se refere a ataques de negação de serviço, seja quanto às técnicas de ataque, seja quanto às soluções anti-DDoS. A Seção 3 apresenta os requisitos desejáveis a um simulador de ataques DDoS em larga escala, assim como descreve os principais cenários de uso de tal simulador. A Seção 4 propõe a arquitetura do SADI, descrevendo as propriedades de cada um de seus componentes. A Seção 5 discute aspectos de segurança da informação e o uso adequado do SADI. A Seção 6 descreve o atual estágio de desenvolvimento do SADI e as expectativas em relação ao projeto deste simulador de ataques DDoS. A Seção 7 contém nossas considerações finais.

## 2. Trabalhos Relacionados e Estado da Arte em Ataques DDoS

Esta seção apresenta os trabalhos relacionados e uma caracterização do estado da arte em ataques DDoS. Na seção 2.1 são apresentados os conceitos gerais referentes a ataques DDoS. Na seção 2.2 é exposto um breve histórico deste tipo de ataque. Finalmente, a seção 2.3 apresenta as principais soluções anti-DDoS.

### 2.1. Conceitos Gerais de Ataques DDoS

Um Ataque Distribuído de Negação de Serviço (ataque DDoS) consiste numa tentativa de tornar indisponível um recurso computacional como consequência de uma sobrecarga de dados ou requisições (Yu et al. 2011), a qual é atingida por meio da ação coordenada de diversos hosts controlados remotamente. Tais hosts são frequentemente denominados *computadores zumbis* ou *bots* (do inglês, robot – robôs), devido ao fato de, tipicamente, agirem sob comando de um computador identificado como seu "mestre", e, ao agirem em conjunto, caracterizam uma *botnet* (do inglês *robot network* - rede de robôs).

Um importante critério de classificação de ataques DDoS considera o protocolo de comunicação e o serviço explorado (Mirkovic and Reiher 2004). A partir desse critério, são denominados *ataques de infraestrutura* aqueles que agem em protocolos de camadas inferiores, notadamente as camadas 3 e 4 (rede e transporte). Tais ataques são essencialmente fundamentados em um elevadíssimo tráfego, o qual leva à sobrecarga e ao mal funcionamento de equipamentos que fornecem a infraestrutura de comunicação de uma rede (roteadores, firewalls, *stack* do servidor etc). Os ataques DDoS tem como principais alvos a infraestrutura. As abordagens mais exploradas nestes ataques são o *SYN flood*, o *UDP flood* e o *ICMP flood* (Radware 2013). *Ataques de aplicação* agem em camadas superiores, geralmente na camada de aplicação. Se, por um lado, estes ataques são mais sofisticados, por outro lado, demandam menor vazão (volume de dados ou requisições por unidade de tempo) para causar elevados danos. Tais ataques agem diretamente sobre provedores de serviço (*load balancers*, bancos de dados, servidores de aplicação, etc.). Dentre os ataque DDoS em camada de aplicação, os mais frequentes são aqueles baseados em requisições do tipo *HTTP GET* (Radware 2013).

Uma outra possível classificação de ataques DDoS diz respeito à estratégia de instanciação da *botnet* e sua topologia (Stankovic and Wood 2004). *Ataques por infecção* são aqueles nos quais máquinas infectadas por *malware*, após o recebimento de ordens, passam a enviar grandes volumes de requisições para a máquina-alvo. *Ataques hacktivistas (Leiderman 2013)* possuem uma rede de ataque organizada de maneira similar aos ataques por infecção, com a diferença que as máquinas atacantes fazem parte da rede de ataque de maneira voluntária. Ataques por reflexão seguem a seguinte estratégia geral (Paxson 2001). Primeiro, o atacante faz-se passar pela máquina alvo (por exemplo, por meio de *IP spoofing*) e faz uma solicitação qualquer a um provedor de algum serviço disponível na Internet. Na sequência, ao responder a solicitação, o provedor de serviço irá responder com dados não mais ao atacante, mas justamente à máquina-alvo - ou seja, aquela pela qual o ataque fez-se passar. Quanto mais provedores de serviço vulneráveis forem localizados na rede, maior será o volume de mensagens enviadas à máquina-alvo. Denomina-se fator de amplificação à razão entre o tamanho das mensagens enviadas pelo atacante ao provedor de serviço e o tamanho das

mensagens enviadas pelo provedor de serviço ao alvo. Um fator de amplificação maior que 1 levará a um aumento no volume de dados enviados ao alvo, em relação ao volume de dados enviado ao provedor. Um terceiro tipo de estratégia de instanciação de *botnet* é possível, embora não haja exemplos registrados deste modelo. Trata-se do cenário em que a *botnet* age voluntariamente. Tal cenário seria possível - e razoável - na hipótese de usuários em protesto contra determinada empresa ou serviço, numa ação que seria o análogo a uma passeata no mundo virtual.

Mais recentemente, o "poder" de uma *botnet* tem sido aplicado não diretamente à tarefa de sobrecarregar uma rede ou sistema, mas a tarefas intermediárias de ataque baseadas em força-bruta - por exemplo, determinar os parâmetros de uma comunicação TCP legítima (Charalampos Z. Patrikakis 2004, Jelena Mirkovic 2014) - para em seguida, já de posse de tais parâmetros, executar uma ação de negação de serviço - por exemplo, enviar um *TCP Reset*. Note que, no exemplo anterior, a ação que resultou em negação de serviço não foi a sobrecarga de solicitações; o poder da *botnet* foi utilizado em um ataque intermediário de força-bruta.

Alguns critérios quantitativos para classificar ataques DDoS são a vazão máxima atingida, o volume total de dados e a duração do ataque, sendo que a vazão costuma ser o aspecto mais amplamente divulgado nos ataques de grande repercussão. Ataques que atinjam até 50 Gbps são considerados de menor porte e, quando exploram protocolos de camadas inferiores, costumam ser tratáveis por meio de equipamentos de rede como roteadores e *firewalls*. Ainda assim, uma vazão como esta explorando camadas superiores pode caracterizar um ataque de efeitos notáveis. Vazões superiores a 50Gbps tendem a demandar respostas específicas e intervenções *ad hoc*.

## 2.2. Breve Histórico dos Ataques DDoS

Embora haja menções a ataques baseados em sobrecarga de sistemas computacionais antes da década de 1980[2], os primeiros ataques DDoS considerados "modernos" foram registrados nos anos de 1997 e 1998, ficando conhecidos como os ataques "*Smurfs*" na Universidade de Minnesota (CNET News 1998), um tipo de ataque DDoS que inundava a rede alvo de respostas para pacotes *ping* especificando o computador alvo como sendo o endereço para o retorno dos pacotes, enviando solicitações suficientes para garantir a negação de serviço.

Em fevereiro de 2000, uma sequência de ataques DDoS teve uma enorme repercussão (BBC News 2000, CNET News 1998). Trataram-se de ataques com o objetivo de derrubar sites de grandes empresas como Yahoo, Ebay, Amazon e CNN. Com picos de vazão chegando 1 Gbps, os sistemas envolvidos nos ataques chegaram a ficar indisponíveis por horas. Como se poderia imaginar, o ataque baseou-se em técnicas rudimentares de sobrecargas volumétricas, as quais não exploravam nenhuma vulnerabilidade em si, mas sim, causavam estresse de requisições, e contra as quais os sistemas-alvos não possuíam mecanismos de defesa.

[2] Por exemplo, há relatos (Radware 2013) de que o Computer-based Education Research Laboratory na University of Illinois at Urbana-Champaign foi alvo de ataques de DoS baseados em sobrecarga no ano de 1974.

O início da década de 2000 também marcou o surgimento das primeiras ferramentas automáticas de ataques DDoS (Radware 2013) - tanto ferramentas que visavam realizar os ataques em si (por exemplo, Teardrop, Boink, Bonk, WinNuke) como ferramentas que "infectavam" ou "controlavam" uma vitima para ser usada como membro de redes *botnet* (por exemplo, trin00, Tribe Flood Network, Stacheldraht). Basicamente, essas ferramentas permitiam que um atacante tivesse acesso a diversas máquinas vítimas - sem seu consentimento - para lançar ataques DDoS contra um *website*.

Nos anos que se seguiram, novos ataques foram registrados - cabe registro do ataque direcionado ao sistema de resolução de nomes da Internet em 2002 (Radware 2013). Durante o ataque contra os servidores de nomes, todos os 13 servidores raízes experimentaram cargas pesadas de requisições, e alguns deles ficaram inacessíveis. Mesmo que o ataque não tenha sido inteiramente bem sucedido, mostrou-se os potenciais impactos que um ataque DDoS pode causar à Internet.

As motivações para a execução de um ataque DDoS são diversas. A seguir, são apresentadas as mais frequentes:

- hacktivismo: trata-se da execução de ataques com motivações ideológicas (alguns defendem, inclusive, a "legalização" do DDoS como um ato legítimo de protesto);
- extorsão: criminosos extorquindo empresas com presença na Internet, ou seja, solicitando dinheiro em troca da interrupção de um ataque;
- competição: empresa executa (ou encomenda) ataque contra concorrente;
- ranqueamento de *websites*: tráfego falso pode ser usado como objetivo de melhorar a posição de um *website* em ferramentas de busca e ranqueamento;
- ataque multivetor: o ataque DDoS é parte de uma ação mais complexa (por exemplo, a indisponibilidade da defesa permitindo posterior invasão);
- *cyber war*: iniciativas nacionais em ataques contra outras nações (até agora, não há nenhuma ação "oficial" registrada);
- recreação: boa parte dos ataques consiste em usuários que buscam apenas o "prazer" de derrubar um grande (ou nem tão grande) *website*.

## 2.3. Soluções anti-DDoS

A experiência mostra que administradores de sistemas que nunca consideraram a questão de vulnerabilidade a ataques DDoS certamente estão vulneráveis a eles[3]. Considerar ataques DDoS, nos dias de hoje, deve fazer parte do roteiro de trabalho de qualquer administrador de sistemas. Alguns controles simples - que não demandam a contratação de empresas especializadas - podem, de fato, reduzir a vulnerabilidade a ataques desta natureza. No entanto, uma solução anti-DDoS para ataques em larga

[3] A maioria dos testes envolvendo o SADI levou à indisponibilidade do sistema testado como consequência da execução de ataques bastante simples (por exemplo, TCP SYN Flood) a taxas moderadas (alguns Gbps).

escala precisa de muito mais recursos de defesa, tipicamente possuindo mecanismos de detecção, análise e mitigação de ataques (Mirkovic and Reiher 2004), descritos a seguir.

**Detecção:** consiste na simples detecção de uma mudança de padrão de uso dos recursos de rede, o qual pode indicar que um ataque DDoS está em curso ou em fase de preparação. Os dados gerados pelo sistema de detecção são encaminhados ao sistema de análise. Ao contrário dos clássicos métodos de detecção de intrusão "baseados em assinatura", mecanismos de detecção de ataques DDoS são essencialmente "comportamentais", o que significa que eles devem tomar decisões a respeito da existência de um ataque apenas com base em padrões de tráfego, sem basear-se em inspeções cuidadosas sobre os pacotes em tráfego.

**Análise:** Uma vez detectado um possível ataque DDoS, o sistema de análise procurará verificar se, de fato, trata-se de um ataque, classificando-o se for o caso. A correta classificação do ataque é fundamental para que o sistema de mitigação tome as providências adequadas para sanar os efeitos do ataque.

**Mitigação:** Após a identificação e classificação de um ataque DDoS em preparação ou em curso, é necessário tomar providências que minimizem os efeitos do ataque. Tais providências dependerão do tipo de ataque em curso; em geral, envolvem a segregação de redes e a eliminação de tráfego malicioso (*blackholing*).

Embora o rastreamento da origem do ataque seja, em alguns casos, uma etapa adicional desejável, esta é uma difícil tarefa que demanda a interação com diversos "participantes da Internet" (de provedores de serviço e mantenedores de *backbones* a autoridades policiais e serviços diplomáticos); na prática, as soluções anti-DDoS atualmente disponíveis não oferecem este tipo de serviço.

## 3. Requisitos para um Simulador de Ataques DDoS em Larga Escala

Um simulador de ataques DDoS em larga escala deve ser concebido de forma a poder ser utilizado no processo de validação de controles anti-DDoS, permitindo estimar com precisão a acurácia dos sistemas de detecção de ataques, a corretude dos sistemas de análise e classificação de ataques, e a eficácia dos sistemas de mitigação de ataques. Defendemos a ideia de que somente a partir da cuidadosa reprodução de um vasto conjunto de ataques (simulados) DDoS, pode-se caracterizar precisamente uma solução anti-DDoS no que diz respeito aos seus mecanismos de detecção, análise e mitigação.

Serviços de ataques DDoS vêm proliferando na comunidade nos últimos tempos. No entanto, a maioria dos serviços disponíveis apresenta baixo rigor técnico, consistindo tão somente na implementação de alguns poucos *scripts* de ataque, e não disponibilizando recursos de personalização de simulação. Além disso, até onde pudemos verificar, nenhum simulador de ataques DDoS conhecido pela comunidade permite mensurar com precisão as grandezas associadas a um cenário de simulação de ataque. Um simulador de ataques DDoS em larga escala deve atender a propriedades que permitam utilizá-lo como um estimador preciso da vulnerabilidade de sistemas de informação face a ataques DDoS, assim como da efetividade de soluções anti-DDoS.

Apresentamos, a seguir, os requisitos que consideramos fundamentais para que um simulador de ataques DDoS possa, de fato, vir a ser utilizado como uma ferramenta

para a validação de soluções anti-DDoS, estimando adequadamente a suscetibilidade de redes e sistemas de informação a ataques deste tipo.

- Banco de ataques. O simulador deve possuir um vasto banco de dados de técnicas de ataque, permitindo caracterizar a efetividade de ferramentas anti-DDoS face a diversos cenários de ataque;

- Personalização. Possibilidade de adequação das características de cada simulação, variando o perfil de cada ataque no que diz respeito aos protocolos explorados, à topologia da rede de atacantes e à vazão alcançada;

- Medição precisa. Capacidade de caracterizar precisamente os cenários de ataque e os parâmetros de ataque que comprometeram a disponibilidade do sistema-alvo.

Alguns requisitos adicionais são considerados desejáveis, no sentido de favorecer a um uso eficiente e escalável da ferramenta.

- Gerenciabilidade. fácil instanciação de cenários de ataque, atualização automática de software e banco de ataques.

- Visibilidade. Caracterização da rede de ataque a cada instante de tempo.

- Otimização. Adequar a execução das simulações de modo a otimizar os recursos do simulador.

- Automatização de relatório. Geração automática de relatórios de uso e de relatórios de resultados de simulações.

## 4. Arquitetura Proposta

Nesta seção, descrevemos a arquitetura de um simulador de ataques distribuídos de negação de serviço, ao qual denominamos SADI (Simulador de Ataques Distribuídos de Indisponibilidade). O simulador possui seis principais componentes: Central de Comando, Cliente de Simulação, Sobree de Ataque, Autoridades Locais, Máquinas de Ataque e Estimadores de Recursos. A Figura 1 apresenta informações de como os componentes estão organizados no SADI.

A Central de Comando (CC) é o componente central do SADI, sendo considerado a "autoridade raiz" do simulador de ataques. Ela é responsável pela instanciação de cenários de ataque. Também faz parte do seu escopo ser responsável por especificar todas as características de cada um dos ataques executados pelo SADI. Finalmente, ela responde, ainda, pelo gerenciamento de demandas do SADI.

Os Clientes de Simulação (CS) são os componentes que solicitam à Central de Comando que seja executada uma simulação de ataque. A execução da simulação é autorizada a partir da identificação do Cliente de Simulação como um usuário válido, da verificação da adequação da simulação solicitada ao perfil do CS, e da viabilidade da simulação tendo em vista a quantidade de recursos disponíveis.

A Sub-rede de Ataque (SA) é um conjunto de máquinas identificadas por características em comum. Exemplos são máquinas virtuais em um mesmo servidor de virtualização, máquinas reais em um mesmo provedor de serviços, máquinas reais em uma mesma região geográfica etc. As SAs são coordenadas pelas Autoridades Locais (AL). As Autoridades Locais são os componentes responsáveis pelo gerenciamento de uma SA. Por um lado, monitoram a disponibilidade das máquinas de uma Sub-rede de

Ataque, repassando à Central de Comando informações que ajudarão no gerenciamento do SADI. Por outro lado, transmitem às Máquinas de Ataque os comandos de ataque associados a cada simulação executada.

As Máquinas de Ataque (MA) são as máquinas que efetivamente executam simulações de ataque contra o sistema alvo. Recebem das Autoridades Locais instruções sobre como executar um ataque, e retornam a estas Autoridades Locais informações relevantes coletadas. Já os Estimadores de Recursos (Est) são máquinas de ataque especiais que mantém contato constante com as Autoridades Locais, transmitindo informações e medições que permitirão determinar o estado de sua Sub-rede de Ataque.

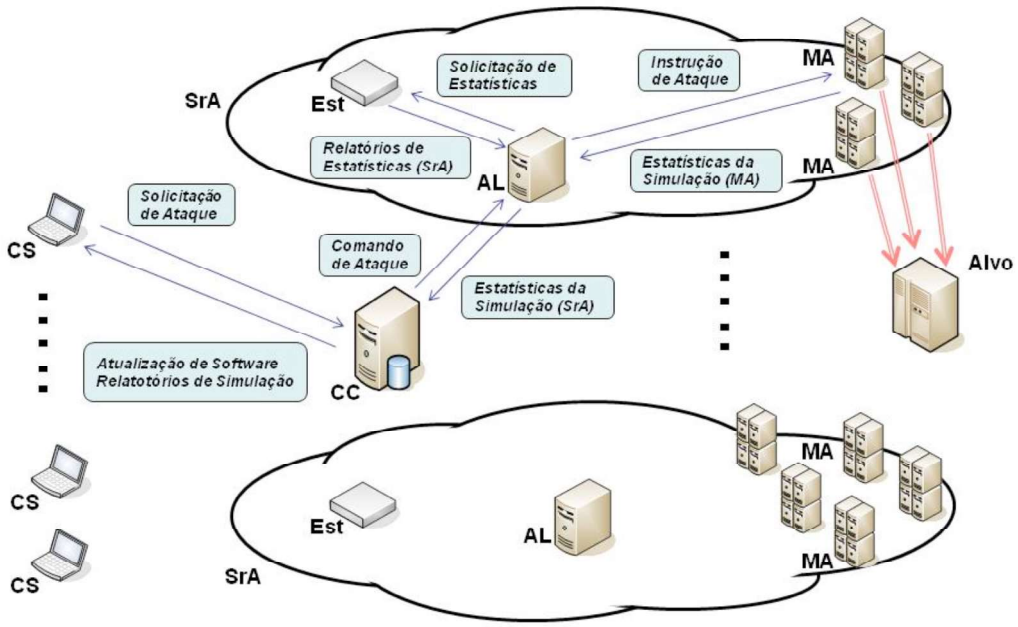


**Figura 1. Arquitetura do SADI.**

## 5. Aspectos de Segurança da Informação

Um simulador de ataques, como o descrito neste trabalho, torna-se uma poderosa arma de ataque, caso seja explorada por usuários maliciosos. Ao mesmo tempo, uma vez que o ataque é, na prática, executado por milhares de máquinas de ataque geograficamente distribuídas e gerenciadas através de uma rede distribuída, a quantidade de potenciais brechas disponíveis para tentativas de exploração é enorme. Desta forma, é fundamental que se conceba uma arquitetura de segurança que garanta o adequado uso de tal ferramenta de simulação de ataques. Descrevemos, a seguir, os controles implementados no SADI com vistas a atingir tais objetivos de segurança.

**Autenticidade e confidencialidade das comunicações.** Todos os canais de comunicação entre componentes do SADI são autenticados, de modo a garantir a integridade de todos os dados que trafegam na rede. Tais mecanismos de autenticação

impedem, por exemplo, que um atacante envie mensagens ou comandos a um componente do SADI fazendo-se passar por um usuário ou componente legítimo do SADI. Na prática, tal autenticidade é obtida através do uso de assinatura digital - ou seja, cada componente possui uma chave privada única protegida contra leitura de terceiros e armazena as chaves públicas de um conjunto de outros componentes com os quais deve comunicar-se, protegendo tais chaves de modificação não-autorizada. Adicionalmente, determinados tipos de comunicação são protegidos por meio de cifração, com o objetivo de garantir a confidencialidade de determinadas informações (por exemplo, especificações de ataques e dados de clientes e alvos). As chaves criptográficas são pré-negociadas no momento de implantação do sistema, não sendo necessário fazer uso de uma infraestrutura de chaves públicas.

**Adequação de solicitação ao perfil contratado.** Cada solicitação feita por um CS é avaliada quanto à sua aderência ao perfil contratado por aquele CS. Exemplos de aspectos que são verificados são: (i) se o CS tem autorização para solicitar uma simulação para determinada faixa de IPs ou (ii) se o CS tem autorização para solicitar simulações de ataque com determinada vazão.

**Testes de plausibilidade da solicitação.** Ainda que uma solicitação esteja aderente ao perfil contratado por um CS, testes adicionais são feitos no sentido de verificar se uma determinada solicitação de simulação é compatível com o histórico recente de solicitações daquele CS. Por exemplo, se um cliente sempre solicita simulações na faixa de 1 Gbps, e faz uma solicitação eventual de simulação de 50 Gbps. Ainda que esta operação seja autorizada para o perfil do CS, a mesma levará a um alerta aos operadores do SADI gerada pela CC (na prática, um operador entrará em contato com o responsável pelo CS, antes de liberar a execução da simulação). Testes de plausibilidade também são efetuados pelas instruções recebidas pelas AL (vindas da CC) e pelas MA (vindas de sua AL).

**Proteção de componentes críticos.** Componentes capazes de instanciar ataques de larga e média escala - como o CC e as AL - estão protegidos por meio de mecanismos de proteção física e lógica. O CC está localizado no quartel general da rede SADI, portanto, fisicamente protegido de acesso indevido. As AL estão localizadas em redes de parceiros do SADI, e protegidas por trás de equipamentos de segurança de redes como *firewalls*.

**Proteção de software.** Para componentes localizados fora do domínio da rede SADI - notadamente, os CS e alguns Est - são utilizadas técnicas de proteção de software que visam dificultar eventuais tentativas de engenharia reversa e a consequente descoberta de informações críticas de segurança. São utilizadas técnicas de ofuscação e de incorruptibilidade. Técnicas de ofuscação (Colher and Thomborson 2002, Dalla Preda and Giacobazzi 2009) comprometem a atuação de *disassemblers* e decompiladores, assim como dificultam o entendimento do software e a consequente localização de dados sensíveis, tais como chaves criptográficas e parâmetros de ataque. Técnicas de incorruptibilidade (Collberg and Thomborson 2002, Li et al. 2009) buscam, através da inserção de "travas lógicas", dificultar modificações maliciosas no software que visam subverter o seu comportamento.

## 6. O Projeto SADI

Na presente seção, apresentamos brevemente a visão da equipe de pesquisa do projeto SADI quanto aos objetivos a serem alcançados, aos resultados e produtos a serem gerados, e aos impactos que devem ocorrer no mercado e na sociedade como um todo. O projeto SADI visa internalizar conhecimento a respeito de uma importante classe de ataques - os ataques DDoS - ao mesmo tempo em que propõe o desenvolvimento de uma ferramenta de simulação de ataques que provavelmente não encontra similar no Brasil ou no exterior. Consideramos que o desenvolvimento deste tipo de ferramenta e a produção de conhecimento relacionada são estratégicos para o país - e o apoio de órgãos como o CNPq e a Finep[4] ao projeto reforçam esta visão.

Os objetivos do projeto, de uma maneira ampla, são a produção de conhecimento - que possa ser aplicado ao desenvolvimento de serviços de Segurança da Informação e à elaboração de políticas públicas de Defesa Nacional - e o desenvolvimento de serviços de avaliação de sistemas de informação quanto à vulnerabilidade a ataques DDoS.

Os produtos gerados pelo projeto SADI, naturalmente, estão associados aos objetivos do projeto. O produto mais evidente gerado pelo projeto é uma ferramenta de simulação de ataques DDoS, a qual irá viabilizar a criação de um serviço de avaliação de vulnerabilidade de sistemas de informação face a ataques distribuídos de negação de serviço. Uma outra importante classe de produtos a ser gerada diz respeito a artefatos que possibilitam consolidar o conhecimento sobre ataques DDoS no país. Nesta classe, incluem-se artefatos indicadores de produção científica (artigos científicos, apresentações em eventos acadêmicos, trabalhos de conclusão de curso) e artefatos de divulgação (livros, palestras de divulgação, webinars, cursos). Acreditamos que a internalização do conhecimento sobre ataques DDoS no país é um passo importante no caminho para se estabelecer uma estratégia de Defesa Nacional relacionada a este tipo de ataque.

O sucesso do projeto SADI causará impactos positivos no mercado de Segurança da Informação e nas políticas de Defesa Nacional, com consequências claras para a Sociedade como um todo. O mercado de Segurança da Informação beneficia-se com a disponibilidade de novo serviço de Segurança da Informação e de Sistemas, eventualmente replicado por outras empresas, levando a uma maior maturidade do mercado e a uma maior disponibilidade de redes e sistemas de informação. As políticas de Defesa Nacional beneficiam-se de um maior entendimento sobre os riscos e potenciais dos ataques DDoS como uma arma de guerra cibernética. Finalmente, a Sociedade como um todo beneficia-se com a maior disponibilidade de sistemas de informação - sejam sistemas comerciais, sistemas do governo, ou sistemas de infraestruturas críticas.

[4] Particularmente, cabe destacar a primeira colocação na chamada Finep 04/2013 TI-Maior

## 7. Considerações Finais

Entendemos que uma cuidadosa validação de uma solução anti-DDoS é crucial para que se tenha confiança naquela solução. Tal validação deve caracterizar a resposta da solução anti-DDoS em cada possível cenário de ataque. Adicionalmente, a validação de soluções anti-DDoS deve ser reexecutada continuamente, de modo a considerar novos ataques em um ambiente de constantes mudanças no mundo dos ataques DDoS. Acreditamos que o único método prático de se efetuar uma validação como a descrita é através do uso de um simulador de ataques DDoS em larga escala, que permite a execução eficiente de simulações reproduzindo diversos cenários de ataque, caracterizando a resposta da solução anti-DDoS em cada caso. De fato, acreditamos que, em um futuro próximo, o SADI poderá ser utilizado como uma "ferramenta-padrão de ataques DDoS", no sentido de executar de maneira normalizada os principais métodos de ataque, considerando todas as possíveis variações e combinações de ataque. Tal característica irá torná-lo a ferramenta ideal para a construção de *datasets* de ataque DDoS, os quais poderão ser utilizados para caracterizar de maneira unificada e científica a eficácia de detectores de ataques DDoS.

**Trabalhos futuros**. Atualmente, a mais nova versão do SADI encontra-se plenamente operacional, sendo capaz de executar simulações de ataques bastante sofisticadas - envolvendo a exploração de cerca de vinte tipos distintos de protocolos - e tendo sido utilizado na identificação de vulnerabilidades a ataques DDoS em mais de uma dezena de organizações. Apesar de já ser uma ferramenta bastante efetiva na identificação de redes e sistemas de informação vulneráveis a ataques DDoS, diversas oportunidades de melhoria se apresentam e deverão ser implementadas nos próximos anos, visando alcançar uma maior precisão, escalabilidade e facilidade de uso, além da manutenção de uma vasta e atualizada base de dados de ataques DDoS, conforme descrevemos a seguir:

- Instanciação rápida das MA: mais velocidade, uso de serviços de virtualização, desenvolvimento de *live flash drives* para a inicialização de máquinas de ataque em computadores de terceiros.

- Medição precisa: estudo de métodos que permitam estimar com maior precisão o estado da rede SADI, assim como mensurar as estatísticas de cada simulação de ataque.

- Otimização: melhor aproveitamento dos recursos da rede SADI, possibilitando o atendimento a uma maior quantidade de solicitações de simulação com a mesma infraestrutura.

- Banco de ataques: manutenção de uma base de dados de ataque atualizada, sempre considerando os mais recentes modelos de ataque DDoS conhecidos e reproduzidos pela comunidade.

## Referências

BBC News, (2000), *Yahoo attack exposes web weakness*, http://news.bbc.co.uk/2/hi/science/nature/635444.stm.

Birsan, D., (2005), "On plug-ins and extensible architectures", *Queue*, v. 3, n. 2, p. 40–46.

Charalampos Z. Patrikakis, M. M., (2004), "Distributed Denial of Service Attacks", *Internet Protocol Journal*, v. 7, n. 4, p. 13–35.

CNET News, (1998), *"Smurf" attack hits Minnesota*, http://news.cnet.com/Smurf-attack-hits-Minnesota/2100-1001_3-209209.html.

Collberg, C. S., Thomborson, C., (2002), "Watermarking, Tamper-proffing, and Obfuscation: Tools for Software Protection", *IEEE Trans. Softw. Eng.*, v. 28, n. 8 (Aug.), p. 735–746.

Dalla Preda, M., Giacobazzi, R., (2009), "Semantics-based Code Obfuscation by Abstract Interpretation", *J. Comput. Secur.*, v. 17, n. 6 (Dec.), p. 855–908.

Jelena Mirkovic, (2014), *DDoS Benchmarks*, http://www.isi.edu/~mirkovic/bench.

Leiderman, (2013), *Justice for the PayPal WikiLeaks protesters: why DDoS is free speech*, http://www.theguardian.com/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech.

Li, D., Hu, Y., Hu, X., Ling, H., (2009), "Self-Checking Tamper-Proofing Based on Software Behavior Model". In: *Fourth International Conference on Frontier of Computer Science and Technology, 2009. FCST '09*, p. 639–643

Mirkovic, J., Reiher, P., (2004), "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *SIGCOMM Comput. Commun. Rev.*, v. 34, n. 2 (Apr.), p. 39–53.

Paxson, V., (2001), "An Analysis of Using Reflectors for Distributed Denial-of-service Attacks", *SIGCOMM Comput. Commun. Rev.*, v. 31, n. 3 (Jul.), p. 38–47.

Radware, (2013), *DDoS Survival Handbook*, http://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf.

Stankovic, J., Wood, A., (2004), "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", In: Ilyas, M., Mahgoub, I. [eds.] (eds), *Handbook of Sensor Networks*, CRC Press

Yu, S., Zhou, W., Doss, R., Jia, W., (2011), "Traceback of DDoS Attacks Using Entropy Variations", *IEEE Transactions on Parallel and Distributed Systems*, v. 22, n. 3 (Mar.), p. 412–425.