Using Mobile Agents for Secure Biometric Authentication

- Marco Tranquillin, Carlo Ferrari, Michele Moro

DEI, University of Padova

Agenda

- Requirements and motivations
- Authentication fundamental issues
- System architecture
  - Components' roles
- The proposed protocol
- Analysis and final remarks

Goal ...

- Design and prototype an agent-based infrastructure for strong authentication of users.
- Mobile devices have an active role
- A demo ...

Requirements

- Authentication is the basis of a user machine interface in pervasive context.
- Strong authentication (...it involves more than one factor...) becomes important in critical contexts
- Robustness and Security level of portable hw/sw are now worth to be considered

Biometrics

- Measuring physical features
  - fingerprints,
  - iris,
  - face,
  - voice,
  - hand geometry
- Measuring dynamic behaviour
  - typing,
  - walking

Biometrics

- Acquiring raw data
- Feature extraction
- Matching
- Evaluation (FAR, FRR...)

Biometric Recognition

- Using different parameters
- Composition
- Multivalue logic
- Adaptation

Biometric System

- Access control
- Application in pervasive context for
  - User tracking
- Heterogeneous system
  - computational power
  - mobility

Motivations

- Mobility of credentials is increasing in importance due to anywhere/anytime operative needs
- Agent mobility allows thin portable applications provided critical software is remotely loaded on-the-fly
- When some critical information are stored uniquely on not easily tamperable portable devices, safer protocols can be applicable

Interesting points

- ... the inclusion of a mobile phone in the authentication infrastructure
- .... an agent-based approach for implementing a suitable protocol
- In which depth agent mobility can be an added value in the proposed infrastructure?

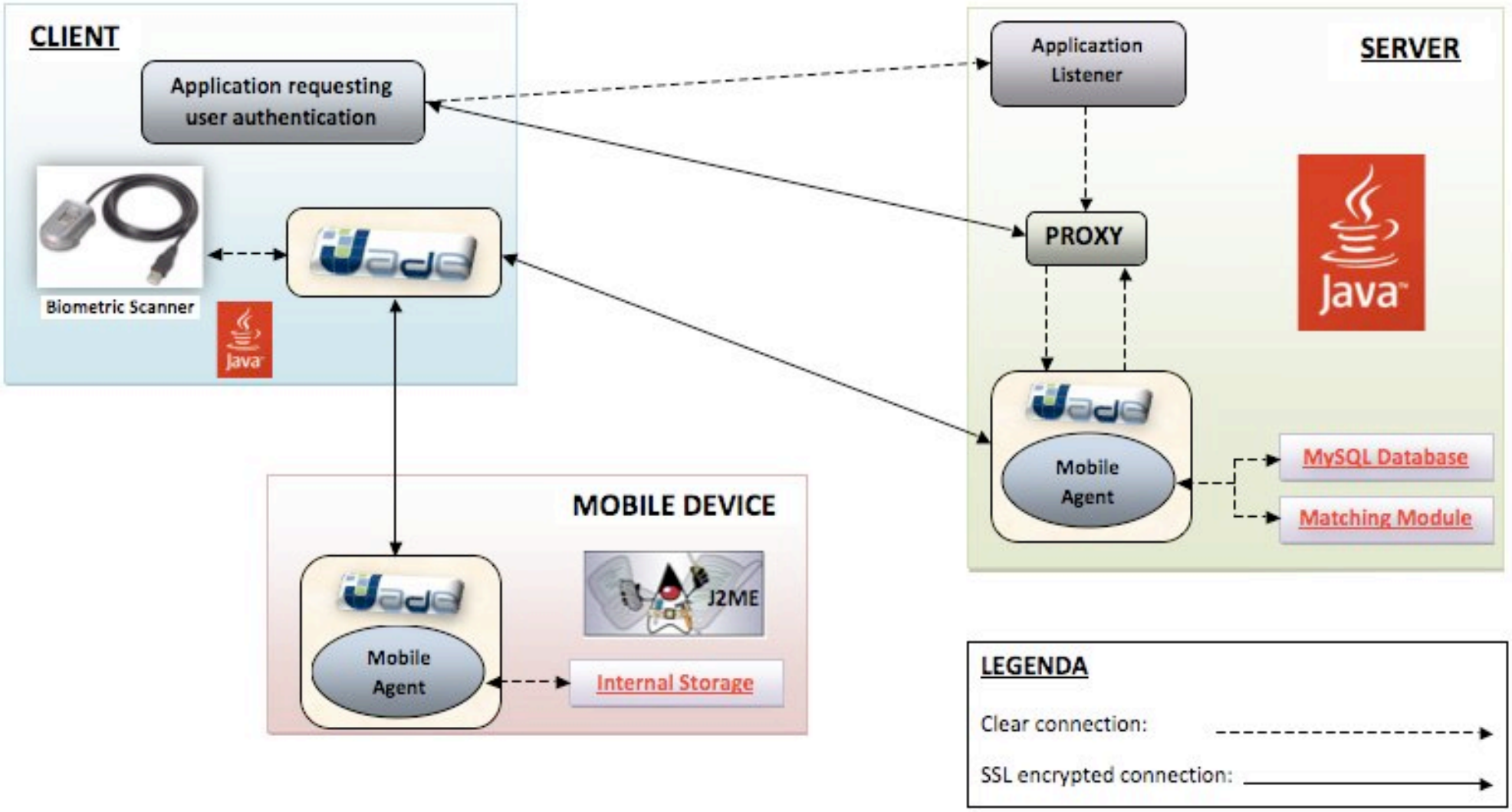
Authentication essential issues

- Strong authentication is based on:
  - Something the user knows (PIN or *similia*)
  - Something the user holds (a mobile device with its SIM/smart card)
  - Something tied to the user (a biometric parameter, a fingerprint in the present case)

Reasoning

- PIN acquired by mobile...
- Device authentication ... SIM
- Biometric authentication is not on mobile
  - Match-on-card
- Deploy agents on mobile devices

System architecture



Roles

- Server
  - Repository of fingerprint templates of all the registered users
  - *The Server Agent (SA)*

Roles

- Client
  - It supports the reading of the biometric parameter
  - It supports the direct communication with the mobile device

Roles

- Mobile
  - PIN acquisition interface
  - Repository of the user fingerprint template...
    - *The UserPhone Agent*

Roles

- Client
  - *The Mobile Agent.....*

...on the Mobile device...

- Generated during the Enrollment phase
  - RSA user key couple (K^+_U, K^-_U)
  - Hash of the user data (H_U)
  - AES user key (K_U)
  - Encrypted fingerprint
- Copied during the Enrollment phase
  - AES server key (K_S)
  - RSA server public key (K^+_S)

phase 1: initialization

- Get the user PIN on the mobile device
- Initialize the agency instances
- Establish the SSL tunnel between client and server
- The client sends a session ID to the server

phase 2: mobile authentication

- S: M1 = [R_{S1}, --]
- S: $K_S(M1), K^-_S(H(M1)) \rightarrow M$

- M: Decrypt M1
- M: CheckSig(K^+_S, $K_S(M1)$, $K^-_S(H(M1))$)
- M : M2 = [R_{S1}+1, K^+_U]
- M : $K_S(M2), K^-_U(H(M2)) \rightarrow S$

- S: Decrypt M2
- S: CheckSig(K^+_U, $K_S(M2)$, $K^-_U(H(M2))$
- S: CheckResponse(R_{S1}, M2)
- S: Save $K_S(K^+_U)$

phase 3: user personal data authentication

- S: M3 = [R_{S1}+2, --]
- S: K_S(M3), K^-_S(H(M3)) → M

- M : Decrypt M3
- M : CheckSig(K^+_S, K_S(M3), K^-_S(H(M3)))
- M : M4 = [R_{S1}+3, H_U , PIN]
- M : K_S(M4), K^-_U(H(M4)) → S

- S: Decrypt M4
- S: CheckSig(K^+_U, K_S(M4), K^-_U(H(M4))
- S: CheckResponse(R_{S1}+2, M4)
- S: CheckUserData(H_U , PIN)
- S: Get K_U from DB

phase 4: user biometric data authentication

- S: M5 = [R_{S1}+4, --]
- S: K_U(M5), K^-_S(H(M5)) → M

- M : Decrypt M5
- M : CheckSig(K^+_S, K_U(M5), K^-_S(H(M5)))
- M : M6 = [R_{S1}+5, K_U(FpTemp)]
- M : K_U(M6), K^-_U(H(M6)) → S

- S: Decrypt M6
- S: CheckSig(K^+_U, K_U(M6), K^-_U(H(M6))
- S: CheckResponse(R_{S1}+4, M6)
- S: Save K_U(FpTemp)

phase 4: user biometric data authentication

- S: M7 = $[R_{S2}, K^{+}_{S}] \rightarrow C$
- C: M8 = $[R_{S2}, K^{+}_{S}(FpLive)] \rightarrow S$
- S: Decrypt $K_U(FpTemp)$ and $K^{+}_{S}(FpLive)$
- S: Rep = Match(FpLive, FpTemp)
- S : M9 = $[R_{S1}+6, Rep]$
- S: $K_U(M9), K^{-}_{S}(H(M9)) \rightarrow M$
- M : Decrypt M9
- M : CheckSig($K^{+}_{S}, K_U(M9), K^{-}_{S}(H(M9))$)
- Show/Use Rep

Some remarks

- 3-steps approach
  - recognizing the mobile device as member of a set of authorized devices,
  - recognizing a user through her personal credentials
  - the biometric match
- The client is simply responsible for the reading of the raw biometric parameter
- The use of a mobile agent “isolate” the client and help to cope with the limitation of the mobile device.

Some remarks

- Basic security is provided by the SSL tunnel.
- Freshness and liveness properties are guaranteed by the challenge-and –response approach, like in the Needham-Schroeder protocol
- An appropriate combination of secret keys related both to the machines and to the single users provides a good balance between performances and the level of security.

Some remarks

- Whenever a step fails the whole authentication process fails.
- If a step is fraudulently passed, no effect of further weakness is propagated at subsequent levels that use new and different critical data.
- The last step, that uses biometric data, is the hardest to be misleaded.

Some remarks

- In perspective the MAS architecture shows a sufficient degree of scalability to adapt our model to significantly more complex situations like those requiring several client locations and a great number of potential users.

Some remarks

- It is worth to point out that the Jade security extension (Jade-S) unfortunately presents some hard limitations that make it unusable when mobile devices are involved.

- The future availability of more powerful smartphones will also bring the conditions for introducing the agent mobility at the phone level.