On An Architecture for Securing Web Objects

ASEE/NCS Conference on April 2, 2004

Dr. Peter H. Chang

Lawrence Technological University

chang@ltu.edu
Topics

- Introduction
- Proposed Security Architecture
- Web Server and Environment Variables
- Session ID
- Placeholder and Encryption
- Example
- Demo and Q&A
E-Commerce, Web Object, Security

- Internet e-commerce activities grow more and more every year
- Reliable Internet security is needed for securing the capitals invested in these activities
- Hyperlink as an Example of Web Object
  - Attribute: link reference
  - Operation: navigation to another web page
- Other Examples of Web Objects
  - XHTML form element
  - JavaScript object

chang@ltu.edu
Topics

- Introduction
- Proposed Security Architecture
- Web Server and Environment Variables
- Session ID
- Placeholder and Encryption
- Example
- Demo and Q&A
Proposed Architecture

- Model the Web Client/Server Entities as Objects
- Add security wrapper to the associations
Propose an approach to add a security wrapper to a web object inside a web document.

An implementation of the security wrapper is encryption. Other implementations are applicable to the architecture.

This approach either replaces a common approach of encrypting the whole web document or complements the common approach by adding an additional encryption to the web object.
Topics

- Introduction
- Proposed Security Architecture
- Web Server and Environment Variables
- Session ID
- Placeholder and Encryption
- Example
- Demo and Q&A
Web Client and Web Server

- Web Client: Web Browser
- Web Server: Apache, Microsoft IIS
- HTTP protocol is used for a session of communication between client and server
- In a session, client sends requests; server processes the requests and sends responses
- Server may either download static web pages or generate web pages and download them

chang@ltu.edu
Environment Variables

- Web server maintains a list of environment variables for the session with a client
- Examples of environment variables for Apache:
  - HTTP_HOST
  - REMOTE_ADDR
  - REMOTE_PORT
  - REQUEST_METHOD
  - SCRIPT_NAME
Topics

- Introduction
- Proposed Security Architecture
- Web Server and Environment Variables
- Session ID
- Placeholder and Encryption
- Example
- Demo and Q&A
Session ID

- Session ID uniquely identifies a session of communication between a server and a client.
- Session ID may be formed by the combination of the values of the environment variables REMOTE_ADDR and REMOTE_PORT.
- This is the simplest form. To be more precise we may append a time stamp to the combination.
- There are other ways to form session id.
Topics

- Introduction
- Proposed Security Architecture
- Web Server and Environment Variables
- Session ID
- Placeholder and Encryption
- Example
- Demo and Q&A

chang@ltu.edu
XHTML Hyperlink as Web Object

- XHTML anchor tag: `<a href="URL">`

- URL (Universal Resource Locator) is the web address of either a web page or a server side script that is executable. A task of such a script is generating a web page. But it may perform other tasks beforehand.

- If the URL refers to a server side script, the GET method of the HTTP protocol allows argument and value pairs to be passed along in the form of `<a href="URL?arg1=val1&arg2=val2…”">`
Placeholder and Encryption

- The values in the argument-value pairs in the anchor tag contain sensitive information that dictates the dynamic behavior of the server side script identified by the URL.

- We propose replacing values in the argument-value pairs by a placeholder that is recognizable by the server side script. The script converts the placeholders to appropriate values and encrypts these values.
Topics

- Introduction
- Proposed Security Architecture
- Web Server and Environment Variables
- Session ID
- Placeholder and Encryption
- Example
- Demo and Q&A
Example – A Company’s Intranet Site with a Hyperlink to Phone Directory

Suppose the home page contains such a hyperlink as shown below:

```html
<a href="getcontent.pl?template=phoneDirTemplate.html&sessionId=ZZZZZZZS&sessionKey=ZZZZZZZK&accessSeqNumber=ZZZZZZZA">Phone Directory</a>
```
Encryption

- Consider a base character array `basechars` with 62 elements matching the alphanumeric characters.
- Randomly generates an encryption key less than 62.
- Split input string into a character array.
- Use a one-to-one mapping that maps each character in the character array to another character. If a character is alphanumeric, then the mapped character is also alphanumeric.
Demo and Q&A

Thank You!

chang@ltu.edu