

# Authentication with Bluestem

<https://www-s4.uiuc.edu/bluestem-notes/>

Milt Epstein

Integration and Software Engineering

CITES

March 29, 2006

# Outline

- What Bluestem is
- How Bluestem works
- Some technical details
- Other Bluestem features
- Installation demonstrations
- Questions

(Note: I will be talking about Bluestem 1.2)

# What Bluestem Is

- A mechanism to authenticate (i.e., identify) web-based users
- A means of protecting (i.e., restricting access to) web-based resources (both static and dynamic)
- “UIUC WWW Authentication Service”
- Developed by Ed Kubaitis (initial beta versions are almost ten years old)

# Bluestem In Action

<https://immix.cso.uiuc.edu/bluestem/test1.cgi>

# Basic Bluestem Flow

1. User visits Bluestem-protected resource (assume first visit)
2. User logs in
3. User gets access to resource

# A note on IDs

- “Full” Bluestem ID: **netid@domain/auth**
  - For example: **mepstein@uiuc.edu/kerberos**
- Bluestem installations have a default domain and a default auth
  - For UIUC: domain=**uiuc.edu**, auth=**kerberos**
- “Short” ID has domain and auth stripped if they match defaults
  - For example: **mepstein**

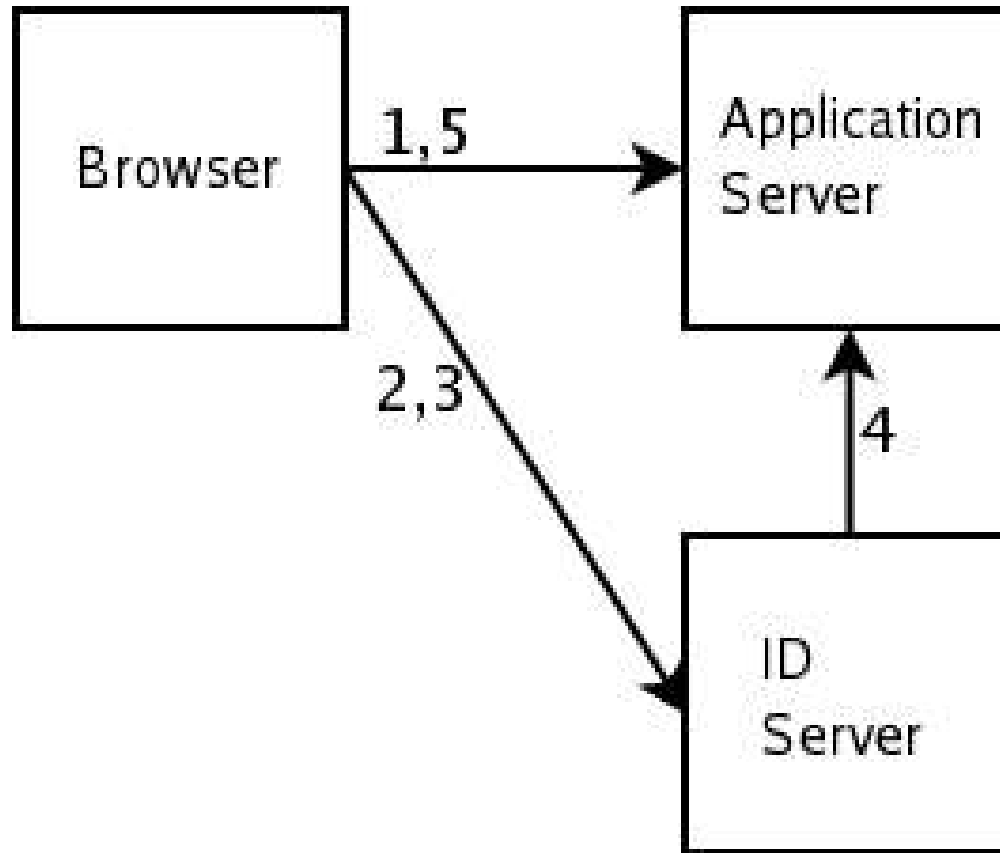
# Bluestem Components

- User
- Browser
- Application server: authorized departmental/unit server running the Bluestem application server code
- ID Server: secure CITES-managed server running the Bluestem ID server code (can be clustered)

# Bluestem Flow, Revisited

1. User directs browser to Bluestem application on Bluestem application server (assume first visit)
2. Bluestem Application Server redirects browser to Bluestem ID server, where user enters their NetID and password
3. Bluestem ID server redirects browser back to Bluestem application server

# Bluestem Flow, Pictorially



# Bluestem Requirements

- User: must have a NetID (and know password)
- Browser: must support SSL and cookies
- Application server: web server with SSL, server certificate, Perl, required Perl modules, authorized to use Bluestem
- ID Server: Unix, Apache with SSL, server certificate, Perl, required Perl modules, stunnel

# How Does Bluestem Know If The User Is Logged In?

- When a user logs in, Bluestem stores a cookie on the browser and creates a *cache file* on the application server
- The cookie is a “key” to find the cache file
- When a user visits a Bluestem application, if it finds a “valid” cache file (as pointed to by the cookie), the user is logged in

# What Bluestem Is, Revisited

- Perl code that Perl CGI scripts can use
- Sample usage pattern

(from <https://www-s4.uiuc.edu/bluestem-notes/perl-api.html>):

```
use lib('BluestemLib');
```

```
use Bluestem;
```

```
($ID, $IdleTime, $SessionTime) = &bluestem_id;
```

```
&bluestem_login($ReturnURL) unless $ID;
```

```
&bluestem_login($ReturnURL, "Idle more than $IdleMax seconds.")
```

```
  if $IdleTime > $IdleMax;
```

- HTTP

Perl  
CGI  
Script



Bluestem  
Code

# What If You're Not Using Perl

- **Bluestem Document Server**

(<https://www-s4.uiuc.edu/bluestem-notes/doc-cgi.html>)

- **Bluestem Little Bluestem API**

(<https://www-s4.uiuc.edu/bluestem-notes/other-api.html>,  
<https://www-s4.uiuc.edu/bluestem-notes/othersoftware.html>)

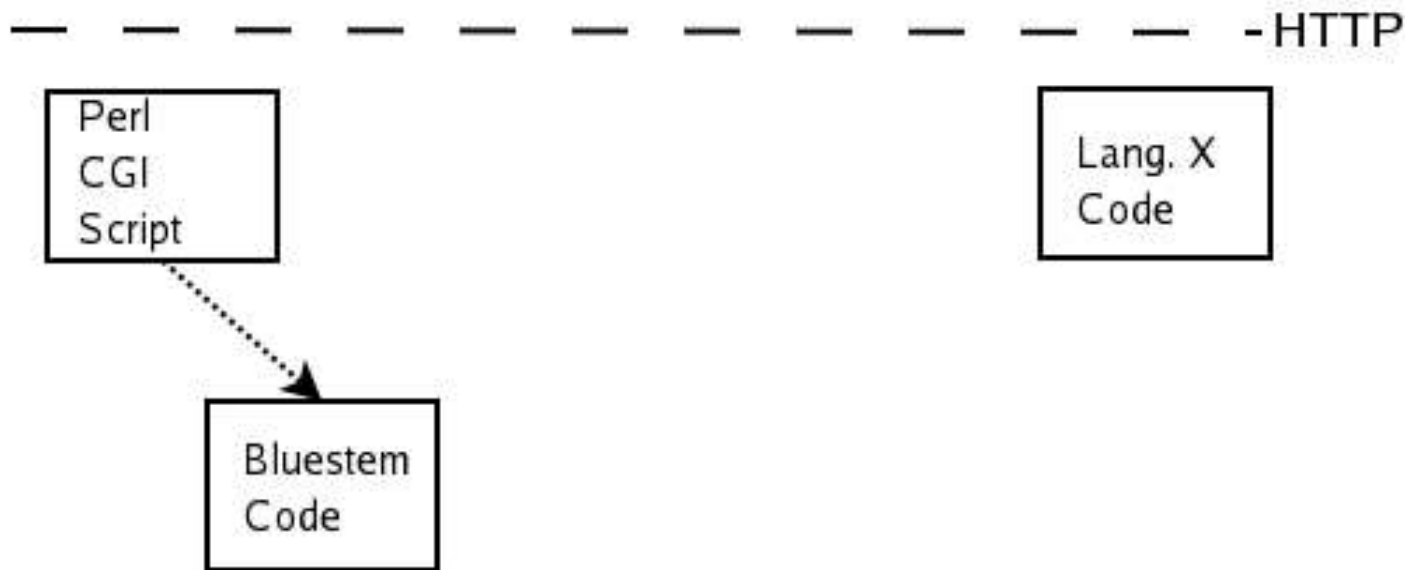
# Document Server (doc.cgi)

- <https://immix.cso.uiuc.edu/bluestem/doc.cgi/test/test.txt>
- Define a directory as the *restricted document root*
- Content underneath this root is controlled by **doc.cgi**
- The Path Info **test/test.txt** specifies the relative path to the desired resource
- Directories in path may contain a file that lists what IDs are allowed to access resources in that directory
- Configuration contained in **doc.conf** file
- Can be used for both static and dynamic resources

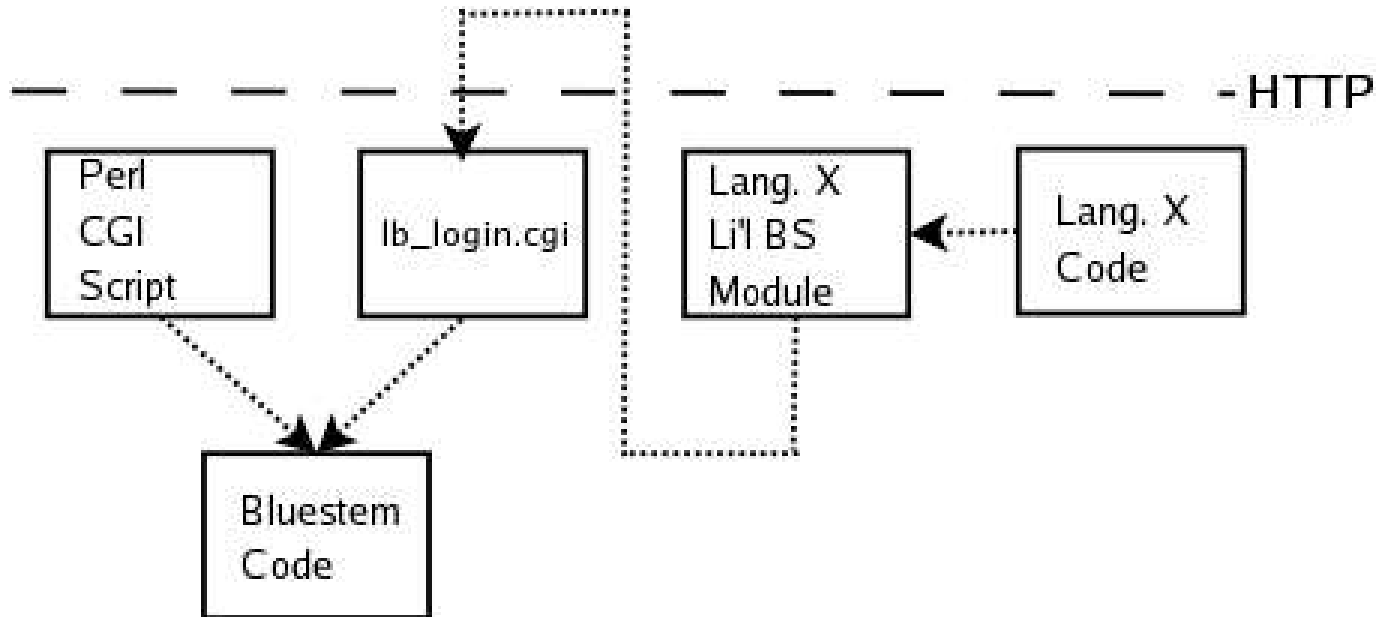
# Little Bluestem API

- Allows Bluestem to be used with non-Perl server-side languages/environments
- “Breaks” Bluestem into two pieces
  - Little Bluestem implementation in target language: checks whether the user is logged in (by looking for the cookie and the cache file)
  - Helper script that calls the main Bluestem Perl code (and redirects to the ID servers for login)

# Little Bluestem API



# Little Bluestem API



# Little Bluestem API (cont'd)

- Bluestem distribution includes
  - reference implementation (**LBluestem.pm**)
  - helper Perl CGI script (**lb\_login.cgi**)
  - test script (**lb\_test.cgi**)
- Implementations available for Apache (**mod\_bluestem**), Java, ASP, ASP.NET, PHP, ColdFusion (unsupported)

# What If You Have Some Non-UIUC Users

- Bluestem Password Facility (PWF)  
(<https://www-s4.uiuc.edu/bluestem-notes/pwf.html>)
- Bluestem admins can request a *PWF database* (essentially a list of users)
- PWF Bluestem ID:  
username/databasename
- Note: PWF databases are global, not per application server

# Bluestem Miscellanea/Trivia

- “Login” page was workaround for server/browser bugs, gone in 1.2
- Separate NetID/password pages because Bluestem is “Federated”
- Stats (activity, browser)  
<https://www-s4.uiuc.edu/bluestem-stats/>

# Authentication vs. Authorization

- Authentication: determining a user's identity
- Authorization: determining what a user is allowed to do (e.g., whether they are allowed to access a certain resource)
- Bluestem does **authentication**
- It's up to the application using Bluestem to do authorization

# Bluestem Troubleshooting

- Inaccurate server time
- Full disk/partition
- Incorrect directory/folder permissions
- Incorrect web server configuration
- Check log file (**<LogDir>/bluestem**) for more detailed error message

# Bluestem Best Practices

- Use `cache_clean` regularly
- Think about whether you really need to put something behind Bluestem
- Set reasonable timeouts (idle, session)
- Encourage logout (provide logout link/button)
- Don't forget authorization

# Bluestem Advantages

- Easy to install and use
- Works with a variety of server-side languages/environments
- Centralized
- Secure
- All UIUC users automatically can login

# The Future of Bluestem?

- Bluestem 1.2
- Prior Auth
- Improved Installation?
- Authentication Roadmap

<http://www.cites.uiuc.edu/roadmaps/authentication/>

# Bluestem Installation

- Prerequisites/assumptions
  - SSL-capable web server
  - Server certificate
  - Perl, certain Perl modules
  - Server has been registered as an authorized Bluestem application server
    - Mail [bluestem-mgr@uiuc.edu](mailto:bluestem-mgr@uiuc.edu) with server name, server admins, usage description

# Bluestem Installation (cont'd)

- Unix

<https://www-s4.uiuc.edu/bluestem-notes/appl-install.html>

- Windows

<https://www-s4.uiuc.edu/bluestem-notes/appl-install-nt.html>