Reasoning about privacy properties of biometric system architectures in the presence of information leakage

Julien Bringer[1] Hervé Chabanne[12] Daniel Le Métayer[3]
Roch Lescuyer[1]

[1]Morpho
[2]Télécom ParisTech
[3]INRIA

Information Security Conference'15
September 11, 2015

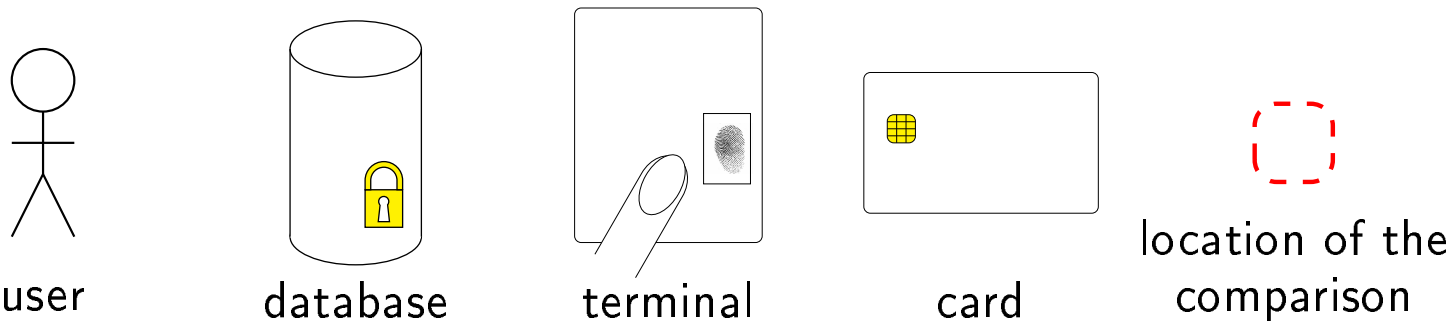
This work has been partially funded by the French ANR BIOPRIV and the European FP7 PRIPARE projects

SAFRAN Morpho

/01/

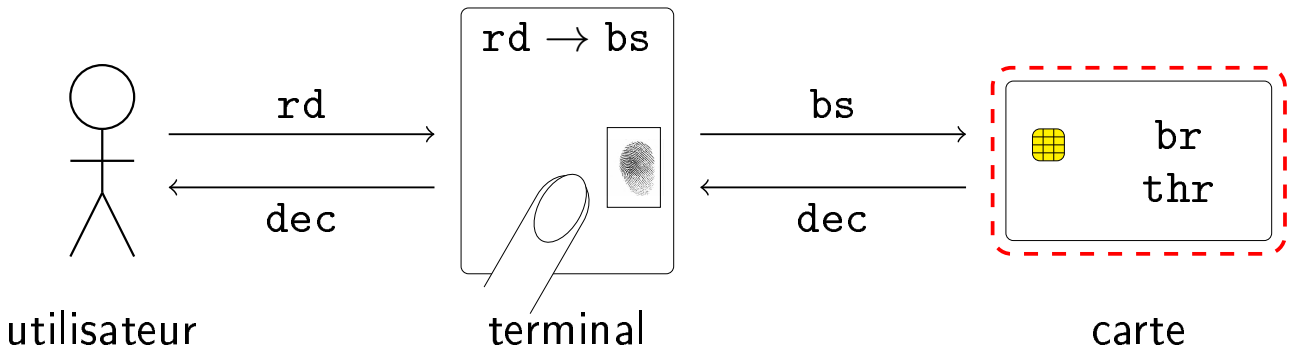
Analysis of Biometric Systems

- typical components



- typical data
  - `br`: biometric reference (of an enrolled user)
  - `rd`: raw biometric data (a image, a fresh capture)
  - `bs`: biometric template to be compared with the reference
  - `thr`: threshold according to a distance between templates
  - `dec`: result of the matching (*decision*)

- the *Match-On-Card* technology



- storage of a reference inside a *secure element*
- the card performs the comparison
- the reference does not leave the card
- the terminal trusts the card

Analysis of Biometric Systems

Motivations

- Precedent work (BCLL'15; AL'14)
  - description of biometric systems within a formal model
  - formal reasoning about privacy properties
  - intuition: the architecture level is the right level to reason about privacy properties
  - assumption: the building blocks do their jobs properly
- This work
  - the precedent model is static
  - no runtime leakage is taken into account
  - we need such an extension for biometric systems

/02/

A Formal Model for Privacy By Design

Formal Model for Privacy-By-Design

Reasoning about architecture

- Analysis of a system
  - components, localisation of data, trust assumptions, *etc.*
- Architecture language
  - Description of a system: a set of *architectural primitives*
    - *e.g.*: $Has_i(X)$, $Receive_{i,j}(\{S\}, \{X\})$, $Compute_i(X = T)$, ...
      $S ::= Attest_i(\{Eq\})$, $Eq ::= Pred(T_1, \ldots, T_n)$
  - a description specifies each component, communication, computation, *etc.*
- Architecture semantics
  - semantics based on *traces* (aka sequences of events)
  - events are instantiations of architectural primitives
  - architecture semantics: the set of states reachable by the (compatible) traces

Formal Model for Privacy-By-Design

Reasoning about architecture

- A dedicated epistemic logic for *privacy properties*
  - following the "*deductive algorithmic knowledge*" paradigm
  - properties: *confidentiality* of data and *integrity* of computations
  - semantics of a property P: set of architectures satisfying P
- Axiomatics
  - aka a set of *deductive rules*, sound and complete with respect to the semantics *e.g.*:

$$\textbf{H2}\ \frac{Receive_{i,j}(S,E) \in A \qquad X \in E}{A \vdash Has_i^{all}(X)}$$

$$\textbf{K1}\ \frac{Compute_i(X = T) \in A}{A \vdash K_i(X = T)}$$

Formal Model for Privacy-By-Design

Extension of the formal model

- Extending the architecture language
  - for each primitive, introduction of a bound on the number of instantiations
    - $Receive_{i,j}^{(n)}(\{S\}, \{X\})$, $Compute_i^{(n)}(X = T)$, ...
- Extending the traces of events
  - introduction of several sessions in the traces (a *Session* event)
    - enable the modelling of several successive sessions
  - enable the use of different values of the same variable
    - motivation: the information leakage due to the access of several values of the same variable across different sessions
  - introduction of a system re-initialization (a *Reset* event)

Formal Model for Privacy-By-Design

Extension of the formal model

- Adapting the trace semantics
  - the architecture semantics is always the set of reachable component states
  - the definition of the component states is adapted to the new events
- Extending the privacy logic
  - enable the reasoning about several access to the same variable
  - axiomatics for this extended logic:

$$\textbf{H2}\ \frac{Receive_{i,j}^{(n)}(S,E) \in A \qquad X \in E}{A \vdash Has_i(X^{(n)})}$$

$$\textbf{H5}\ \frac{Dep_i(Y,\mathcal{X}) \qquad \forall X^{(n)} \in \mathcal{X}:\ A \vdash Has_i(X^{(n)})}{A \vdash Has_i(Y^{(1)})}$$

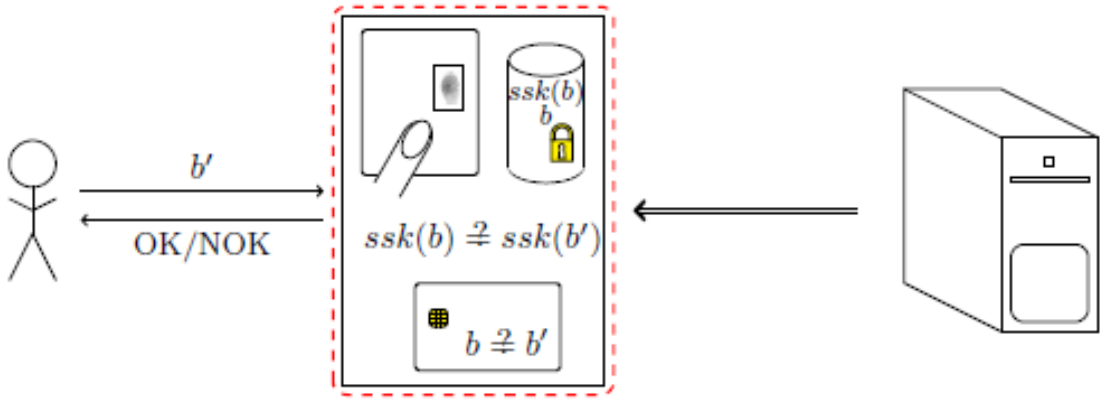
/03/

Back to Biometric Systems

Analysis of Biometric Systems

Another biometric system

- Extending *Match-On-Card* to biometric identification (BCKK'09)

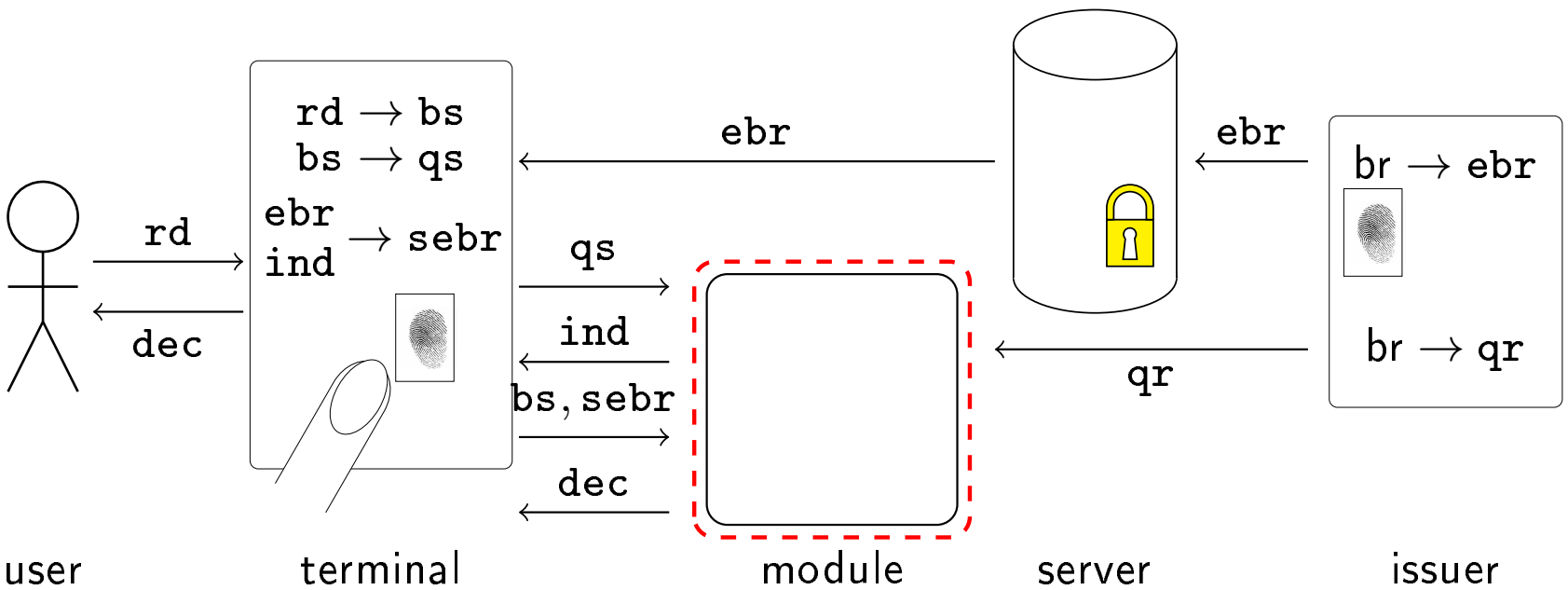


  - terminal with extended functionalities
    - sensor + database + *smart card inside the terminal*
  - biometric data are stored in two ways
    - a *secure sketch* for filtering; a *ciphertext* for identifying
  - templates comparison carried out inside the card

SAFRAN Morpho

- information leakage
  - the result of the authentication *leaks information* about the quantizations ...
  - ... even if the functionality is seen as *black-box* (BCS'10)
- idea of the attack
  1. successive queries to the card with random values
  2. analysis of the indices queried by the card

- description of this system and some variants inside the extended formal model
  - $Compute_{\mathsf{T}}^{(n)}(\mathtt{sebr} = EGet(\mathtt{ebr}, \mathtt{ind}))$, ...



- description variants with counter-measures
  - variant 1: ask all indices (no more dependencies on indices)
  - variant 2: block the number of queries before a critical bound
  - variant 3: re-initialization (re-encryption the database, permutation of the indices, etc.)
- then, analysis of the confidentiality of the secure sketches; *e.g.*:

$$\frac{\nexists X : Dep_{\mathsf{T}}(\mathtt{qr}, X) \in A^{\text{mi-e1}} \qquad \nexists j : Receive^{(n)}_{\mathsf{T},j}(S, \{\mathtt{qr}\}) \in A^{\text{mi-e1}} \qquad Has^{(n)}_{\mathsf{T}}(\mathtt{qr}) \notin A^{\text{mi-e1}} \qquad \nexists T : Compute^{(n)}_{\mathsf{T}}(\mathtt{qr} = T) \in A^{\text{mi-e1}}}{\mathbf{HN}\ \dfrac{\forall n : A \nvdash Has_{\mathsf{T}}(\mathtt{qr}^{(n)})}{A \vdash Has^{none}_{\mathsf{T}}(\mathtt{qr})}}$$

/04/

Conclusion

Conclusion

- precedent work
  - description of biometric system architectures within a formal model
  - reasoning about privacy properties of the architectures
- our contribution
  - extending the formal model (semantics and epistemic logic) to catch the runtime leakage
    - important for biometric comparison
  - analysis of a variants a biometric system within this extension

thank you for your attention