BAFTA View Security Overview

Author: Ben Jefferson, BAFTA and BAFTA Media Technology CTO
Date: 07.09.22
Version: 1.2

1. Introduction

BAFTA has developed a web interface to provide BAFTA members with a single central location to access online screeners.

This is not a video delivery platform itself, rather it collates all of the videos available to members and allows them to quickly and easily access the videos on whichever platform the studio/distributor has chosen to use to provide online streaming.

Part of the vision for this system is that studios and distributors trust BAFTA to authenticate BAFTA members and provide access to the videos without those members having to go through a secondary platform-specific authentication process when they want to watch a video.

This single sign-on approach will not be mandatory and we accept that some video delivery platforms may still require additional separate authentication processes, however we would like to do all we can to reassure studios and distributors that this will not be necessary.

We appreciate that buying into this single sign-on model will require that the studios and distributors have faith in the security of the BAFTA View platform and the user authentication processes that it uses.

This web based platform is delivered through both a desktop web interface and via an Amazon Firestick wrapper which makes the BAFTA app available on Firestick devices through the Amazon app store. Although the BAFTA app will be available publicly on the app store, no functionality will be available without a login and only BAFTA members will be able to login.

2. User Authentication

BAFTA View will be available to all BAFTA members. The content visible to each member will depend on their voting rights (e.g. if they are a TV or film voting member, what chapters they belong to etc).

Login to BAFTA view is a two step process. The first step is to use a username and password to log into the BAFTA Hub. This is a central portal page which gives members access to the BAFTA members area, the event booking system and the voting and viewing systems. Access to the voting system or BAFTA View requires members to complete the additional two factor authentication step described below.

2.1. Two Factor Authentication

BAFTA members already sign in to BAFTA's online voting system using a combination of username and password and a 6 digit code sent to their mobile. This same system is also used for logging in to BAFTA View. Once the user has successfully logged in, and assuming they have ticked the "remember me on this computer" tick box, then a secure cookie is stored by their browser to act as the second factor for future logins. This means that they are able to log in using the same browser (or Firestick-enabled TV) with just their username and password for 6 months without needing the accompanying 6 digit code. This provides a good balance of security and usability.

BAFTA View also has an administrative interface which gives administrators within BAFTA access to the content. All BAFTA View administrator accounts require either a fixed IP address, or, for staff accessing from outside the office, a time-base one time password (TOTP) for all logins.

2.2. Brute Force Protection

A "brute force" attack consists of an attacker using automated tools to make repeated login attempts to try and guess a user's password. BAFTA Single signon system limits attempts to login with the same username to a maximum of 5 failed attempts per minute. This approach stops brute force attacks by requiring human input for each individual guess, administrative burden and user frustration of account locking based approaches.

2.3. Password Strength

BAFTA members will log into BAFTA View using the same username and password as they use to access the BAFTA online voting system. In line with current guidance from the UK National Cyber Security Centre (see https://www.ncsc.gov.uk/collection/passwords/updating-your-approach) the voting system does NOT force users to change passwords regularly, or impose arbitrary password complexity rules. Rather password security is enforced through ensuring adequate password length.

3. Network Security

3.1. Firewalls

All BAFTA View API servers will be hosted on Amazon AWS EC2 servers. These will be protected using the Amazon AWS firewall. The firewall will be configured to allow public access to the web server (ports 80 and 443), but block public inbound access to all other services on the server. Port 80 will only be used to server redirects to the user's browser to direct them to the secure (https) site. The only service, other than web which will be available on the server is SSH (port 22). The firewall will be configured such that SSH access is not public but allowed only from a limited number of BAFTA's fixed IP addresses.

As an additional fail-safe, the same rules will be configured on the Linux kernel firewall on the server so that even if the AWS firewall was misconfigured or accidentally switched off the same protection would be provided on the server itself.

4. Server Security

4.1. Single Purpose Virtual Server

BAFTA View will be hosted on its own EC2 server instance. This means that the site and data is not put at risk by the possibility of software malfunction or configuration errors in other sites hosted on the same server.

4.2. Security Updates

The BAFTA View API server runs Ubuntu 18.04 LTS (Long Term Support) server. This version of Ubuntu is supported until April 2028.

The BAFTA View server runs Amazon Linux 2. This version of Linux is supported until June 2024 (see https://aws.amazon.com/amazon-linux-2/faqs/)

Each server will be configured to automatically apply security updates using the relevant package manager.

Applying updates automatically brings a very slight risk that these updates might introduce unexpected incompatibilities, but by only applying essential security upgrades this risk is minimised. We feel that the risk from allowing security vulnerabilities to go unpatched far outweighs the risk of problems arising from automatically applying security fixes without prior testing.

4.3. Backups

The BAFTA View server does not store any user data, this server simply hosts the HTML and Javascript code for the system. All of this is stored in BAFTA's Github code repository. In addition to this 7 daily EBS snapshots of the server are retained to speed up reinstatement in the event of server failure.

5. Application Security

5.1. HTTPS

BAFTA View will be accessed over a secure web connection (HTTPS). The server will be configured to accept unsecured HTTP connections, however it will immediately redirect the user to the equivalent secure page. Using a secure web connection means that all data exchanged between the user's browser and the server is encrypted. It also makes it impossible for anyone to set up a spoof website with the same domain name.

BAFTA View will be configured to issue HTTP Strict Transport Security headers (HSTS) - these ensure that browsers know to connect to the site only using a secure connection. This protects the site from protocol downgrade attacks (where an attacker tricks users to connecting to an unsecured version of the site).

5.2. Password Storage

User and administrator passwords will be stored using the PHP password_hash function (see http://php.net/manual/en/function.password-hash.php). This is the best practice approach recommended by PHP authors. This means that even if an attacker were to gain access to the password store it would require an unfeasibly large amount of computing power to decrypt these passwords.

5.3. Penetration Testing

Most software authors will claim that their systems are secure, but the real proof of the pudding is when this is put to the test by independent security experts who have been tasked with finding security vulnerabilities. This is called “penetration testing”.

BAFTA have an ongoing contract for the provision of penetration testing from Armadillo Security (https://www.armadillosec.co.uk/). They will be tasked with penetration testing BAFTA View on its completion. We will be happy to share their report and details of the actions taken in response to it with studios and distributors where an NDA is in place.