Web Encryption 101: Secure Sockets Layer (SSL)

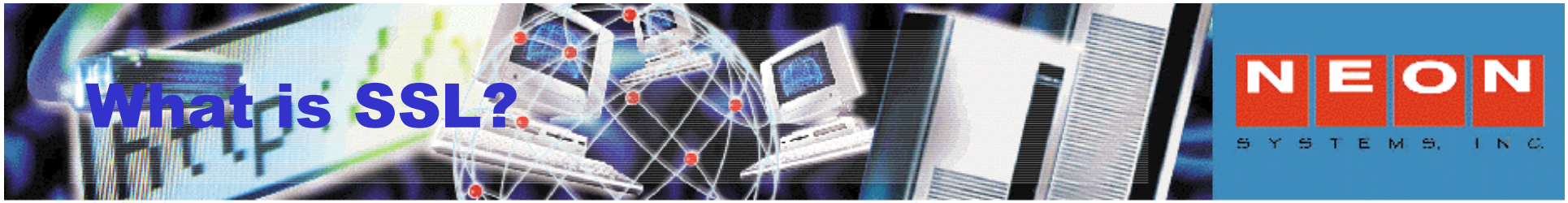
Session G22

Michael Ludé -- mlude@neonsys.com

NEON Systems, Incorporated

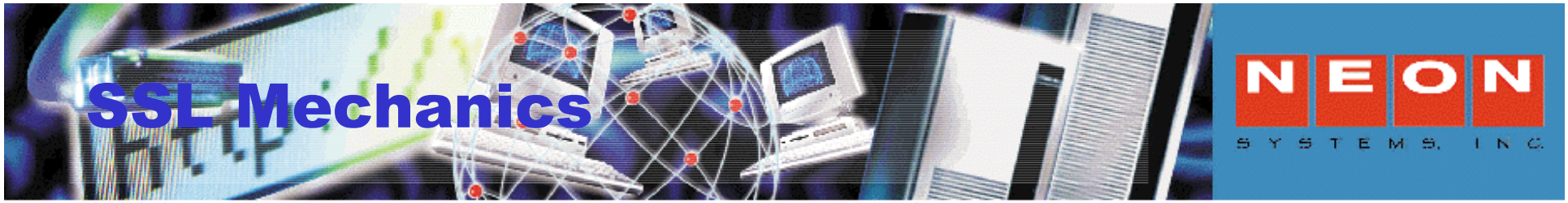
http://www.neonsys.com

RETURN TO INDEX



What is SSL?

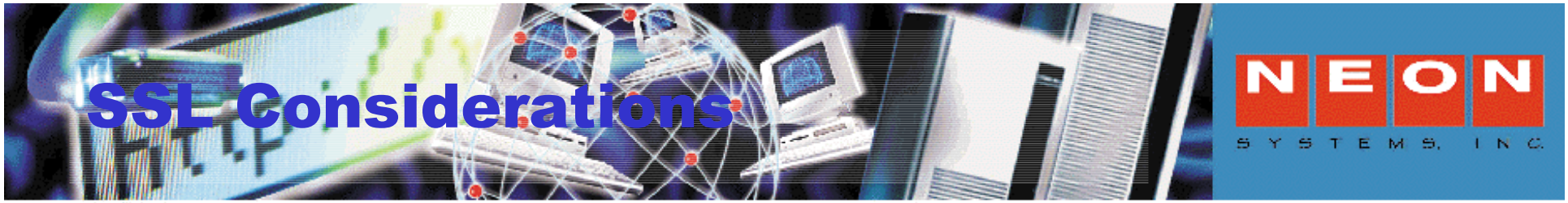
- Secure Sockets Layer
- Can be (theoretically) added to any existing protocol
  - HTTP plus SSL equals HTTPS
- Provides point-to-point encryption of entire session
- No change necessary to CGIs, etc.



SSL Mechanics

- URLs start with HTTPS, not HTTP
  - https://www.nesy.com
- The default port is 443, not 80
- Everything else is the same
- Insecure sites show:

- Secure sites show:



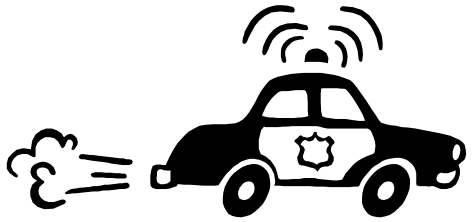
SSL Considerations

- Performance is not as good
  - Computing keys is processor-intensive
- *Each transaction* requires an SSL handshake
  - Eliminate superfluous images from secure pages
- Run both secure and non-secure servers
  - This may be two copies of same server, one with SSL enabled, one with it disabled

Internet Security Threats

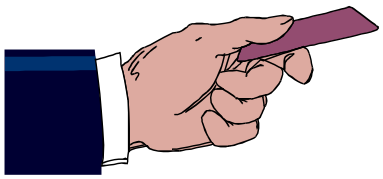
NEON SYSTEMS, INC.

- Unauthorized bad guy accesses private information
- Bad guy pretends to be trusted location
- Data sent from server to user intercepted (and maybe replaced) by bad guy
- All can be prevented by proper use of SSL



Countermeasures

- Access control
  - Interface to External Security Manager
- Authentication
  - Username/password OR digital certificate
  - Authenticate client and/or server
- Encryption
- Accountability



WWW Security Threats

NEON SYSTEMS, INC.

- All traffic to/from the browser is in cleartext
  - HTML, GIFs, reports etc. from the server
  - User-entered form data from the browser
  - Userids/passwords entered from the browser
- What is your risk?
  - Internet vs. Intranet
  - Is the routing hardware secure?

Browser Password Prompt


```
GET /index.html HTTP/1.0
Connection: Keep-Alive
User-Agent: Mozilla/4.04 [en] (Win95; I)
Host: jupiter.beyond-software.com:83
Authorization: Basic anF1c2VyOnNlY3JldA==
```

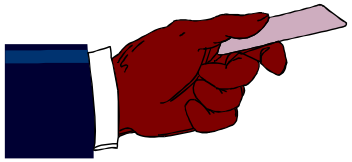
Digital Certificates

- Electronic document
- Impossible to forge
- Contains information about the “owner”
- Digitally “signed” by a trusted authority
- Server sends certificate at the start of an SSL conversation (the “handshake”)

How do Certificates Work?

NEON SYSTEMS, INC.

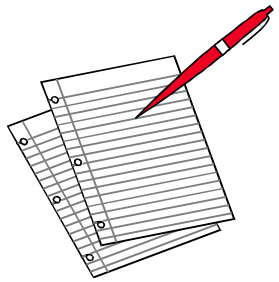
- It's like an ID card
  - Issued by a certificate authority
- Is this ID accepted?
  - Well, who's the CA?
- You must have the CA's card on file
  - Their ID might be issued by another CA
  - It might be issued by themselves
    - A self-signed ID is called a *trusted root*



What's in a (server) certificate?

NEON SYSTEMS, INC.

- Organization name ("NEON Systems Inc")
- Organizational unit ("Engineering")
- State or Province ("Texas")
- Country ("US")
- Domain name ("www.neonsys.com")
- Plus information on the certificate authority

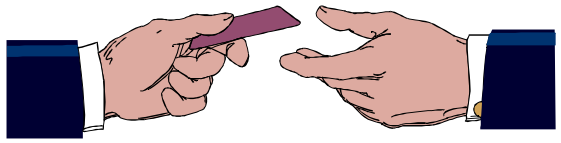


What's a Certificate Authority?

- Commonly referred to as a "CA"
- It's a third party that vouches for you
- Some certificate authorities:
  - RSA, VeriSign, Thawte, AT&T, Canada Post
  - Click "Security", then "Certificates" and "signers" from Netscape to see a list
  - Click "Options", "Security", then "Sites" for IE

How do I get a certificate?

NEON SYSTEMS, INC.

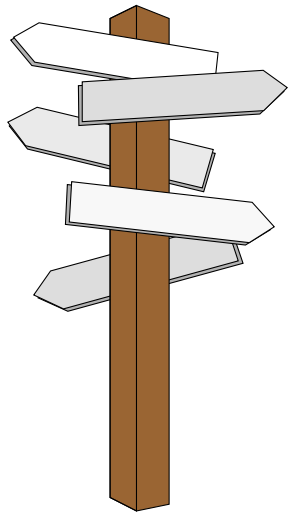


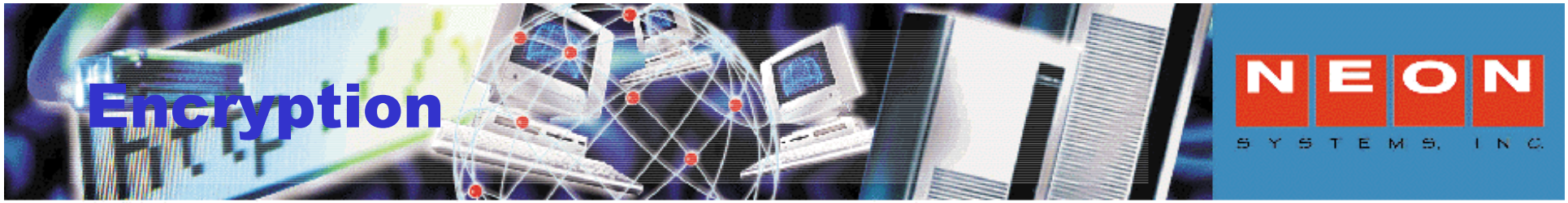
- Contact your favorite CA
- Provide documentation
  - DUNS number, incorporation papers, or even CPA audit
  - There are several classes of certificates
  - Prices start at around $400
- You get a certificate and insurance

What do I do with the certificate?

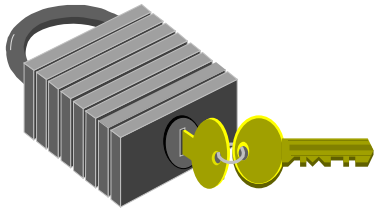
NEON SYSTEMS, INC.

- Install it on your server
  - See server documentation for details
- You'll also need a trusted root
  - A certificate self-signed by your CA
  - The SSL code requires this
- All certificates reside in a "key file" on the server





- Both Encryption and Decryption require the use of a key
  - If same key is used for both, it's symmetric
    - If someone discovers your key, you're toast!
  - If not, it's asymmetric
    - Public-key encryption is one example
- SSL uses both symmetric and asymmetric encryption



Symmetric vs. Asymmetric

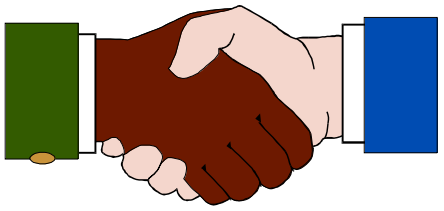
NEON SYSTEMS, INC.

- Symmetric is much faster
  - But, how do you exchange the key?
- Solution: use asymmetric encryption to exchange the key, then switch to symmetric
- Before you bother to compute the key, trade certificates
- This is the essence of SSL

The SSL Handshake

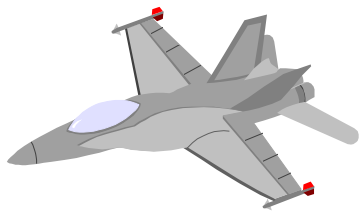
NEON SYSTEMS, INC.

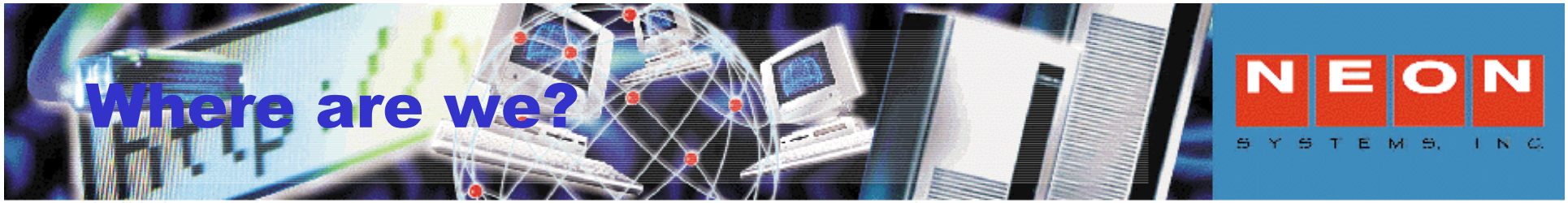
- Client requests URL, server sends certificate
- Client verifies certificate, sends cipher list
- Server selects cipher, tells client
- Client generates session key, encrypts it using server's public key, and sends it
- Server gets session key, then uses it to encrypt data sent to client



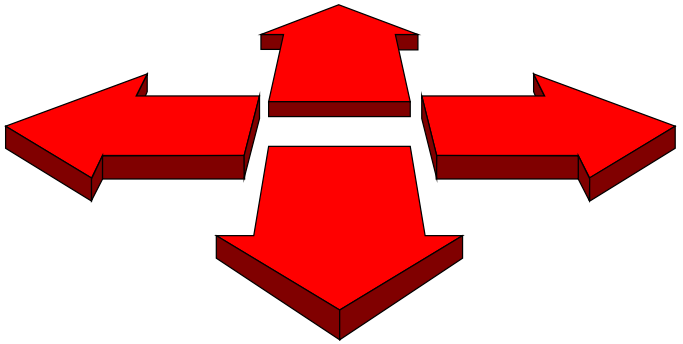
Session Key Caching

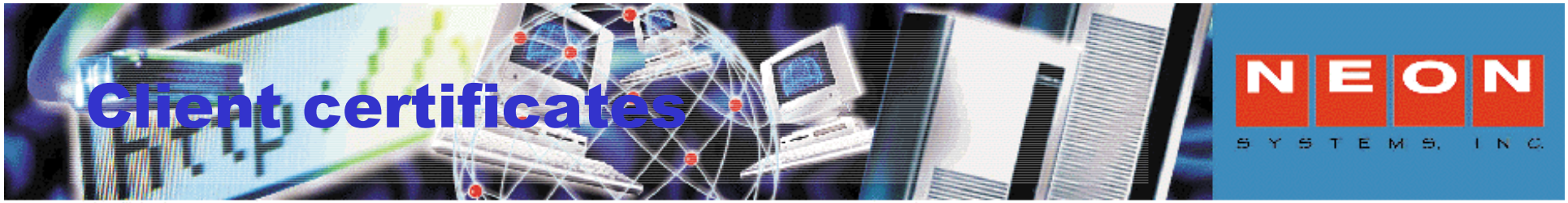
- The symmetric key used for encryption is also called a "session key", and is normally used for a single transaction.
- Some servers can cache this key and use it in later transactions.
- This saves the overhead of renegotiating the SSL handshake each transaction.





- The client trusts the server because of a signed digital certificate
- Traffic can't be intercepted, because everything's encrypted
- What's missing?





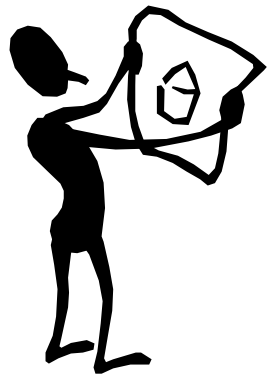
Client certificates

- Servers always have them, but client (browser) certificates are optional
- If you use them, password prompts are no longer necessary
- Identity proved by certificate more reliably than with userid/password combination

Why a client certificate?

NEON SYSTEMS, INC.

- The certificate can contain lots of information about the user:
  - e-mail address
  - RACF username and password
  - Other statistics (birthday, SSN, etc.)



- All of this information is available to a CGI
- No password prompts are necessary

Field	Value
Encryption cipher used	RC4-40, 40 bit
SSL Version	300
Client Certificate	
Serial number	f1f382f3f884f184 f9f48382f28182f8 858182f082f9f6f8 82f582f1f681f3f5
E-mail address	mike_lude@beyond-software.com
Common name	Michael Lude
Organizational unit	VeriSign Class 1 CA - Individual Subscriber
Organization	VeriSign, Inc.
Locality	Internet
Client's state or province	
Client's country	
Issuer's organizational unit	VeriSign Class 1 CA - Individual Subscriber
Issuer's organization	VeriSign, Inc.
Issuer's locality	Internet
Issuer's state or province	
Issuer's country	
Certificate valid from	Wednesday, February 18, 1998 at 12:00:00 AM
Certificate valid until	Monday, April 20, 1998 at 12:59:59 AM
Status	REVOCATION UNKNOWN

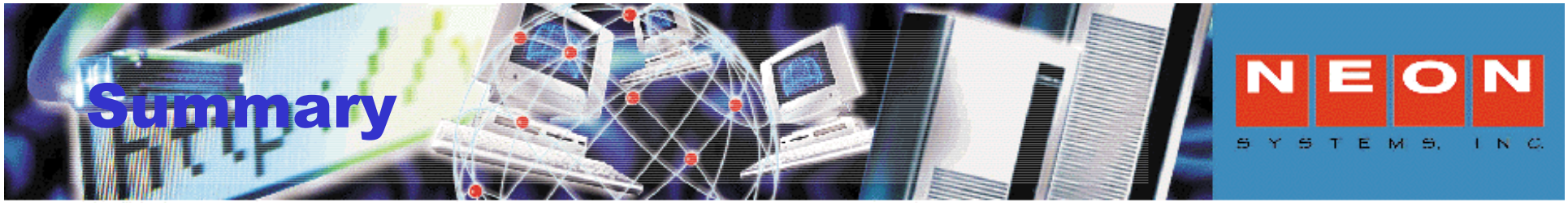
Client Certificate Considerations

NEON SYSTEMS, INC.

- Client certificates start at $10 for one year
- You can become your own CA for $1500
  - Software generally runs on Unix or NT
  - Send certificates and your trusted root to all of your users
  - Manage revoked certificates

- Administrative headache, but may be worth it

Summary



- Access control, Authorization, and Encryption should be used in combination
- SSL is the correct answer for Web servers
- Start out with just server certificates
- A move to client certificates provides better authentication, but more hassle