Network Authentication

What problems do you see here?

Network Authentication Security

We can enhance the previous model by adding encryption. This is done as follows:

- client connects
- server sends cert
- client encrypts message using public key, sends to server
- server decrypts message using private key

Difficult to break private key

Related info

- Cert? Contains an entities public key. Could contain 3rd party verification.
- Keys?
- Examples?
  - ssh
  - https
  - ftps
  - imaps

More stuff

- TLS: Transport layer security
  - tcp socket is fully encrypted at transport layer
- StartTLS
  - socket began as normal TCP, but now requesting encryption using TLS
- Clear
  - Plaintext/no encryption
