



xmitm: xml man-in-the-middle

Daniel Martín Gómez

[etd\[-at-\]nomejortu.com](mailto:etd[-at-]nomejortu.com)



february '08

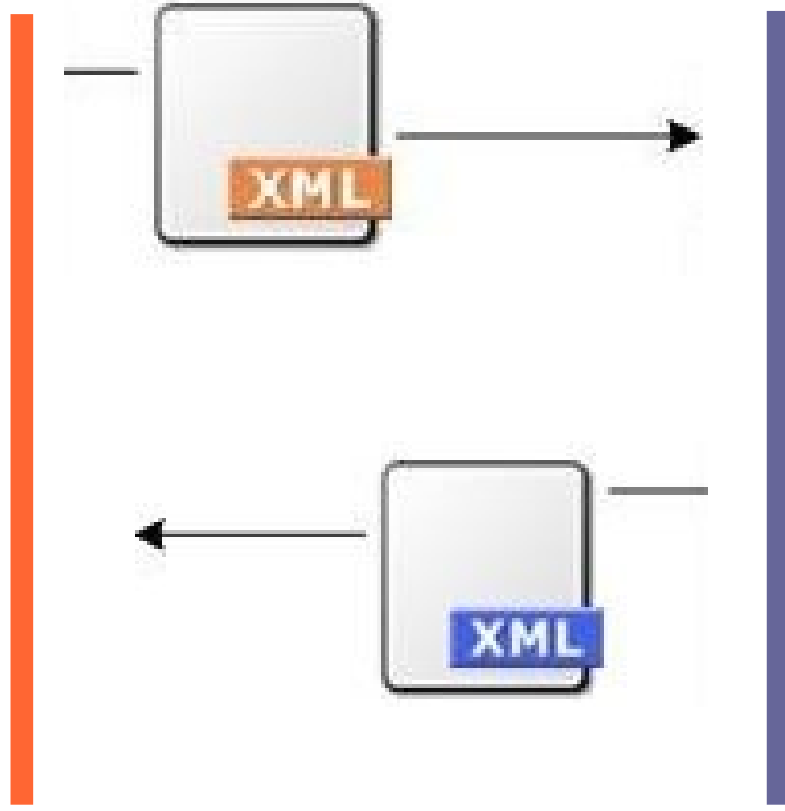
Agenda

- the problem
- the idea
- the tools
- the Kung-Fu





the problem



tcp/1234



Agenda

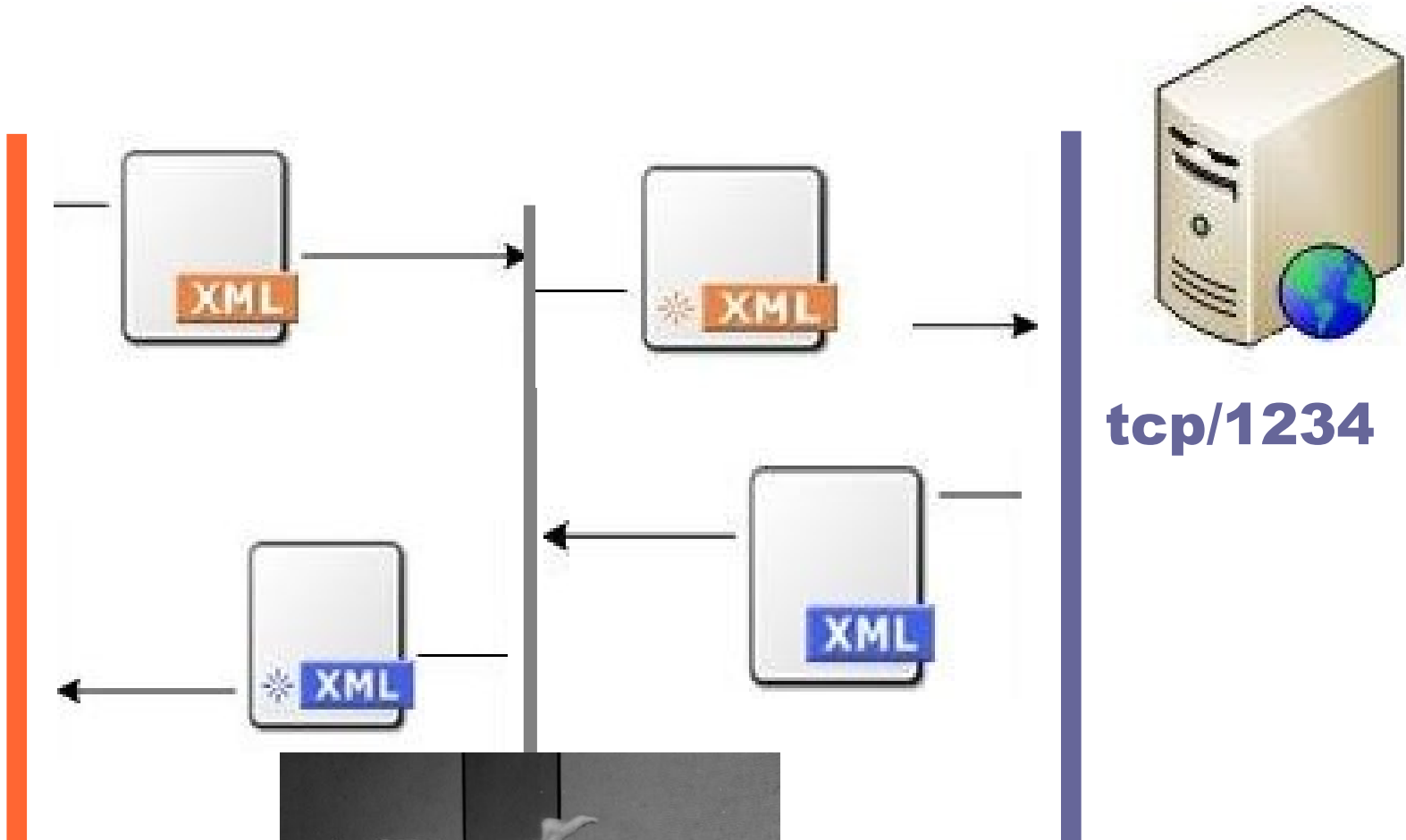
→ ~~the problem~~

→ the idea





the idea



Agenda

→ ~~the problem~~

→ ~~the idea~~

→ the tools

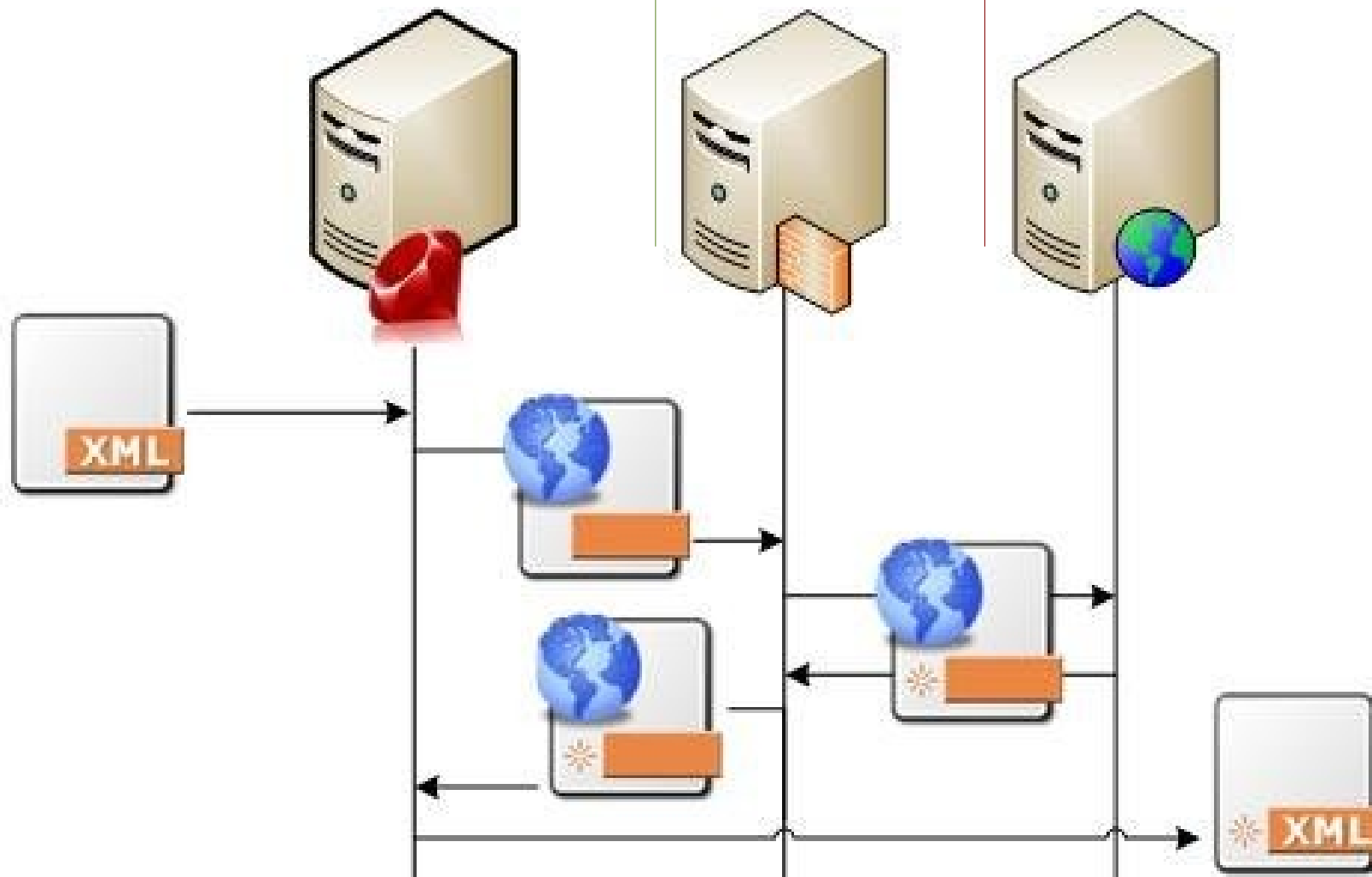




the tools

burp / paros / pick your choice

dummy server: ruby / java



Agenda

→ ~~the problem~~

→ ~~the idea~~

→ ~~the tools~~

→ the Kung-Fu





```
# read the information that one peer wants to send to the other
data = socket.gets($eom)

# encapsulate the data into an HTTP proxy request
res = Net::HTTP.new($proxy_host, $proxy_port).start do |http|

  req = Net::HTTP::Post.new("http://#{$dummyhttp_host}:#{$dummyhttp_port}/")
  req.body= data

  http.request(req)
end

modified_data = res.body.chomp

# send the modified data to the other end of the connection
if (socket == local)
  remote.puts(modified_data)
else
  local.puts(modified_data)
end
socket.flush
```



the socket fun

```
# create a server that accepts connections from the client
server = TCPServer.new($local_host, $local_port)

while(local = server.accept ) do
  # everytime we accept a connection for the client, we open a connection
  # with the server to stablish the dialog.
  remote = TCPSocket.new($remote_host, $remote_port)

  # if one of the ends of the communication closes the socket, we
  # toggle this flag
  alive = true

  while alive do
    result = select([local, remote], nil, nil)

    # the previous code
    # [...]
  end
end
```





dummy server: ruby

```
require 'webrick'

include WEBrick

# create the server, no output, disable logging
s = HTTPServer.new(
  :Port => 2000,
  :Logger => Log.new(nil, BasicLog::FATAL),
  :AccessLog => [] )

# the *echo* functionality
s.mount_proc("/") do |req, res|
  res.body = req.body
  res['Content-Type'] = req['Content-Type']
end

# clean tear down
trap('INT') { s.shutdown }

s.start
```





→ References:

- ✓ blog posts:
 - xmitm: xml man in the middle ([link](#))

<http://weblog.nomejortu.com/>





Questions?

Daniel Martín Gómez

etd



february '08