CoFee: Uma Federação de Identidade para IoT

Pedro Micael T. L. N. Pinto[1], Antonio L. Maia Neto [1], Maria Luiza B. A. Santos[1]
Artur Souza[1], Marco A. Amaral Henriques[2],Leonardo B. Oliveira[1]

[1]Universidade Federal de Minas Gerais (UFMG)
[2] Universidade Estadual de Campinas (Unicamp)
{pedromicael,lemosmaia,mburga,arturluis,leob}@dcc.ufmg.br
marco@dca.fee.unicamp.br

Abstract. *Due to the constraints of IoT elements, even widely adopted schemes such as digital certificates/PKI (Public Key Infrastructure) are inadequate to this context. Our goal is, therefore, to come up with an Federated Identity Management solution exclusively tailored to IoT. We also evaluate alternatives to traditional PKI and our results indicate that an approach using ECQV (Elliptic Curve Qu-Vanstone) is around 10% better than the traditional approach.*

1. Introdução

A Internet das Coisas (IoT – *Internet of Things*) é um tópico de pesquisa cada vez mais relevante (Atzori et al. 2010; Wangham et al. 2013). A ideia básica deste conceito é que o ambiente no entorno de usuários seja repleto de elementos computacionais chamados de "coisas" (*things*).

A área de Gestão de Identidade, por sua vez, tem recebido grande atenção por parte de empresas, provedores de serviço e pelas redes que dão suporte ao ensino ao redor do mundo (Torres et al. 2013; Horrow and Sardana 2012). Com a proliferação de provedores de serviços na Internet, aumentam os usuários e, por conseguinte, a necessidade de se estabelecer controle de acesso a serviços e/ou informações mais efetivos. Temos também uma maior incidência de fraudes a tais serviços, o que impõe uma infinidade de desafios técnicos, científicos e tecnológicos à comunidade de Segurança Digital.

Tais desafios são ainda maiores quando olhados pela perspectiva do mundo conectado de IoT. Isso porque algumas das estratégias para viabilizar a Gestão de Identidade na Internet tradicional não são adequadas à IoT. Por exemplo, autenticação na Internet tradicional é usualmente obtida por meio de uma Infraestrutura de Chaves Públicas (*Public Key Infra-Structure* – PKI), que muitas vezes não é adequada ao ambiente de IoT.

O objetivo deste trabalho é propor uma solução de Gestão de Identidade Federada para IoT, para tanto apresentamos uma Federação de Identidade para a Internet das Coisas chamada de **Co**isas **Fed**eradas (CoFee). A CoFee substitui criptossistemas assimétricos empregados numa PKI convencional por outros mais leves (*lightweight*) e, portanto, se adequa aos recursos computacionais de IoT.

2. CoFee

O esquema de gestão de identidade federada proposto, visa garantir acesso de um dispositivo fora do seu domínio de origem a um serviço provido em um domínio distinto do seu, utilizando-se para isso do processo de autenticação de seu próprio provedor de identidade. É assumido que foi realizado um cadastro do dispositivo D no seu provedor de

identidade. Utilizamos de premissas criptográficas para garantir a autenticação, integridade das mensagens e sigilo nas comunicações entre as entidades envolvidas, que neste caso são: dispositivo D, provedor de identidade IdP e o provedor de serviço SP. Para

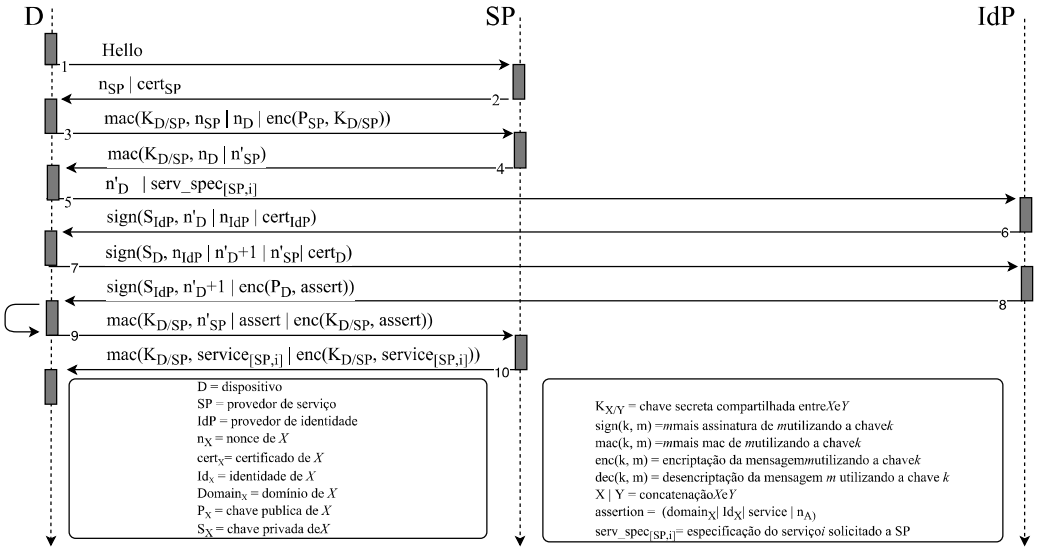

Figura 1. Ilustração de um Protocolo genérico de federação de identidade

que D utilize os serviços disponibilizados por SP é necessário que se autentique no seu provedor de identidade, que têm uma relação de confiança estabelecida com SP.

A utilização de certificados convencionais em conjunto com assinaturas para garantir a autenticidade de entidades em uma infraestrutura PKI tradicional pode não ser adequada para o ambiente de IoT.

2.1. Avaliação dos Protocolos

O alto custo de gerenciamento e verificação de certificados digitais tradicionais os tornam inadequados a estratégias de Gestão de Identidade no contexto de IoT. Note-se que não existe uma solução que atenda todos os requisitos desejáveis de um cenário de IoT. Abaixo apresentamos um levantamento de algumas características dos criptossistemas.

DSA+PKI: o Algoritmo de Assinatura Digital (*Digital Signature Algorithm* – DSA) é um esquema de assinaturas comumente utilizado na Internet em conjunto com certificados digitais tradicionais (PKI). A segurança do esquema é baseada no problema do logaritmo discreto (*Discrete Logarithm Problem* – DLP). O tamanho dos parâmetros e a necessidade dos certificados tradicionais tornam o esquema inviável para a Internet das Coisas.

ECQV: no esquema de certificados implícitos baseado em curvas elíptica de Qu-Vanstone (Brown et al. 2002), a chave pública de uma entidade é combinada com o certificado de forma a criar um elemento único, do qual a chave pública pode ser extraída sendo implicitamente verificada. Uma grande vantagem desse método reside no tamanho consideravelmente reduzido dos certificados implícitos, que os torna muito menores do que certificados tradicionais, o que torna o esquema muito interessante em cenários IoT.

Foram avaliados também os esquemas de Boneh e Franklin (Boneh and Franklin 2001), Cocks (Cocks 2001), Boneh-Gentry-Hamburg (Boneh et al. 2007) (BGH) e *Certificateless* com e sem emparalhemantos. De

forma qualitativa foram avaliados aspectos como custo computacional das operações utilizadas nos esquemas, tamanho de cifras gerados, ser baseado ou não em identidades e por fim a custódia de chaves. O custo das operações de emparalhamento presentes em alguns dos esquemas os tornam inviáveis pra o contexto de IoT. É importante ressaltar que que nenhum dos esquemas é totalmente adequado para o ambiente de IoT.

3. Resultados e Análise

Avaliação Analítica. Esta análise pretende determinar o custo analítico total para que D acesse um serviço provido por SP, o que envolve a autenticação de D por seu IdP (figura 1). Para tal, são avaliados os esquemas PKI e ECQV, ambos em conjunto com o ECDSA e o esquema de cifração (*Elliptic Curve Integrated Encryption Scheme* – ECIES).

Note-se que os esquemas avaliados são baseados em curvas elípticas, onde as operações que influenciam significativamente o custo de computação, especialmente quando se considera dispositivos com limitações de recursos, são a multiplicação de pontos de curva elíptica por escalar e os emparelhamentos bilineares. Dessa forma, considerar o número de execuções dessas operações no custo dos esquemas é uma métrica válida de avaliação analítica. Tanto PKI quanto ECQV não utilizam-se de operações de emparelhamentos, direcionando essa análise à quantidade de multiplicações de ponto por escalar. Como apontado em (Oliveira et al. 2009), o esquema *Certificateless*, ao fazer uso de emparelhamentos bilineares, incorre em uma alta sobrecarga computacional, o que justifica a sua exclusão desta avaliação.

O processo do acesso de D a um serviço de SP envolve as seguintes operações: geração e verificação de assinatura, cifração e decifração. O número de operações de (de)cifração é comum às duas estratégias, logo, o número de multiplicações de pontos, neste caso, é o mesmo. Para as operações que envolvem assinaturas, no entanto, há diferenças. No esquema PKI, a verificação de uma assinatura envolve, como passo complementar, a validação do certificado, o que, por sua vez, requer a verificação da assinatura contida no mesmo. Já na abordagem que usa ECQV, a verificação do certificado é realizada de maneira implícita, existindo a necessidade de uma operação de extração da chave pública. tabela 1 apresenta a quantidade de operações de multiplicação de pontos. Note-se que o PKI necessita de duas operações de multiplicação de ponto a mais que o ECQV, característica que deve estar refletida nos resultados experimentais, apresentados adiante.

Tabela 1. Custo Computacional e Tempos de Execução: PKI x ECQV

	Multiplicação de Pontos		**Tempo de Execução**	
	PKI	ECQV	PKI	ECQV
validação do certificado	4	n.a.	16.31 ±0.48	n.a.
extração da chave pública	n.a.	2	n.a.	10.98 ±0.49
geração de assinatura	1	1	6.80 ±0.40	6.80 ±0.40
verificação de assinatura	4	4	16.31 ±0.48	16.31 ±0.48
cifração	2	2	17.00 ±0.55	17.00 ±0.55
decifração	1	1	11.05 ±0.38	11.05 ±0.38

Avaliação Experimental. Os experimentos visaram avaliar os tempos de execução de cada um dos esquemas apresentados na avaliação analítica. Os códigos foram implementados na linguagem C, tendo como base a biblioteca criptográfica *RELIC*[1].

[1] `https://github.com/relic-toolkit`

Os testes foram executados na plataforma *Intel Edison Kit for Arduino*, com CPU *dual-core 500 MHz Intel Atom* e cada esquema foi executado 100 vezes. Avaliando os tempos totais de execução foi observado que, o menor tempo de execução obtido pelo PKI na amostra é maior do que o maior tempo de execução obtido pelo ECQV. A diferença média entre eles é de aproximadamente 10 ± 1.6675 ms, com o ECQV sendo, em média, 10% mais rápido. Calculando-se o intervalo de confiança, pode-se dizer que o ECQV executa em menor tempo que o PKI com 95% de confiança.

Os resultados experimentais confirmam os resultados analíticos esperados, com o tempo de execução do ECQV inferior ao PKI. A tabela 1 mostra o tempo em milisegundos necessário para execução de cada operação do PKI e do ECQV. As operações como geração e verificação de MAC, assim como as operações envolvendo criptografia simétrica não foram avaliadas nem analiticamente e nem experimentalmente pois tem tempos de execução desprezíveis frente ao custo demandado pelas operações em curvas elípticas.

Embora a diferença percentual entre a abordagem ECQV e PKI em relação as operações em multiplicação de pontos seja de 16,6%, isso não se reflete no percentual percebido no tempo de execução das abordagens a diferença é de 10%. Isso pode ser explicado pelo fato do ECDSA permitir o uso de primos de Mersenne, que possuem uma forma eficiente para computar reduções modulares, uma operação essencial no algoritmo.

4. Conclusão

A abordagem utilizando ECQV, foi cerca de 10% melhor que a PKI convencional, sendo mais rápida com 95% de confiança. Nossa proposta se mostra, portanto, atraente para o contexto de IoT, resultando em uma melhoria no desempenho e redução no consumo energético dos dispositivos utilizados.

Referências

[Atzori et al. 2010] Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805.

[Boneh and Franklin 2001] Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *CRYPTO*, pages 213–229. Springer.

[Boneh et al. 2007] Boneh, D., Gentry, C., and Hamburg, M. (2007). Space-efficient identity based encryptionwithout pairings. In *FOCS*, pages 647–657. IEEE.

[Brown et al. 2002] Brown, D. R. L., Gallant, R. P., and Vanstone, S. A. (2002). Provably secure implicit certificate schemes. In *FC*.

[Cocks 2001] Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In *Cryptography and coding*, pages 360–363. Springer.

[Horrow and Sardana 2012] Horrow, S. and Sardana, A. (2012). Identity management framework for cloud based internet of things. In *SECURIT*, pages 200–203.

[Oliveira et al. 2009] Oliveira, L. B., Kansal, A., Priyantha, B., Goraczko, M., and Zhao, F. (2009). Secure-tws: Authenticating node to multi-user communication in shared sensor networks. In *IPSN*, pages 289–300.

[Torres et al. 2013] Torres, J., Nogueira, M., and Pujolle, G. (2013). A survey on identity management for the future network. *Communications Surveys Tutorials, IEEE*, 15(2):787–802.

[Wangham et al. 2013] Wangham, M. S., Domenech, M. C., and de Mello, E. R. (2013). Infraestrutura de autenticação e de autorização para internet das coisas. In *Minicursos: SBSeg*, volume 1. SBC.

