

---

# Identification, authentication and trust in a ubiquitous computing environment

Chris Mitchell

<http://www.isg.rhul.ac.uk/~cjm>

---

## This talk ...

- Introduces a range of problems, relating to identification and authentication, arising in a pervasive and mobile computing environment.
- Also sketches possible directions for solutions to some of the problems.

---

# Agenda

- **Background**
- Privacy issues
- Ad hoc relationship establishment
- Layering issues
- Key management
- Single sign-on
- Authentication and trusted computing

## Terminology (not necessarily universally agreed!)

- *Identification*: Learning a (claimed) identifier for an entity – may be a pseudonym.
- *Authentication*: Verifying that an entity does correctly possess a certain identifier.
- *Authorisation*: Checking that a particular entity has permission to access certain resources.  
**Requires authentication since permissions typically bound to an identifier.**

---

# Environment

- Ubiquitous computing environment ...
- For this talk this is assumed to mean an environment in which multiple devices, some personal, some mobile, combine to provide an all-pervasive computing and communications service to end-users.
- Requires automatic configuration of certain aspects of some devices, since it is assumed that there is no global management infrastructure.

# Requirements

- Mobile and fixed devices need to identify and authenticate one another.
- This needs to work in cases where there is no pre-existing relationship between the two devices.
- Techniques used must, where necessary, protect privacy of device owners, e.g. provide anonymity, prevent linking of transactions, ...

---

# Agenda

- Background
- Privacy issues
- Ad hoc relationship establishment
- Layering issues
- Key management
- Single sign-on
- Authentication and trusted computing

---

## Privacy background

- Many of the devices providing the ubiquitous environment will be personal devices; they may thus 'leak' personal information to each other.
- In a context where devices cannot be assumed to belong to a single trusted domain, there are thus major privacy issues.
- We review issues relating to identification/authentication.

# Interrogation of mobile devices

- Communications protocols for mobile devices inevitably require some form of routine ‘polling’.
- Responses to polls (e.g. from a network access point) need to contain some kind of identifier, e.g. a network address.
- Thus can be used to ‘track’ devices, and potentially track the location of device owners.
- Solutions? GSM/3GPP use temporary identifiers (pseudonyms) distributed in a way that prevents linking. Provide confidentiality protection for exchange.

## Use and abuse of authentication

- Authentication of a device can pose a denial of service threat.
- For example, if protocol requires one device to store state and/or do computations, repeated fake requests can cause memory/processing exhaustion.
- Solutions? Use stateless protocols. Require requester to do at least as much work as the responder.

## Location information use/privacy

- Service providers in a ubiquitous computing environments may wish to provide services based on user location, e.g. targeted advertising, emergency services, broadcast blackout, ...
- Owner of computing device may wish to restrict dissemination of such location info.
- How should this be controlled?
- Solutions? Anonymity (see also Frank Stajano's talk). Mandatory inclusion of policy data with location information. TTPs.

## Denial of Service versus privacy

- In any protocol it seems that one party has to reveal their identity first. This argues that (mostly) the requester of service should reveal their ID last. (P2P an exception?)
- However, this potentially increases the risk of Denial of Service attacks against the responder.
- Indeed, more generally, the tension between DoS-resistance and user privacy has been noted by a number of authors.
- Solutions? New ideas needed? (Also see last week's protocols workshop).

---

# Agenda

- Background
- Privacy issues
- **Ad hoc relationship establishment**
- Layering issues
- Key management
- Single sign-on
- Authentication and trusted computing

---

## General problem

- Previous talks at this workshop have noted issues in establishing as hoc working relationships.
- Initial trust setting is a major issue.
- We look at trust issues relating to identification and authentication.

---

## Automatic address assignment

- In an ad hoc network, newly admitted devices will typically need to be assigned a network address (or addresses).
- In the absence of a fixed infrastructure this is problematic.
- Solutions can easily lead to the possibility of denial of service attacks.
- Just one part of ‘zero-config’ problem.

---

# Agenda

- Background
- Privacy issues
- Ad hoc relationship establishment
- **Layering issues**
- Key management
- Single sign-on
- Authentication and trusted computing

## End-to-end versus point-to-point

- Need for security between service provider and service consumer argues for end-to-end authentication.
- Need for control of access to resources, e.g. network access, argues for point-to-point authentication.
- If both provided in ‘unlinked’ way then man-in-the-middle attacks can become possible.
- Great care needed in combining protocols at different levels in protocol hierarchy.

## Protocol statefulness

- As mentioned previously, protocol state can be used as a means of launching DoS attacks.
- ‘Accepted wisdom’ is to require protocols to be stateless, at least for responder.
- However, there is an efficiency cost (state must be shipped in protocol messages). It also either requires synchronised clocks or regular key changes (a bit like state).

---

# Agenda

- Background
- Privacy issues
- Ad hoc relationship establishment
- Layering issues
- **Key management**
- Single sign-on
- Authentication and trusted computing

## Background

- Authentication requires either shared secret keys (using symmetric crypto) or trusted copies of public keys (using asymmetric crypto).
- Shared secrets can be set up via a mutually trusted TTP.
- Public keys can be obtained via public key certificates, although trusted means to verify certificates (CA public keys) required.

# Heterogeneous networks

- The pair of devices may not share an online TTP (or even share 'trust-connected' TTPs).
- Public key crypto (and PKI) looks more promising, but it is still necessary to have mutually verifiable certificates. Finding certification paths could be infeasibly complex for a bandwidth-limited device.
- Solutions? Delegated Path Discovery/Delegated Path Validation.

## PKI interoperability

- Finding a certification path is by no means only problem with using PKI.
- Certificates issued by different CAs (with different policies) may ‘mean’ different things – e.g. different liability protection, different ID checking for certificate issue, etc.
- Certificate status management systems may vary.

## ID-based cryptography

- One possible solution to key management problems is used of ID-based crypto.
- Here a user public key is derivable from a user identifier (possibly plus other data).
- Requires TTP to issue private keys (and TTP public parameters to derive public key from ID).
- Hence we have major interoperation issues if two devices served by different TTPs. Only now being addressed.

---

# Agenda

- Background
- Privacy issues
- Ad hoc relationship establishment
- Layering issues
- Key management
- **Single sign-on**
- Authentication and trusted computing

# Background

- Desire for an Internet single sign-on solution.
- That is, instead of a user authenticating him/herself to multiple service providers (SPs), the user authenticates him/herself to an Identity Provider who then provides assurances (*assertions*) regarding the user identity to SPs.
- This requirement becomes even more important in a ubiquitous environment, where a user will not wish to authenticate him/herself to every device/service.

---

## Microsoft Passport

- (Originally) a proprietary SSO solution, which also (originally) involved the possibility of managing other personal data, all stored on a server somewhere ...
- Problems with guardians of end-user privacy, including European Commission.
- MS appears to be moving towards a Web Services based solution.

## Liberty Alliance

- Consortium set up to provide an open system (protocol suite) to support SSO.
- Provides variety of alternative means of transferring assertions from IP to SP.
- E.g. using SOAP, web redirection.
- Possible problems, as with any scheme using web redirection, if man-in-the-middle attacks.

---

## WS Federation

- Part of Web Services Security.
- Covers federation of identifiers, and also allowed 'brokering' of identity/authentication services.
- Would appear that it can be used as the basis of an SSO scheme.

---

# Agenda

- Background
- Privacy issues
- Ad hoc relationship establishment
- Layering issues
- Key management
- Single sign-on
- **Authentication and trusted computing**

# On trusted computing I

- Many parallel and related developments:
  - TCPA/TCG
  - Palladium/NGSCB
  - La Grande technology
  - Perseus, ...
- All seek to provide a ‘trusted computing environment’ within a device, in which external parties can verify that interactions are taking place with a particular piece of code, and that data will only be available to this code.

## On trusted computing II

- It seems plausible that such technology – some proprietary, some standards conformant – will be included in most future computing devices (PDAs, notebooks, phones, ...)
- Many applications for such technology have been proposed, most controversially for DRM.
- We consider how it might be used to address identification/authentication issues in a ubiquitous computing environment.

## What can we use it for?

- Possible applications relating to identification/authentication include:
  - single sign-on (SSO) implemented on a mobile/personal computing platform;
  - control of transfer and use of personal/contextual information;
  - verification of correct (unselfish) performance of a protocol requiring co-operation, e.g. for MANET routing.

## TC-based single sign-on

- SSO typically requires an external TTP to act as the Identity Provider (IP).
- Why not use TC component to act as the IP, which authenticates the user once, and then asserts that user is present to other devices?
- Why should other devices believe assertions – well, by checking out the TC component, and knowing that the program making the assertion is not compromised.

## TC-based personal information control

- One partial solution to the problem of controlling personal information (PI) e.g. location info, is by attaching policy info.
- However, such a system needs enforcement.
- Of course, part of that is regulation.
- However, TC can help – that is, if the intended destination for PI is a TC-platform, the holder of PI can potentially verify the software to which it may be passing PI (indeed, it might be obliged to!).

## TC-based co-operation enforcement

- The support of MANETs typically requires co-operation by the nodes, e.g. to support routing.
- As discussed previously in the workshop, malicious users may replace their network software with a 'selfish' version, e.g. to save battery power.
- TC could help guarantee that a network element is running the 'correct' software, and hence will not behave selfishly.
- (Of course, this requires the communications hardware to be part of the TC subsystem.)

## TC-based type approval

- The spread of computers everywhere (cars, fridges, toasters, ...) gives rise to major problems regarding safety.
- For example, a car owner could replace the engine management software to radically increase engine power.
- Not only will this potentially wreck the engine, it may also be a major safety problem, since the brakes/suspension won't match performance.
- Traditional solution is a closed environment which will only run authorised software – however the trend is to open platforms everywhere, and TC may help give back control.