Graduate Course on **Computer Security**

Lecture 10: Beyond Authentication

Iliano Cervesato `iliano@itd.nrl.navy.mil`

ITT Industries, Inc @ NRL - Washington DC

http://www.cs.stanford.edu/~iliano/

Outline

- Zero-knowledge proofs
- Fair exchange
- Anonymity
- Privacy
- Group protocols
- Denial of service
- …

Readings

Exercises for Lecture 10

Final Exam

PGP is a simple but effective encryption algorithm

- Describe PGP
  - Purpose
  - Encryption and signature algorithms
  - Known vulnerabilities
- Send me your report at `iliano@itd.nrl.navy.mil`
  - Up to 5 pages ASCII
  - Encrypted using PGP
    - Set up PGP under your account
    - My PGP key is …

... my PGP Public Key

```
-----BEGIN PGP MESSAGE-----
Version: 2.6.3in

iQCVAwUAPAvlsZHtY5veG61TAQGBLQP+LoF906j3EdQ892u3nmBt4GmE2qTgIpBc
zLHZoFI1SGlOy/JqLSWC/QCWIJhr4Br/v/te0KnkQQN0DnZ4NIsY7kOg3EBlG0zE
2mmzsJq6oCeBjS66zTpX4aFPQ0PgP7D/Y4XD1qfhDZP0Z2VZgZqy6SRCkpVDFS4c
7lO1mQ752seZAI0DPAveWQAAAQQA2ICEOi3Wh/evDvQDp+40W8lBFp9ild3CLb2b
lnonlRJWADLgtOJGXM1p82fgjhgUG5cPrMxpvq6J5YqwpGNhEnXJ6sFbuFM23YTn
L/ILMD1BnDoCZuILNeeQ6WjldU5c7/F/rO0kXaj1nk2rbWnAYk+DiHQLgh+Fke1j
m94brVMABRGwAYe0KklsaWFubyBDZXJ2ZXNhdG8gPGlsaWFub0BpdGQubnJsLm5h
dnkubWlsPrABA4kAlQMFEDwL3r+R7WOb3hutUwEBGQ0D/1TjPHEFdpzVXvhU3iO/
EDTCXih+Dh1V5yPKQP1gXshUaSM786y8Hv8iCN3bHAEI8ldugQ8+cwWpERYZcP5s
PDsFU9ZA5gBQbb5eiRjpss8h9zKAObtqMoTZ+WXcROtkfH3kdjAcAI/HGmjxvplx
LloFEb7lG1COlMYdgIUGduNusAHH
=DbxM
-----END PGP MESSAGE-----
```

The end

http://www.cs.stanford.edu/~iliano/