Um Mecanismo *Simples* e *Eficiente* para a Autenticação de Dispositivos na Comunicação por Campo de Proximidade

ADAPTADO DE

SILVIO E. QUINCOZES E JULIANO F. KAZIENKO – UNIPAMPA

LUIZ FERNANDO PUTTOW SOUTHIER

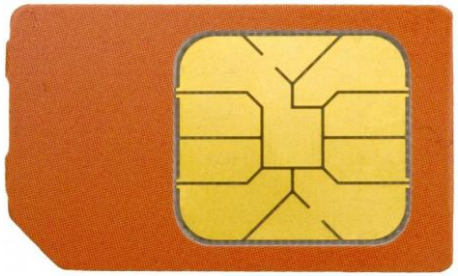
Near Field Communication (NFC)

- Comunicação por Campo de Proximidade
- Troca de mensagens entre dispositivos, como celulares, notebooks, crachás, etc.
- ondas de rádio de alta frequência (13,56 MHz)
- alcance máximo de dez centímetros
- maior usabilidade e menor tempo de configuração que o Bluetooth

E a segurança?

- Curta distância é vantagem
- Se um dispositivo camuflado for inserido na área de cobertura?
- Mecanismo de autenticação

Trabalhos Relacionados



[Chen et al. 2010],

- mecanismo de autenticação
- Primitivas criptográficas GSM
- Utiliza o Subscriber Identity Module (SIM) como identificador
- as chaves são geradas dinamicamente a cada autenticação.
- "Como a operadora de telefonia participa na geração da chave compartilhada, o uso do mecanismo fica limitado a dispositivos da mesma operadora."

O Mecanismo Proposto

A	$\mathrm{ID_A}$ (púbico)	$LA \leftarrow \{K_i, K_{i+1} \ldots\}$

B	ID_B (privado)	$LB \leftarrow \{K_{ID_A}, K_{ID_C} \ldots\}$

O Mecanismo Proposto

LA

$\{K_I\}$

LB

$\{K_{ID_A}\}$

M1 = $\{ ID_A, N_1 \}$

$K_{ID_A} = hash\,(PIN, N_1)$

$\beta = 0$

$H_1 = hash(N_1, K_{ID_A})$

M2 = $\{ \beta, H_1, N_2 \}$

$se\ \beta = 0,\ K_I = hash\,(PIN, N_1)$

O Mecanismo Proposto

A

B

LA

$\{K_I\}$

LB

$\{K_{ID_A}\}$

M1 = $\{ ID_A, N_1 \}$

$\beta = 1$

$H_1 = hash(N_1, K_{ID_A})$

M2 = $\{ \beta, H_1, N_2 \}$

$se\ \beta = 1,\ H_i = hash\ (N_1, K_i)$

$se\ H_1 = H_i,$

$H_3 = hash\ (N_2, K_i)$

$K_i = hash(K_i, M_1)$

$H_4 = hash(N_2, K_{ID_A})$

$se\ H_3 = H_4,$

$K_{ID_A} = hash(K_{ID_A}, M_1)$

M3 = $\{ H_3 \}$

Protótipo

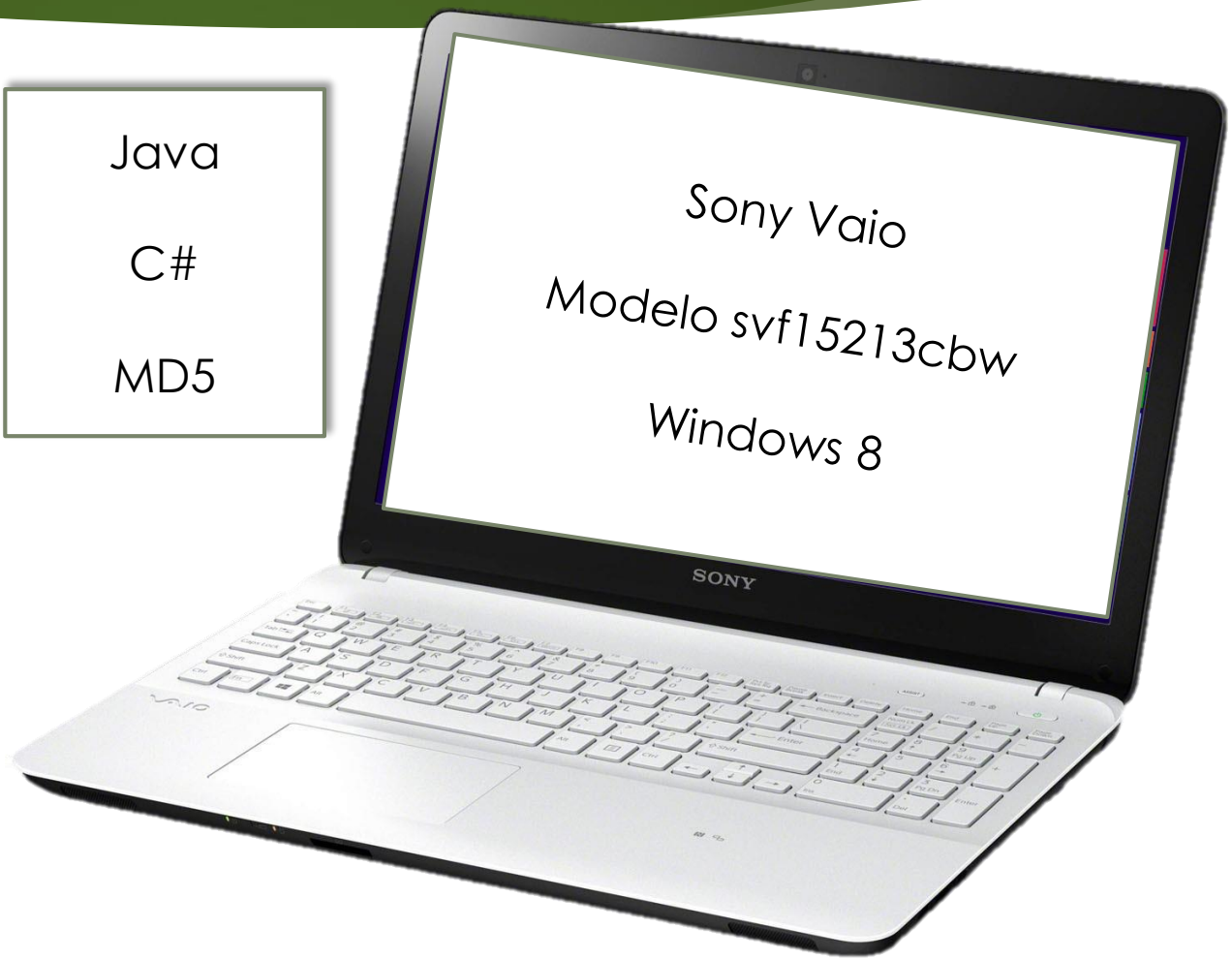
Sony Xperia M

Android 4.2

Java

C#

MD5



Sony Vaio

Modelo svf15213cbw

Windows 8

Comparação

	[Chen et al. 2010]	**Mecanismo Proposto**
Privacidade do Usuário	Parcial	Satisfatória
Terceiro Confiável	Dependente	Independente
Simplicidade	Médio	Simples
Espaço de Armazenamento	Pouco	Pouco
Autenticação Mútua	Possui	Possui
Renovação de Chaves	Razoável	Aceitável

Referências

- Alzahrani, A., Alqhtani, A., Elmiligi, H., Gebali, F., and Yasein, M. S. (2013). NFC security analysis and vulnerabilities in healthcare applications. In IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), pages 302–305. IEEE.
- Chen, W., Hancke, G., Mayes, K., Lien, Y., and Chiu, J.-H. (2010). NFC mobile transactions and authentication based on GSM network. In Second IEEE International Workshop on Near Field Communication (NFC), pages 83–89. IEEE.
- Coskun, V., Ozdenizci, B., and Ok, K. (2013). A Survey on Near Field Communication NFC Technology. Wireless Personal Communications, 71:2259–2294.
- Eun, H., Lee, H., and Oh, H. (2013). Conditional privacy preserving security protocol for NFC applications. IEEE Transactions on Consumer Electronics, 59(1):153–160.
- Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7):1497–1516.