Internet infrastructure

Prof. dr. ir. André Mariën
HTTP and sessions

• TCP session: virtual session
  – IP packets: linked via session IDs
    • Request
    • Reply

• HTTP < 1.1
  – One request/reply: one TCP connection
  – One session: multiple TCP/IP connections
HTTP sessions

• HTTP 1.1
  – Multiple request/reply over one TCP connection

• HTTP session
  – One or more TCP connections
  – Session: managed otherwise
HTTP session management

– Based on client IP address
  • Instable
    – Time
    – NAT
  • Multiple clients from same IP
    – Proxies
    – Firewalls

– Based on URL parameter
  • Querystring element
  • Transmitted via HIDDEN fields in forms

– Cookies

(c) A. Mariën -
HTTP cookies

• Initial specification: netscape
• RFC2109: HTTP State Management Mechanism
• HTTP headers
  – Reply
    • Set-Cookie
  – Request
    • Cookie
The syntax for the Set-Cookie response header

- "Set-Cookie:" (<cookie>)+
- cookie = <name> "=" <value> ( ";" cookie-av)*
- cookie-av =
  - "Comment=" value
  - "Domain=" value
  - "Max-Age=" value
  - "Path=" value
  - "Secure"
  - "HTTPOnly"
  - "Version=" (DIGIT)+

(c) A. Mariën -
Cookies

• Domain cookies
  – Cookies for a site
    • Default
    • Only sent back to issuer
  – Cookies for a domain
    • Sent back to any host in the domain
    • Usage: Single Sign On (SSO)
  – Do not allow cookies for domain .be, .com etc.

• Storage control
  – Max-age: expiration
  – Replay header
    • Cache-control: no-cache="set-cookie"
    • Cache-control: private
  – Expires: old-date
    • Documents with cookies: most often should not be cached; expires header with old date: prevents caching

(c) A. Mariën -
Parameters

• Path
  – Limit cookies to subparts of the site
  – Extra cookies for specific parts

• Secure
  – Cookies identify sessions
  – Sessions can be authenticated
  – Cookies: highly sensitive
  – Cookie sharing between HTTP and HTTPs: problematic
  – Secure: only over secure connections
Tracking users

• Tracking users intra-domain: domain cookies
• How to track users cross-domain?
Central server

• Participating server
  – Connect to central
  – Obtain unique ID

• Central server
  – Maintains ID per user
  – Provides unique ID to requesting servers
Technology: cookies and redirect

• Page contains link
  – http://server-a/setCentralID

• No centralID: triggers redirect to central
  – http://central/server-a/

• Central: redirect back
  – http://server-a/setCentralID?centralID

• Server-a now has uniqueID for user

(c) A. Mariën -