HTTP & Encryption

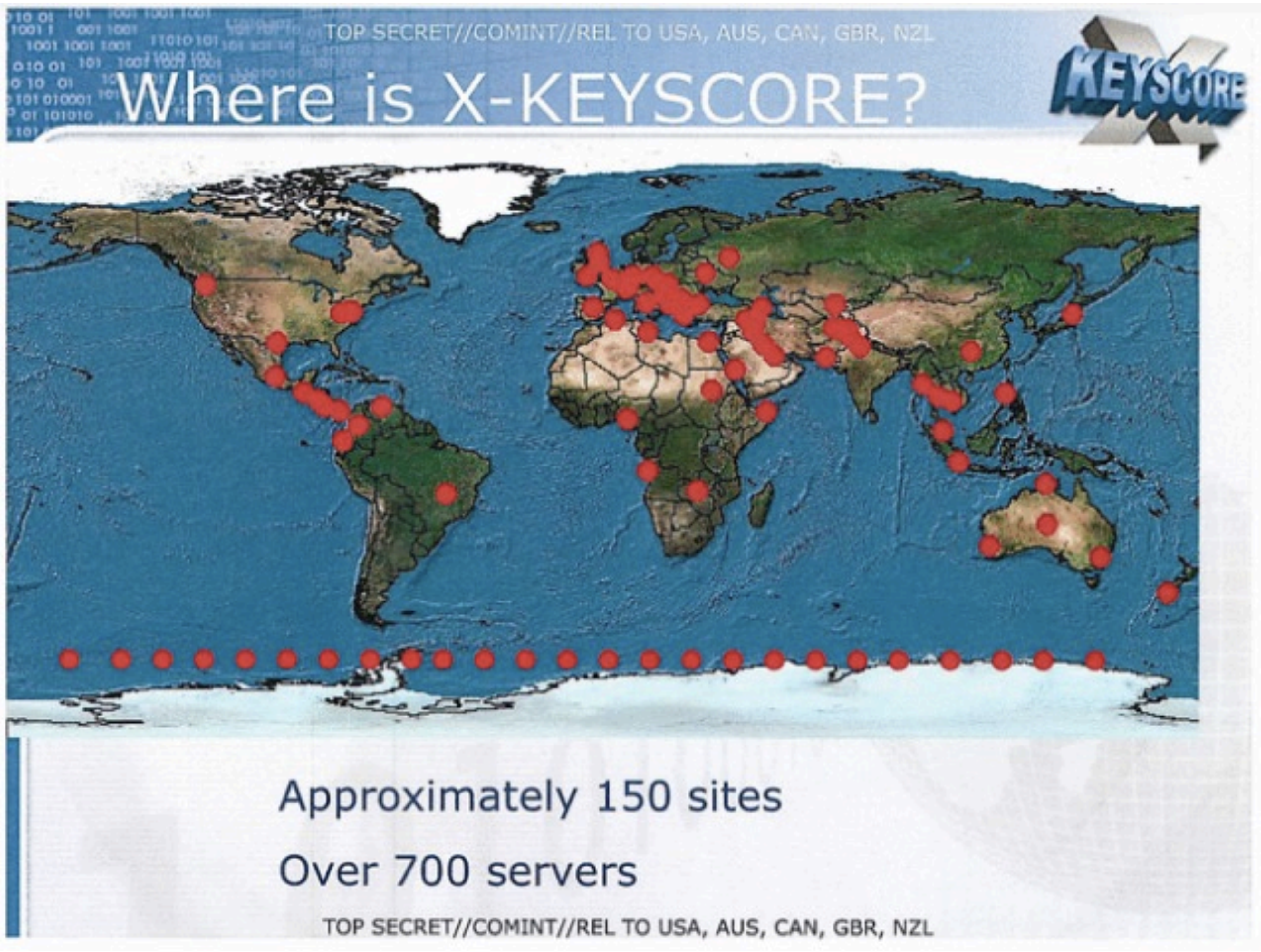
HTTP/1.1 has no Mandatory to **Implement** Security

SPDY introduced
Mandatory to **Use** Security

...but we declined.

Status Quo:
Server Chooses

New Information



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?

Approximately 150 sites

Over 700 servers

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Proposed HTTP/1.1 Actions

Additions to SC

- HTTP/1.1 Does not make TLS MTI/MTU because of the age of the protocol
- Negotiation for encryption through the URI scheme places control server-side, disempowers clients
- Common use of HTTP has a tremendous amount of PII and other sensitive data
  - ... even without cookies
- Once on the wire, it is vulnerable to intercept, and there are known, wide deployments that exploit this actively
- Therefore, servers ought to implement and prefer HTTPS
- Even this is not necessarily adequate; see TLS WG for more info

Proposed HTTP/2.0 Actions

1. New issue: Mandatory to Implement Security

... including concept
of equal power;
i.e., client can
negotiate / require use
of encryption for
HTTP URIs

2. New issue: proxy discovery / interactions

(Still) Out of Scope: enabling interception of encrypted traffic

3. Liaison with TLS WG and W3C as appropriate

Q&A