Autenticação e Controle de Acesso na Arquitetura ETArch

Pedro H. A. Damaso Melo[1], **Flávio de O. Silva**[1], **Pedro F. Rosa**[1]

[1]Faculdade de Computação (FACOM)
Universidade Federal de Uberlândia (UFU) – Uberlândia, MG – Brasil

{pedro.damaso,flavio, pfrosi}@ufu.br

Resumo. *Apesar das evoluções, a Internet atual não consegue tratar adequadamente requisitos como* multihoming*, QoS, mobilidade,* multicast *e segurança. Vários grupos de pesquisa ao redor mundo estão envolvidos em criar, de forma experimental e incremental, a próxima geração da arquitetura da Internet. Uma inciativa brasileira nessa área é a* Entity Title Architecture *(ETArch) cujo protótipo é baseado no conceito de* Software Defined Networking *e utiliza o protocolo OpenFlow. Este trabalho apresenta duas contribuições implementadas na ETArch, sendo um mecanismo de autenticação e um de controle de acesso, cujas análises de custo-benefício são apresentadas neste artigo.*

Abstract. *Despite of evolutions, the current Internet can not adequately handle requirements such as multihoming, QoS, mobility, multicast and security. Several research groups around the world are involved in creating, experimentally and incrementally, the next generation of Internet architecture. A Brazilian initiative in this area is the Entity Title Architecture (ETArch) whose prototype is based on the concept of Software Defined Networking and uses the OpenFlow protocol. This work presents two contributions implemented in ETArch, being an authentication mechanism and an access control, whose trade-off is presented in this work.*

1. Introdução

Os avanços tecnológicos tanto em hardware quanto em software, as novas tecnologias de acesso em banda larga e as redes de telecomunicações móveis propiciaram o surgimento de novos serviços e aplicações que seriam difíceis de se imaginar nos anos setenta quando os protocolos da internet foram especificados. Mesmo com evoluções, a Internet atual não consegue tratar adequadamente requisitos como *multihoming*, QoS, mobilidade, *multicast* e segurança [Handley 2006]. Vários grupos de pesquisa ao redor mundo estão envolvidos em criar a próxima geração da arquitetura de Internet [Pan et al. 2011].

No que tange às novas arquiteturas, o Brasil possui algumas iniciativas, sendo uma delas a *Entity Title Architecture* (ETArch) [Guimaraes et al. 2014]. Ela possui uma visão conceitual muito próxima da abstração proposta pelas Redes Definidas por Software e, portanto, desde o seu primeiro protótipo utiliza o protocolo OpenFlow para materializar essa visão. Desde a sua criação, pesquisadores de várias universidades vêm trabalhando para incorporar à ETArch, de forma incremental, soluções que visam atender os requisitos de Internet do Futuro.

Na ETArch o endereçamento e a identificação são baseados em uma designação independente da topologia que identifica de forma única uma entidade, chamada Título.

A comunicação entre múltiplas entidades ocorre através de barramento lógico, chamado *Workspace*.

Um componente central da ETArch é o *Domain Title Service* (DTS) que representa o plano de controle da rede. O DTS é composto de *Domain Title Service Agents* (DTSAs) que mantém informações sobre as entidades registradas no domínio e os *Workspaces* em que as mesmas estão anexadas. O DTSA é responsável por configurar os elementos de rede para permitir as entidades associadas a um dado *Workspace* possam participar da comunicação.

Apesar dos diversos incrementos projetados, implementados e agregados à ETArch, nenhum deles se relaciona aos aspectos da segurança. Sendo assim, as principais contribuições deste trabalho são elaborar e implementar dois mecanismos: um para autenticação; e outro para o controle de acesso ao ambiente de comunicação oferecido pela ETArch.

Para validar os mecanismos de autenticação e controle de acesso, foi realizada uma avaliação experimental, que objetiva demonstrar os benefícios dos mecanismos criados para a arquitetura. O cenário de testes apresentado demonstra a viabilidade e a importância deste trabalho.

Este trabalho está organizado da seguinte forma: A Seção 2 apresenta a visão geral dos mecanismos de segurança. A Seção 3 descreve o cenário utilizado para avaliação experimental e apresenta os resultados obtidos. Finalmente, a Seção 4 apresenta as conclusões e trabalhos futuros.

2. Proposta

O surgimento de SDN na área de redes de computadores modifica a maneira como alguns aspectos da comunicação de dados podem ser tratados. O SDN impõe que alguns aspectos relacionados à segurança seja tratado no plano de controle, por exemplo, no momento em que uma entidade solicita o seu registro na arquitetura ETArch. O presente trabalho objetiva demonstrar experimentalmente o uso do plano de controle para fornecer mecanismos de autenticação e controle de acesso.

Na arquitetura ETArch, a autenticação de uma entidade é realizada no momento em que a entidade se registra na rede e o controle de acesso é realizado no momento em que uma entidade tenta se conectar a um *Workspace*, ou seja, quando deseja participar de um domínio de comunicação.

O mecanismo de autenticação foi desenvolvido tendo como ponto de partida a recomendação X.811 [UNION 1995a], porém considerando a filosofia do paradigma SDN e as particularidades da arquitetura. Na ETArch, o conceito de entidade é genérico e pode ser entendido como tudo que possui capacidade de se comunicar, sendo assim, a autenticação é tratada de uma forma onde é possível adaptar-se a diversos cenários. Por exemplo, esse mecanismo precisa autenticar aplicações, elementos de rede, sensores, *smartphones*, usuários, entre outros.

O controle de acesso se baseou na recomendação X.812 [UNION 1995b], e é aplicado ao plano de controle da arquitetura ETArch para verificar quais entidades possuem privilégio para fazer parte de determinado *Workspace*. A *Access Control Enforcement Function* (AEF) é uma função especializada que faz parte do caminho de acesso entre as

entidades e um *Workspace* em cada solicitação de acesso e reforça a decisão tomada pela *Access Control Decision Function* (ADF).

3. Avaliação Experimental e Análise de Resultados

Nesta seção são avaliados os mecanismos de autenticação e controle de acesso propostos tendo-se como cenário uma aplicação de $chat$. Inicialmente descreve-se o cenário usado na prova de conceito e, posteriormente, uma análise dos resultados obtidos.

3.1. Cenário Experimental

Para o DTSA foi utilizado um computador com o sistema operacional Ubuntu 16.04.1 LTS, com o processador Intel(R) Core(TM) i5-2430M CPU @ 2.40GHz e 6 GB de memória RAM. Foi utilizado o Mininet para simular uma topologia de rede usando uma maquina virtual com sistema operacional Ubuntu 14.04 LTS com 512MB de memória RAM. Foi criada uma topologia com *OpenFlow Switches* representados pelo conjunto $\{$s1, s2, s3, s4, s5, s6$\}$ e 15 hosts $\{$h1, h2, h3, h4, h5, h6, h7, h8, h9, h10, h11, h12, h13, h14, h15$\}$.

Para o teste, foi utilizado uma aplicação de $chat$, onde foi criado um *Workspace* chamado $W1$ e os *hosts* representados na topologia se conectaram a esse $W1$, sendo assim, foi medido o tempo que os *hosts* levaram para realizar o seu registro no ETArch (primitiva *Entity Register*) e o tempo para realizar o *Workspace Attach*, ou seja, para conectar-se ao *Workspace*. Cada experimento, envolvendo toda a topologia, foi executado 10 vezes.

3.2. Resultados Obtidos

Antes dessa implementação a ETArch não dispunha de mecanismo de segurança, o que pode causar diversos problemas, sendo que após essa proposta é possível realizar a autenticação e o controle de acesso de entidades na arquitetura ETArch. Para os testes foram utilizados certificados digitais próprios para cada *host*.

A Figura 1 apresenta dois gráficos: à esquerda, os tempos auferidos para o serviço de autenticação *Entity Register*; à direita, os tempos do serviço de controle de acesso *Workspace Attach*, considerando dois cenários, com (azul) e sem (vermelho) o uso dos mecanismos de segurança. No *Entity Register*, o tempo médio com segurança foi de 28.08 ± 2.67 ms enquanto que o tempo médio sem segurança foi de 17.64 ± 4.05 ms. Isso representa um acréscimo médio de 10.45ms no cenário com segurança. Para o *Workspace Attach*, o tempo médio foi de $28.47 \pm 6.33ms$ e $19.10 \pm 4.1ms$ nos cenários com e sem segurança respectivamente, indicando um acréscimo médio de 9.37 ms. Os valores médios são mostrados com um intervalo de confiança de 95% utilizando uma distribuição T-Student.

O acréscimo médio é comparativamente pequeno em termos de tempo se se considerar os benefícios dos mecanismos de autenticação e controle de acesso incorporados à ETArch.

4. Conclusões e Trabalhos Futuros

Neste trabalho foi apresentada a inclusão de mecanismos na arquitetura ETArch com o objetivo de realizar a autenticação e o controle de acesso de entidades no plano de controle. O trabalho mostrou o custo-benefício dos mecanismos acrescentados. Apesar do

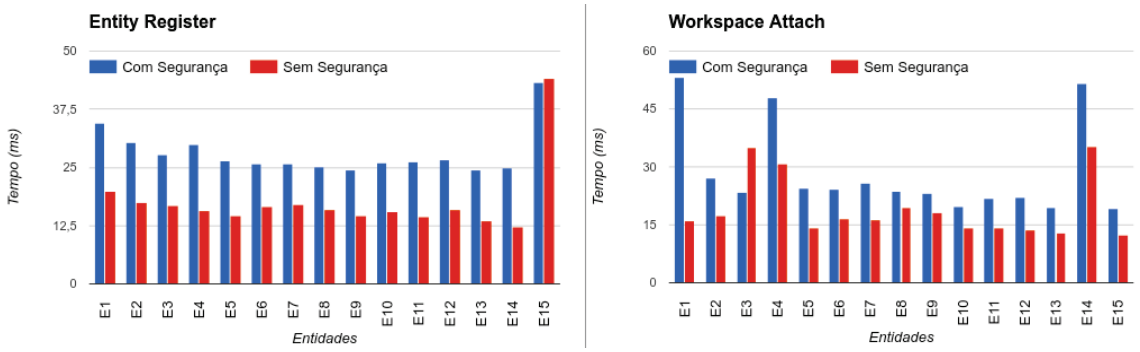

Figura 1. Avaliação Comparativa para o *Entity Register* e o *Workspace Attach*

acréscimo médio de tempo ser de 10.45ms para o *Entity Register* e 9.37ms no *Workspace Attach* há um ganho indiscutível em relação à segurança com os mecanismos de autenticação e autorização desenvolvidos.

Aspectos tais como detecção de intrusos e confidencialidade serão tratados pela arquitetura futuramente. Considerando que os DTSAs (agentes do plano de controle) mantêm uma relação de confiança, então esse processo é realizado uma vez. Em caso de mobilidade, por exemplo, quando a entidade troca de localidade, esse outro DTSA se encarregará de obter essas informações de acesso no DTSA de origem, onde foi feito o registro da entidade.

5. Agradecimento

Esse trabalho foi financiado pela CAPES atraves do Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Defesa Nacional (Pró-Defesa).

Referências

[Guimaraes et al. 2014] Guimaraes, C., Corujo, D., Silva, F., Frosi, P., Neto, A., and Aguiar, R. (2014). IEEE 802.21-enabled Entity Title Architecture for handover optimization. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2671–2676.

[Handley 2006] Handley, M. (2006). Why the Internet Only Just Works. *BT Technology Journal*, 24(3):119–129.

[Pan et al. 2011] Pan, J., Paul, S., and Jain, R. (2011). A survey of the research on future internet architectures. *IEEE Communications Magazine*, 49(7):26–36.

[UNION 1995a] UNION, I. T. (1995a). X.811:Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework.

[UNION 1995b] UNION, I. T. (1995b). X.812:Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework.