MIT Crypto Card, Progress Presentation

Chris Laas

November 30, 2000

`$Id: handout.tex,v 1.1 2000/11/30 23:19:36 golem Exp $`

1 Purpose of the project

- The MIT Crypto Card project will develop a successor to the MIT Card which, using modern cryptographic techniques which were not available to the designers of the original MIT Card, will provide authorization functionality to the MIT campus without compromising the security or privacy of the card users.
- The new Card will serve as identification, authorize access to reader-equipped doors on campus, and mediate small "pocket change" cash transfers.
- The system will include the following elements:
  - Microcontroller-based portable "MIT Card" tokens.
  - A set of trusted authentication servers, or CAs (Certificate Authorities).
  - A network of vendor terminals, authentication terminals, and interface terminals.

2 What we've done so far

- Literature review (CAFE, secure cash, group identification protocols)
- Extensive documentation of system requirements:
  - Identification, group authorization, pocket change, administration

- Scaling requirements
- Management and administration — decentralization of control, data quality, data privacy policies

- Evaluated hardware:
  - Several smart cards (e.g. Gemplus): the market is rather homogeneous.
  - iKey: advantage is form factor, compatibility, and LED; disadvantage is reliability (sturdiness)
  - Gemplus CAFE token: Gemplus never turned them into a real product, but perhaps could be convinced to make a new prototype.
  - PDAs: Still too expensive. Give it a few years?

- Protocol and system design:
  - Identification protocols
    * Researched options; will take one that works "out of the box."
    * Fiat-Shamir is current default.
    * Modular "pluggable" part of system.
  - Cash protocols
    * Researched options; there is a great variety.
    * Will choose a conservative, but flexible design.
    * This module is a low priority — authentication comes first.
  - Group authorization protocols
    * Researched existing protocols — none provide anonymity and revocation.
    * Designed a new system and set of protocols.
      · Heavily based on Ohta, Okamoto, and Koyama's system [OOK90], which is heavily based on Chick and Tavares's system [CT89]. A few minor changes to support anonymity were made, and a system to provide revocation functionality was built on top of it.
      · Security rests on the RSA assumption.
  - CA and key management protocols

        * Resilient and simple certificate management hierarchy, based on standard models.

- Results of independent interest:
  - New privacy-preserving practical group authorization protocols.
  - Formulation of the problem of "identity escrow".

3 Plans for the immediate future

- Hire someone! Talent with free time is hard to find and retain.
- IAP: Concretize the protocols in preparation for review.
- End of IAP: Submit protocols for review.
- Spring: Begin software prototypes.
- **Where have the plans changed?**
  - We are taking a much more conservative view of hardware than we initially envisioned. Given budget constraints, we will have to work with some primarily off-the-shelf system; this also means that the technology we will have available is less predictable. Hence, the protocols we design have more of an emphasis on technology agnosticism. In addition, there is more of an emphasis on flexibility, as we cannot predict what will be the best platform options in a decade.

4 Long term plans

- Hire someone!
  - In general, increase the size of the core group. Must find good systems programmers and good network programmers.
  - Also, work on increasing the budget. Budget will have a direct effect on ability to hire talent.
- Technical plans
  - (ongoing) Keep an eye on hardware developments.

      * consider likely technology developments: e.g. pan-campus wireless Ethernet coverage, advanced PDAs, more embedded computation.
  - Finish software prototypes.
  - Audit software.
  - Port software to hardware embodiments.
  - Set up a demo cluster.

- Documentation
  - Write design documentation, technical specs, and manuals for the modules of the system.
  - Document operations of the system, including contingency plans.