Wi-Trust

Improving Wi-Fi Hotspot Trustworthiness with Computational Trust Management

Jean-Marc.Seigneur@reputaction.com

UNIVERSITÉ DE GENÈVE

Reputaction

Agenda

- Hotspots Security and Remaining Threats
- Computational Trust Management
- Wi-Trust, our new proposal to promote trustworthy hotspots easily on top of Hotspot 2.0
- Q&A

Legacy Hotspots Remaining Security Holes

- Issues
  - Eavesdropping on unencrypted Wi-Fi
  - Legitimate hotspot spoofing
  - Session hi-jacking
  - Legal liability of the Wi-Fi hotspot sharer in several countries

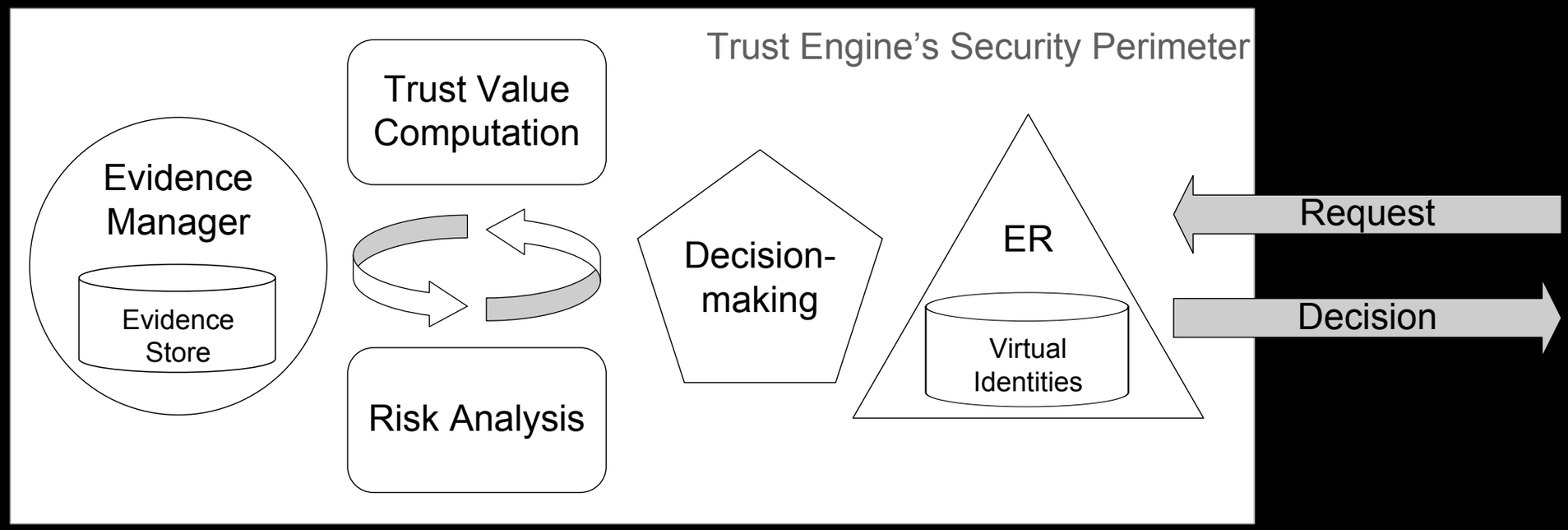
- Failed workarounds
  - WPA2-Enterprise technology cannot be applied to legacy Wi-Fi hotspot networks because the access point's 802.1X port blocks all communications prior to authentication
  - 802.1X client-side software and user credentials configuration too difficult on large-scale
  - Most users do not know or want to pay for a VPN

Hotspot 2.0

- Advances
  - Over-the-air encrypted transmissions with Certified WPA2-Enterprise
  - Granting access to the network based upon credentials
    - such as SIM cards, based on EAP
    - without user intervention, even when Wi-Fi roaming between trusted providers
    - Selecting Wi-Fi networks based on user preferences and network optimisation

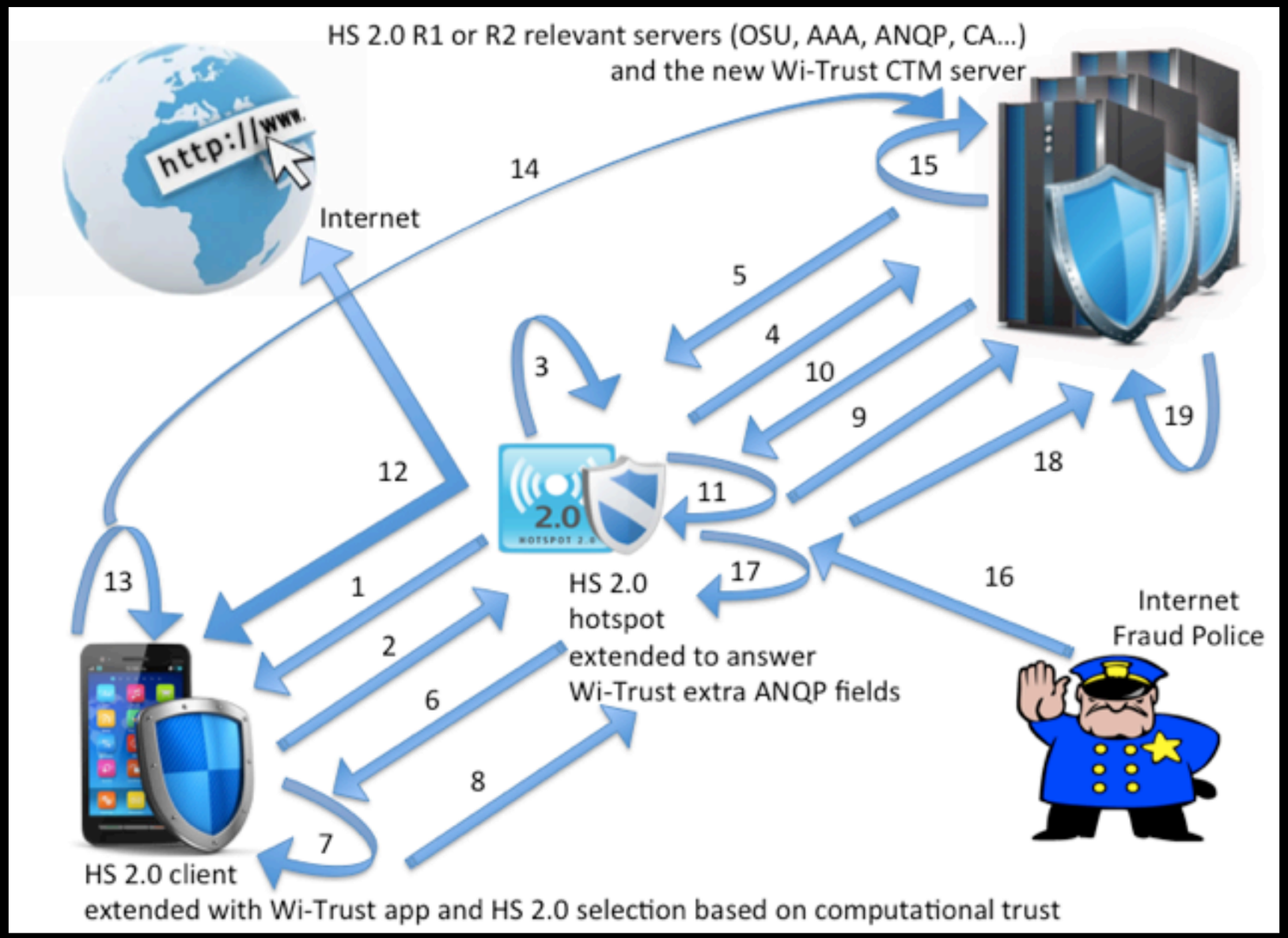
- Remaining issues
  - Eavesdropping at the hotspot after encryption between client and hotspot
    - Malicious hotspot owner, only Wi-Fi service provider is authenticated
    - Compromised legitimate hotspot
  - Untrustworthy provider providing low QoS

Computational Trust Management



- Previous work applied to Wi-Fi trust required too many changes at the hotspot firmware level

Wi-Trust Overview



- Easier to deploy on a large-scale
  - Trust engine ER mapped to Hotspot 2.0 EAP
  - Hotspot 2.0 ANQP available extra elements to communicate trust in providers, clients and potentially hotspots communicated

Features Comparison

	Legacy Hotspot	Hotspot 2.0	Wi-Trust
Wi-Fi roaming authentication without initial manual intervention		*	*
Client/Hotspot encryption against eavesdropping		*	*
Strong authentication of the hotspot service provider and user client		*	*
Automated hotspot selection	*	*	*
Automated hotspot selection based on computational trust in hotspots and service providers			*
Hotspot owner legal liability mitigation by malicious user client exclusion based on computational trust			*

Q&A

Jean-Marc.Seigneur@reputaction.com

UNIVERSITÉ DE GENÈVE

Reputaction