Guidelines for Secure Deployment of Video-Based Digital Diagnostics: Case Study of a Game-Based System for Developmental Delays, SocialPlai, on UCSF Infrastructure

Aayush Nandkeolyar[1], Md Rahat Shahriar Zawad[2], Katy Tarrit Mirakhorli[3], Peter Washington[1]

[1]University of California – San Francisco, San Francisco, CA, USA;

[2]Rice University, Houston, TX, USA;

[3]University of Hawaii at Manoa, Honolulu, HI, USA

INFORMATICS PROFESSIONALS. LEADING THE WAY.

Abstract

SocialPlai is an AI-powered website delivering two-player browser games for ADHD and autism screening. This poster outlines UCSF's secure deployment, including Amazon Web Services (AWS) hosting under a Secure Enterprise Cloud (SEC), a public-facing F5 load balancer for Network Address Translation (NAT), and restrictive firewall rules at the network and cloud levels. We present implementation requirements for this system, offering a blueprint for other academic centers to deploy complex digital health tools with HIPAA-compliant infrastructure.

Introduction

We have developed a system for remote two-player games, SocialPlai[1] (**Figure 1**), with the goal of making diagnosis of autism and Attention-Deficit/Hyperactivity Disorder (ADHD) scalable, accessible, and engaging. During gameplay, video and audio are recorded of both players, to be used in multimodal diagnostic deep learning models that predict diagnoses from video, audio, and gameplay metadata. Innovative digital health tools like SocialPlai require robust IT infrastructure to protect patient data and meet compliance standards. Deploying SocialPlai at UCSF involved integrating the app into UCSF's secure digital ecosystem (**Figure 2**). UCSF hosts sensitive applications in special AWS accounts: for example, the SEC is an AWS account governed by UCSF security policies for sensitive data. This poster describes our secure deployment of SocialPlai on UCSF's infrastructure, providing a step-by-step guide for researchers at other institutions aiming to deploy remote digital assessments that capture video data.

Methods and Results

We implemented SocialPlai on UCSF's IT infrastructure using the following components and processes:

- **AWS Secure Enterprise Cloud:** SocialPlai is hosted on AWS in UCSF's SEC account. We configured a Virtual Private Cloud (VPC) with public and private subnets. An AWS Application Load Balancer (ELB) sits in front to distribute HTTPS traffic. Security groups and network ACLs restrict inbound ports to only 443 (HTTPS). This leverages UCSF IT Cloud Services, which provides AWS environments for sensitive data.
- **TLS Certificate:** The ELB terminates TLS using a UCSF-issued certificate. UCSF policy mandates using the internal certificate service; external CAs like Let's Encrypt or GoDaddy are not allowed. We requested a certificate via UCSF IT Security and installed it on the ELB. This ensures all client connections are encrypted and authenticated.
- **Network & Firewall:** The server instances reside in UCSF's network (via AWS VPC). UCSF campus firewalls only permit HTTPS (443) traffic to the ELB's static IP/DNS. Outbound requests (to MuleSoft or other services) are limited by security groups and firewall rules. VPN/MFA is required for admin access.
- **UCSF IT Collaboration:** Throughout, UCSF IT staff provisioned AWS resources, issued the TLS certificate, configured firewall and DNS, and reviewed security. UCSF IT's role was critical: they ensure MuleSoft (ESB/API Manager) is available and assist with building secure connections.

Methods Figure

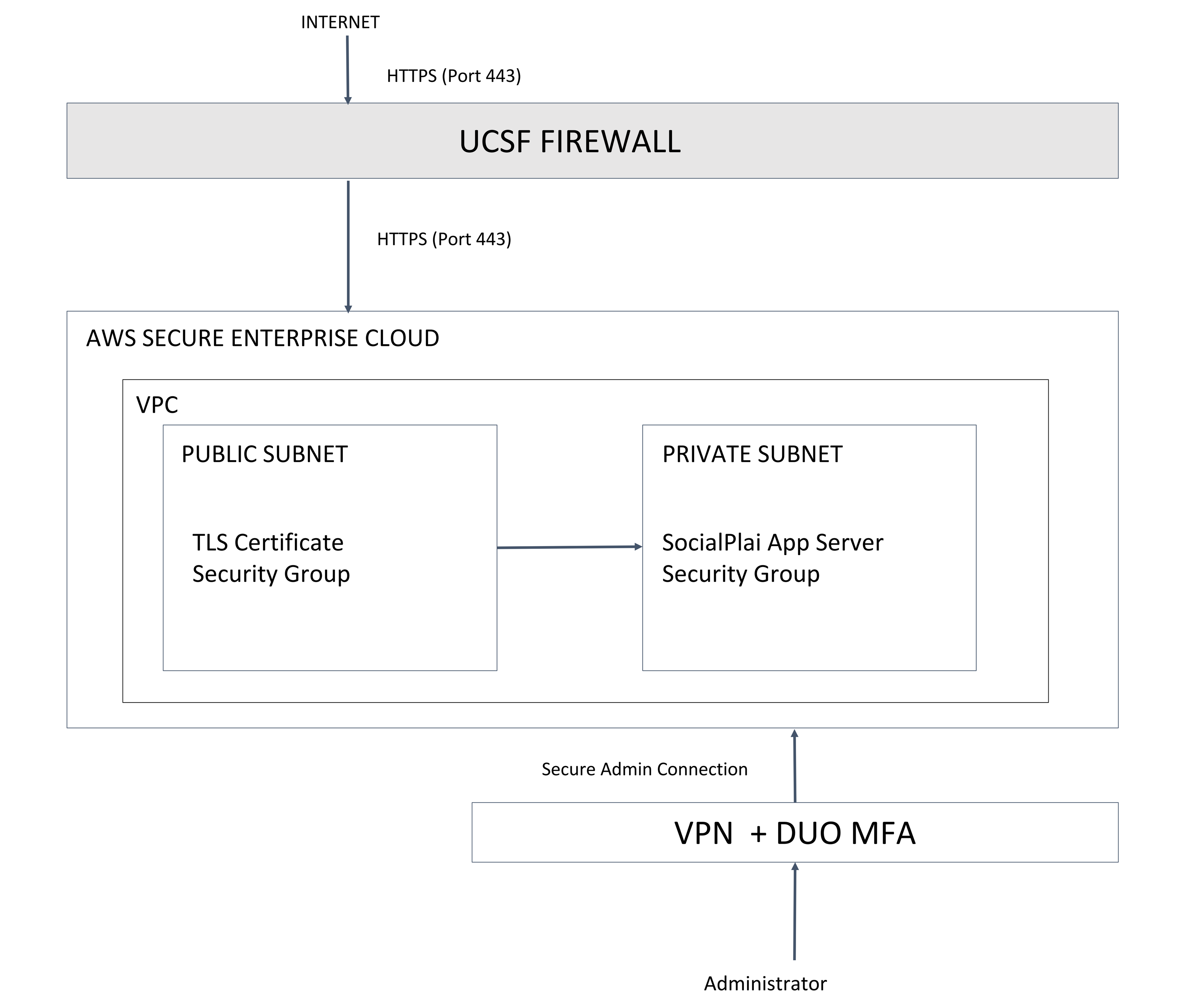

Figure 1. The multi-layered security approach for SocialPlai, using UCSF's firewalls and a segregated AWS Virtual Private Cloud (VPC) to protect application servers and ensure secure data flow.

Website Demo

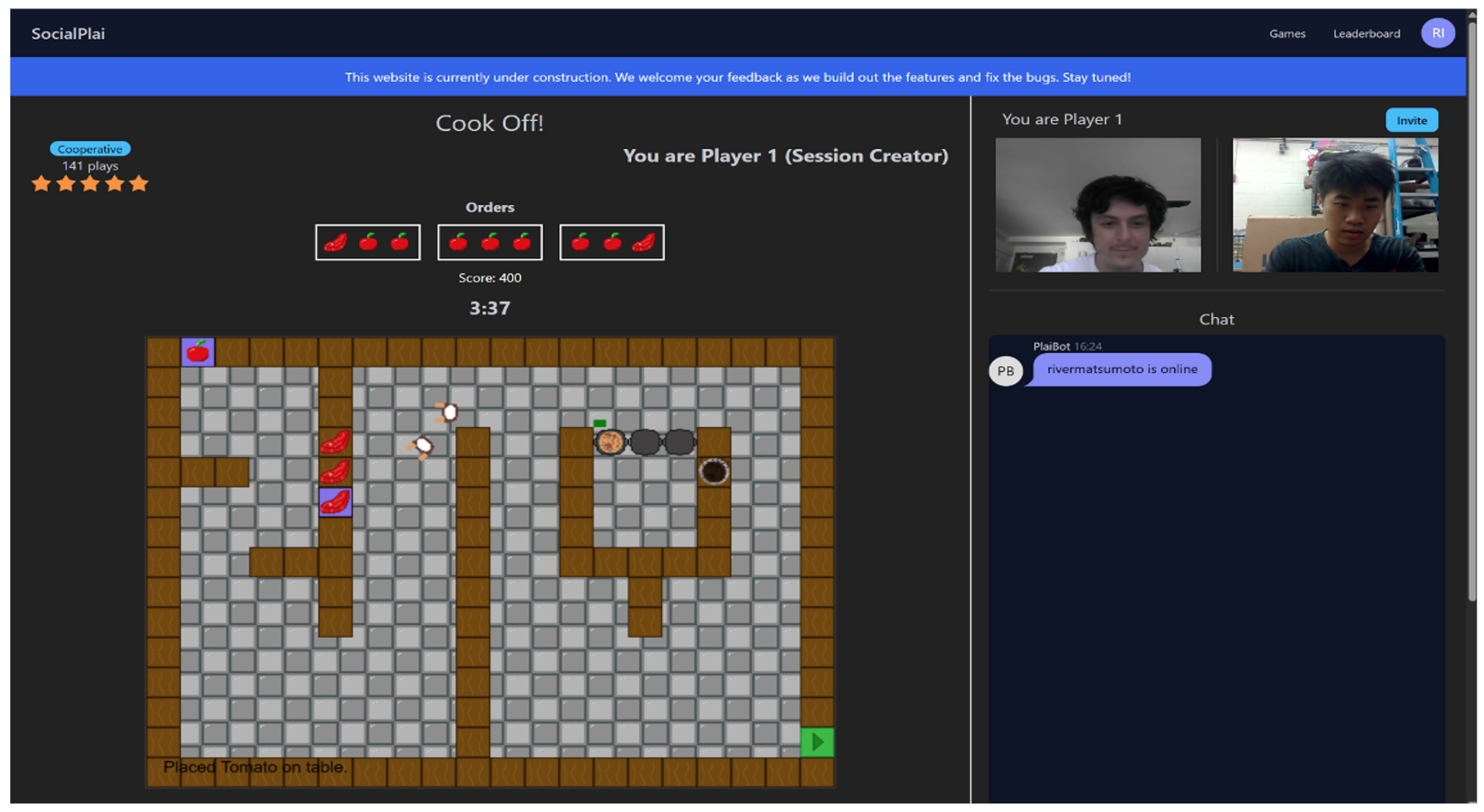

Figure 2. Example of a 2-player game on SocialPlai. Real-time video and audio are recorded and stored in a HIPAA-aligned server on AWS.

Acknowledgements

This work was funded by the National Institutes of Health (DP2EB0358584) via the Director's New Innovator Award. The content is solely the responsibility of the authors and does not necessarily represent the official views of the National Institutes of Health.

References

1. A. Jaiswal et al. "Digitally diagnosing multiple developmental delays using crowdsourcing fused with machine learning: Protocol for a human-in-the-loop machine learning study." *JMIR Research Protocols* 13, no. 1 (2024): e52205.