Part I: Classic Authentication

- passwords
- SSL/TLS ...
- Kerberos
- ssh ...
- PGP ...
SSL/TLS

- CA – Certificate Authority
- (RA – Registration Authority)
- Certificate Storage
- Key Management
ssh

- PKC – DSA/RSA
- No CA
- Diffie-Hellman
- Binary Trust
  - your pub key is in .ssh/authorized_keys2
  - or it isn’t…
- (Kerberos)
PGP/GnuPG

• DSA and ElGamal*
• (RSA for signing only)
• Key Management
• Audrey Tang – 0x3C3501A0
• Web of Trust:
  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately

http://pgp.mit.edu/
Part II: Id-Based PKI

• No more CA (TA)
  – public key is generated from Id
  – signature verification also from Id
  – private key generated by TA
  – public key before private key

• repudiable? (PKC, IBE) – Bohen/Franklin
  – Authenticated-Encrypt(M,d_a,B) = Authenticated-Encrypt(M,d_b,A)
  – many public keys
Problems with Id-Based PKI

• Revocation
  – How do you revoke an Id?
  – Build in the date!
  – Ask the TA for your Key every day…

• ID Dups
  – Suppose two John Smiths
  – (suppose one has left…)
  – big database (CA?)

[1]
Part III: Authentication in Oppnets

- OpenVPN / SPKI / SDSI
  - local trust
  - local CAs
    - police
    - fire
    - DHS
- Web of Trust – [b,d,u]
References


In case any of these are hard to find, go here:
http://voltar.org/cs691/
http://cs691:in691@voltar.org/cs691/