Programa de Grupos de Trabalho da RNP
2014-2015

Proposta para Grupo de Trabalho

GT-ACTIONS: Ambiente Computacional para Tratamento de Incidentes com Ataques de Negação de Serviço

Coordenador: Iguatemi E. Fonseca, UFPB

Coordenador Adjunto: Moisés R. N. Ribeiro, UFES

1 Título

Título: Ambiente Computacional para Tratamento de Incidentes com Ataques de Negação de Serviço
Sigla: GT-ACTIONS

2 Coordenadores

Coordenador: Iguatemi Eduardo da Fonseca
e-mail: iguatemi@ci.ufpb.br. Curriculum: http://lattes.cnpq.br/4519016123693631
Programa de Pós-Graduação em Informática
Centro de Informática, Universidade Federal da Paraíba (UFPB)
João Pessoa - Paraíba. http://www.ppgi.di.ufpb.br
Coordenador Adjunto: Moisés Renato Nunes Ribeiro
e-mail: moises@ele.ufes.br. Curriculum: http://lattes.cnpq.br/1005553714687743
Programa de Pós-Graduação em Engenharia Elétrica
Departamento de Engenharia Elétrica, Universidade Federal do Espírito Santo (UFES)
Vitória - Espírito Santo. http://www.ele.ufes.br

3 Resumo

Segundo relatórios do CAIS/RNP (Centro de Atendimento a Incidentes de Segurança da RNP), ataques DDoS (*Distributed Denial-of-Service*) na Rede Ipê da RNP tem ocorrido com frequência entre 2009 e 2013 sendo portanto um dos principais desafios da segurança na Internet. Sites comerciais, academicos e governamentais, *e.g.*, do Governo Federal Brasileiro, são alvos frequentes destes ataques. Ataques DDoS tem uma capacidade grande de mudança assumindo novas características. Portanto, ao invés de construir defesas específicas a para ataques DDoS específicos, é mais importante desenvolver uma metodologia para adequar rapidamente os algoritmos para o tratamento de novas versões de ataques. Partindo de dois protótipos em desenvolvimento pelos proponentes, esse projeto trata da concepção de uma plataforma computacional para identificação e tratamento em tempo real de ataques DDoS, chamado ACTIONS, e a proposta de uma metodologia para invenção de novos de algoritmos.

4 Abstract

According to reports from the CAIS/RNP (*Centro de Atendimento a Incidentes de Segurança da RNP*), DDoS (*Distributed Denial-of-Service*) attacks in the Ipê Network have been often carried out between 2009 and 2013, being one of the main challenges of Internet security. Comercial, academic and governamental sites are its main targets, including sites from the Brazilian Federal Government. As DDoS attacks can change quickly its characteristics, instead of developing specific algorithms for mitigating specific attacks, one should develop a methodology for quickly configuring defenses against new DDoS attacks and for attack identification. Starting from two prototypes developed by our team, this project's main goal is to develop a framework for the real-time identification and mitigation of DDoS attacks, called ACTIONS, as well as a methodology for the development of new defense algorithms.

5 Parcerias

Esse projeto será executado em parceria com as seguintes instituições (a Seção 7.4 "Metodologia e cronograma"apresenta as atividades de cada uma delas):

- UFABC - Universidade Federal do ABC - Programa de Pós-Graduação em Engenharia da Informação
  Participante: Prof. Hélio Waldman;
- UFES - Universidade Federal do Espírito Santo - Programa de Pós-Graduação em Engenharia Elétrica
  Participante: Prof. Moisés Renato Nunes Ribeiro;
- UFPB - Universidade Federal da Paraíba - Programa de Pós-Graduação em Informática
  Participantes: Prof. Iguatemi Eduardo da Fonseca, Prof. Vivek Nigam;
- IFPB - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
  Participantes: Prof. Leandro Cavalcanti de Almeida;

Os Profs. Hélio Waldman e Moises Ribeiro possuem vasta experiência em modelagem de tráfego em redes de comunicação e, portanto, darão decisiva contribuição neste projeto. Os Profs. Iguatemi E. Fonseca e Vivek Nigam têm trabalho conjuntamente no desenvolvimento de técnicas e algoritmos para identificação de ataques DDoS [1, 2, 3, 4], orientam atualmente três dissertações de mestrado e alunos de Iniciação Científica em temas relacionados aos ataques DDoS. O Prof. Leandro Almeida concluiu sua dissertação de Mestrado sob orientação do Prof. Iguatemi E. Fonseca em tema relacionado aos ataques DDoS [1].

6 Duração do projeto

A execução do projeto está prevista para 12 (doze) meses.

7 Sumário executivo

7.1 Os ataques DoS e DDoS

Ataques de Negação de Serviço Distribuído (DDoS - *Distributed Denial-of-Service*) e de negação de serviço (DoS - *Denial of Service*) têm sido um dos maiores problemas da Internet [1] – [17]. Recentemente, ocorreu um dos maiores ataques DDoS da história, no qual cerca de 300 Gbps de tráfego inútil foi gerado em uma espécie de guerra cibernética envolvendo o grupo Spamhaus e a empresa Cyberbunker [5]. Entre 2009 e 2013, sites do Governo Brasileiro, do Governo do Iran, Paypal, Amazon, Mastercard, Visa, Sony, FBI e Senado Americano também sofreram ataques usando principalmente um tipo mais recente de ataque DDoS, o DDoS HTTP. Nos anos 2000, um grande número de ataques foi realizado contra grandes portais de empresas como Yahoo, eBay, e Amazon [14] usando técnicas tradicionais de ataques como ICMP, UDP e TCP *SYN flooding*. No Brasil, além dos incidentes mencionados contra sites do Governo Brasileiro, segundo relatórios do CAIS/RNP, ataques DDoS na Rede Ipê da RNP tem ocorrido com bastante frequência. Por

exemplo, em 2009 foram reportados ao CAIS/RNP 11 casos. Em 2010 esse número cresceu para 26 ataques reportados. Já em 2011, 38 ataques críticos de negação de serviço envolvendo endereços IP da Rede Ipê foram detectados e reportados ao CAIS/RNP, em um desses ataques em novembro de 2011, foram detectados mais de 1,9 *Gbit/s* de tráfego malicioso. Até setembro de 2012, ocorreram cerca de 70 casos de ataques registrados, o que mostra um crescimento considerável no número de ataques na Rede Ipê da RNP entre 2009 e 2012. Vale a pena mencionar que muitos ataques DDoS na Rede Ipê não são informados ao CAIS e, portanto, o número real de incidentes com ataques DDoS pode ser bem maior.

Tradicionalmente, ataques DDoS acontecem nas camadas de rede e transporte do modelo TCP/IP [6], com os conhecidos ataques de inundação utilizando protocolos como o ICMP (*Internet Control Message Control*), UDP (*User Datagram Protocol*) e o TCP (*Transport Control Protocol*) [7]. Um ponto em comum destes ataques é que eles afetam a infraestrutura de hardware dos sistemas alvos, consumindo ciclos do processador e bytes de memória RAM, assim o alvo deixa de responder a requisições legítimas por não ter mais recursos disponíveis. Uma versão mais sofisticada de um ataque DDoS, agora na camada de aplicação do modelo TCP/IP [8], tem sido utilizada em muitos ataques desse tipo. Nesses casos, usa-se o protocolo de transferência de hipertexto (HTTP - *Hypertext Transfer Protocol*), que faz uso de métodos para realizar a comunicação entre cliente e servidor Web. É possível observar que o atacante utiliza os métodos GET, PRAGMA e POST de uma conexão HTTP válida para esgotar os recursos do serviço Web disponibilizado pelo servidor, ou seja, a infraestrutura de hardware do sistema alvo permanece quase que intacta. Também protocolos usados na communicação VoIP (*Voice over IP*), como o protocolo SIP (Session Initialization Protocol), tem sido utilizados para derrubar serviços VoIP, *e.g.*, os ataques SIP-flooding [26]. Recentemente [3], nós identificamos um novo ataque DDoS que explora o protocolo SIP, chamado *Coordinated VoIP Attack*, onde pares de atacantes esgotam os recursos do servidor VoIP ao estabelecer (um número grande de) connexões de longa duração.

Em [1, 2, 3, 4], os proponentes do GT-ACTIONS propõem ferramentas que podem ser utilizadas para mitigar os efeitos de versões mais sofisticadas de ataques DDoS, incluindo os ataques realizados na camada de rede, como na camada de aplicação usando protocolos HTTP e SIP.

O grande desafio para os administradores de sistemas e redes é conseguir diferenciar tráfego gerados por usuários legítimos de tráfego de um ataque DDoS [17]. Aplicações caracterizadas por serem aceleradores de *downloads*, como o Orbit [18], Flashget [19] e Freedownload [20], podem ser confundidas com um ataque DDoS. Quando estas aplicações estão em funcionamento criam um alto número de conexões, utilizando múltiplas portas de origem, em um único servidor web, utilizando uma única porta de destino, para realizar o *download* de um arquivo. Este modo de funcionamento poderia ser confundido com um ataque TCP SYN flooding [17].

7.2 Objetivos e produtos gerados

O objetivo principal do GT-ACTIONS é desenvolver uma plataforma computacional, metodologias e técnicas para identificação e tratamento de ataques de negação de serviços (DDoS). Para isso, baseado na modelagem matemática e análise do perfil do tráfego dos ataques, será implementada uma ferramenta

computacional, chamada ACTIONS (Ambiente Computacional para Tratamento de Incidentes com Negação de Serviço), que seja capaz de perceber em tempo real a existência de ataques e tomar medidas preventivas. O ACTIONS será implementado usando *software* livre e código desenvolvido pela equipe científica e poderá ser instalado nas instituições que fazem uso da rede da RNP. Como ponto de partida, serão utilizados dois protótipos em desenvolvimento/aprimoramento em dissertações de mestrado sob orientação de professores da equipe científica dessa proposta [1, 2, 3, 4]. Tais ferramentas já possuem modelos e algoritmos de identificação e tratamento para tipos sofisticados de ataques DDoS. Nos experimentos realizados com uma dessas ferramentas, o tempo médio para a identificação e bloqueio dos ataques DDoS foi de 40 segundos [1].

Para alcançar o objetivo geral proposto, os seguintes objetivos específicos também deverão ser alcançados:

1. **Modelo matemático e perfil do ataque:** Identificar o perfil dos diversos tipos de ataques DDoS e modelar formalmente usando modelos matemáticos os seus aspectos fundamentais;

2. **Metodologia:** Criar uma metodologia para o desenvolvimento de algoritmos e técnicas de identificação e tratamento dos ataques DDoS. Com a metodologia, caso o perfil do ataque DDoS seja mudado pelos atacantes, será possível adaptar rapidamente os algoritmos e técnicas para o novo perfil de ataque;

3. **Algoritmos e técnicas:** Desenvolver e validar técnicas e algoritmos para neutralizar ataques DDoS. A validação será através do uso de métodos formais em computação e como também de simulações numéricas e experimentos na rede da RNP. O uso de métodos formais será importante no processo de desenvolvimento de sistemas, seguindo [23], no qual foi concebida uma metodologia de desenvolvimento de política de roteamento para provedores de Internet usando métodos formais.

4. **Plataforma computacional:** Implementar a plataforma computacional ACTIONS para a defesa em tempo real contra ataques DDoS.

Algumas contribuições científicas e tecnológicas da proposta são enumeradas a seguir:

- Um produto tecnológico que pode ser instalado na Rede Ipê para identificação e tratamento em tempo real de ataques DDoS;

- Uma metodologia para identificação e tratamento de ataques DDoS. Dado que os ataques DDoS estão sempre mudando e assumindo novas características, é fundamental que haja uma metodologia de desenvolvimento de ferramentas para seu tratamento e identificação. Isso talvez seja mais importante do que se desenvolver uma técnica que sirva apenas para um tipo específico de ataque, pois caso o atacante mude o perfil do tipo de ataque, essa ferramenta poderá não ser mais útil para a proteção dos usuários;

- Um modelo matemático para a especificação e verificação formal dos atuais ataques DDoS;
- Técnicas e algoritmos para identificação e tratamento de ataques DDoS.

7.3 Requisitos para a operação e instalação na rede

O ACTIONS poderá ser instalado nos servidores já presentes nas instituições que fazem parte da Rede Ipê. Outra opção é usar servidores dedicados para a instalação da ferramenta que deverão ser alocados nas instituições pertencente a rede Ipê e que desejarem ter a ferramenta instalada. A primeira opção já foi testada em trabalhos prévios realizados pelo grupo proponente para identificação e tratamento em tempo real de um ataque DDoS e, nesse cenário, o tempo médio de identificação e bloqueio dos ataques foi de 40 segundos. Foram usados servidores com configuração comum aos encontrados na Rede Ipê e que possuiam o sistema operacional GNU/Linux, que é um sistema operacional de código aberto e bastante difundido nas redes do mundo. Caso se decida pela instalação da ferramenta em servidores dedicados em Pontos de Presença (PoPs) e clientes da Rede Ipê, pode-se optar pela compra de máquinas com configuração mais atualizada.

Portanto, de maneira geral, para a operação e instalação na rede é necessaria apenas a existência de servidores com sistema operacional GNU/Linux e com configuração similar aos já encontrados na Rede Ipê.

7.4 Metodologia e cronograma

Nesse projeto serão utilizados tanto modelos analíticos quanto simulação numérica em computador e experimentos em uma rede real para o teste e validação dos algoritmos e da plataforma ACTIONS. Como dito anteriormente, será aproveitado um protótipo desenvolvido previamente para a execução desse projeto. Na dissertação de mestrado do Leandro A. Cavalcanti foi desenvolvida uma versão inicial dos modelos e algoritmos de identificação e tratamento para um tipo específico de ataque DDoS, como também uma arquitetura para a plataforma computacional, a qual é composta por três módulos: módulo de coleta de tráfego, módulo de análise e módulo de bloqueio e prevenção. Nos experimentos realizados com um essa ferramenta, o tempo médio para a identificação e bloqueio dos ataques DDoS foi de 40 segundos.

A ideia agora é aprofundar a modelagem dos ataques DDoS usando outras abordagens, como modelagem do perfil de tráfego dos ataques e validação usando métodos formais. Nós já começamos a desenvolver modelos formais para a análise de defesas contra ataques DDoS [2, 3]. Nossos experimentos iniciais são muito promissores. Nós propusemos uma metodologia para a configuração de defesas contra ataques DDoS e sua validação formal usando métodos formais. Nós demonstramos que nossas defesas conseguem manter um nível alto de disponibilidade apesar da presença de um número grande de atacantes. Nós também fizemos uma trabalho para avaliar se é possível dectetar ataques DDoS tradicionais (TCP ou UDP *SYN flooding*) utilizando apenas ferramentas comuns disponíveis para os administradores de redes [4].

Além das atividades de gerencia de projeto descritas na Seção 7 ("Produtos e Relatórios a serem entregues") do edital GT-RNP 2014-2015, o cronograma de execução do GT-ACTIONS é baseado nas seguintes etapas principais:

E1. Mapeamento de algoritmos/técnicas de identificação e tratamento de ataques DDoS, incluindo a pesquisa bibliográfica complementar dos temas a serem abordados;

E2. Modelagem do perfil do tráfego de ataques DDoS e implementação dos novos algoritmos/técnicas para identificação e tratamento;

E3. Validação formal e avaliação de técnicas e modelos propostos, usando ferramentas computacionais automatizadas também usadas para a verificação de protocolos de segurança [21], [22] e de ataques DDoS [2, 3, 24, 25];

E4. Modelagem e implementação da plataforma computacional ACTIONS e integração com os algoritmos desenvolvidos;

E5. Realização de testes experimentais e aprimoramento dos algoritmos/técnicas desenvolvidos;

E6. Elaboração do relatório final do projeto.

Para executar as etapas descritas, pretende-se seguir o cronograma descrito na Tabela 1, a qual também mostra a participação das instituições parceiras em cada etapa.

Etapas / Executores	Q1	Q2	Q3	Q4	Q5	Q6
E1 / Todos	✓					
E2 / UFABC, UFES, UFPB	✓	✓	✓			
E3 / UFPB, IFPB, UFES		✓	✓	✓	✓	✓
E4 / UFPB, UFES, IFPB		✓	✓	✓		
E5 / Todos				✓	✓	✓
E6 / Todos						✓

Tabela 1: Cronograma do projeto. Cada variável em Q1, . . . ,Q6 corresponde a um período consecutivo de dois meses, totalizando portanto 12 meses.

Aproveitando a vasta experiência em modelagem de tráfego em redes de comunicação, os grupos da UFABC e UFES, liderados pelos Profs. Hélio Waldman e Moisés R. N. Ribeiro, participarão da modelagem do tráfego dos ataques DDoS e no desenvolvimento/aprimoramento dos novos algoritmos e técnicas, bem como na realização dos experimentos na rede e concepção do ACTIONS. O grupo do IFPB participará da implementação dos algoritmos e execução dos testes experimentais, enquanto que o da UFPB contribuirá com todas as etapas, incluindo a parte da verificação formal dos modelos e algoritmos, a qual será capitaneada pelo Prof. Vivek Nigam.

8 Ambiente para testes do protótipo

Identificar e tratar ataques de negação de serviço de origem externa que tem como alvo a Rede Ipê é a maneira mais natural de se pensar em segurança da informação e da rede. Entretanto, é necessário entender que o risco de se utilizar equipamentos distribuídos que compõem a própria Rede Ipê para a realização dos testes é muito grande. Isto acontece devido ao impacto que poderá ser causado pela dimensão da rede. Portanto, o protótipo será testado em cenários de rede seguros e planejados para tal fim. O cuidado também é importante para se evitar que usuários não autorizados possam ter acesso ao ambiente de testes. Casos nos quais foi utilizada a infraestrutura da Rede Ipê para ataques de negação de serviço foram discutidos no GTER 33/GTS 19, que aconteceu em Maio de 2012 na cidade de Natal/RN.

São propostos para a execução dos experimentos dois cenários distintos. No primeiro cenário, frações da rede (Slices) da RNP serão utilizadas para realizar o experimento no ambiente PLANETLAB, de maneira que deve ser possível identificar e tratar ataques de negação de serviço que são direcionados aos equipamentos da RNP, bem como os ataques que são originados na própria rede da RNP. Neste caso, a ideia é utilizar ferramentas geradoras de tráfego malicioso que possuem sua origem fora e dentro da rede da RNP, possibilitando tratar ataques internos e externos à Rede Ipê.

No segundo cenário, os experimentos serão realizados num ambiente interligando as instituições participantes do GT-ACTIONS. Neste caso, será utilizada a infraestrutura existente da Rede Ipê, que interliga as instituições participantes, na qual também deve ser possível criar mecanismos de identificação e tratamento de ataques de negação de serviço que são direcionados aos equipamentos da RNP, bem como os ataques que são originados na própria Rede Ipê. Como no cenário anterior, deve-se utilizar ferramentas geradoras de tráfego malicioso que possuem sua origem fora e dentro da Rede Ipê, possibilitando tratar ataques com origem fora e dentro da própria rede.

Referências

[1] Leandro C. Almeida, "Ferramenta Computacional para Identificação e Bloqueio de Ataques de Negação de Serviço em Aplicações Web", dissertação de mestrado, PPGI/UFPB, Julho 2013.

[2] Yuri G. Dantas, Vivek Nigam, and Iguatemi E. Fonseca, "A Selective Defense for Application Layer DDoS Attacks", aceito no *IEEE International Conference on Intelligence and Security Informatics 2014 - IEEE ISI 2014*.

[3] Yuri G. Dantas, Vivek Nigam, Iguatemi E. Fonseca, and Pedro V. V. P. Clis, "Formal Specification and Verification of a Selective Defense for VoIP DDoS Attacks", submetido no *Simpósio Brasileiro de Métodos Formais 2014 - SBMF 2014*.

[4] Diego V. Queiroz, Jânio C. M. Vieira; Iguatemi E. FONSECA, "Detecção de Ataques de Negação de Serviço Utilizando Ferramentas de Monitoramento e Análise de Tráfego", *Revista de Tecnologia da Informação e Comunicação*, v. 4, p. 28-35, 2014.

[5] L. Dave, Global Internet slow after "biggest attack in history". http://www.bbc.co.uk/news/technology-21954636. Acessado em 30 de Março de 2013.

[6] T. Socolofsky; C. Kale. A TCP/IP Tutorial - RFC 1180. http://tools.ietf.org/html/rfc1180. Acessado em 30 de Março de 2013.

[7] Y. Xie; S. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites", *IEEE/ACM Transactions on Networking*, Vol. 17, No 1, February 2009.

[8] L. Wei-Zhou, Y. Shun-Zheng, "An HTTP Flooding Detection Method Based on Browser Behavior", *International Conference on Computational Intelligence and Security*, 2006.

[9] T. Yatagai, T. Isohara, I. Sasase, "Detection of HTTP-GET Flood Attack Based on Analysis of Page Access Behavior Communications", *IEEE Pacific Rim Conference on Computers and Signal Processing*, 2007.

[10] Y. Li, T. Lu, L. Guo, Z. Tian, Q. Nie, "Towards Lightweight and Efficient DDoS Attacks Detection for Web Server", *18th International World Wide Web Conference*, 2009.

[11] T. Berners Lee, P. Leach, L. Masinter, J. Mogul, R. Fielding, "HyperText Transfer Protocol - HTTP 1.1", June 1999.

[12] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations", RFC 4987, Network Working Group, August 2007.

[13] H. Beitollahi; G. Deconinck, "Analyzing well-know countermeasures against distributed denial of service attacks", *Elsevier Computer Communications*, vol. 35, pp. 1312-1332, June 2012.

[14] CNN, "DDoS Attacks on Yahho, Buy.com, eBay, Amazon, Datek, E Trade", CNN Headline News, 2000.

[15] P. Arun, S. Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptative and hybrid neuro-fuzzy systems", *Elsevier Computer Communications*, vol. 36, pp. 303-319, February 2013.

[16] Trustwave, "Web Hijacking Incident Database (WHID) Semianual Report", January 2011.

[17] P. Arun Raj Kumar, S. Selvakumar, "Mathematical modeling of DDoS Attack and defense - A survey", *3rd International Conference on Computer Modeling and Simulation*, 2011.

[18] Orbit - http://www.orbitdownloader.com/br, acessado em 24/04/2013.

[19] Flashget - http://www.flashget.com, acessado em 24/04/2013.

[20] Free Download Manager - http://www.freedownloadmanager.org acessado em 24/04/2013.

[21] G. Lowe, "Breaking and fixing the Needham-Schroeder public-key protocol using FDR", *TACAS*, 1996.

[22] I. Cervesato, A. D. Jaggard, A. Scedrov, J. Tsay, and C. Walstad, "Breaking and fixing public-key kerberos", *ACM Journal Information and Computation*, vol. 206, pp. 402-424, February 2008.

[23] A, Wang, L. Jia, W. Zhou, Y. Ren, B. Loo, J. Rexford, V. Nigam, A. Scedrov, and C. Talcott, "Fsr: Formal analysis and implementation toolkit for safe inter-domain routing", *IEEE/ACM Transactions on Networking*, vol. 20, pp. 1814-1827, 2012.

[24] R. Shankesi, M. AlTurki, R, Sasse, C. Gunter, and J. Meseguer, "Model-checking dos amplification for voip session initiation", *European Symposium on Research in Computer Security*, 2009.

[25] C. Meadows, "A formal framework and evaluation method for network denial of service", *12th IEEE workshop on Computer Security Foundations*, 1999.

[26] Saman Taghavi Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys and Tutorials*, 15(4):2046–2069, 2013.