# Class Discussions: Adding Security to our App-layer Protocol

## Monday, October 16, 2017

Discussed the first seven security design principles: Economy of mechanism, Fail-safe defaults, Complete mediation, Open design, Separation of privilege, Least privilege, and Least common mechanism.

### Authentication

* 23-digit machine ID
  + Is this stored in plaintext in the machine?
  + How does HQ store these machine ID values?
* Each vending machine will have a unique IP address.
  + Company will have a range of valid IP addresses that is uses.
* Digital signature (uses public-private key pair)

|  |  |
| --- | --- |
| Client (HQ) | Server (a vending machine) |
| * Use a digital vault to store the private key used for digital signatures. (We may decide that this is outside our project scope.) | * Stores the public key used for digital signatures. This public key can be stored in plaintext on each machine. |
| * Do authentication on both sides, i.e.:   + Have client authenticate to server.   + Have server authenticate to client. | |
| * After authentication is verified, have client and server agree to a secret key to be used during this session. That is:   + We will use symmetric encryption on all of the protocol data. | |

### Items that are likely out-of-scope (but important to think about if we care about end-to-end security!)

* Who is allowed to run the client-side application at HQ?
* How many clients can run concurrently?
* Once client gets machine data, what happens to this data? Does HQ persistently store the machine data in a database? What security mechanisms should we use when storing this data persistently?

## Wednesday, October 18, 2017

Discussed the last eight security design principles: Psychological acceptability, Work factor, Compromise recording, Secure the weakest link, Defend in depth, Be reluctant to trust, Promote privacy, and Use your resources.

* Record (or log) protocol events as they occur.
* Analyze entire system associated with protocol to determine whether any areas need to have their security improved.
* Possibly use different cryptographic algorithms and keys for different parts of the system.