Ten Risks of PKI:
What You're not Being Told about Public Key Infrastructure

Joshua Schiffman
Archana Viswanath

Computer Security

PENNSTATE

- Security is a business
  - Especially PKI
- PKI needs business to thrive
  - Buy certificates
  - PKI equipment
- Certificates are the commodity
  - How trustworthy are they?

Categories of Risk

PENNSTATE

- Security is a chain
  - Only as strong as the weakest link
- We identify three main categories for risk
  - Trust in the Certification Authority (CA)
  - Trust in the encryption keys
  - Trust in the users