P4Sec
Securing Networks in the Programmable Data Plane Era

EQUIPE

Coordenador no Brasil:
Marinho Barcellos (UFRGS)

Coordenador nos Estados Unidos:
Kirill Levchenko (UCSD)

Parceiros brasileiros:
Universidade Federal do Rio Grande do Sul (UFRGS)
Universidade de Brasília (UnB)
Universidade Federal de Pernambuco (UFPE)

Parceiros
University of California San Diego (UCSD)
University of Texas A&M (UTAM)

SITE
http://www.inf.ufrgs.br/p4sec

CONTATO
marinho@inf.ufrgs.br

DESCRIÇÃO

Os avanços recentes em Redes Definidas por Software (*Software Defined Networking*, SDN) expandiram nossa capacidade de programar a rede em direção ao plano de dados. Por meio de linguagens específicas de domínio como o P4, os operadores de rede podem rapidamente implementar novos protocolos em dispositivos de encaminhamento, personalizar suas funcionalidades e desenvolver serviços inovadores. Essa flexibilidade vem, no entanto, com um custo: as propriedades de segurança e de corretude em toda a rede (por exemplo, isolamento, acessibilidade, etc.) tornam-se muito mais difíceis de garantir, porque o comportamento da rede agora é determinado por uma combinação da configuração mantida pelo plano de controle e os programas do plano de dados que reside nos dispositivos (também chamados de *switches*). As ferramentas existentes para verificação de redes, que dependem de um modelo fixo e invariante do plano de dados, são inadequadas para planos de dados programáveis.

O projeto tem dois objetivos principais. Primeiro, desenvolver novas técnicas para **verificar e impor propriedades de segurança** em planos de dados programáveis. As técnicas de verificação a serem propostas ampliam as ferramentas de verificação existentes, gerando automaticamente um modelo de plano de dados a partir de um programa P4. Em seguida, as ferramentas de verificação existentes são adaptadas para trabalhar com os modelos gerados dinamicamente para verificar as atualizações de configuração de rede emitidas por um controlador SDN. Também se propõe uma nova abordagem para garantir que as propriedades de segurança de rede sejam satisfeitas por uma configuração de rede baseada na imposição (*enforcement*) em nível de plano de dados. Propõe-se desenvolver um monitor, implementado no próprio plano de dados, que impõe propriedades de segurança críticas, como isolamento e limites de largura de banda, mesmo na presença de um programa ou controlador de plano de dados de usuário com defeito ou malicioso.

O segundo objetivo diz respeito a **novos serviços de segurança de planos de dados** viabilizados por redes de planos de dados programáveis. Propõe-se desenvolver novas funções e técnicas de segurança baseadas em planos de dados para compô-las de forma a equilibrar as características de desempenho do plano de dados (muito rápido, mas de baixa complexidade) e unidades de função de rede virtualizadas dedicadas conectadas à rede (mais lentas, mas sofisticadas) para implementar a função de segurança necessária.

P4Sec: Protegendo Redes na Era do Plano de Dados Programáveis

O projeto **P4Sec** investiga tecnologias de segurança para redes com planos de dados programáveis, com foco nas redes baseadas na linguagem P4. O projeto está organizado em quatro eixos principais, conforme abaixo.

Propriedades de segurança de rede. Políticas de segurança podem ser usadas para definir o fluxo de informação entre hospedeiros. Propõe-se desenvolver um idioma específico de domínio simples para expressar essas políticas, que será utilizado por um operador para especificar (a) como identificar as entidades principais e (b) quais políticas de segurança devem ser aplicadas às mesmas.

Verificação. Propõe-se desenvolver técnicas para verificar os tipos de propriedades de segurança discutidas no âmbito de planos de dados programáveis, incluindo uma ferramenta para transformar automaticamente um programa P4 em um conjunto de asserções de solver SMT (*satisfiability modulo theories*).

Imposição (*enforcement*). Alternativa à verificação, propõe-se desenvolver um núcleo que garanta que as ações tomadas pelos programas de planos de dados sejam consistentes com a política de segurança declarada. Propõe-se ainda generalizar esse mecanismo para permitir que um programa de supervisor arbitrário seja combinado, em tempo de compilação, com um programa de usuário arbitrário. O núcleo e o mecanismo podem proteger a rede contra programas e controladores de plano de dados defeituosos ou maliciosos.

Novos serviços de segurança do plano de dados. Propõe-se implementar novos serviços de segurança no plano de dados programável, que é uma ordem de grandeza mais rápida do que o plano de controle e não requer o tráfego de direção para dispositivos dedicados. Três iniciativas estão sendo exploradas: adicionar proteção de segurança e primitivas de ação no plano de dados programável; programação de funções de segurança baseadas em plano de dados; composição de serviços de segurança consistentes.

Impacto. Planos de dados programáveis em dispositivos de encaminhamento SDN são uma mudança de paradigma muito recente no panorama das tecnologias de rede. Esperamos avançar substancialmente o conhecimento no campo da segurança para redes com dispositivos programáveis de plano de dados, projetando, desenvolvendo e avaliando os mecanismos de segurança correspondentes.

Resultados parciais.

L. Freire, M. Neves, L. Leal, K. Levchenko, A. Schaeffer-Filho, M. Barcellos. Uncovering Bugs in P4 Programs with Assertion-based Verification. 4th Symposium on SDN Research (**ACM SOSR 2018**), Los Angeles, p1-8., 2018

W. L. da C. Cordeiro, J. Marques, L. P. Gaspary. Data Plane Programmability Beyond OpenFlow: Opportunities and Challenges for Network and Service Operations and Management. Journal of Network and Systems Management (**Springer JNSM**): 1-35. 2017

M, Neves, K. Levchenko, M. Barcellos. Sandboxing Data Plane Programs for Fun and Profit. In Proceedings of the SIGCOMM Posters and Demos (**ACM SIGCOMM 2017**). ACM, New York, NY, USA, 103-104. 2017

L. Freire, M. Neves, A. Schaeffer-Filho, M. Barcellos. 2017. Finding Vulnerabilities in P4 Programs with Assertion-based Verification. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (**ACM CCS 2017**). ACM, New York, NY, USA, 2495-2497. 2017

Consórcio: