CISION

SÁBADO

Meio: Imprensa
País: Portugal
Área: 910,8cm²
Âmbito: Interesse Geral
Period.: Semanal
Pág: 16-17

ID: 106614314 10-08-2023

C-STUDIO

Projeto de Doutoramento com reconhecimento e validação por um júri multidisciplinar

Uma abordagem inovadora para fazer face ao atual cenário de prevalência de riscos de cibersegurança que complementa as abordagens mais tradicionais. Este projeto de doutoramento foi o vencedor da edição do ano passado do Altice International Innovation Award.

Vítor Cunha, aluno do Programa Doutoral em Engenharia Informática, no DETI-UA, submeteu a tese de doutoramento ao Altice International Innovation Award (AIIA), na categoria Academia, e venceu a edição do ano passado com o projeto Defesa Dinâmica para Redes Softwarizadas e Virtualizadas. Falámos com o investigador do Instituto de Telecomunicações de Aveiro para perceber a inovação apresentada neste trabalho e a importância de participar e vencer a categoria Academia do AIIA. Um reconhecimento para lá dos pares da academia, e a validação prática de um júri multinacional de vários quadrantes da sociedade.

Como chegou ao conceito do projeto Defesa Dinâmica para Redes Softwarizadas e Virtualizadas?

A ideia surgiu em forma muito inicial antes de me inscrever no doutoramento, quando ainda trabalhava no desenvolvimento de funções de rede para descarregar tráfego para computação na borda (do inglês *offloading* para edge *computing*) e assim libertar recursos na rede nuclear do operador. Estas funções exigem enorme flexibilidade na seleção de fluxos ativos na rede e depois elevada performance no movimento dos fluxos selecionados para outros pontos de presença. Como é procedimento em qualquer programa doutoral, conduzi uma análise exaustiva do estado da arte que descrevia as soluções de defesa já existentes no âmbito da componente de pré-tese, que é desenvolvida no primeiro ano do doutoramento e visa o estabelecimento de um plano para o trabalho vindouro, e identificaram-se as lacunas que ainda impediam a transposição das abordagens similares do meio académico para o uso em ambientes mais realistas. Foi aí que a experiência no desenvolvimento de funções de *offloading* de tráfego se manifestou, e a ideia original começou a ganhar forma, surgindo assim a "Defesa Dinâmica para Redes Softwarizadas e Virtualizadas". "Defesa Dinâmica" porque esta solução permite o uso de diferentes técnicas e alteráveis consoante a necessidade do momento.

Como testaram a aplicabilidade da Defesa Dinâmica para Redes Softwarizadas e Virtualizadas?

Na prova de conceito já contemplamos técnicas como a defesa dando mobilidade ao alvo - do inglês *Moving Target Defense* (MTD) – e de redes de contenção de segurança – ou *honeynets*. Estas defesas podem ser introduzidas a qualquer momento, mesmo que a função a proteger anteriormente não tivesse qualquer defesa do género, enfatizando assim o aspeto dinâmico. Já a parte de ser para redes "Softwarizadas e Virtualizadas" surge parcialmente como uma necessidade técnica para algumas das estratégias de defesa, mas é principalmente para não prescrever nenhuma rede ou fabricante em particular e poder ser uma aposta para um futuro de longo prazo que permita a adoção mais além das tecnologias atuais (atualmente o core 5G já é softwarizado e virtualizado, mas a inovação viverá além do 5G).

Quais os principais desafios enfrentados na implementação de uma defesa dinâmica para redes software-defined e virtualizadas?

Há vários desafios de monta a ser considerados. Primeiro, os utilizadores legítimos não podem ser privados do acesso aos serviços protegidos, nem a sua experiência de utilização deve ser degradada. Isto é particularmente desafiante porque se o acesso aos serviços se move rapidamente ao longo de um espaço de exploração – que, já agora, é o princípio-base do MTD e que dificulta a realização de ataques bem-sucedidos –, os utilizadores legítimos têm de continuar a acertar no alvo, isto é, no serviço, de forma constante e certeira. É necessária uma elevada sincronização entre o utilizador e o serviço para que o acerto no alvo aconteça, mas introduzir um protocolo de rede para esta sincronização iria ele próprio contribuir como uma sobrecarga ao próprio sistema e criar, por si só, mais uma superfície de ataque. Por outro lado, apesar de toda a variabilidade causada pelo movimento, o sistema tem de permanecer

CISION
SÁBADO
Meio: Imprensa
País: Portugal
Área: 910,8cm²
Âmbito: Interesse Geral
Period.: Semanal
Pág: 16-17
ID: 106614314
10-08-2023

Em parceria com a Altice International Innovation Award

Vítor Cunha, venceu a edição de 2022 do Altice International Innovation Award, na categoria Academia

auditável na eventualidade de ocorrer uma falha, e ver a sua manutenção fácil de ser gerida. Em suma, o grande desafio é que queremos frustrar os esforços de atacantes que podem ser sofisticados, mas não frustrar os gestores dos sistemas, nem muito menos os utilizadores legítimos.

Quais os resultados alcançados com o projeto?

Os resultados mostraram que o sistema era, por si só, bastante eficaz a detetar ações adversárias nos cenários considerados (acima de 99,9% de deteção) e sem grandes penalizações nos parâmetros que afetavam a funcionalidade (latência e largura de banda). Contudo, os cenários considerados eram em redes privadas nos quais os utilizadores autorizados eram previamente conhecidos, e dada a criticidade das funções protegidas o custo de implantação do sistema não era um problema. As soluções tradicionais também teriam números impressionantes de sucesso contra os ataques conhecidos (provavelmente até com mais noves após a vírgula), a vantagem da nossa abordagem é manter a eficácia mesmo contra os ataques desconhecidos (*zero-days*).

Que lições aprenderam durante o processo?

As principais lições aprendidas remetem-se à necessidade de processar os alarmes de forma conveniente para evitar falsos positivos (eventos normais classificados como ataques). Contudo, sempre que se tenta eliminar os falsos positivos, incorre-se no risco de criar falsos negativos, isto é, deixar passar ataques como eventos normais. Aquilo que a nossa solução faz é, quando ocorre um falso negativo, barra na mesma o tráfego, apenas não se identificando o mesmo como um ataque. Quando se detetam muitos falsos positivos, criam-se eventos que sinalizam a necessidade de averiguar a sincronização com o cliente e/ou qualidade da rede. Apesar dos números impressionantes, a abordagem está longe de ser infalível, e é recomendado usar sempre em conjunto com defesas tradicionais sem nunca esquecer as boas práticas de segurança e desenho de sistemas.

Como decidiu concorrer ao prémio Academia do Altice Innovation Award?

Confesso que, mais do que tudo, fui encorajado pelos meus orientadores, os professores João Paulo Barraca e Daniel Corujo. Encontrava-me numa fase em que aguardava pelas provas finais da defesa do doutoramento, e naquele contexto fazia todo o sentido concorrer ao prémio Academia do Altice Innovation Award. Agradeço, obviamente, ao professor Daniel Corujo por todo o apoio nesta candidatura e aos meus colegas no Instituto de Telecomunicações (Mário Antunes, que foi um dos finalistas de uma edição anterior do Altice International Innovation Award, e José Quevedo) pela ajuda e clarividência em todo este processo.

Qual a importância de ser reconhecido por este prémio?

O simples facto de ser selecionado para a fase final de um concurso de inovação internacional e tão concorrido como o Altice International Innovation Award já é uma forma excelente de validar para lá da academia a qualidade do trabalho construído ao longo do doutoramento, e o seu potencial contributo para a sociedade. Este é o aspeto-chave e de extrema importância para qualquer académico, reconhecimento para lá dos pares da academia, teoria posta em prática validada por um júri multinacional de vários quadrantes da sociedade.

Este projeto científico tem hoje continuidade no âmbito de um outro projeto europeu dedicado a privacidade e cibersegurança, no qual já abordamos outras soluções de segurança, *Moving Target Defense* (MTD) e a sua integração com inteligência artificial no contexto das futuras redes 6G.

Quais os motivos pelos quais os alunos de doutoramento se devem candidatar ao prémio AIIA na categoria Academia?

Sem dúvida pelo reconhecimento para lá dos pares da academia, contribuição e impacto além das muralhas dos nossos laboratórios, avaliado por um júri de vários quadrantes da sociedade (que tem vindo a incluir a principal agência de inovação em Portugal, a ANI). Adicionalmente, terão a oportunidade de discutir novas e revolucionárias ideias com os finalistas e convidados da cerimónia. Este prémio internacional da Altice, por ser um grupo com reconhecida dimensão internacional nas áreas de inovação, mas que mantém uma forte ligação a Portugal, permite o melhor dos dois mundos, participar num concurso internacional em que todos os procedimentos de participação podem ser feitos sem ter de sair de Portugal. Para além disso, a submissão para consideração é gratuita, o que remove barreiras monetárias no caminho para o reconhecimento do mérito do nosso trabalho.

Que conselhos deixaria aos concorrentes da categoria Academia desta edição?

Foquem-se no essencial, aquilo que tem maior impacto para a sociedade e um suporte mais sólido para ser transformado num modelo de negócio. Descrevam muito bem como funcionaria esse modelo de negócio. Acima de tudo sejam honestos com aquilo que o trabalho faz (ou não faz) e, apesar de o concurso ser fora da academia, isso não é desculpa para esquecer as boas práticas científicas de suportar as afirmações com evidências.