CACert

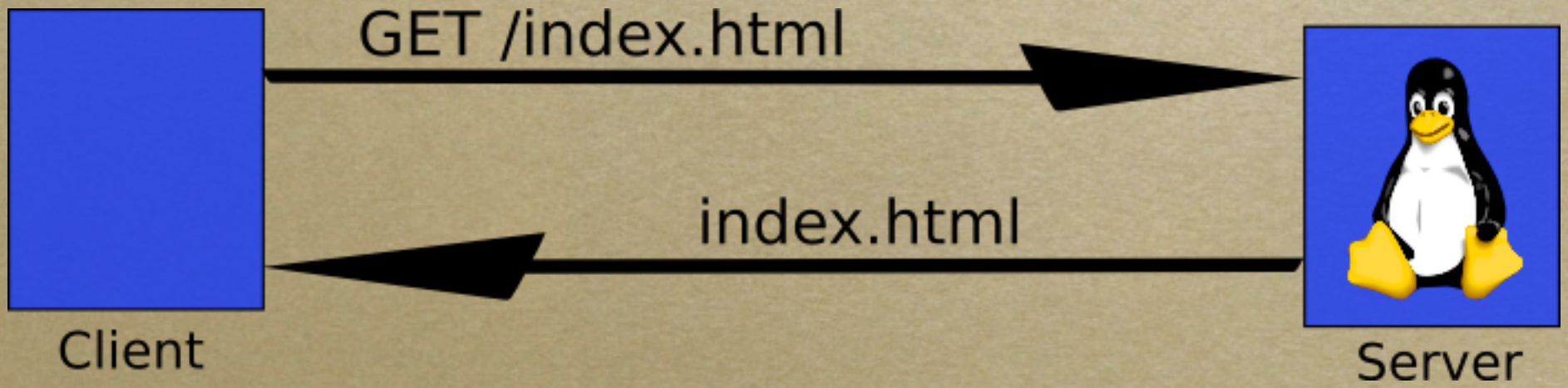
Tanner Lovelace
Triangle Linux Users Group
11/May/2006

Outline

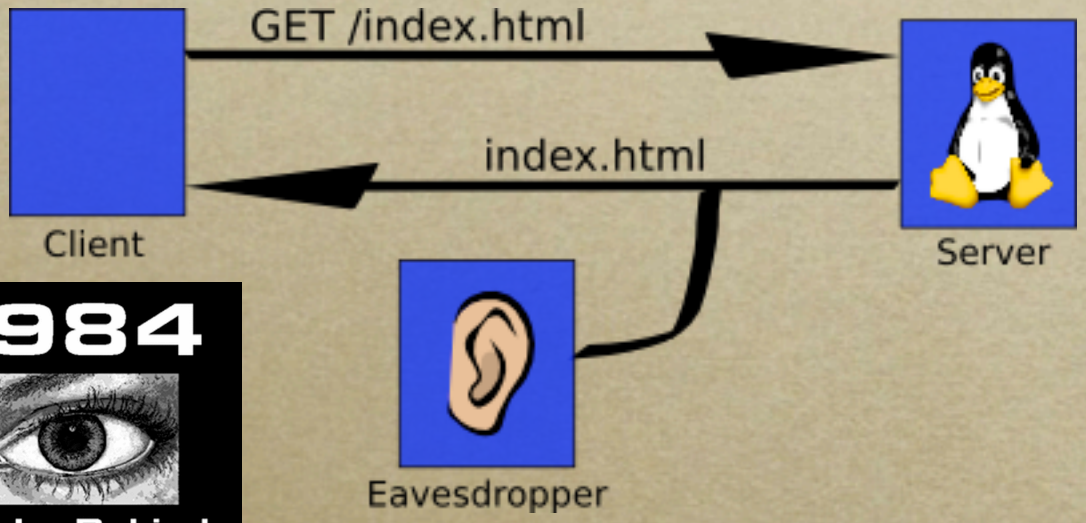
- *What is SSL and why do we need it?*
- *What is a Certificate Authority?*
  - *What is CACert?*
- *How does CACert verify identity?*
- *How do I use CACert?*
- *Conclusion and Mass Assurance*

How Does the Web Work?

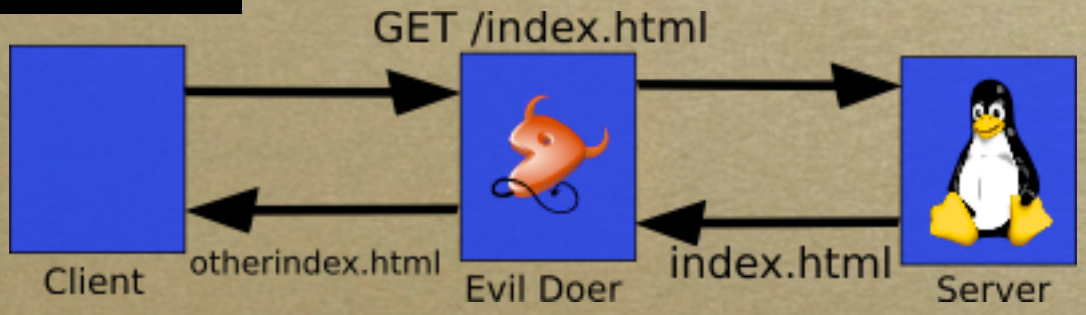
- *Client-server*
- *No verification or encryption (in standard model)*



Problems with Standard Web



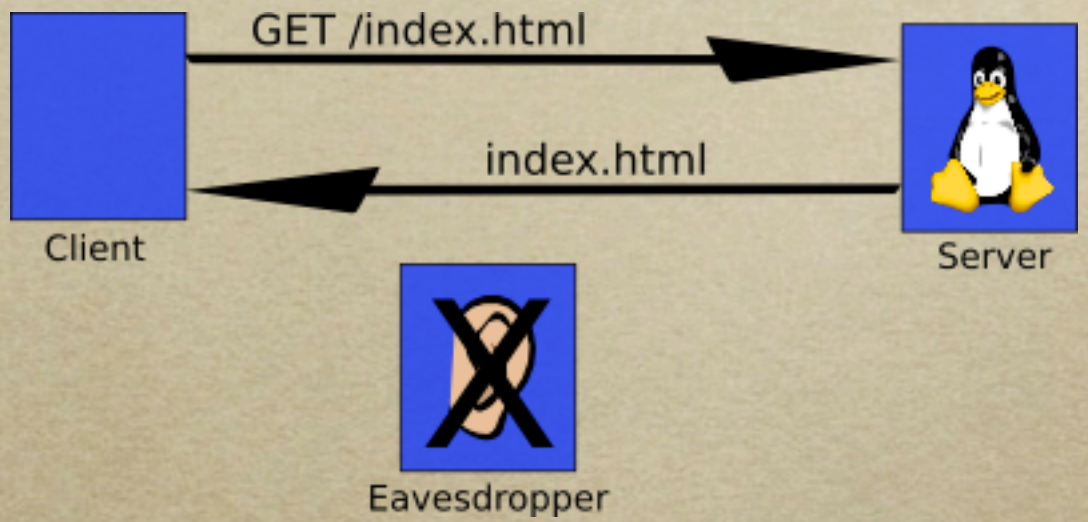
- *Susceptible to eavesdropping*



- *Man-in-the-middle (i.e. transparent proxies)*

The Web with SSL

- *Encryption of Traffic*



- *Verification of Identity*

Outline

- *What is SSL and why do we need it?*
- *What is a Certificate Authority?*
  - *What is CACert?*
- *How does CACert verify identity?*
- *How do I use CACert?*
- *Conclusion and Mass Assurance*

Trusted Third Party

- *Checks identity*
- *Based on identity check, it vouches for a server*

Standard Certificate Authorities

- *Verisign*
- *Thawte*
- *AOL*
- *GoDaddy*
- *Many more...*

CACert

- *Community driven Certificate Authority*
- *Primary goals:*
  - *Inclusion into mainstream browsers! (Mozilla bug #215243, opened 8/6/03, currently with 63 votes, 107 subscribers)*
    - *http://wiki.cacert.org/wiki/InclusionStatus*
  - *To provide a trust mechanism to go with the security aspects of encryption.*

Outline

- *What is SSL and why do we need it?*
- *What is a Certificate Authority?*
  - *What is CACert?*
- *How does CACert verify identity?*
- *How do I use CACert?*
- *Conclusion and Mass Assurance*

CACert Assurance Program

- *Identify Verification Program*
  - *CACert Assurer*
  - *Trusted Third Party*
  - *Being a notary for another authority*

Point System

- *0-49 points - Considered “unassured”*
- *50 points - Full name on client certs, Server certs valid for 24 months, GPG key signed by CACert*
- *100 points - Maximum available through WoT, can apply for codesigning cert and assure others*
- *150 points - Fully assured, can issue 35 points*
- *200 points - Super Assurer, temporary increase*

Issuing Points

- *If you have 100 points, you can assure others.*
- *You get 2 points for each assurance*
- *The maximum points you can issue is a sliding scale*

Own points	Issuable points
100	10
110	15
120	20
130	25
140	30
150	35

Outline

- *What is SSL and why do we need it?*
- *What is a Certificate Authority?*
  - *What is CACert?*
- *How does CACert verify identity?*
- *How do I use CACert?*
- *Conclusion and Mass Assurance*

Installing the Root Certificate

- *Go to http://www.cacert.org/*
- *Click on "Root Certificate"*
- *Check the fingerprint and if correct...*
- *Import into the browser*

Getting a Certificate

- *Client Certificates*
- *Server Certificates*
  - *Generating the certificate*
  - *Getting it signed*

Using Your Certificate

- *Using a client certificate*
- *Using a server certificate*
  - *Installation on a server*

Outline

- *What is SSL and why do we need it?*
- *What is a Certificate Authority?*
  - *What is CACert?*
- *How does CACert verify identity?*
- *How do I use CACert?*
- *Conclusion and Mass Assurance*