### This Time
- RFCs
- review
- course evaluations

### RFC
- universality assured by requirement that entire text be in ASCII
- diagrams done in ASCII—art:

```plaintext
+----------+                +----------+
+------+    |          |                |          |
| User |<-->|          |      SMTP      |          |
+------+    |  Client- |Commands/Replies| Server- |
| File |<-->|          |    and Mail    |          |<-->| File |
| System|    |          |                |          |    |System|
+------+

SMTP client                SMTP server

from: rfc282 “Simple Mail Transfer Protocol”
```

### RFC
- result of extensive review process
- document first submitted as ‘internet-draft-xxxx’
**RFC 3751: Omniscience Protocol**

A new IETF protocol to stem piracy and aid law enforcement

- problem addressed: copyright infringement
  - proposed action: remotely destroy computers of those who illegally download copyrighted material
    - e.g., Senator Orin Hatch (R-Utah)
    - need to identify users whose *intent* when copying a file is to infringe copyright
  - different problem than RFC3514 addressed
    - there, concern was action packet performed
    - here (3751), state of user
    - can be applied to other criminal activity
      - e.g., plagiarism

**OP: Implementation Model**

- client installed on users’ machines
- server runs on computer at:
  - law enforcement agency
  - copyright enforcement agency
- clients may be distributed/diffused using p2p model

**OP: Terminology**

- evil-doer: ≥ 1 individuals who perform acts that OP server operator has legally recognized right to prevent
- good-guy: ≥ 1 individuals who have legally recognized right to prevent certain acts that users may attempt to perform with their computers

**OP Operational Requirements**

1. client must be able to install itself on any platform irrespective of user attempts to prevent it
   - all new computers will come with
   - old computers have to be updated to include it
2. genuine OP clients must be unfindable by any means, but non–genuine must be findable
   - needed to prevent bona fide OP client from being disabled
3. OP client must be able to communicate:
   - through fire-walls
   - through NAT boxes
   - when disconnected from network
     - may require client to have ability to reconfigure user’s machine into cell phone or support GMPLS-WH
4. neither server nor client can be spoofed
   - so evil-doers cannot misrepresent to server
   - so evil-doers cannot access other users’ private info by appearing as a server
   - server authorization must be possible with no prior knowledge on part of client
**OP Operational Requirements**

5. client must be installable on any device able to play/render copyrighted material
   - e.g., mp3 players

**OP Functional Requirements**

1. client must be able to determine user’s intent
   - must correctly distinguish legally-obtained from illegally-obtained copyrighted material
   - must correctly distinguish between legitimate back-up copies and copies made for trafficking
   - must be able to determine user’s purpose for some software
   - e.g., security-defeating software is illegal under DMCA
   - e.g. crypt-analysis software

2. client must differentiate files of same name w.r.t. copyrighted material
   - must not confuse a file on a remote site that is copyrighted protected with a user’s file which is not protected

3. client must identify illegal copies even if name is different

4. client must identify illegal copies even if user has modified it
   - irrespective of user’s modification, client must identify it as the original protected work, subject to legal definition of ‘same’ or different

**OP Functional Requirements**

5. client must not be accessible to be run or exploited by any evil-doer/hacker
   - since has total access privileges, is attractive target

6. server must not run if operator’s motives are impure
   - client must be able to refuse server interaction if server’s actions are motivated by evil-doer at server site

7. client cannot be exploited to provide information unrelated to protected material
   - so as not to infringe on user’s privacy and legitimately held data

**OP Functional Requirements**

8. client must distinguish provenance of protected material
   - illegal material not placed by user on computer cannot falsely incriminate user, even if that third-party used the user’s login name and password

9. client must only implement laws relevant to its current physical location
   - must know its own location and that of its server (to know if in same jurisdiction)

**The April RFCs**

RFC 3751 joins a well established family of revolutionary and groundbreaking standards and protocol RFCs, including:
- 3514 “Security Flag in the IPv4 Header”
- 3251 “Electricity Over IP”
- 2324 “Hyper Text Coffee Pot Control Protocol”
## Basic Network Technology

- **network technology:**
  - transmission media and characteristics
  - wire, fibre, wireless (IR, microwave, satellite)
  - switches, bridges
  - network layer protocols + routing
  - major IP transport protocols
  - unicast, multicast

## Internet Servers & Services

- boot time services: BOOTP, DHCP, RARP
- DNS
- SMTP, POP, IMAP
- RTP, SIP, H.323; VoIP as example service
- Web: HTTP, HTML, CGI, Java Applets, Javascript, XML
- RSS

## Server details

- processes and threads
- data:
  - formats and encodings
  - compression
- client-server dialogue models
  - e.g., SMTP
- sockets programming
- middleware: its role, some varieties of
- platform issues

## Technologies

- wireless
  - Bluetooth
  - 802.11x
- agents, service discovery
- RFID and some sample applications
- Jini

## Security Considerations

- some concepts
- encryption
  - symmetric key, e.g., 3DES
  - public key, e.g., RSA
- certificates
- IPsec
- private networks: combining several ideas
- 'malware': what to defend against

## Lab Exercises

- ping and traceroute
- DNS
- security: SSL & use of tcpdump
<table>
<thead>
<tr>
<th>Protocols</th>
<th>Major RFCs Cited</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>791, 1991, 3376</td>
</tr>
<tr>
<td>ICMP</td>
<td>793, 2045–2049, 3411–3418</td>
</tr>
<tr>
<td>IP</td>
<td>821, 2141, 3501</td>
</tr>
<tr>
<td>OSPF</td>
<td>822, 2328, 3514</td>
</tr>
<tr>
<td>RIP</td>
<td>951, 2440, 3550</td>
</tr>
<tr>
<td>DHCP</td>
<td>1521, 2453, 3751</td>
</tr>
<tr>
<td>SMTP</td>
<td>1522, 2821</td>
</tr>
<tr>
<td></td>
<td>1939, 2827</td>
</tr>
</tbody>
</table>

**Exam Tips**

- Make sure you answer the question that was asked
  - Including any sub-parts of questions: get them all
- Make sure your answer says what you intend it to say
  - And not what you don’t want it to say
- Don’t write more than you need to answer
- Do questions worth the most points first
- Always put units on any result where appropriate
- Use units in equations to ensure solution is right
- Your answer is judged only and entirely by what you write: make it count...we’re not mind readers