Privacy-Preserving Telemonitoring for eHealth

Mohamed Layouni⋆, Kristof Verslype†, Mehmet Tahir Sandıkkaya‡, Bart De Decker†, Hans Vangheluwe⋆

⋆School of Computer Science, McGill University, Canada
†Department of Computer Science, KULeuven, Belgium
‡ Katholieke Hogeschool Sint-Lieven, Gent, Belgium

MSDL 2009 Summer Presentations
27 August 2009
McGill University

Telemonitoring $\equiv$ monitoring patients' health in their natural environment (home, work, family etc.)

Why is it useful?

- Reduces the burden on public healthcare system
- Helps patients remain active and improves the healing process
- Helps elderly people remain active/independent and avoid nursing homes . . .

But!

- Privacy concerns are still a big obstacle to the adoption of such a system/service
- Patients are skeptical about the way their data is handled
- Patients are also concerned about the dependability/ reliability of the system

We try to answer questions such as :

- **Who** gets to see the patient's information?
- **How** is this information stored? retained? processed?
- **Can the patient decide** what information gets revealed? to whom?
- In case a monitoring device is used, **is it possible to control** what data this device communicates to the outside world?

Outline

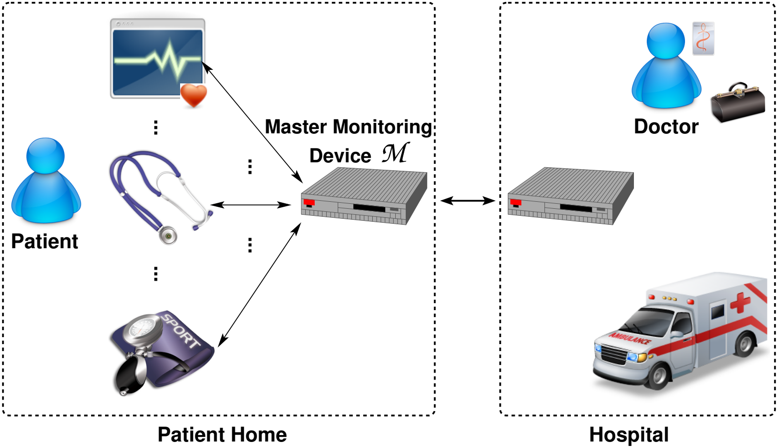

Figure: Setting of the Health Telemonitoring System

Privacy Requirements

- Selective disclosure
- Patient-centricity
- Pseudonimity
- Conditional deanonymization

Security Requirements

- Confidentiality
- Integrity

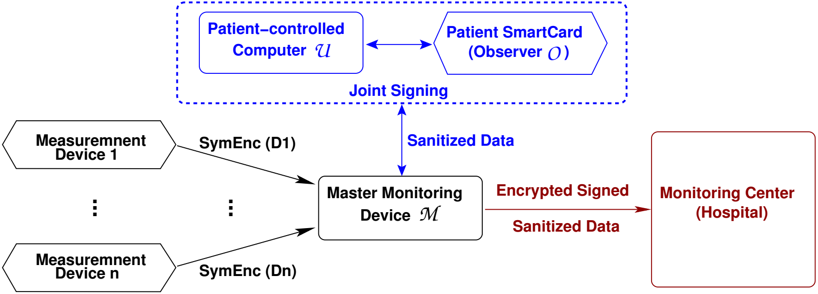

Figure: Health Telemonitoring System – General Overview

Execution sequence : **Black**, **Blue**, **Red**

Proposed construction based on :

- Wallet-based Anonymous Credentials.
- Perfectly Blinding Commitment Schemes.
- Conventional Symmetric-Key Cryptosystems.

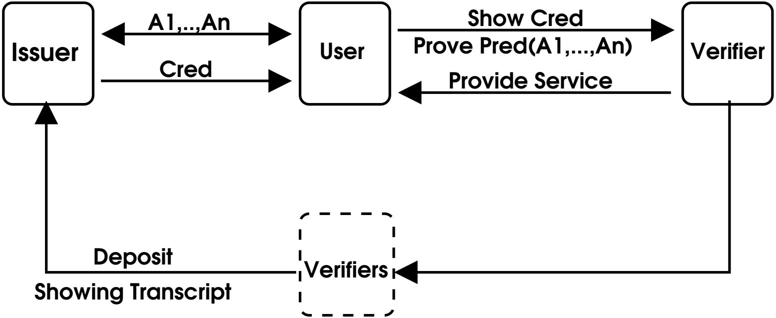

Figure: Anonymous Credential Issuing, Showing, and Depositing

Properties of Privacy-preserving (Anonymous) Credentials

- **Selective disclosure** (in the sense of Zero Knowledge)
- Unforgeability (issuing)
- Soundness (no false claims)
- No framing (showing transcript unforgeability)
- **Untraceability** (showings unlinkable to user's identity)
- **Unlinkability** (between showings)
- *Limited-show* unlinkability, untraceability . . .

Existing Commercial Implementations

- IBM's **IDEMIX** (Camenisch and Lysyanskaya)
- Credentica's (now Microsoft) **U-Prove** (Brands)

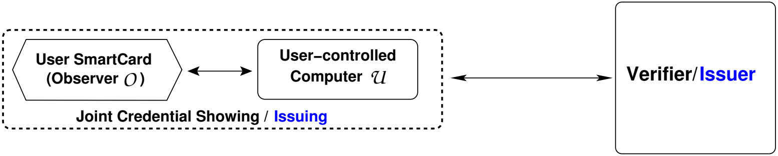

Figure: Wallet-based Anonymous Credential Showing (Wallet-based Issuing is similar)

- *Wallet-with-Observer* paradigm invented by Chaum and Pedersen [CP92]. Improved by Cramer and Pedersen [CP93], and later by Brands [Br00].
- Properties of *wallet-based* Anonymous Credentials:
  - Inflow/Outflow prevention
  - Cred showing fraud prevention
  - Two-factor authentication . . .

Wallet-based Anonymous Credentials

Public Info: $(g_i)_{0\le i\le \ell}, h_0 = g_0^{x_0}, (g_i^{x_0})_{1\le i\le \ell}, h_0^{x_0}, q, G_q, H, g_{\mathcal{O}}$

Observer $\mathcal{O}$ $(x, e, cert_{\text{CA}}(e))$ — **User's computer $\mathcal{U}$** $(x_3, \cdots, x_{\ell-1})$ — **Issuer CA** $(x_0, x_{\ell'+1}, \cdots, x_{\ell-1})$

Issuer CA: $m_0 = nonce||...$

CA → $\mathcal{U}$ → $\mathcal{O}$: $\xleftarrow{m_0}$ $\xleftarrow{m_0}$

Observer $\mathcal{O}$:

$x_1, x_2 \in_R \mathbb{Z}_q$

$com_1 := g_1^{x_1} g_2^{x_2}$

$com_1^{x_0} := (g_1^{x_0})^{x_1} (g_2^{x_0})^{x_2}$

$\mathcal{O}$ → $\mathcal{U}$: M_1 = { $\xrightarrow{com_1, com_1^{x_0}, (e, cert_{\text{CA}}(e))}$, $SPK\{\alpha_1, \alpha_2, \beta : com_1 = g_1^{\alpha_1} g_2^{\alpha_2} \wedge e = g_{\mathcal{O}}^{\beta}\}(m_0)$ }

Observer $\mathcal{O}$: Store (x_1, x_2)

User's computer $\mathcal{U}$:

$x_\ell \in_R \mathbb{Z}_q$

$com_2 := g_3^{x_3} \cdots g_{\ell'}^{x'_\ell} g_\ell^{x_\ell}$

$\mathcal{U}$ → CA: $\xrightarrow{com_2, M_1}$ $SPK\{\varepsilon_3, \cdots, \varepsilon_{\ell'}, \varepsilon_\ell : com_2 = g_3^{\varepsilon_3} \cdots g_{\ell'}^{\varepsilon'_\ell} g_\ell^{\varepsilon_\ell} \wedge \mathcal{P}(\varepsilon_3, \cdots, \varepsilon_{\ell'}, \varepsilon_\ell) = \text{TRUE}\}(m_0, M_1)$

Issuer CA:

$w_0 \in_R \mathbb{Z}_q$

$a_0 := g_0^{w_0}$

$b_0 := (com_1.com_2 \,.\, g_{\ell'+1}^{x_{\ell'+1}} \cdots g_{\ell-1}^{x_{\ell-1}} \,.\, h_0)^{w_0}$

CA → $\mathcal{U}$: $\xleftarrow{a_0, b_0}$

User's computer $\mathcal{U}$:

$\alpha_1, \alpha_2, \alpha_3 \in_R \mathbb{Z}_q,$

$f := com_1.com_2.\, g_{\ell'+1}^{x_{\ell'+1}} \cdots g_{\ell-1}^{x_{\ell-1}} \,.\, h_0$

$h := f^{\alpha_1}$

$z = f^{x_0} := com_1^{x_0}.(g_3^{x_0})^{x_3} \cdots (g_{\ell-1}^{x_0})^{x_{\ell-1}}.h_0^{x_0}$

$z' := z^{\alpha_1}$

$a'_0 := h_0^{\alpha_2} g_0^{\alpha_3} a_0$

$b'_0 := (z')^{\alpha_2} h^{\alpha_3} b_0^{\alpha_1}$

$c'_0 := H(h, z', a'_0, b'_0)$

$c_0 := c'_0 + \alpha_2 \mod q$

$\mathcal{U}$ → CA: $\xrightarrow{c_0}$

Issuer CA: $r_0 := c_0 x_0 + w_0$

CA → $\mathcal{U}$: $\xleftarrow{r_0}$

User's computer $\mathcal{U}$:

$r'_0 := r_0 + \alpha_3$

Accept iff $a'_0 b'_0 = (g_0 h)^{r'_0} (h_0 z')^{-c'_0}$

Store h, $\sigma_{\text{CA}}(h) = (z', r'_0, c'_0), com_1, \alpha_1, (x_3, \cdots, x_\ell)$

Figure: Wallet-based Anonymous Credential Issuing

Issuing Protocol Summary

At the end of the issuing protocol, the pair $(\mathcal{O}, \mathcal{U})$ obtains an anonymous credential $(h, \sigma_{CA}(h))$ with attributes $x_1, \cdots, x_\ell$, such that:

- $\mathcal{U}$ knows only $x_3, \cdots, x_\ell$.
- $\mathcal{O}$ knows only x_1, x_2.
- *Issuer* knows only $x_{\ell'+1}, \cdots, x_{\ell-1}$, where $\ell' \leq \ell - 2$.
- $\mathcal{O}$ and *Issuer* do *not* learn information on $(h, \sigma_{CA}(h))$.

Wallet-based Anonymous Credentials

Public Info: $(g_i)_{0 \le i \le \ell}, h_0 = g_0^{x_0}, (g_i^{x_0})_{1 \le i \le \ell}, h_0^{x_0}, q, G_q, H, g_{\mathcal{O}}$

Observer $\mathcal{O}(x_1, x_2)$		$\mathcal{U}(x_3, \cdots, x_\ell, \alpha_1, com_1, h, \sigma_{CA}(h))$		Verifier
		$\sigma_{CA}(h) = (z', r'_0, c'_0)$ $h = (h_0 . \prod_{i=1}^{\ell} g_i^{x_i})^{\alpha_1}$ $= h_0^{\alpha_1} . \prod_{i=1}^{\ell} g_i^{(\alpha_1 x_i)}$		
			$\xleftarrow{m}$	$m := nonce\|\|..$
$w_1, w_2 \in_R \mathbb{Z}_q$ $a_{\mathcal{O}} := g_1^{w_1} g_2^{w_2}$	$\xrightarrow{a_{\mathcal{O}}}$	$\beta, \gamma_1, \gamma_2, w_0, w_i \in_R \mathbb{Z}_q$, where $i \in [3, \ell]$ $a_{\mathcal{U}} := h_0^{w_0} . \prod_{i=3}^{\ell} g_i^{w_i}$ $a := a_{\mathcal{O}} . a_{\mathcal{U}} . com_1^{(\alpha_1 \beta)} g_1^{\gamma_1} g_2^{\gamma_2}$ $c := H(h, a, m)$		
$r_{\mathcal{O},1} := w_1 + c_{\mathcal{O}} x_1$ $r_{\mathcal{O},2} := w_2 + c_{\mathcal{O}} x_2$	$\xleftarrow{c_{\mathcal{O}}}$ $\xrightarrow{r_{\mathcal{O},1}, r_{\mathcal{O},2}}$	$c_{\mathcal{O}} := \alpha_1 (c + \beta)$ $r_1 := r_{\mathcal{O},1} + \gamma_1$ $r_2 := r_{\mathcal{O},2} + \gamma_2$ $r_i := w_i + c(\alpha_1 x_i)$, where $i \in [3, \ell]$ $r_0 := w_0 + c\alpha_1$	$\xrightarrow{h, \sigma_{CA}(h), a, (r_0, \cdots, r_\ell)}$	
				$c := H(h, a, m)$ accept iff $\sigma_{CA}(h)$ is valid AND $a \stackrel{?}{=} \left(h_0^{r_0} . \prod_{i=1}^{\ell} g_i^{r_i}\right) . h^{-c}$

Figure: Wallet-based Anonymous Credential Showing

Showing Protocol Summary

At the end of the showing protocol, the Verifier is convinced that:

- $\mathcal{U}$ holds a valid credential $(h, \sigma_{\text{CA}}(h))$.
- $\mathcal{U}$ knows the attributes $x_3, \cdots, x_\ell$ (ie., is the cred owner).
- $\mathcal{O}$ approved the showing.

The verifier learns only information *willingly* disclosed by the pair $(\mathcal{O}, \mathcal{U})$.

High-level description

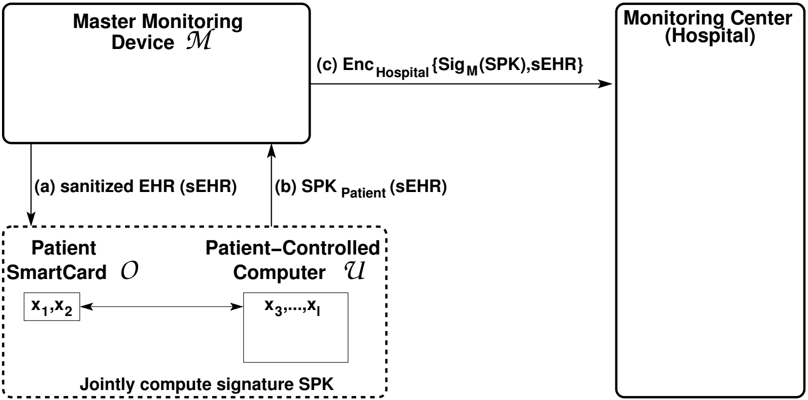

Figure: High-level Protocol Architecture (with two-factor message authentication)

- **Selective disclosure** (Anon Creds)
- **Patient-centricity** (*Wallet-based* Signed Proof of Knowledge)
- **Pseudonimity & Conditional Deanonymization** (Data Sanitization + Anon Cred Sig + *Group Signature*)
- **Defense against covert channels** (Wallet-with-Observer Inflow/Outflow Prevention Mechanisms)
- **Integrity** (Secure Sig Schemes)
- **Confidentiality** (Secure Encryption)

Thank you!