ECE 435 – Network Engineering
Lecture 22

Vince Weaver

http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

28 November 2016

Announcements

- HW#9 was posted
- Projects

RSA example

Run through the RSA prime number example from last lecture.

ssh security

- Fail2ban
- Nonstandard port
- Port knocking
- Call asterisk for one-time pin?
- No-password (key only)
- LCD device

encryption problems

- Keys leaked (DVD/game console issues)
- poor random numbers used (debian problem)
- differential cryptanalysis (start with similar plaintexts and see what patterns occur in output) [DES IBM/NSA story]
- Power/Timing analysis – note power usage or timing/cache/cycles when encryption going on, can leak info on key or algorithm

Other common protocols we won’t cover

- Legacy (inetd): echo, chargen, discard, time, finger (.profile, .plan), qotd, systat, write, talk
  why no longer supported? security? lack of interest?
- Messaging:
  - IRC – internet relay chat
  - AIM/ICQ/MSN etc
  - unix talk/write
  - MUDs, talkers
- IPP – printer protocol (CUPS, lpd, jetdirect)

- backup software
- syslog
- telephony
  - skype
  - facetime
  - VOIP
  - ASTERISK
- ntp – network time protocol
- LDAP/Authentication
- Network Attached Storage/Fileservers
  - NFS

  - Samba/CIFS
  - andrewfs (afs)
- Databases: mysql
- Distributed/Torrent sites
- Distributed computing (SETI@Home)