BAFTA Nucleus – Security Overview

Author: Ben Jefferson
Date: 30/5/2017
Version: 1.0

Introduction

BAFTA developed Nucleus to allow film and televisions makers, distributors and broadcasters to enter BAFTA's range of awards and learning programmes. The importance of the BAFTA brand as a synonym for excellence, and the damage that could be done to this through a security breach, means that security has been paramount from the very start of the project.

The comprehensive functionality and the ease of use of Nucleus has resulted in interest in using the system from other organisations. This document has been drawn up to enable prospective users of the system to assess whether the security measures which have been put in place to protect the data held in the system from loss of confidentiality are in line with their organisational security policies.

Network Security

Firewalls

All entry system instances are protected using the Amazon AWS firewall. The firewall is 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. The only service, other than web which is available on the server is SSH (port 22). The firewall is configured so that SSH access is not public but allowed only from a limited number of BAFTA fixed IP addresses.

As an additional fail-safe, the same rules are 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.

Server Security

Dedicated Server

Each client has their own separate instance of the entry system running on a dedicated server. This means that even if there is a software malfunction or configuration error, there is no way that data belonging to one client can be revealed to another.

This approach also means that peaks in demand for one client will not affect other clients. The size of each server can also be configured separately for each client to give the desired balance between, cost, capacity and speed.

Security Updates

Nucleus is currently installed on Ubuntu 14.04 LTS (Long Term Support) server. This version of Ubuntu is supported until May 2019. BAFTA will test the entry site against Ubuntu 16.04LTS (or another suitable Linux distribution with long term support) before the end of 2018 and provide any necessary updates to support this.

Each server is configured to automatically apply security updates as described here: https://help.ubuntu.com/lts/serverguide/automatic-updates.html

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 from automatically applying security fixes without prior testing.

Backups

Each instance is configured to use Tarsnap (http://www.tarsnap.com/) for backups. Tarsnap is a cloud based backup service which automatically encrypts all data stored in it. Data is encrypted before it even leaves the originating machine using a 2048 bit RSA key. This means that even if the storage behind Tarsnap (which is actually Amazon's S3 service) is compromised, even then no one can read the data. This also ensures that not even Tarsnap staff can read the data of Tarsnap customers.

Each customer instance of the entry system is set up with a separate backup key so that one customer cannot access the backups of another customer.

Application Security

HTTPS

Nucleus is accessed over a secure web connection (HTTPS). The server is 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.

Password Storage

Passwords are stored by the entry system 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.

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. Nucleus automatically uses a CAPTCHA (specifically, Google's free ReCAPTCHA service) after 4 failed login attempts using the same username in any 30 minute period. This approach stops brute force attacks by requiring human input for each individual guess, whilst being completely invisible to users for most of the time. Crucially this approach avoids the administrative burden and user frustration of account locking based approaches.

Password Strength

Nucleus provides functionality to stipulate a minimum length and maximum age for administrator passwords. This functionality currently only applies to administrators i.e. there are currently no age, complexity or length requirements for entrant account passwords.

2 Factor Authentication

Nucleus supports Google Authenticator 2FA for administrator logins. This is configured on a per-user basis so it can be enabled for one user and not for another. There is also the option to require 2FA for a user only when they are accessing the system from an unrecognised IP address. This features provides a good balance of usability and security with the user required to use the Google Authenticator app. only when they are trying to access the system from outside their normal work network (this assumes that the work network has a fixed IP address and does not use any outbound web proxy).

This functionality can also be used to block administrative access outside the normal office network by configuring 2FA on the user account but not actually configuring the Google Authenticator app for the user. Using this approach, any attempt to log on outside of the normal work network will prompt them for an additional 6 digit code which they have no way of knowing.

Permissions model

Nucleus implements 2 levels of permissions for administrators. "Superusers" can see and administer all entries and all aspects of the entry system except for finance-related fields (see below). Ordinary administrators (non-superusers) cannot see or edit entries for the awards which have not been assigned to their user. Non-superusers cannot change which awards are assigned to them.

A third permission which can be assigned to administrators (be they superusers or not) is a finance permission. Only administrators who have been assigned the finance permission are allowed to perform sensitive operations relating to modifying pricing and invoices.

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”. Nucleus has been subjected to penetration testing by security experts at Matta Consulting (http://www.trustmatta.com). This was an invaluable exercise which highlighted several potential weaknesses which we were able to address. We are happy to share their report and details of the actions taken in response to it with prospective customers once an NDA has been signed.