Leksioni 4

Frida GJERMENI
Sistemet e Postes Elektronike

Protokolli MIME

- MIME Compliant Mailer

– **MIME Compliant Mailer**

MIME eliminon perdorimin e utiliteteve uuencode/uudecode. Me ane te MIME, procesi i dergimit te skedareve binare me ane te emailit eshte transparent dhe perdoruesit mund te ndjekin cdo hap te procesit pasi te percaktojne dhe perzgjedhin skedarin/skedaret nepermjet email klientit ose webmail. Keta te fundit kane pergjegjesi per procesin.

- Standartet specifikohen nga RFC 1521 dhe RFC 1522
- MIME eliminon perdorimin e uuencode/uudecode
- Mesazhi elektronik (Email) ndahet automatikisht ne pjese ku secila identifikohet nga tipi i permbajtjes (content type) specifik pra tipi i te dhenave qe permban. Shembuj: Content-type: image/gif, Content-type: text/html
- Keto content types perdoren nga HTTP serverat per te pershkruar permbatjen e faqeve web qe do te shfaqen ne web browser
- Kur MIME perdoret nga email klientet, keta te fundit i konvertojne skedaret binare ne nje format teksti duke perdorur kodimin me baze 64, i cili ndryshon nga uuencode
- MIME u lejon email klienteve te perdorin bashkesi karakteresh te shumellojshme duke plotesuar kerkesat e perdoruesve per te derguar te dhena te tipeve dhe formative te ndryshme
- Disa email kliente qe perdorin MIME: Pine, Outlook Express, Netscape, Microsoft Outlook, Eudora

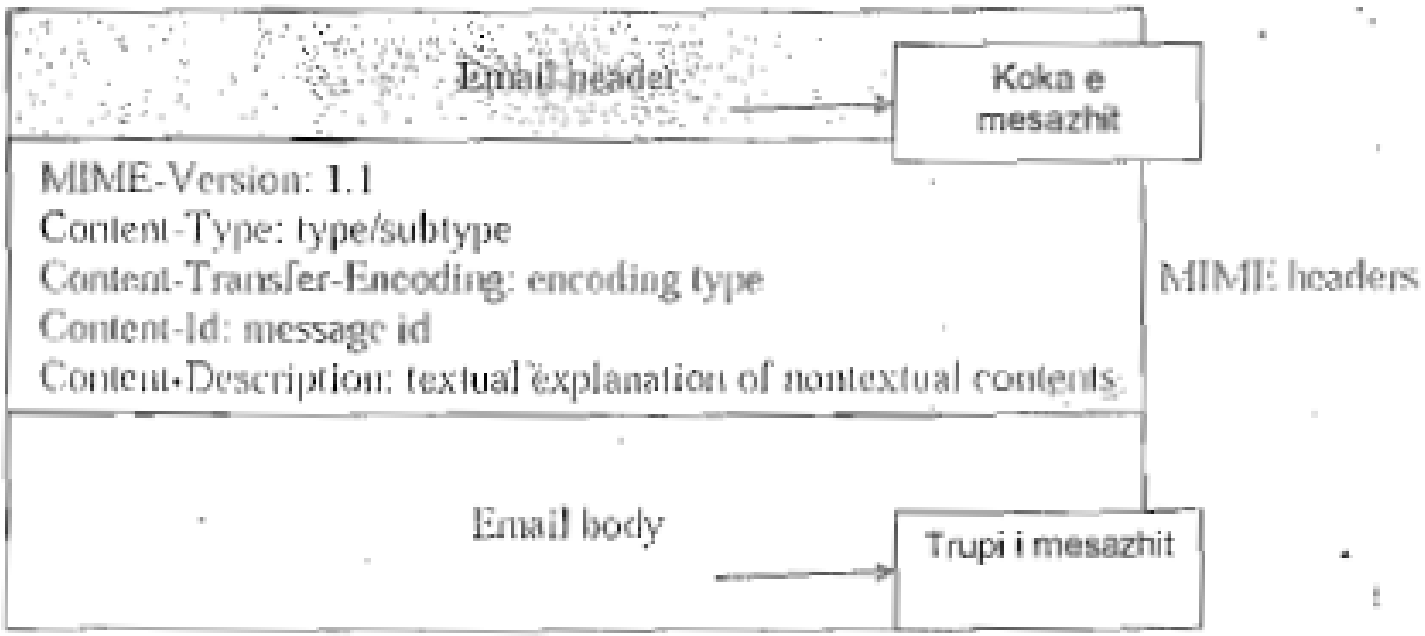
Skema e kodimit dhe transferimit te mesazhit elektronik

Hapat e kodimit dhe transferimit te mesazhit elektronik (perfshire edhe skedaret binare):

1. Email Klient 1 -> MIME (Skedar Binar)
2. MIME -> MTA 1 (Konvertuar ne 7-bit NVT Ascii)
3. MTA 1 -> MTA 2 (Transferohet si 7-bit NVT Ascii)
4. MTA 2 -> MIME (Transferohet si 7-bit NVT Ascii)
5. MIME -> Email Klient 2 (Konvertohet ne skedar binar)

Mesazhi elektronik ndahet ne 3 pjese gjate procesit te kodimit dhe me pas keto dergohen.

MIME Headers shfaqen pas kokes se mesazhit dhe paraprijne trupin e mesazhit. Ato japin informacion rreth: Versionit te perdorur te MIME, tipit/nentipit te te dhenave, tipi i kodimit te perdorur, id e mesazhit, pershkrimi i permbajtjes jotekstuale. Fjalet kyce te perdorura ne MIME Headers do t'i shqyrtojme ne vijim. Filimisht le te shohim tipet dhe nentipet e te dhenave te perdorura per percaktimin e content type-ve. Tabelat ne vazhdim japin nje pershkrim te detajuar.


Email header
Koka e mesazhit
MIME-Version: 1.1
Content-Type: type/subtype
Content-Transfer-Encoding: encoding type
Content-Id: message id
Content-Description: textual explanation of nontextual contents
MIME headers
Email body
Trupi i mesazhit

```
MIME-Version: 1.0

Content-ID: <5.31.32252.1057009685@server01.example.net>

Content-Type: text/plain

Content-Disposition: attachment; filename=genome.jpeg;
modification-date="Wed, 12 Feb 1997 16:29:51 -0500";
```

Figura 26 – Mesazh MIME

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="frontier"

This is a message with multiple parts in MIME format.
--frontier
Content-Type: text/plain

This is the body of the message.
--frontier
Content-Type: application/octet-stream
Content-Transfer-Encoding: base64

PGh0bWw+CiAgPGhlYWQ+CiAgPC9oZWFkPgogIDxib2R5PgogICAgPHA+VGhpcyBpcyB0aG
Ug
Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+Cg==
--frontier--
```

Figura 27 – Mesazh MIME Multipart

Kodimi i permbajtjes qe do te transferohet

- Kodimet e pershtatshme per t'u perdorur me protokollin e zakonshem SMTP:
  - **7bit** – Lejohen deri ne 998 oktete per cdo mesht, kodet e karaktereve te perdorura bejne pjese ne intervalin 1..127; karakteret CR dhe LF (perkatesisht me kodet 13 dhe 10) mund te shfaqen vetem ne fund te nje rreshti qe permban CRLF. Kjo eshte vlera e paracaktuar.
  - **quoted-printable** – Perdorur per te koduar sekuencat arbitrare te okteteve ne nje forme qe kenaq rregullat e kodimit 7bit. Dizenjuar te jete efikase dhe e lexueshme nga njerezit ne me se shumti, kur perdoret per te dhenat tekst te perbera kryesisht nga karaktere te bashkesise US-ASCII, por gjithashtu permban nje perqindje te vogel *bytesh* me vlera jashte kesaj bashkesie.
  - **base64** – Perdorur per te koduar sekuencat arbitrare te okteteve ne nje forme qe kenaq rregullat e kodimit 7bit. Dizenjuar te jete efikase per te dhena jo-tekst 8 bit-eshe. Ndonjehere perdoret per te dhenat tekst qe shpesh perdor karakteret jo US-ASCII.
- Kodimet e pershtatshme per t'u perdorur me protokollin SMTP qe suporton ekstensionin *8BITMIME SMTP*:
  - **8bit** – Lejohen deri ne 998 oktete per cdo mesht, kodet e karaktereve te perdorura bejne pjese ne intervalin 1..127; karakteret CR dhe LF (perkatesisht me kodet 13 dhe 10) mund te shfaqen vetem ne fund te nje rreshti qe permban CRLF.
- Kodimet e pershtatshme per t'u perdorur me protokollin SMTP qe suporton ekstensionin *BINARYMIME SMTP*:
  - **binary** – Per cdo sekuence oktetesh.

Protokolli PEM dhe S/MIME

- **PEM** (*Privacy Enhanced Mail*) eshte nje protokoll qe perdoret per shifrimin, autentifikimin dhe integritetin e mesazheve elektronike te tipit teksti.
- **S/MIME** (**Secure/ Multipurpose Internet Mail Extensions**): Versioni hibrid i protokollit MIME. Ai mbart edhe karakteristika te protokollit PEM.

Struktura e protokollit PEM

-----BEGIN PRIVACY ENHANCED MESSAGE-----
...<data>...
-----END PRIVACY ENHANCED MESSAGE-----

1. Te dhena te **zakonshme**, te **pakoduara** (Ordinary, unsecured data)
2. Te dhena te pandryshuara me integritet ose **MIC-CLEAR** (Integrity protected unmodified data)
3. Te dhena te koduara me integritet ose **MIC-ONLY** (Integrity-proteced encoded data)
4. Te dhena te koduara dhe shifruara me integritet ose **ENCRYPTED** (Encoded encrypted intgrity-protected data)

Kater tipet e te dhenave te mesiperme mund te kombinohen ne nje mesazh PEM si dhe te nderfuten tek njera tjetra.

Shembuj

Kodimi PEM

PEM mud te perdoret per infrastrukturat me celes sekret dhe ato me celes publik por vlen te thuhet se nuk shfaqet interes ne perdorimin e PEM me celes sekret.

- Eshte nje kodim me Baze 64 (base-64 encoding) ku cdo 6-bite kodohen si 8-bite karakter ne bashkesine e karaktereve {A-Z,a-z,0-9,+,/}
- Cdo mesht qe fillon me karakterin "-", zevendesohet nga PEM me "- "; pra shtohet nje hapesire boshe pas vizes. Kjo ilustrohet si me poshte:

- Vetem mesazhet e tipit MIC-CLEAR dhe MIC-ONLY mund te pasohen
- Mesazhet e tipit ENCRYPTED, duhen deshifruar pastaj rishifrohen