A device management framework for secure ubiquitous service delivery

Adrian Leung and Chris Mitchell

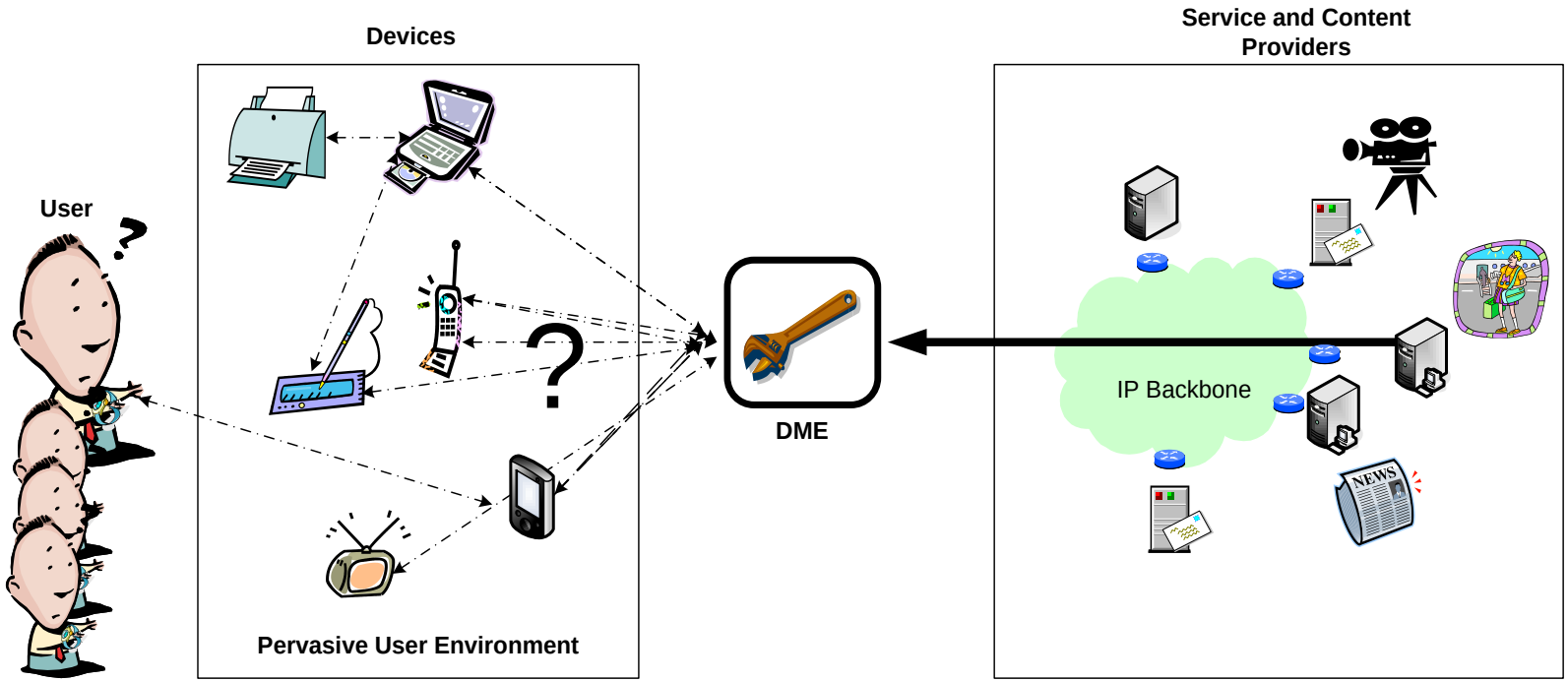
Royal Holloway

University of London

Agenda

- Motivation
- Security issues
- Building blocks
- A Secure Device Management Framework
- Analysis
- Conclusion

Ubiquitous service delivery



Goals

- Provide a complete framework for secure delivery of services to a mobile user in a ubiquitous environment.
- Framework covers:
  - enrolment;
  - secure service discovery;
  - secure service provision;
  - secure service redistribution.

Agenda

- Motivation
- Security issues
  - Security threats
  - Security requirements
- Building blocks
- A Secure Device Management Framework
- Analysis
- Conclusion

Security threats

- Spoofing (of service provider or user device);
- Tampering (with service provision);
- Information disclosure:
  - during communications; or
  - through physical loss of device;
- Malicious software attack in user device;
- Unauthorised sharing of credentials.

Security requirements

- Entity authentication;
- Integrity protection;
- Service confidentiality and user privacy protection;
- Device integrity assurance;
- Credential sharing prevention.

Agenda

- Motivation
- Security issues
- Building blocks
  - DME
  - Manual Authentication (MANA) protocol
  - Trusted computing
  - Ninja secure service discovery scheme
- A Secure Device Management Framework
- Analysis
- Conclusion

Device Management Entity (DME)

- Component of the Mobile VCE *Personal Distributed Environment* (see Atkinson et al., 2007).
- The DME is designed to abstract complexities faced by users, and maintains:
  - Features register;
  - Location register;
  - Security register.
- DMEs organised in a hierarchy, with a root DME:
  - DMEs communicate securely with each other.

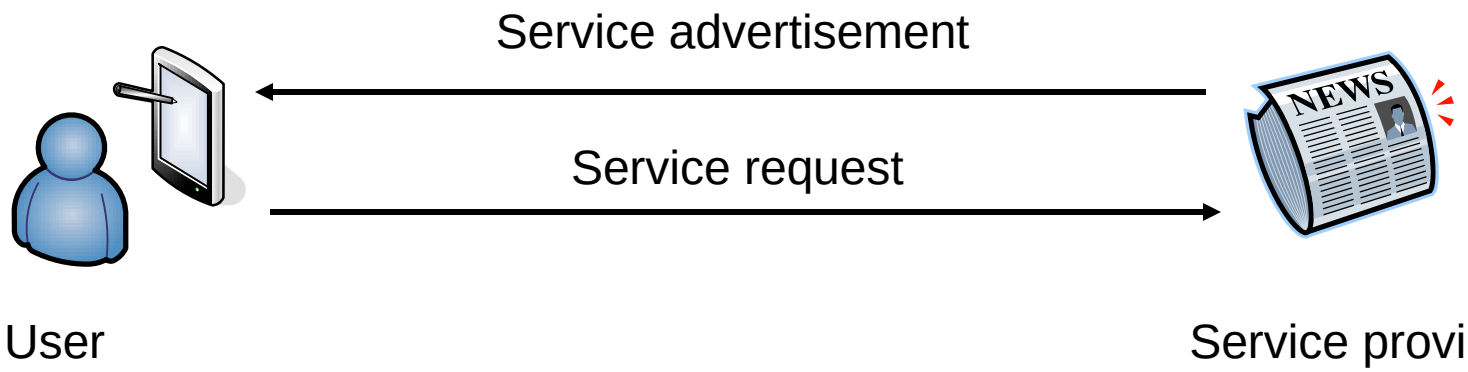
MANA protocols

- Manual Authentication (MANA) protocols allow two devices to authenticate each other using a combination of:
  - an insecure channel, and
  - manual data transfer.
- Standardised in ISO/IEC 9798-6.
- Much recent work, resulting in provably secure protocols with provably minimal user input.

Trusted Computing

- Shielded locations
- Protected capabilities
- Attestation
- Integrity measurement, storage and reporting
- Binding and Sealing

Ninja: Secure service discovery scheme



- Designed to provide secure service discovery in mobile ubiquitous environment.
- Proposed by Leung and Mitchell (2007).

Ninja – properties

- Enables mobile user to pseudonymously access advertised services.
- Also enables service provider to ‘pseudonymously authenticate’ user, and verify properties of user device.
- Builds on DAA protocol (built into TCG-compliant trusted platforms).

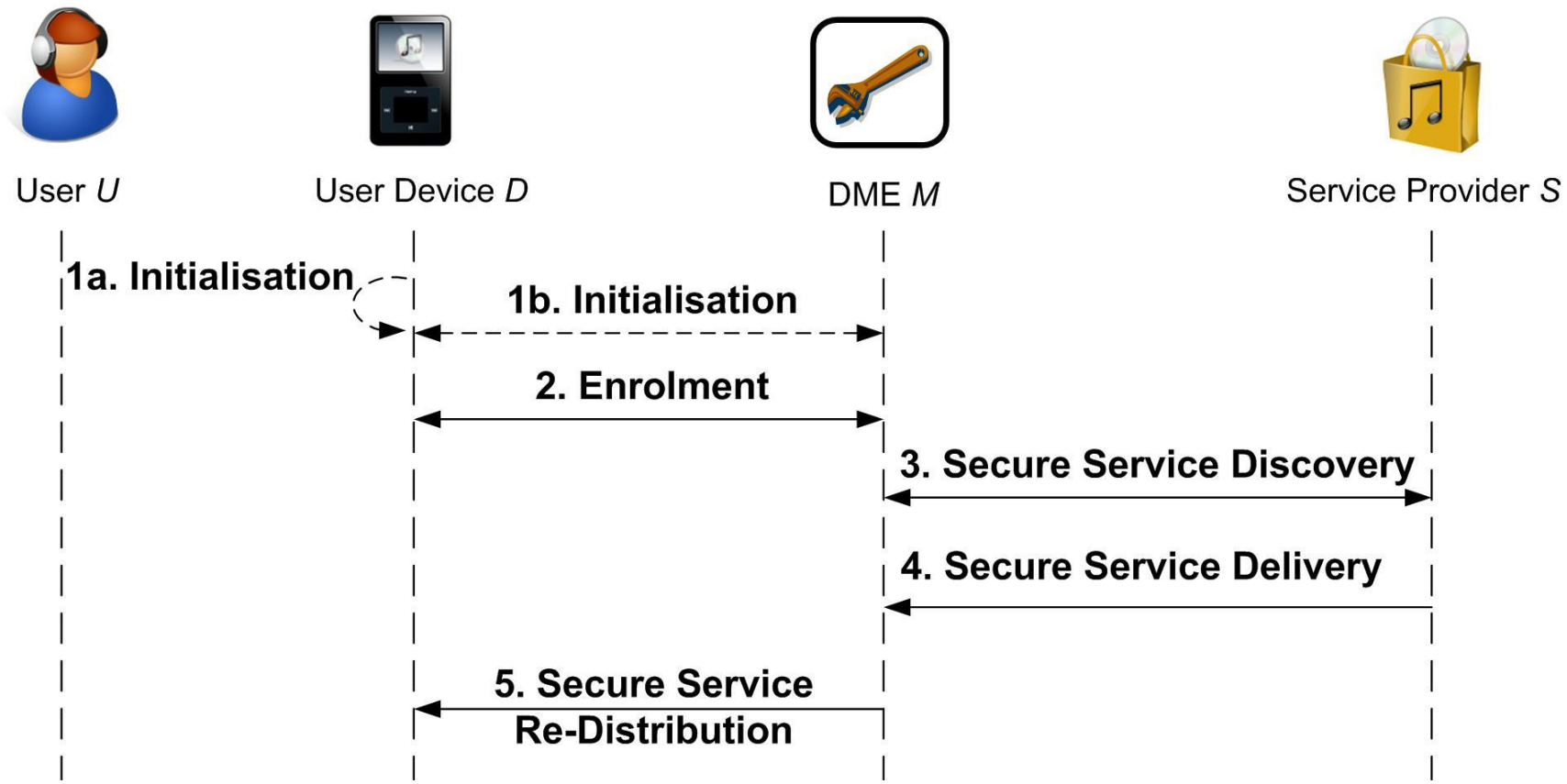
Agenda

- Motivation
- Security issues
- Building blocks
- A Secure Device Management Framework
- Analysis
- Conclusion

Assumptions

- User is in possession of:
  - a device to access service; and
  - a ‘local’ DME.
- User device and local DME are TCG-compliant trusted platforms.

SDMF: phases of operation



SDMF: initialisation

- Goals:
  - prepare device for use.
- Involved parties:
  - user, device and DME.
- Protocol:
  1. user authenticates to device;
  2. user instructs device and (local) DME to use MANA protocol to set up secret key and reliably transfer DME public key to device.

SDMF: enrolment

- Goals:
  - securely enrol device with DME.
  - device obtains DME's security credentials.
- Involved parties:
  - device and DME.
- Protocol:
  - uses session key from initialisation;
  - uses trusted computing attestation to prove current state of device to DME;
  - credentials bound to current device state (so that device can only access service when in trusted state).

SDMF: service discovery

- Goals:
  - enable service provider to securely advertise service, and DME to initiate access to service (on behalf of user device);
  - set up shared secret key between DME and service provider.
- Involved parties:
  - DME and service provider.
- Protocol:
  - uses Ninja protocol (based on DAA).

SDMF: service delivery

- Goals:
  - enable service provider to securely deliver services to DME.
- Involved parties:
  - DME and service provider.
- Protocol:
  - secure delivery uses keys established by Ninja.

SDMF: service redistribution

- Goals:
  - securely redistribute service from DME to user device.
- Involved parties:
  - DME and user device.
- Protocol:
  - uses keys established during enrolment.

Agenda

- Motivation
- Security Issues
- Building Blocks
- A Secure Device Management Framework
- Security Analysis
- Conclusion

Security analysis

- Framework provides:
  - user to device authentication;
  - device integrity assurance (using platform attestation);
  - service confidentiality;
  - service integrity;
  - prevention of unauthorised credential sharing.

Agenda

- Motivation
- Security Issues
- Building Blocks
- A Secure Device Management Framework
- Analysis
- Conclusion

Concluding remarks

- Have proposed a secure device management framework for secure service delivery.
- This framework:
  - uses trusted computing functionality;
  - integrates other security mechanisms;
  - meets the identified security requirements.

Contact details

- Adrian Leung and Chris Mitchell
  a.leung@rhul.ac.uk
  c.mitchell@rhul.ac.uk

- Information Security Group
  Royal Holloway, University of London
  www.isg.rhul.ac.uk