1

C-HTTP
The development of a secure, closed HTTP-based network on the Internet

Takahiro Kiuchi, M.D.

Dep. of Epidemiology and Biostatistics,
Faculty of Medicine, University of Tokyo, Japan

Shigekoto Kaihara, M.D.

Hospital Computer Center,
University of Tokyo Hospital, Japan

Introduction (1)

Medical Community

1. Needs for secure data communications

Multi-institutional clinical research
Case reports
Patient referral

2. Unskilled computer users

Keys? Certificates? Encryption?

3. Security insensitive users

Security of their patient's information, not their own

Introduction (2)

Current Medical Information Networks in Japan

1. UMIN (University Medical Information Network)

Participants	University Hospitals
Protocol	N1 Protocol
Internet	Not accessible

2. Cancer Center Network

Participants	Central and regional national cancer centers
Protocol	TCP/IP
Internet	Accessible via a gateway

4

Introduction (3)

"Physical" closed network

1. Expensive

2. Not flexible

Virtual closed network

Introduction (4)

Why HTTP? Why not our own?

1) Flexibility of HTTP

Most services can be provided using HTTP.

2) User friendly interface

3) User agents and servers available on almost all platforms

C-HTTP Overview (1)

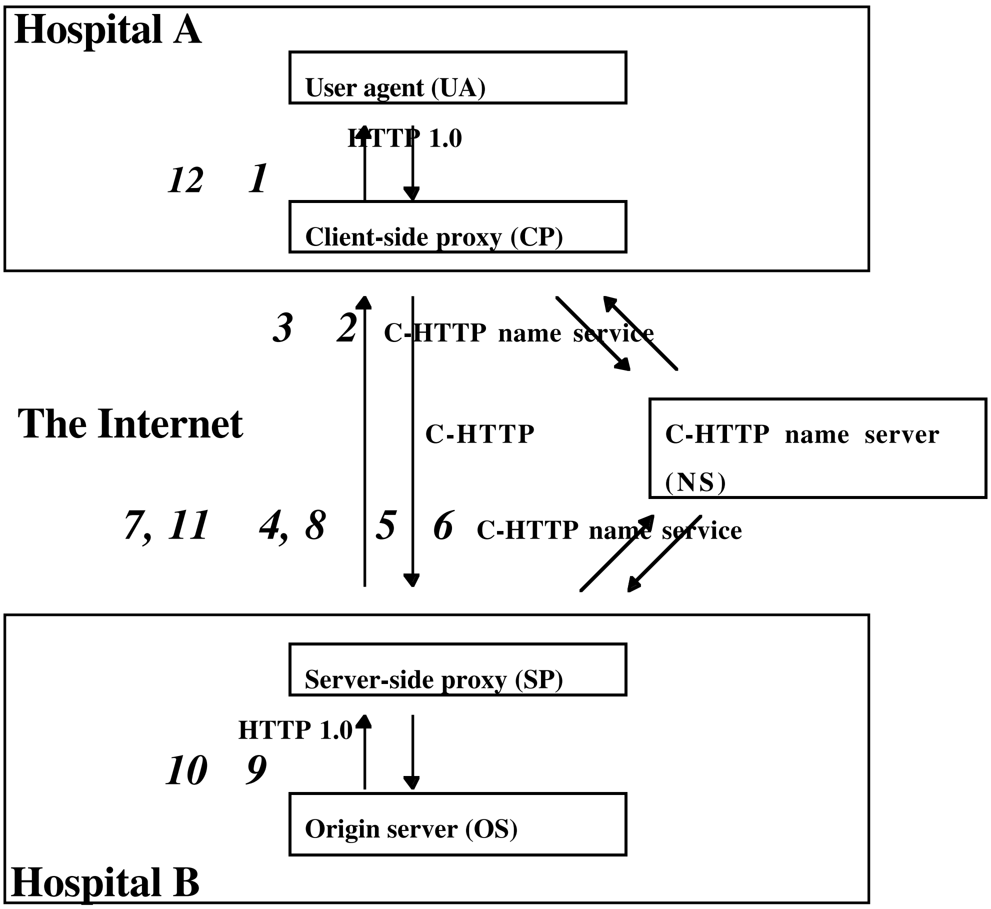
Overview

1. C-HTTP
   *Proxy on a firewall of each site
   *Secure data communication between proxies
   *Proxy-proxy authentication (Institutional authentication)

2. C-HTTP name service
   *Centralized name, certificate and public key administration
   *Secure name service, using encryption (DNS not used)

3. Scalability
   *A few hundreds of hospitals (proxies)

C-HTTP overview (2)



C-HTTP overview (3)

Security technology

SSL (SSLeay 0.5.1a)

- **Asymmetric key encryption**
- **Symmetric key encryption**
- **Electronic signature**
- **One-way hush function**
- **Random key generation**

Protocol layer

1. HTTP/1.0
↓
2. C-HTTP
↓
3. SSL
↓
4. TCP/IP

1. C-HTTP name service
↓
2. SSL
↓
3. TCP/IP

C-HTTP overview (4)

Information each component keeps

1. C-HTTP name server (NS)
- Own IP address and port number
- Own private key
- Own public key
- Public keys of all proxies
- Resource names, IP address, port numbers of all proxies
- Connection table for all the combinations of proxies

2. Client-side proxy (CP)
- Own private key
- Own public key
- Own resource name and IP address

3. Server-side proxy (SP)
- Own private key
- Own public key
- Own resource name, IP address and port number

C-HTTP overview (5)

Example of Connection Table stored in C-HTTP name server

SCP (IP:Port)	CP		
	u-tokyo.hospital	nagano.hospital	osaka-u.hospital
medical.server (222.222.222.222:2222)	X	X	X
CAG.project (222.222.222.222:1234)	X		X
Lung.cancer.trial (130.69.109.61:9876)	X	X	
AMI.trial (130.69.109.61:8765)	X	X	
AntibiotiCProject (130.69.109.57:2345)	X		

C-HTTP overview (6)

How to participate in a closed network

1. Determine resource name, IP address and port number (in case of server-side proxy) of own proxy.

2. Generate own private key and public key (certificate request).

3. Send own resource name, IP address port number and public key (certificate request) to an administrator of C-HTTP name server (or C-HTTP-based network) in a secure manner.

4. Obtain a public key (certificate), IP address and port number of the C-HTTP name server in a secure manner.

C-HTTP-based communication (1)

Overview

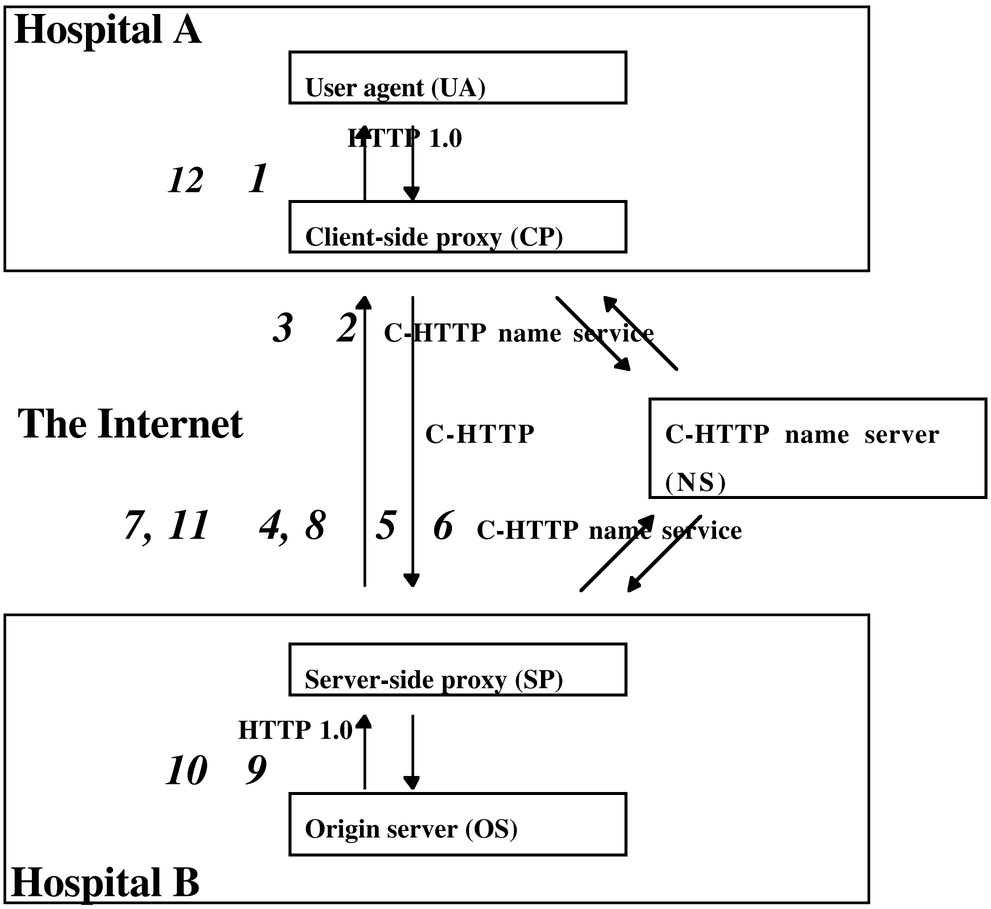
NS: C-HTTP name server, CP: Client-side proxy,
SP: Server-side proxy, OS: Origin server, UA: User agent

	Type	From	To	Explanation
1.	HTTP request	UA	CP	Resource in the closed network requested
2.	C-HTTP name request	CP	NS	Request for SP information
3.	C-HTTP name response	NS	CP	SP information returned if available
4.	C-HTTP request	CP	SP	Request for connection
5.	C-HTTP name request	SP	NS	Request for CP information
6.	C-HTTP name response	NS	SP	CP information
7.	C-HTTP response	SP	CP	Connection acknowledged
8.	C-HTTP request	CP	SP	Object requested
9.	HTTP request	SP	OS	Object requested
10.	HTTP response	OS	SP	Object sent
11.	C-HTTP response	SP	CP	Object sent
12.	HTTP response	CP	UA	Object sent
19.	HTTP request	UA	CP	Object requested
20.	C-HTTP request	CP	SP	Object requested
21.	HTTP request	SP	OS	Object requested
22.	HTTP response	OS	SP	Object sent
23.	C-HTTP response	SP	CP	Object sent
24.	HTTP response	CP	UA	Object sent
31.	HTTP request	UA	CP	Object not in closed network requested

32.	C-HTTP request	CP	SP	Request for disconnection
33.	C-HTTP response	SP	CP	Disconnection acknowledged
34.	HTTP request	CP	OS	Ordinary HTTP/1.0 request

14

C-HTTP overview (2)



C-HTTP-based communication(2)

Example

	Resource name	IP	Port
UA		192.168.111.111	
CP	u-tokyo.hospital	111.111.111.111	
SP	medical.server	222.222.222.222	2222
OS		192.168.222.222	
NS		123.123.123.123	

C-HTTP-based communication (3)

	Type	From	To	Explanation
1.	HTTP request	UA	CP	Resource in the closed network requested
2.	C-HTTP name request	CP	NS	Request for SP information
3.	C-HTTP name response	NS	CP	SP information returned if available

Example:

GET http://medical.server/index.html HTTP/1.0<CR><LF>

C-HTTP-based communication (4)

	Type	From	To	Explanation
1.	HTTP request	UA	CP	Resource in the closed network requested
2.	C-HTTP name request	CP	NS	Request for SP information
3.	C-HTTP name response	NS	CP	SP information returned if available

Protocol

C-HTTP-NAME-SERVICE-VERSION<CR><LF>
SERVICE-TYPE<CR><LF>
RESOURCE-NAME<CR><LF>

Example

C-HTTP-NS/0.2<CR><LF>
ServerInfo<CR><LF>
medical.server<CR><LF>

C-HTTP-based communication (5)

Stateless HTTP to stateful C-HTTP

a. The HTML document sent from a origin server to a client-side proxy

```
<TITLE>SAMPLE</TITLE>
<BODY>
<A HREF ="http://medical.server/sample.html">

Please click here.</A>
<A HREF ="http://another.server/">Another server.</A>

</BODY>
```

b. The HTML document rewritten and forwarded to a use agent by the client-side proxy. The string, "6zdDfldfcZLj8V!i", attached to the end of the URLs is a connection ID

```
<TITLE>SAMPLE</TITLE>
<BODY>
<A HREF ="http://medical.server/sample.html=@=6zdDfldfcZLj8V!i">

Please click here.</A>
<A HREF = "http://another.server/=@=6zdDfldfcZLj8V!i">

Another server.</A>
</BODY>
```

c. HTTP/1.0 request from the user agent (1) and HTTP/1.0 request encrypted and wrapped in C-HTTP request dispatched by the client-side proxy (2)

```
(1) GET "http://medical.server/sample.html=@=6zdDfldfcZLj8V!i" HTTP/1.0<CR><LF>
(2) GET "http://medical.server/sample.html" HTTP/1.0<CR><LF>
```

C-HTTP-based communication (6)

C-HTTP session table

ConnectionID	SP	IP	Port	UA
azd3wzece3Zj5hJKP	CAG.project	222.222.222.222	1234	192.168.109.2
2z4RTswWsdfuiOsa	Lung.cancer.trial	130.69.109.61	9876	192.168.108.3
bcui2s9deklwWjP	AMI.trial	130.69.109.61	8765	192.168.111.4

C-HTTP-based communication (7)

2.	C-HTTP name request	CP	NS	Request for SP information
3.	C-HTTP name response	NS	CP	SP information returned if available
4.	C-HTTP request	CP	SP	Request for connection

Protocol

C-HTTP-NAME-SERVICE-STATUS<CR><LF>
SERVER-SIDE-PROXY-IP<CR><LF>
SERVER-SIDE-PROXY-PORT<CR><LF>
SERVER-SIDE-PROXY-CERTIFICATE<CR><LF>
REQUEST-NONCE<CR><LF>

Example

OK<CR><LF>
222.222.222.222<CR><LF>
222<CR><LF>
-----BEGIN X509 CERTIFICATE-----
MIICkjCCAjwCAQAwDQYJKoZIhvcNAQEEBQAwgdMxCzAJBgNVBAYTAkpQMQ4wDAYD
VQQIEwVUb2t5bzESMBAGA1UEBxMJQnVua3lvLWt1MSwwKgYDVQQKEyNGYWN1bHR5
IG9mIE1lZGljaW5lLCBVbml2LiBvZiBUb2t5bzEvMC0GA1UECxMmRGVwLiBvZiBF
cGlkZW1pb2xvZ3kgYW5kIEJpb3N0YXRpc3RpY3MxEjAQBgNVBAMTCUtpdWNoaSBD
QTEtMCsGCSqGSIb3DQEJARYea2l1Y2hpQGVwaXN0YXQubS51LXRva3lvLmFjLmpw
MB4XDTk2MDIxNDExMzcyMVoXDTk2MDMxNTExMzcyMVowgdMxCzAJBgNVBAYTAkpQ
MQ4wDAYDVQQIEwVUb2t5bzESMBAGA1UEBxMJQnVua3lvLWt1MSwwKgYDVQQKEyNG
YWN1bHR5IG9mIE1lZGljaW5lLCBVbml2LiBvZiBUb2t5bzEvMC0GA1UECxMmRGVw
LiBvZiBFcGlkZW1pb2xvZ3kgYW5kIEJpb3N0YXRpc3RpY3MxEjAQBgNVBAMTCUtp
dWNoaSBDQTEtMCsGCSqGSIb3DQEJARYea2l1Y2hpQGVwaXN0YXQubS51LXRva3lv
LmFjLmpwMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKHWVLOml02szEb7WHOILMAy
1bTh9KpbFMb+/Ib8hEAEKBUlkRVxjdWeEtD4JTw2U1dDRZc6SVq7Vo4/65IbnZ0C
AwEAATANBgkqhkiG9w0BAQQFAANBAJK1kVbk35i7gaBGR0+CmN2XUDgY7TlcpmNY
AwXqcbHJN1C6rfoyBrn6dW08pi4Vnd1VUFYILKtJf39+tFvBupE=
-----END X509 CERTIFICATE-----**<CR><LF>**
8abd853f<CR><LF>

C-HTTP overview (8)

3.	C-HTTP name response	NS	CP	SP information returned if available
4.	C-HTTP request	CP	SP	Request for connection
5.	C-HTTP name request	SP	NS	Request for CP information

Example

CONNECT C-HTTP/0.7<CR><LF>
Client-Side-Proxy-Name: u-tokyo.hospital<CR><LF>
Request-Nonce: 8abd8540<CR><LF>

C-HTTP overview (9)

4.	C-HTTP request	CP	SP	Request for connection
5.	C-HTTP name request	SP	NS	Request for CP information
6.	C-HTTP name response	NS	SP	CP information

Protocol

C-HTTP-NAME-SERVICE-VERSION<CR><LF>
SERVICE-TYPE<CR><LF>
RESOURCE-NAME<CR><LF>

Example

C-HTTP-NS/0.2<CR><LF>
ClientInfo<CR><LF>
u-tokyo.hospital<CR><LF>

C-HTTP-based communications (10)

5.	C-HTTP name request	SP	NS	Request for CP information
6.	C-HTTP name response	NS	SP	CP information
7.	C-HTTP response	SP	CP	Connection acknowledged

Protocol

C-HTTP-NAME-SERVICE-STATUS<CR><LF>
Client-SIDE-PROX-IP<CR><LF>
CLIENT-SIDE-PROXY-CERTIFICATE<CR><LF>
RESPONSE-NONCE<CR><LF>

Example

OK<CR><LF>
111.111.111.111<CR><LF>
-----BEGIN X509 CERTIFICATE-----
MIIChDCCAi4CAQIwDQYJKoZIhvcNAQEEBQAwgdMxCzAJBgNVBAYTAkpQMQ4wDAYD
VQQIEwVUb2t5bzESMBAGA1UEBxMJQnVua3lvLWt1MSwwKgYDVQQKEyNGYWN1bHR5
IG9mIE1lZGljaW5lLCBVbml2LiBvZiBUb2t5bzEvMC0GA1UECxMmRGVwLiBvZiBF
cGlkZW1pb2xvZ3kgYW5kIEJpb3N0YXRpc3RpY3MxEjAQBgNVBAMTCUtpdWNoaSBD
QTEtMCsGCSqGSIb3DQEJARYea2l1Y2hpQGVwaXN0YXQubS51LXRva3lvLmFjLmpw
MB4XDTk2MDIxNDExNDc0MVoXDTk3MDIxMzExNDc0MVowgcUxCzAJBgNVBAYTAkpQ
MQ4wDAYDVQQIEwVUb2t5bzEsMCoGA1UEChMjRmFjdWx0eSBvZiBNZWRpY2luZSwg
VW5pdi4gb2YgVG9reW8xLzAtBgNVBAsTJkRlcC4gb2YgRXBpZGVtaW9sb2d5IGFu
ZCBCaW9zdGF0aXN0aWNzMRgwFgYDVQQDEw9UYWthaGlybyBLaXVjaGkxLTArBgkq
hkiG9w0BCQEWHmtpdWNoaUBlcGlzdGF0Lm0udS10b2t5by5hYy5qcDBcMA0GCSqG
SIb3DQEBAQUAA0sAMEgCQQDPZy4ABrzjxLOjdfrZ8OQyVQnwIRbP0fyhAVT8D9qO
3oSPeXnpNi1zjnn0B8tg2E4uf/HGIe6YhxsEIxqfOjsNAgMBAAEwDQYJKoZIhvcN
AQEEBQADQQBcw17ia0W5Jyh+Sy2DJNoAl3OP0E9IM7CV1EiCuGOYgB+Swg9EicDK
MrrLezvA4INeh1iGyTw0kOGEoSZpc0a9
-----END X509 CERTIFICATE-----**<CR><LF>**
ef23cd99<CR><LF>

C-HTTP-based communications (11)

6.	C-HTTP name response	NS	SP	CP information
7.	C-HTTP response	SP	CP	Connection acknowledged
8.	C-HTTP request	CP	SP	Object requested

Example

C-HTTP/0.7 OK<CR><LF>
Response-Nonce: 8abd853f <CR><LF>
Connection-ID: 6zdDfldfcZLj8Vli<CR><LF>

C-HTTP-based communications (12)

7.	C-HTTP response	SP	CP	Connection acknowledged
8.	C-HTTP request	CP	SP	Object requested
9.	HTTP request	SP	O S	Object requested

Example

Request C-HTTP/0.7<CR><LF>
Request-Nonce: 8abd8541<CR><LF>
Connection-ID: 6zdDfldfcZLj8Vli <CR><LF>
<CR><LF>
GET /index.html HTTP/1.0<CR><LF>

C-HTTP-based communications (13)

8.	C-HTTP request	CP	SP	Object requested
9.	HTTP request	SP	OS	Object requested
10.	HTTP response	OS	SP	Object sent

Example

GET /index.html HTTP/1.0<CR><LF>

C-HTTP-based communications (14)

9.	HTTP request	SP	OS	Object requested
10.	HTTP response	OS	SP	Object sent
11.	C-HTTP response	SP	CP	Object sent

Example

HTTP/1.0 OK 200<CR><LF>
Content-Type: text/html<CR><LF>
Content-Length: 345<CR><LF>
<CR><LF>
<TITLE>Example</TITLE>
<H1>This is an example HTML text.</H1>

C-HTTP-based communications (15)

10.	HTTP response	O S	SP	Object sent
11.	C-HTTP response	SP	CP	Object sent
12.	HTTP response	CP	UA	Object sent

Example

Response C-HTTP/0.7 OK<CR><LF>
Response-Nonce: 8abd8541<CR><LF>
Connection-ID: 6zdDfldfcZLj8Vli <CR><LF>
<CR><LF>
HTTP/1.0 OK 200<CR><LF>
Content-Type: text/html<CR><LF>
Content-Length: 345<CR><LF>
<CR><LF>
<TITLE>Example</TITLE>
<H1>This is an example HTML text.</H1>

C-HTTP-based communications (16)

11.	C-HTTP response	SP	CP	Object sent
12.	HTTP response	CP	UA	Object sent

Example

HTTP/1.0 OK 200<CR><LF>
Content-Type: text/html<CR><LF>
Content-Length: 345<CR><LF>
<CR><LF>
<TITLE>Example</TITLE>
<H1>This is an example HTML text.</H1>

C-HTTP-based communications (17)

31.	HTTP request	UA	CP	Object not in closed network requested
32.	C-HTTP request	CP	SP	Request for disconnection
33.	C-HTTP response	SP	CP	Disconnection acknowledged
34.	HTTP request	CP	OS	Ordinary HTTP/1.0 request

Example

DISCONNECT C-HTTP/0.7<CR><LF>
Request-Nonce: 8abd8554 <CR><LF>
Connection-ID: 6zdDfldfcZLj8Vli <CR><LF>

C-HTTP-based communications (18)

31.	HTTP request	UA	CP	Object not in closed network requested
32.	C-HTTP request	CP	SP	Request for disconnection
33.	C-HTTP response	SP	CP	Disconnection acknowledged
34.	HTTP request	CP	O S	Ordinary HTTP/1.0 request

Example

C-HTTP/0.7 OK<CR><LF>
Response-Nonce: 8abd8549 <CR><LF>
Connection-ID: 6zdDfldfcZLj8Vli <CR><LF>

Discussion (1)

Secure HTTP for medical use

“Proxy-proxy” v.s. “End-to-end”

1. All hospitals are protected using firewalls.

Discussion (2)

Secure HTTP for medical use

“Proxy-proxy” v.s. “End-to-end”

2. Key management

Personal risk

Commercial service

v.s.

Institutional or patients’ risk

Medical information exchange

Discussion (3)

Secure HTTP for medical use

“Proxy-proxy” v.s. “End-to-end”

3. Unskilled and users

Easy installation essential

Discussion (4)

C-HTTP Name Service

1. Efficient

Provide name service and certificate (public key) simultaneously

2. Secure as compared with DNS

a. Client and server authentication

C-HTTP name server not available to public

b. Communication encrypted

Server IP and port number not detected even if its resource name ("http://medical.server/index.html") is made public.

Discussion (5)

Disadvantage and limitations

1. Current C-HTTP can accommodate up to only a few hundreds of proxies
2. Addition of a new proxy cannot be automated.

Discussion (6)

Relation to other secure HTTPs

C-HTTP is NOT ALTERNATIVE, but can CO-EXIST with them

C-HTTP	**Institutional level security**
Other end-to-end secure HTTPs	**Personal level security**

Discussions (7)

C-HTTP v.s. Secure HTTP compatible proxy servers

1. Centralized network management

2. C-HTTP name service

Discussion (8)

Use in areas other than in medicine

For example,

Virtual closed network between

headquarters and branches of

a small or middle size private company

Concluding remarks (1)

Closed network on the Internet ?

	Internet	C-HTTP
Participation	Open	Closed
No. of computers	Huge	Limited
Flexibility	Yes	No
Standardization	Necessary	Not necessary
Administration	Distributed	Centralized

Concluding remarks (2)

More investments to the Internet, rather than the development of physical closed network.

42

How to introduce “status” to stateless HTTP