CSE 543 - Computer Security

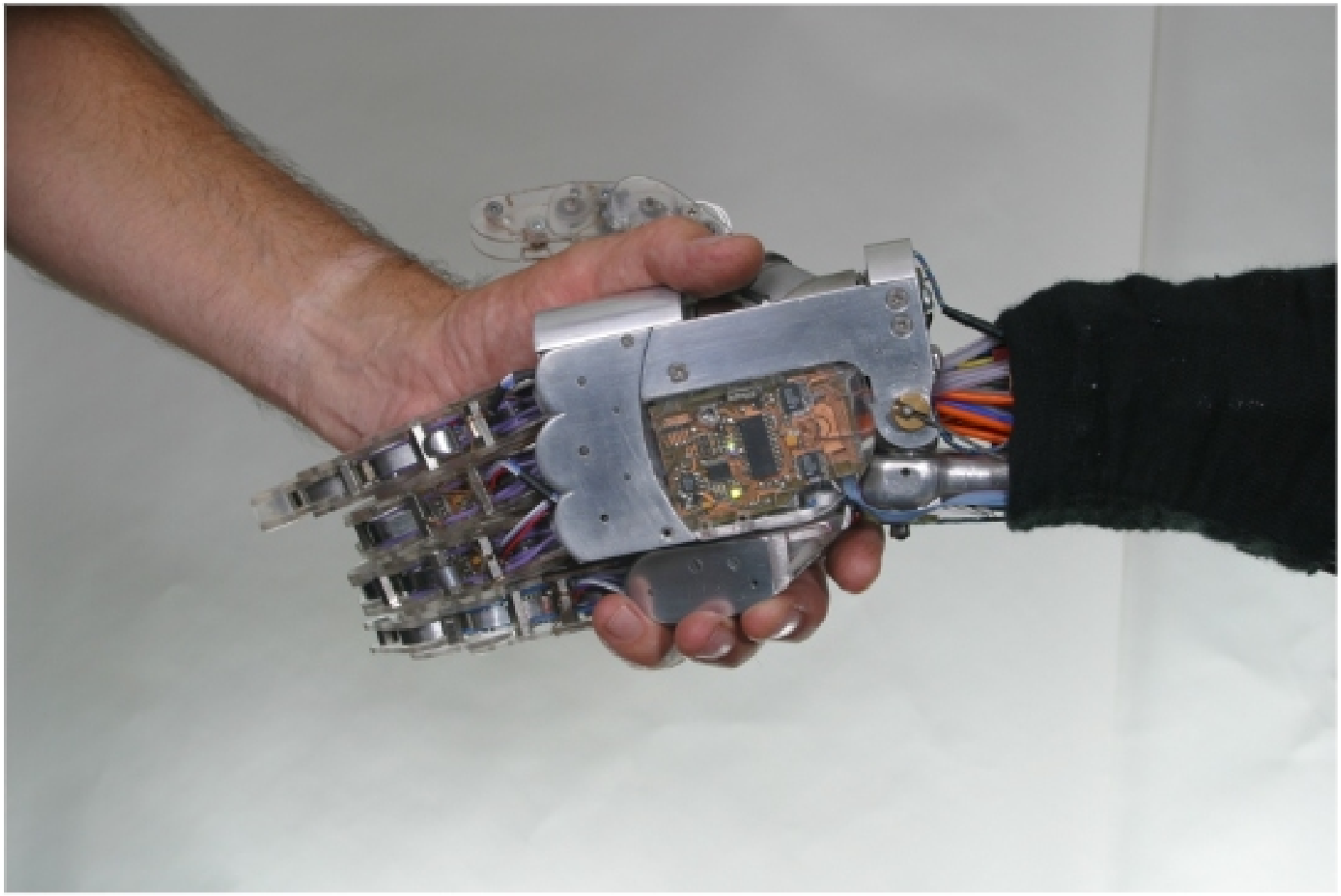
Lecture 8 - PKI

September 20, 2007

URL: http://www.cse.psu.edu/~tjaeger/cse543-f07/

Meeting Someone New

- Anywhere in the Internet



Public Key Infrastructure

- System to "securely distribute public keys"
  - Q: Why is that hard?

- Terminology:
  - Alice signs a certificate for Bob's name and key
    - Alice is **issuer,** and Bob is **subject**
  - Alice wants to find a path to Bob's key
    - Alice is **verifier,**and Bob is **target**
  - Anything that has a public key is a **principal**
  - Anything trusted to sign certificates is a **trust anchor**
    - Its certificate is a **root certificate**