GT-COFEE
Protocolo de Autenticação Federada para IoT

Marco Aurélio Amaral Henriques
Coordenador Associado do GT
UFMG/Unicamp

19º WRNP
Workshop RNP
7 | 8 MAIO
Campos do Jordão | SP

RNP

1. O que é o produto desenvolvido e quem são os usuários alvo?

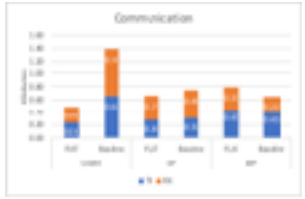
Protocolo de Autenticação Federada para Internet das Coisas (IoT)

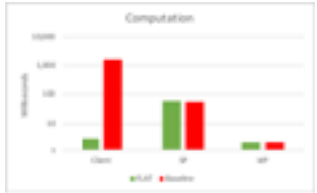
- Produto:
  - Prova de conceito de novo protocolo de autenticação federada leve, voltado para dispositivos de baixo custo com restrições de memória e de processamento.
    - Uso mais intensivo de criptografia simétrica e adoção de técnicas mais eficientes de criptografia assimétrica permitiram reduções muito significativas de tempo e de espaço em comparação com protocolo tradicional.
- Usuários alvo
  - Todas as instituições de ensino e pesquisa que necessitem futuramente disponibilizar serviços federados para dispositivos em redes IoT.
    - Dispositivos de uma instituição poderão se autenticar e ter acesso de forma transparente a serviços disponibilizados por outras instituições.

2. Qual é o principal resultado tecnológico alcançado na fase atual?

Um protocolo de autenticação federada leve o suficiente para satisfazer os requisitos de eficiência e economia de recursos de dispositivos IoT

- Dispositivos clientes dos serviços (mais restritos)
  - Utilizam apenas criptografia simétrica (chave única ou secreta), evitando os elevados custos impostos por certificação digital e outras técnicas presentes em infraestruturas de chaves públicas tradicionais.
- Dispositivos provedores de serviços e provedores de identidade (menos restritos)
  - Utilizam criptografia simétrica (chave única ou secreta) e assimétrica (chave pública).
  - Na criptografia de chave pública, adotam técnicas de certificação implícita, mais leves e econômicas que as tradicionalmente usadas em infraestruturas de chaves públicas e certificados digitais.
- Resultados
  - Reduções significativas em relação a um protocolo tradicional baseado totalmente em infraestrutura de chaves públicas e certificação digital.
    - Dados trafegados: redução de 31%
    - Tempo de processamento: redução de 96%

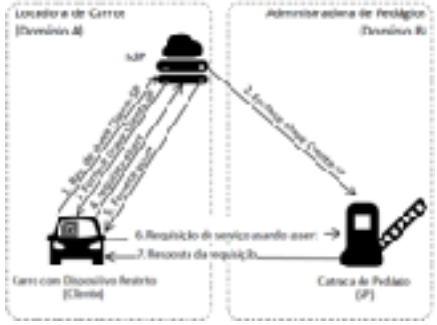




3. Qual é a inovação que os resultados potencializam?

Uso federado de serviços voltados para dispositivos de mais baixo custo em redes IoT.

- Novos serviços disponibilizados pelas instituições de ensino e pesquisa poderão se tornar acessíveis em nível federado também por dispositivos mais restritos e/ou de mais baixo custo.
  - Equipamentos de uma instituição que necessitam de serviços na rede, poderão ter acesso a tais serviços mesmo em instituições diferentes da sua sem alterações em suas configurações e/ou credenciais.
  - Exs:
    - Controle de acesso automatizado nos estacionamentos de universidades para veículos visitantes de outras instituições.
    - Autenticação mais leve e rápida para smartcards, agilizando o controle de acesso.
    - Autenticação de drones que voam sobre um domínio externo ao seu original a fim de controlá-lo e/ou extrair dados do mesmo.
    - Autenticação de equipamentos médicos implantados no corpo de alguém para controlá-lo ou extrair dados do mesmo em um domínio (hospital) diferente daquele onde ocorreu a implantação.



4. Qual a sua visão para a sustentabilidade dos resultados no curto prazo (6 a 18 meses)?

Desenvolvimento em parceria com empresas do ramo e formação de fórum multinacional com outras NRENs para promoção de um padrão de autenticação federada para IoT

- Como se trata de uma prova de conceito de um protocolo novo para autenticação federada de dispositivos IoT, é preciso um trabalho de desenvolvimento para deixá-lo adequado para entrar em produção.
  - Etapas ainda por tratar: descoberta de serviços, autorização, descredenciamento de dispositivos, entre outros.
  - Além do suporte da RNP, o projeto poderá contar (para seu desenvolvimento) com parcerias com empresas focadas em IoT interessadas em agregar um novo tipo de serviço aos seus sistemas.
- Como se trata de um novo tipo de protocolo, federado e voltado para as futuras redes de dispositivos, RNP poderia ter um papel mais protagonista no cenário internacional, propondo uma norma baseada neste protocolo.
  - Junto com várias outras NRENs, RNP poderia formar um fórum específico para propor uma nova forma de autenticação federada mais leve voltada para redes futuras com muitos dispositivos restritos.

5. Há alguma sinergia com alguma startup? Como você vê a oportunidade de criação de uma startup a partir do GT?

Contato inicial estabelecido com startup da área de IoT

- Há várias startups que estão se dedicando ao desenvolvimento de produtos baseados no conceito de IoT.
  - Em conversas iniciais, a empresa DevTeconologia se mostrou interessada em conhecer melhor o protocolo e avaliar a possibilidade de adotá-lo em seus produtos e serviços.
- A oportunidade de se criar uma startup a partir deste GT é concreta.
  - Alunos que já participaram do projeto e outros que venham a participar sempre estão muito motivados a iniciar seus próprios negócios baseados em propostas inovadoras.
  - Um dos alunos em nível de mestrado que participaram do projeto até aqui já tem sua própria empresa na área de segurança da informação e poderia eventualmente expandir sua oferta de serviços com a adoção do protocolo proposto.

19º WRNP
Workshop RNP
7 | 8 MAIO
Campos do Jordão | SP

Obrigado

Marco A. A. Henriques

maah@unicamp.br

RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CULTURA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES BRASIL GOVERNO FEDERAL