CMPUT 333

SECURITY IN A NETWORKED WORLD

Lab Assignment 1

Block cipher modes of operation

Part 3

- **Encryption command:**
  "openssl enc -e -des-XYZ -nosalt -in plaintext -out cipherXYZ.enc"
- **You can use the 'xxd' command, when you need to replace the 19th byte with a different byte.**
- **Make sure to explain the reasons for your observations**
- **For information about the different block cipher modes you can check Wikipedia:**

  https://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

PASSWORD CRACKING

John the Ripper

Steps

1. **Download John the Ripper**
   - http://www.openwall.com/john/j/john-1.8.0.tar.gz
2. **Extract the file on your Desktop**
   - tar –xzf john-1.8.0.tar.gz
3. **Compile the source file as follows:**
   - Navigate to the extracted folder ‘john-1.8.0’
   - Navigate to src/
   - Enter the command “make linux-x86-64”
4. **A ‘john’ executable will be created in the ‘../john-1.8.0/run’ directory**
5. **You can test that it works by navigating in the directory mentioned in step 4 through your console and by entering**
   - ./john --test

PASSWORD CRACKING

Documentation

- doc/README – general information
- doc/EXAMPLES – usage examples
- doc/MODES – the different cracking modes
- doc/RULES – wordlist mangling rules

PASSWORD CRACKING

John the Ripper

Wordlist mode

- Given a list of words, will try each of them
- Mangling rules: allows applying various transformations to the words in the list
  - Specified in 'john.conf' in the run folder
  - Documentation in doc/RULES
  - You can also produce customized wordlist using your own code
- doc/MODES for more details

PASSWORD CRACKING

John the Ripper

Single crack mode

- Will use information in the password list
  - Usernames, real names, etc.
- Will apply a variety of mangling rules
  - Specified in 'john.conf'
  - Documentation in doc/RULES
- See doc/MODES for more details

PASSWORD CRACKING

John the Ripper

Incremental mode

- Brute force mode
- Can be used if nothing else works
- Can specify min/max length and character set in john.conf
- doc/MODES for more details

PASSWORD CRACKING

Tips

- Read the documentation of the different modes in order to decide which ones can help you the most
  - Also check doc/EXAMPLES
- You can run John the Ripper in the background
  - Check the “screen” command
  - Read about sessions in John the Ripper
- You MUST only use your assigned machine for cracking
- Make sure you describe everything you do in the assignment report
- Make sure you check the forum for hints

QUESTIONS?