AdC: Um Mecanismo de Controle de Acesso Para o Ciclo de Vida das Coisas Inteligentes

ANTONIO L. MAIA NETO1, ARTUR LUIS FERNANDES1, ITALO CUNHA1

MICHELE NOGUEIRA2, IVAN OLIVEIRA NUNES1, LEONARDO COTTA1

NICOLAS GENTILLE3, ANTONIO A. F. LOUREIRO1, DIEGO F. ARANHA4

HARSH KUPWADE PATIL5, LEONARDO B. OLIVEIRA1

Introdução

IdC é uma realidade.

Autenticação e segurança.

Abordagens ineficientes.

- Sobrecarga dos dispositivos
- Diferentes domínios.

Ciclo de vida.

AdC

Conjunto de protocolos para incorporar autenticação e controle de acesso para todo o ciclo de vida dos dispositivos na Internet das Coisas (IdC).

- Manufatura.
- Aquisição.
- Implantação.
- Operação.
- Descarte.

Contribuições – Baseado em [Maji et al. 2008]

- AdC
- Validação
- Disponível Publicamente

AdC – Autenticação das Coisas

Premissas:

- Mensagens enumeradas. Id do interlocutor;
- Material criptográfico na manufatura;
- PINS seguros;
- Primitivas criptográficas ideais.

AdC – Autenticação das Coisas

Problemas

- Soluções ineficientes.
- Criptografia de chaves públicas
- Gerir as listas de permissão

Objetivos

- Solução Adequada
- Dispositivos inteligentes
- Atender às restrições

AdC – Autenticação das Coisas

Abordagem

- Solução Inovadora
- Distribuição de chaves.
  - Criptografia baseada em identidade. [Shamir 1984, Sakai et al. 2000, Boneh and Franklin 2001]
- Controle de acesso.
  - Criptografia baseada em atributos. [Goyal et al. 2006, Bethencourt et al. 2007]

Problema da custódia de chaves

- Cloud
- Doméstico

Dispositivos implantados sem a necessidade de conexão cabeada.

- Proteção física e dispositivo ponte

AdC – Autenticação das Coisas

Protocolos Auxiliares:

- Chave de sessão;
- Acordo de Chaves;
- Distribuição;
- Vinculação;
- Desvinculação.

Objetivo

- Derivar chaves de sessão, acordar chaves par a par, distribuir chaves privadas e vincular e desvincular um usuário de um dispositivo no domínio *Cloud*
- Desafio-resposta

AdC – Autenticação das Coisas

Manufatura

- Material criptográfico do domínio Cloud é carregado nos dispositivos

  - C – Cloud; D – Dispositivo; i – identidade; S – chave privada; K – Par a par; Cd – contador; Fis – Canal Físico – Td - Distribuídor

$$
\begin{array}{l}
\textsc{Manufatura}(D) \\
\quad 1. \qquad C: \quad id_{D,C} := serial\#\text{de } D,\ S^{\mathrm{I}}_{D,C} \\
\quad 2. \quad C \rightarrow D: \quad \textsc{Fis}(id_{D,C}, S^{\mathrm{I}}_{D,C}, k_{D,C}, \mathrm{c}_D) \\
\quad 3. \quad C \Rrightarrow T_D: \quad D
\end{array}
$$

AdC – Autenticação das Coisas

Aquisição

- Gere a comercialização do dispositivo

  - D – Dispositivo; Td – Distribuidor; U – usuário; TLS – Comunicação Digital Segura

$$
\begin{array}{l}
\textsc{Aquisição}(D, U) \\
\quad 1. \quad U \rightarrow T_D : \quad \mathrm{TLS}(\$) \\
\quad 2. \quad T_D \rightarrow C : \quad \mathrm{TLS}(\mathrm{D} \mid \mathrm{U}) \\
\quad 3. \quad C \rightarrow U : \quad \mathrm{TLS}(\mathrm{pin}_D) \\
\quad 4. \quad T_D \Rrightarrow U : \quad D
\end{array}
$$

AdC – Autenticação das Coisas

Implantação

- Inicializa a segurança dos dispositivos no domínio domestico
  - Ur – Usuario máster; Dur – dispositivo pessoal; H - Criptossistema

IMPLANTAÇÃO(D)

1. $U_r \rightarrow D$: FIS(pin_D)
2. $D_{U_r} \rightarrow D$: FIS($id_{U_r,\mathcal{H}}$,$P^{\text{I}}_{H,\mathcal{H}}$,$\text{c}_{\mathbb{G}_H}$)
3. $D \rightarrow D_{U_r}$: FIS($id_{D,\mathcal{H}}$,$info_D$, CIP($k_{D,H}$)$_{P^{\text{I}}_{H,\mathcal{H}}}$)
4. $U_r \rightarrow D_{U_r}$: FIS($\mathbb{A}_D$,$\mathbb{Y}_D$)
5. $D_{U_r} \rightarrow H$: $\text{n}_{D_{U_r}}$, imp_req
6. $H \rightarrow D_{U_r}$: n_H, MAC($\text{n}_{D_{U_r}}$)$_{k^i_{D_{U_r},H}}$
7. $D_{U_r} \rightarrow H$: imp, $id_{D,\mathcal{H}}$, $\mathbb{A}_D$, $\mathbb{Y}_D$, $info_D$, CIP($k_{D,H}$)$_{P^{\text{I}}_{H,\mathcal{H}}}$, SIG($\text{n}_H \mid \text{n}_{D_{U_r}}$)$_{S^{\text{I}}_{D_{U_r},\mathcal{H}}}$
8. H : $S^{\text{I}}_{D_U,\mathcal{H}}$, $S^{\text{A}}_{D_U,\mathcal{H}}$
9. D : DISTRIBUIÇÃO(D, H, $\mathcal{H}$, I)
10. D : DISTRIBUIÇÃO(D, H, $\mathcal{H}$, A)
11. $H \Rightarrow \mathbb{G}_H$: $\mathbb{Y}_{\mathbb{G}_H}$, $\mathbb{A}_{\mathbb{G}_H}$,$\text{c}_{\mathbb{G}_H}$, $\text{SIG}_{S^{\text{I}}_{H,\mathcal{H}}}$
12. D : VINCULAÇÃO (D, U_r)
13. $H \rightarrow D_{U_r}$: imp_ack, MAC($\text{n}_{D_{U_r}} + 1$)$_{k^i_{D_{U_r},H}}$

AdC – Autenticação das Coisas

Operação

- O usuário *U* requisita a execução da operação ‘op’ no dispositivo *B* usando o dispositivo *A*
  - *Sig – assinatura; CBA – Chave privada; Op-req - Requisição*

$$
\begin{array}{lll}
\textsc{Operação}(U, A, B, \text{op}) & & \\
1. & U: & \text{usa } A \text{ para executar op em } B \\
2. & A \rightarrow B: & \mathrm{n}_A, \text{op\_req} \\
3. & B \rightarrow A: & \mathrm{n}_B, \Upsilon_{op}, \textsc{Mac}(\mathrm{n}_A)_{k^i_{A,B}} \\
4. & A \rightarrow B: & \text{op}, \textsc{Sig}(\mathrm{n}_B \mid \mathrm{n}_A)_{S^{\mathrm{A}}_{A,\mathcal{H}}} \\
5. & B: & \text{executa operação op} \\
6. & B \rightarrow A: & \text{op\_ack}, \textsc{Mac}(\mathrm{n}_A + 1)_{k^i_{A,B}}
\end{array}
$$

AdC – Autenticação das Coisas

Descarte

- *U* usa o dispositivo *A* para requisitar a operação de descarte do dispositivo *B*

DESCARTE(U, A, B)

1. A : $\{Requisita\ Descarte\}$
2. B : DESVINCULAÇÃO(B, U)
3. B : apaga $S^{\mathrm{I}}_{B,\mathcal{C}}$, $S^{\mathrm{I}}_{B,\mathcal{H}}$, $S^{\mathrm{A}}_{B,\mathcal{H}}$ e $\mathbb{R}_B$
4. B : exibe '*descarte conluído*' na tela

AdC – Autenticação das Coisas

Aspectos Complementares:

Transferência de Dono:

- Protocolo Transferência
- Similar ao Descarte
- Chaves não são apagadas

AdC – Autenticação das Coisas

Aspectos Complementares:

Revogação de Chaves

- Não é o foco principal
- Chaves com data de validade

AdC – Autenticação das Coisas

Aspectos Complementares:

Operação Inter Domínios

- Protocolo AcordoDeChavesInterDominio
- Baseado em [McCullagh and Barreto 2005].
- Possibilita Interoperação
- Derivem uma mesma chave par a par autenticada.

AdC – Desenvolvimento

Arquitetura

- Servidor Cloud
  - Robustos
- Dominios Domésticos
  - Capacidade sempre disponível
  - Videogames, desktops.
- Dispositivos IdC
  - Dispositivos variados

AdC – Desenvolvimento

Implementação

- Cloud e Doméstico
  - Linux, Apache, MySQL e PHP
  - HTTP e PHP
- Dispositivos
  - Android
  - JNI

AdC – Desenvolvimento

Criptografia

- C – biblioteca RELIC [Aranha and Gouvêa].
- Processadores de 8 e 16 bits e 4KB de RAM
- ARM
- (i) *Sakai-Ohgishi-Kasahara (SOK)* para acordo de chaves simétricas.
- (ii) *Boneh-Franklin (CBE)* para cifração CBI (adaptado para utilizar emparelhamentos assimétricos).
- (iii) *Bellare-Namprempre-Nevem (ABI)* para assinaturas CBI.
- (iv) *Maji-Prabhakaran-Rosulek (ABA)* como ABA resistente a conluio.
- (v) *keyed-Hash Message Authentication Code (HMAC)* para MAC (baseado em *hash* SHA256).
- (vi) *Advanced Encryption Standard (AES)* para cifração simétrica, modo CBC.

AdC – Avaliação

Segurança

- Ferramenta de verificação: *Scyther* [Cremers 2008]
  - Eficiência e suporte a diferentes tipos de ataques.

- Propriedades
- (i) Autenticação, usando MACs e assinaturas digitais;
- (ii) Confidencialidade, usando cifras;
- (iii) *Freshness*, usando *nonces* e contadores;
- (iv) Integridade, usando MACs, assinaturas digitais e funções de *hash*;
- (iv) Não-repúdio, usando assinaturas digitais.

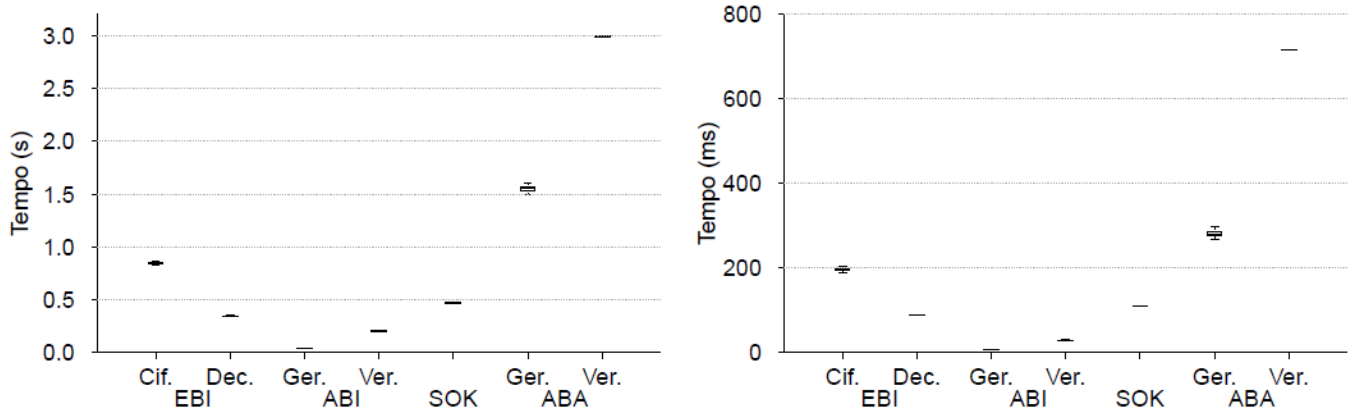
AdC – Avaliação

Experimentos

- Arduino Due
  - Processador ARM M3 de 32 bits e 84 MHz;
  - 96 KB de RAM;
  - 512 KB de memória *flash.*
- Intel Edison
  - Processador Atom de 32 bits e 500 MHz;
  - 1 GB de RAM;
  - 4 GB de memória *flash*.

AdC – Avaliação

*Cif*ração, *Dec*ifração, *Ger*ação de assinatura, e *Ver*ificação de assinatura nas plataformas Due e Edison

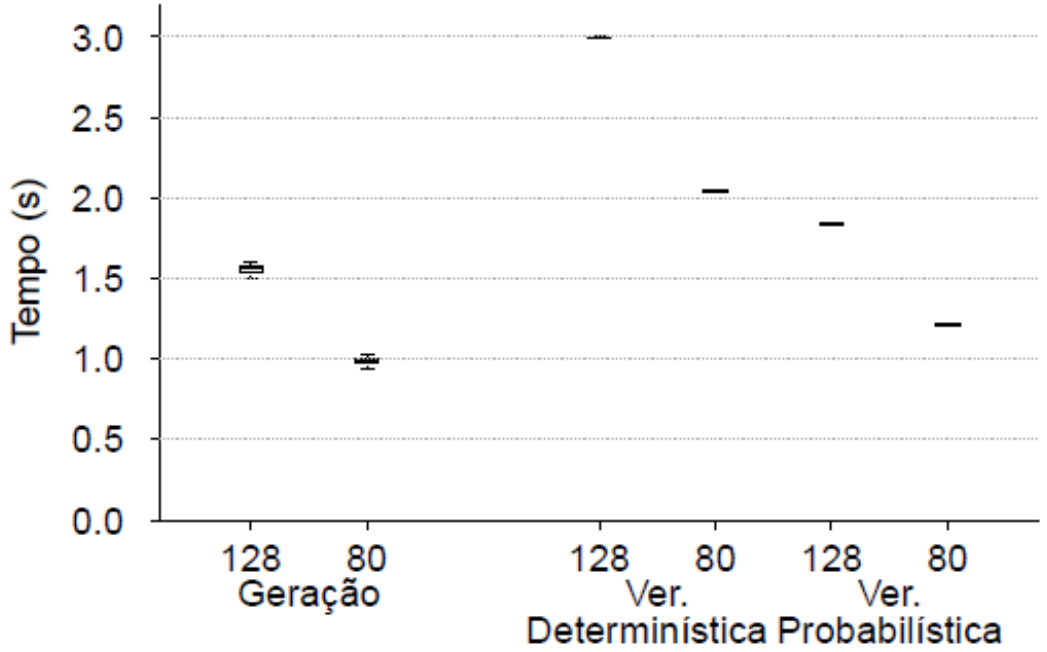


(a) Due

(b) Edison

AdC – Avaliação

Diferentes níveis de segurança



AdC – Conclusão

Fator crítico

- Troca de informações privadas
- Execução automática de operações

AdC – Família de Protocolos

- Autenticação forte e controle de acesso

Avaliação

- Limitação de recursos
- Validadas as propriedades de segurança
- Dispositivos variados