POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

FinTech Tycoon: un serious game per accrescere la consapevolezza della sicurezza informatica in ambito open banking

Relatori
prof. Antonio Lioy
prof. Andrea Atzeni

Candidato
Stefano Gennero

Anno accademico 2021-2022

Sommario

Negli ultimi anni l'utilizzo dei sistemi informatici ha registrato una notevole espansione in quasi tutti gli ambiti, sia quelli industriali che quelli sociali. Analogamente è aumentata la preoccupazione per la sicurezza informatica. Per valorizzare il fattore umano e fare sì che non diventi l'anello debole sfruttato per portare a termine gli attacchi è necessario che l'utente sia consapevole dei rischi che si corrono in un ambiente informatico. I serious games si sono dimostrati uno strumento efficace per portare avanti questo obiettivo. In questo studio viene effettuata un'analisi critica dello stato dell'arte per identificare un ambito non ancora considerato dai serious games esistenti. Nella seconda parte il lavoro si è concentrato nel design e nell'implementazione di un nuovo gioco con lo scopo di trasmettere concetti relativi alla sicurezza informatica nell'ambito identificato.

Ringraziamenti

Questo lavoro non sarebbe stato possibile senza la supervisione ed i consigli dei miei relatori, il Prof. Antonio Lioy e il Prof. Andrea Atzeni.

Vorrei ringraziare inoltre l'assistente di laboratorio e ricercatore Ignazio Pedone per avermi concesso l'utilizzo di una macchina virtuale del Politecnico di Torino al fine di rendere disponibile al pubblico il gioco realizzato.

Ringrazio la mia famiglia, che mi ha supportato lungo tutto il percorso universitario, anche nei momenti più difficili. Ringrazio in particolare mio padre Ezio e mia madre Paola che mi hanno permesso di studiare al Politecnico di Torino.

Infine un ringraziamento speciale va a Chiara, che mi ha sempre mostrato il suo supporto e il suo amore in questi anni di studio.

Indice

Capitolo 1

Introduzione

1.1 La sicurezza informatica

Negli ultimi anni l'utilizzo dei sistemi informatici ha registrato una notevole espansione in quasi tutti gli ambiti, sia quelli industriali che quelli sociali. Ciò ha permesso la creazione di nuove possibilità e l'utilizzo di nuovi spazi. Di conseguenza è stato, ed è tutt'ora, necessario occuparsi attivamente di sicurezza informatica. Questa ha come obiettivo la protezione dei sistemi informatici da attacchi, danneggiamenti e accessi illegittimi, che possono verificarsi intenzionalmente o accidentalmente. Ciò si traduce nell'utilizzo di tecniche, regole e comportamenti per mantenere l'integrità, la confidenzialità e la disponibilità dei dati presenti in un sistema informatizzato.

L'ambito della sicurezza informatica a livello globale acquista importanza di anno in anno, come suggerisce ad esempio un report di mercato di Cybersecurity Ventures: gli investimenti nel settore sono in continua espansione, passando da un valore di circa 75 miliardi di dollari nel 2015 [1] a un mercato da oltre 250 miliardi nel 2021. Questo aumento consistente è dovuto anche all'altrettanto consistente aumento dei danni provocati dai crimini informatici, che sono passati da un valore stimato di 3 bilioni di dollari nel 2015 a 6 bilioni nel 2021 [2]. Si stima che nei prossimi anni questo mercato continuerà a crescere per fronteggiare le continue nuove minacce ai sistemi informatici fino a raggiungere i 450 miliardi di dollari nel 2025 [3].

1.2 Il fattore umano

Un elemento ritenuto fondamentale per la sicurezza informatica è il fattore umano. Spesso gli utenti ritengono che la protezione di un sistema dipenda unicamente dall'utilizzo di antivirus, o più in generale di software apposito, ignorando il proprio ruolo nella prevenzione degli attacchi informatici. Molti esperti del settore hanno sottolineato negli anni con la frase "La sicurezza è un processo, non un prodotto" [4] il concetto che non esiste una soluzione definitiva al problema. In questo contesto l'utente ricopre un ruolo importante, perché con i suoi comportamenti può contribuire con un impatto sostanziale alla protezione del sistema.

Per valorizzare il fattore umano e fare sì che non diventi l'anello debole sfruttato per portare a termine gli attacchi è necessario che l'utente sia consapevole dei rischi che si corrono in un ambiente informatico. Date la scarsa efficacia e la difficoltà nel trasmettere conoscenze puramente tecniche ad una platea ampia ed eterogenea, sono stati introdotti i Serious Games.

I serious games rappresentano una tipologia di giochi che persegue degli obiettivi che vanno oltre il semplice intrattenimento, proponendosi come uno strumento informativo e educativo. Dopo le prime proposte di utilizzo dei serious games negli anni '70 [5], questi giochi sono stati gradualmente accettati e adottati, anche grazie allo sviluppo che ha caratterizzato l'industria dei giochi digitali [6]. L'utilizzo di giochi per scopi educativi è in rapido aumento: il mercato dei serious games ha visto negli ultimi anni un'espansione che lo ha portato ad un valore stimato di 6.29 miliardi di dollari nel 2020, con prospettive di crescita costante fino a raggiungere oltre 26 miliardi di dollari nel 2026 [7].

1.3 Obiettivi del lavoro

La copertura delle tematiche trattate nei Security Serious Games non è esaustiva, perché l'applicazione dell'informatica a nuovi ambiti comporta il proliferare di diversi contesti che è possibile trattare. Quindi l'obiettivo di questa tesi è allargare l'offerta dei serious games in ambito security. Partendo da un'analisi critica dello stato dell'arte è stato possibile individuare i giochi che più hanno inciso in questo ambito e i motivi del loro successo. Inoltre questa analisi ha portato anche all'identificazione di un tema non ancora considerato dal lavoro esistente, ovvero l'open banking.

Nella seconda parte il lavoro si è concentrato nel design e nell'implementazione di un nuovo gioco, Fintech Tycoon, con lo scopo di trasmettere concetti relativi alla sicurezza informatica. In questo contesto i dati raccolti nella prima fase hanno costituito il punto di partenza per costruire un serious game efficace, dotandolo anche di un sistema di valutazione dell'apprendimento interno che verrà descritto in seguito.

Capitolo 2

Serious Games

2.1 Concetti generali

Il concetto di serious game non è particolarmente recente: già nell'omonimo libro di Clark Abt del 1970 [5] si parla di questa particolare tipologia di giochi che "hanno un intento educativo esplicito e attentamente ponderato e non sono concepiti per essere giocati primariamente con fini di divertimento". Tuttavia è nel 2002 che questo concetto inizia ad assumere il significato che gli si attribuisce tuttora, principalmente per via di due eventi che si verificarono quell'anno.

Per prima cosa venne fondato il "Serious Game Initiative" [8], un progetto che si proponeva di supportare gli studi nel campo dei serious games e che ha contribuito a rendere noti questi nuovi strumenti di apprendimento. Inoltre durante lo stesso anno venne pubblicato "America's Army" [9], un videogioco realizzato su commissione del governo federale degli Stati Uniti, che mira a favorire il reclutamento nell'esercito americano, proponendo scenari di gioco realistici e simulazioni accurate della vita nell'esercito e delle operazioni militari. Questo viene considerato il primo serious game di successo, dato che riuscì a farsi notare da un ampio pubblico.

Dopo il 2002 i serious games hanno visto un crescente interesse da parte della comunità scientifica e delle istituzioni che si occupano di educazione. Nel corso del tempo sono state quindi elaborate ulteriori definizioni per questi nuovi strumenti. David Michael e Sande Chen, ad esempio, li hanno definiti come "giochi che non hanno l'intrattenimento, lo svago o il divertimento come loro scopo primario" [10]. Altri studiosi hanno preferito concentrarsi sulla definizione di cosa un buon serious game dovrebbe fare, come Kevin Corti che sostiene che "è tutta una questione di bilanciare il potere dei videogiochi per accattivarsi ed attrarre l'utente finale con uno scopo specifico, come ad esempio sviluppare nuove conoscenze e abilità" [11].

I serious games non si limitano all'ambiente videoludico, dato che esistono molti giochi da tavolo e basati su mazzi di carte che presentano uno scopo educativo. Tuttavia, per quanto riguarda questo lavoro, d'ora in poi dalla trattazione saranno considerati solamente i videogiochi. Questo perché Fintech Tycoon è un videogioco e quindi si è ristretto il campo di ricerca a questo medium specifico, in vista della sua realizzazione.

2.1.1 Classificazione dei serious games

I serious games costituiscono una categoria di giochi abbastanza ampia ed eterogenea, che è andata allargandosi nel corso del tempo. Data la grande varietà in molti hanno proposto vari sistemi di classificazione per inquadrare al meglio le differenze e le somiglianze all'interno della categoria. Tuttavia di tutte le proposte avanzate a partire dal 2002 nessuna è riuscita a imporsi nettamente sulle altre.

Le più semplici metodologie di classificazione si basano su un singolo criterio di valutazione sulla cui base viene effettuata la divisione in categorie. Principalmente si tratta di metodi market-based, che valutano la tipologia di utente a cui è destinato il serious game, oppure purpose-based,

che valutano lo scopo con cui è stato concepito il gioco. L'eccessiva semplicità nella valutazione non li rendono molto efficaci, dato che non tengono conto dell'effettivo contenuto dei giochi che vorrebbero classificare.

Tuttavia è a partire da questi metodi che nel 2008 gli studiosi Sawyer e Smith hanno tentato di creare un sistema di classificazione più completo [12]. Si tratta di una metodologia che utilizza entrambi i criteri precedenti e introduce maggiore complessità, andando ad aggiungere altre sotto-categorie. Anche questo sistema presenta delle imperfezioni: il criterio purpose-based risulta ancora troppo poco accurato per giochi elaborati.

Nonostante ciò l'idea di utilizzare più elementi di classificazione risulta convincente, dato che nel 2011 Damien Djaouti, Julian Alvarez e Jean-Pierre Jessel riprendono i 2 principi utilizzati da Sawyer e Smith e ne affiancano un terzo, il gameplay [13]. Si tratta di un elemento che è presente in qualsiasi gioco e, dato che i serious games non prescindono dalla propria dimensione ludica, viene introdotto nel nuovo sistema di classificazione. Con questo nuovo metodo i giochi vengono classificati secondo:

- il gameplay, che riguarda la struttura e le meccaniche che determinano come il serious game è giocato;
- lo scopo, che riguarda l'obiettivo che gli sviluppatori avevano in mente e che è stato tradotto nel design, che determina perché il serious game è giocato;
- l'ambito, che riguarda l'ambientazione e il contesto del gioco e determina da chi è giocato il serious game.

Per via di questa tripartizione è stato chiamato G/P/S Model (Gameplay, Purpose, Scope) ed è stato utilizzato per la creazione di un database in cui vengono catalogati i serious games [14] (Fig. 2.1). Anche questo modello presenta dei limiti, soprattutto nella granularità delle distinzioni (ad esempio giochi educativi molto diversi tra loro vengono classificati all'interno dello stesso mercato). Tuttavia si tratta di una classificazione più raffinata e funzionale delle precedenti.

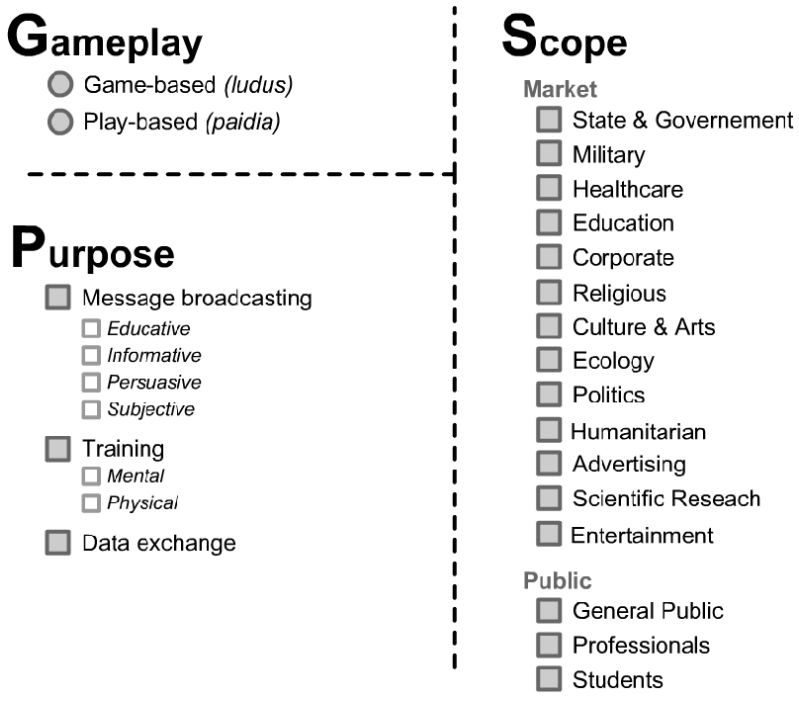

Figura 2.1. Schema che riassume la struttura del G/P/S Model (tratto da [13]).

2.1.2 Benefici dei serious games

Gli effetti benefici dei serious games sono stati e sono tuttora studiati da numerosi scienziati. Nel corso degli anni è stato confermato il fatto che utilizzare videogiochi possa aiutare ad aumentare le capacità di problem-solving, affinare il pensiero strategico e migliorare l'attenzione, la vista e la coordinazione, a seconda dell'area cerebrale attivata dal gioco in questione [15]. I videogiochi hanno trovato applicazione anche in ambito medico, sia per questioni legate alla riabilitazione fisica [16][17], sia per il trattamento di problemi psicologici: fobie, paure, disturbo da stress post-traumatico (PTSD) [18][19] o disturbo da deficit di attenzione e iperattività (ADHD) [20]. Questo è in parte dovuto al progresso tecnologico che ha garantito una maggiore immersività del paziente nel mondo di gioco.

D'altra parte sono stati effettuati numerosi studi per analizzare e individuare eventuali effetti negativi, che potrebbero essere conseguenza di un loro uso improprio. Alcuni risultati mostrano che un utilizzo di videogiochi prolungato e concentrato in brevi periodi può condurre il giocatore ad assumere comportamenti aggressivi [21] e abbracciare uno stato di distaccamento dalla realtà; addirittura nei casi più gravi può causare l'insorgere di stress, ansia o depressione. Questi sintomi, nel 2018, sono stati ufficialmente identificati all'interno dell'undicesima revisione della Classificazione Internazionale delle Malattie (ICD-11) dal World Health Organization (WHO) come "gaming disorder", malattia appartenente alla famiglia dei disturbi mentali e comportamentali [22]. Tuttavia questa decisione è stata ampiamente criticata e ritenuta prematura, data anche la limitatezza di dati a supporto della teoria [23].

Parlando ora in modo specifico di serious games, oltre ai vantaggi elencati in precedenza, bisogna considerare anche i benefici che sono una stretta conseguenza della loro natura pedagogica.

Coinvolgimento. I serious games sono prima di tutto dei videogiochi e sicuramente una componente fondamentale è quella ludica. Il fatto che sia possibile trascorrere molto tempo a giocare senza particolari remore è dovuto al coinvolgimento, una conseguenza del divertimento che un videogioco ben strutturato riesce a regalare al giocatore. Questo è l'aspetto fondamentale che i serious games sfruttano per mantenere alto il livello di concentrazione di chi gioca, evitando distrazioni dovute a poco interesse e noia tipiche dello studio scarsamente motivato. Tuttavia per coinvolgere il giocatore è possibile sfruttare anche altri aspetti psicologici come la curiosità, che può spingere un utente ad immergersi più a fondo nel mondo di gioco per esplorarlo e scoprire tutti i suoi aspetti. Il metodo più efficace per generare coinvolgimento in chi gioca consiste nel creare continue sfide: proponendo ostacoli da superare e obiettivi da raggiungere è possibile mantenere alta la concentrazione e procurare un senso di soddisfazione al giocatore dopo che questo ha completato una sfida, spingendolo a gettarsi nella prova successiva. Questo aspetto è stato analizzato in molti studi che esplorano gli stati mentali che un soggetto attraversa quando affronta un'attività basata sulle sfide [24][25].

Uno sviluppatore di serious games dovrebbe porsi l'obiettivo di mantenere il giocatore all'interno del cosiddetto "Canale di Flusso" per mantenere alta la sua motivazione a giocare. Per questa ragione all'interno del gioco dovrebbe essere integrato anche un sistema di feedback per rendere l'utente consapevole dei propri progressi e coinvolgerlo attivamente nel processo di apprendimento. Inoltre i serious games offrono la possibilità di compiere errori senza ansie tipiche del mondo reale, dato che sbagliare nel mondo di gioco non porta con sé conseguenze tangibili; il fatto di poter riprovare più volte dopo aver sbagliato permette di capire e imparare in modo più efficace. Naturalmente, per ottenere i risultati migliori sotto quest'ultimo aspetto, il contesto del gioco deve essere il più vicino possibile ad uno reale, per raggiungere un buon grado di immersione e coinvolgimento.

Apprendimento situato e contesto Nel 1991 Jean Lave e Etienne Wenger propongono una rivisitazione del concetto di apprendimento slegato dal contesto dell'insegnamento [26]. Nel loro studio sostengono che si tratta di un processo ottenuto in determinati contesti, rapportandosi con altre persone (formando una comunità di "practioners") e in relazione al coinvolgimento in attività specifiche. In questa visione l'apprendimento è il risultato di un processo attraverso il quale i membri novizi di una comunità, svolgendo inizialmente compiti semplici, acquisiscono con gradualità le competenze necessarie a diventare membri esperti della comunità stessa. Basandosi

su questa teoria, nel 2000, Jan Herrington [27] ha elaborato una lista di caratteristiche per identificare un modello di apprendimento situato, definendo uno standard per il design degli ambienti d'insegnamento che segue alcuni requisiti:

1. fornire contesti che rispecchino il modo in cui le conoscenze verranno applicate nella realtà;
2. fornire attività realistiche;
3. permettere l'accesso alle performance di esperti;
4. fornire ruoli e prospettive multiple;
5. supportare la costruzione di conoscenza collaborativa;
6. promuovere la riflessione;
7. rendere esplicita la conoscenza tacita;
8. fornire l'aiuto e il sostegno degli insegnanti nei momenti critici;
9. fornire giudizi durante le attività di insegnamento.

Nel 2004 David Williamson Shaffer [28] evidenzia l'efficacia con cui il mondo di gioco rende possibile lo sviluppo dell'apprendimento situato, permettendo al giocatore di acquisire concetti e competenze senza perdere di vista la loro relazione con il mondo reale. Insegnare non significa fornire solamente nuove informazioni: affinché queste siano assimilate nella maniera più corretta è necessario che siano integrate con il bagaglio di conoscenze dello studente. I serious games offrono la possibilità di inserirle nel loro contesto per via dell'immersione nel mondo di gioco, rendendo possibile la creazione di legami con quanto già appreso dal giocatore.

Responsabilizzazione Molto spesso nel contesto virtuale dei serious games il giocatore si trova a ricoprire posizioni importanti e di alta responsabilità; quindi le decisioni intraprese avranno un grande impatto nell'ambiente che lo circonda. Con l'aiuto di un buon sistema di feedback visivi chi gioca può riconoscere la corretta relazione causa-effetto tra le decisioni e le loro conseguenze, per distinguere quelle corrette da quelle errate e rendere l'apprendimento più semplice ed efficace.

Necessità di creare un modello della realtà Apprendere nozioni nella realtà può risultare difficile a causa della sua complessità e della quantità di stimoli da questa forniti, molti dei quali sono superflui. Nella creazione di un serious game (e in generale di un qualsiasi videogioco), lo sviluppatore deve applicare delle operazioni di semplificazione della realtà per questioni di tempo e costi, scegliendo quanto rappresentare fedelmente certi elementi e cosa ignorare del tutto. Questo aspetto comporta un vantaggio in termini di apprendimento, perché il giocatore si trova ad interagire con un ambiente più semplice, privo o quasi di distrazioni causate da elementi superflui.

2.2 Serious Games e Cybersecurity

Data la crescente importanza della sicurezza informatica nella vita di tutti i giorni non stupisce che negli anni siano stati realizzati numerosi serious games che mirano al miglioramento di ciò che è stato precedentemente definito come "fattore umano" (Sez. 1.2). Di seguito questi giochi verranno analizzati, per fornire una visione d'insieme completa dello stato dell'arte e ottenere informazioni utili in vista del lavoro di design e implementazione del gioco Fintech Tycoon (Sez. 4.2).

2.2.1 CryptoClub

Da parecchi anni è attivo CryptoClub, un progetto del Center for STEM Education all'università di Chicago finanziato dalla National Science Foundation [29]. Si tratta di un'iniziativa per avvicinare i giovani studenti al mondo della matematica affrontando laboratori di crittografia di

base tenuti nelle scuole. Sebbene si tratti di un progetto con un focus scolastico, molto materiale è stato publicato senza barriere di accesso sul sito CryptoClub.org [30].

Il sito ospita alcuni mini-giochi che mostrano il funzionamento degli algoritmi di cifratura più semplici (ad es. cifrari di Cesare e Vigènere), presentando anche alcune tecniche per decifrare messaggi senza possedere la chiave. Nonostante non si tratti di veri e propri serious games, possono risultare utili per introdurre concetti basilari della crittografia in maniera interattiva e interessante a utenti che si approcciano per la prima volta all'argomento.

Sul sito è presente anche un gioco scaricabile dal titolo VORTEX [31], il cui primo livello è giocabile online sul sito stesso (descritto con il nome di Desert Oasis). Si tratta di un gioco il cui gameplay si basa su una specie di caccia al tesoro che ha luogo in tempi e luoghi differenti. Questo espediente permette di presentare al giocatore una serie di messaggi da decodificare per ottenere una ricompensa finale. Per struttura il gioco è simile a un'avventura grafica e si divide in 3 livelli con altrettanti scenari: un'oasi nel deserto, un pianeta lontano e un villaggio di montagna abbandonato. La difficoltà aumenta con il procedere dei livelli ed è rispecchiata dagli algoritmi, sempre più complessi, che devono essere utilizzati per risolvere gli enigmi.

In generale si tratta di un gioco che ha lo scopo di far esercitare gli studenti per cui è stato pensato, rendendo gli esercizi più interattivi rispetto ad un approccio tradizionale. La componente didattica perciò prevale su quella ludica. Nonostante non tratti di sicurezza informatica si è voluto dare spazio a questo progetto sia per la sua utilità nell'approcciarsi alla crittografia (argomento trasversale a matematica e informatica), sia perché il progetto è tuttora attivo e nuovi giochi potrebbero essere rilasciati in futuro.

2.2.2 CyberCIEGE

CyberCIEGE [32] è un videogioco sviluppato nel 2006 dalla Naval Postgraduate School con lo scopo di insegnare concetti di sicurezza informatica, in particolare per quanto riguarda l'ambito delle reti. Il progetto è stato sponsorizzato da vari enti, anche se principalmente dalla marina statunitense, e viene utilizzato all'interno di corsi didattici da numerose agenzie ed istituzioni scolastiche come strumento di addestramento. Il gioco completo viene fornito solo a queste agenzie; tuttavia è aperta al pubblico una versione di prova altrettanto completa, che però concede un massimo di 20 minuti di gioco senza interruzioni.

CyberCIEGE è stato creato con l'intento di simulare fedelmente i meccanismi reali della sicurezza informatica, permettendo così agli studenti di muoversi in un ambiente che incoraggia la sperimentazione e la riflessione. L'obiettivo del gioco è mostrare un'ampia varietà di tecniche e concetti; per riuscirci efficacemente sono proposti oltre 20 scenari diversi (Fig. 2.2). Lo studente nel gioco veste i panni dell'amministratore di sistema di una azienda che deve completare gli obiettivi proposti dallo scenario. Quando li ha completati tutti il giocatore può avanzare al livello successivo.

Per perseguire gli obiettivi è necessario prendere delle decisioni che possono intaccare in positivo o negativo la sicurezza dell'ambiente informatico. Il gameplay è simile a quello di un gioco gestionale, in cui il giocatore ha delle risorse a disposizione (in questo caso denaro) e deve decidere come investirle al fine di proteggere in modo efficiente ed efficace il sistema dagli attacchi informatici, con la possibilità di implementare una grande varietà di contromisure. Date la loro complessità e vastità gli argomenti vengono presentati in modo incrementale con il progredire degli scenari, accompagnati da vari tutorial interattivi e da una guida che fornisce spiegazioni più approfondite.

Le azioni del giocatore prevedono conseguenze che si ripercuotono sul gameplay: decisioni errate possono portare l'azienda verso la bancarotta (e quindi terminare la partita), mentre le decisioni corrette portano al guadagno di denaro e al proseguimento del gioco. Inoltre una volta terminata la partita è possibile consultare un log (anche da parte di un insegnante) che riassume le azioni effettuate in gioco per valutare i progressi e gli errori che sono stati commessi.

Nel corso degli anni, CyberCIEGE ha ottenuto ottimi risultati come strumento didattico [33], anche se presenta alcuni punti deboli: il gioco richiede una conoscenza di base degli argomenti

Figura 2.2. Come si mostra uno scenario all'interno del gioco CyberCIEGE.

trattati e in alcune occasioni risulta poco chiaro data la mole di informazioni contenuta nelle sue interfacce. Tuttavia questo è anche il suo maggior pregio, dato che questi argomenti vengono trattati con un buon grado di approfondimento e realismo.

2.2.3 BigBro

BigBro [34] è un gioco ideato e sviluppato nel 2017 da Gaetano Mondelli, uno studente di Ingegneria informatica al Politecnico di Torino. Si tratta di un serious game abbastanza semplice, che consiste in una serie di quiz a risposta multipla che trattano vari argomenti di sicurezza informatici; alcuni di questi sono molto generali, come i concetti di autenticazione e integrità, mentre altri sono più specifici, come gli algoritmi di cifratura simmetrica.

Una componente importante del gioco è il sistema di valutazione: infatti viene tenuta traccia dei progressi e degli argomenti su cui il giocatore risulta meno ferrato, in modo da riproporli più volte durante i quiz. Lo scopo del gioco è prettamente didattico, dato che l'obiettivo che si prefigge è di fissare concetti che sono stati oggetto di uno studio precedente da parte del giocatore.

2.2.4 CyberCraft

CyberCraft [35] è un gioco ideato e sviluppato nel 2018 da Lu Yang, uno studente di Ingegneria informatica al Politecnico di Torino. Si tratta di un serious game che ha lo scopo di introdurre concetti e tecniche di sicurezza informatica enfatizzando il rapporto tra attacchi e contromisure. Presenta la struttura di un gioco strategico a turni in cui il giocatore può vestire i panni di più personaggi. In alcuni momenti della storia al giocatore viene richiesto di difendere un sistema dagli attacchi di un hacker; in altri il punto di vista è quello dell'hacker. Questa alternanza arricchisce l'esperienza di gioco, perché permette di analizzare la questione della sicurezza informatica con uno sguardo più ampio del singolo punto di vista del difensore o dell'attaccante.

In entrambi i ruoli il giocatore ha a disposizione un budget che deve utilizzare per contrastare l'azione dell'avversario. Lo scopo di chi gioca in difesa è di resistere fino al termine dei turni, evitando la totale compromissione del sistema. Analogamente giocando in attacco l'obiettivo

consiste nel compromettere completamente il sistema preso di mira entro il termine della partita. I requisiti e gli effetti di attacchi e contromisure sono stilizzati nel mondo di gioco, ma vengono descritti chiaramente nella guida che è possibile consultare in qualsiasi momento.

CyberCraft è un serious game che punta molto sull'intrattenimento ricavato dal gameplay, che si basa su una serie di sfide. Al termine di ognuna viene calcolato un punteggio che dipende dalle scelte effettuate nella partita. Il modo stilizzato con cui vengono messi in campo i concetti di sicurezza informatica permette anche a giocatori senza particolari conoscenze pregresse di giocare serenamente e capire che cosa accade.

2.2.5 SimSCADA

SimSCADA [36] è un gioco ideato e sviluppato nel 2019 da Andrea Marchetti, uno studente di Ingegneria informatica al Politecnico di Torino. Si tratta di un serious game che ha lo scopo di introdurre concetti e tecniche di sicurezza informatica in ambienti SCADA.

Presenta la struttura di un gioco gestionale, in cui il protagonista deve gestire la sicurezza di un'azienda che lavora con sistemi SCADA. Il giocatore deve decidere come investire i fondi a disposizione, tenendo sott'occhio anche la sostenibilità economica delle proprie scelte; una gestione poco oculata del budget a disposizione può portare velocemente alla bancarotta e di conseguenza al game over. Una parte essenziale del gameplay è la reazione agli attacchi andati a segno: dopo che l'azienda viene colpita da un attacco il giocatore deve occuparsi di risolvere il problema nel minor tempo possibile per contenere i danni. Un altro aspetto rilevante a riguardo è la prevenzione, che implica l'adozione di contromisure atte a prevenire gli attacchi. Tra queste è prevista anche la procedura di controllo del personale che ha accesso al sito di lavoro.

In qualsiasi momento è possibile consultare una guida per approfondire e comprendere i meccanismi di attacchi e difese. Le scelte del giocatore vengono registrate nei log e contribuiscono a nutrire le statistiche visibili durante la partita. In questo modo chi gioca può comprendere meglio su quali argomenti ha maggiori difficoltà. In generale si tratta di un gioco pensato e sviluppato per studenti universitari che possiedono nozioni di informatica e vogliono approfondire l'ambito della sicurezza.

2.2.6 DropIt!

DropIt! [37] è un gioco ideato e sviluppato nel 2015 da Antonino Aloi, uno studente di Ingegneria informatica al Politecnico di Torino. Lo scopo del serious game è di sensibilizzare il giocatore riguardo le minacce alla sicurezza che si devono fronteggiare nella vita di tutti i giorni, fornendo in particolare un'introduzione all'utilizzo di un personal firewall.

La struttura del gioco è quella di un quiz game con uno stile platform, in cui il giocatore deve fare le veci di un firewall in un ambiente 2D in cui le connessioni sono rappresentate dagli altri personaggi dello scenario (Fig. 2.3). La struttura dei livelli è abbastanza semplice: prima di iniziare la partita vengono presentati brevemente gli argomenti specifici che saranno trattati nel gameplay; successivamente il livello vero e proprio ha inizio e il giocatore si trova ad accettare o scartare le connessioni che gli vengono presentate. Per fare ciò deve muoversi su un totale di 6 porte (3 in entrata e 3 in uscita) dietro le quali attendono i personaggi (le connessioni). Se il giocatore accetta una connessione malevola il personaggio corrispondente danneggia uno dei mainframe presenti nella stanza. Una volta che tutti i mainframe sono danneggiati o non restano connessioni da valutare il livello termina.

Al termine di un livello vengono mostrate le statistiche che ricapitolano le azioni effettuate e viene calcolato un punteggio in base ad esse. I punteggi vengono poi registrati per tenere traccia dei progressi di ogni giocatore. DropIt! vuole rivolgersi anche agli utenti meno esperti di sicurezza informatica, in modo da mostrare loro l'importanza di adottare un comportamento più consapevole quando si ha a che fare, ormai quotidianamente, con dispositivi informatici personali.

Figura 2.3. L'ambiente di gioco all'interno di DropIt!.

2.2.7 Insector

Insector [38] è un gioco ideato e sviluppato nel 2019 da David Perez, uno studente di Ingegneria informatica al Politecnico di Torino. Questo serious game ha lo scopo di fornire al giocatore conoscenze basilari riguardo la sicurezza informatica. La sua struttura è quella di un quiz game a scelta multipla con una o più opzioni di risposta corrette. Per accedere ai quiz il giocatore naviga in uno scenario interattivo con elementi simili a quelli di un avventura grafica. Le domande proposte vertono principalmente su attacchi informatici e relative contromisure da adottare.

Lo scopo del gioco è prettamente didattico ed è concepito per valutare le conoscenze che il giocatore ha acquisito in precedenza. Questo aspetto non impedisce di giocare ai non esperti del settore: infatti gli argomenti trattati svolgono più che altro il ruolo di introduzione all'ambito della sicurezza informatica.

2.2.8 INPRINT serious games

INPRINT (INPacting Research INnovation and Technology) è un'iniziativa sponsorizzata dal Ministero dell'Educazione dell'India per lo sviluppo di policy a sostegno dell'ambito educativo. Uno dei progetti lanciati con questa iniziativa è stato il *Game-based Interactive Simulator for Training Professionals in Cybersecurity Vulnerabilities* [39] che ha lo scopo di facilitare l'insegnamento della sicurezza informatica utilizzando un approccio interattivo basato sui serious games.

Molti dei giochi sviluppati da questo progetto sono disponibili al pubblico[1] e possono essere giocati all'interno del browser. Sono stati sviluppati molti serious games con l'obiettivo di fornire conoscenze di base riguardo le principali tematiche della sicurezza informatica, coprendo un gran numero di argomenti.

[1] i giochi si trovano alla pagina web http://gost.iitd.ac.in/serious_games/pages/ser.html

2.2.9 Interland

Interland è un serious game realizzato da Google che si prefigge l'obiettivo di introdurre un pubblico molto giovane al mondo del web, soffermandosi in particolare sui pericoli che può comportare muoversi online e sui comportamenti da tenere o evitare quando si ha a che fare con social network e pagamenti digitali. Il gameplay consiste in una serie di semplici minigiochi che si trovano in scenari diversi in base alla tematica che trattano.

Fiume della realtà. L'obiettivo è imparare a distinguere il vero dal falso. Il mini-gioco consiste nell'attraversare un fiume senza cadere nell'acqua, rispondendo ad un quiz a risposta multipla.

Monte responsabile. L'obiettivo è imparare ad utilizzare la tecnologia con buon senso. Il mini-gioco consiste nel condividere le informazioni con le persone adatte, tramite un laser che rimbalza in un sistema di specchi.

Torre del tesoro. L'obiettivo è imparare a custodire le informazioni personali. Il mini-gioco consiste nel difendere i dati personali dagli hacker che tentano di impadronirsene, scegliendo le password migliori tra quelle proposte.

Regno cortese. L'obiettivo è imparare a diffondere la gentilezza online. Il mini-gioco consiste nello spargere positività tra gli utenti all'interno di un ambiente platform, evitando e segnalando gli individui che hanno atteggiamenti aggressivi e negativi.

Al termine di ognuno di questi mini-giochi viene calcolato un punteggio ed è presente un test a risposta multipla che riassume i concetti affrontati nel gioco precedente, che è utile per valutare se questi sono stati capiti e appresi. In generale si tratta di un gioco realizzato per un pubblico molto giovane e possiede una grafica giocosa e ben curata, che aiuta a veicolare efficacemente i concetti.

2.2.10 Targeted Attack e Data Center Attack

Trend Micro è un'azienda multinazionale che si occupa di cyber security e per sensibilizzare gli utenti sul tema (e probabilmente sponsorizzare i propri servizi) ha rilasciato al pubblico due serious games. Entrambi presentano una struttura di storia interattiva, da seguire attraverso filmati e che prende una direzione diversa a seconda delle scelte del giocatore (Fig. 2.4).

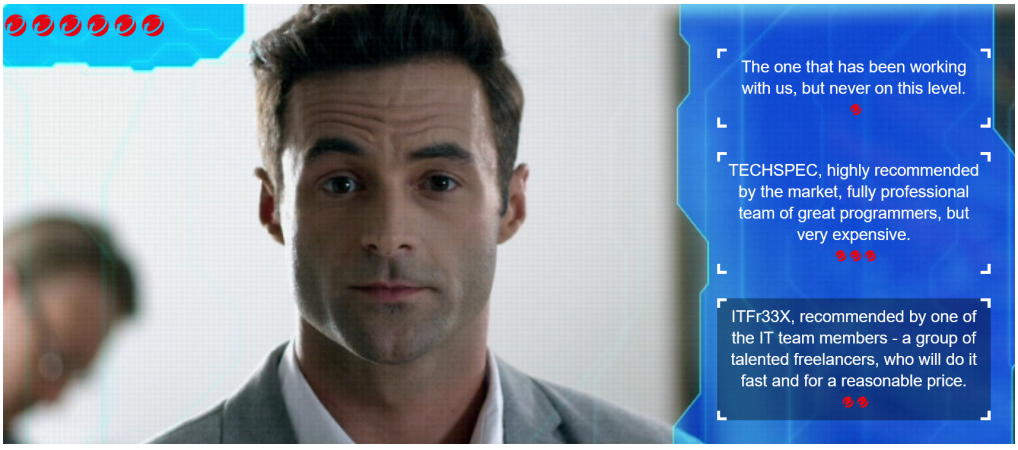

Figura 2.4. Un esempio di scelta a cui è sottoposto il giocatore in Targeted Attack: The Game.

Targeted Attack: The Game [40] All'interno del gioco si vestono i panni del CIO di un importante azienda di software chiamata The Fugle, che sta per rilasciare una rivoluzionaria applicazione per pagamenti online. Il compito del protagonista è di interagire con le altre figure dell'azienda (CEO, security manager, direttore marketing, etc.) in modo da rendere il lancio del

nuovo prodotto un successo. Ogni decisione presa condizionerà degli aspetti della vicenda fino a giungere ad un finale positivo o negativo.

Data Center Attack: The Game [41] Il punto di vista nel gioco è quello del CISO di un ospedale che è stato appena assunto, e che per questo motivo deve da subito valutare lo stato della sicurezza in modo da proteggere adeguatamente i servizi cruciali forniti dalla struttura. Anche in questo caso le decisioni prese caratterizzeranno le vicende della storia, conducendo il giocatore verso un finale positivo, medio o negativo.

2.2.11 Cybersecurity Lab

NOVA Labs è una piattaforma digitale che ospita contenuti educativi interattivi per giovani studenti. Tra gli altri è disponibile CyberSecurity Lab [42] un serious game con l'obiettivo di accrescere la consapevolezza del giocatore riguardo gli attacchi informatici. Il gioco è composto di diversi mini-giochi legati da un unica storia: il protagonista deve gestire la crescita di un nuovo social network e di conseguenza difendersi da una serie di attacchi sempre più sofisticati ai danni della sua start-up.

Programmazione. Il giocatore deve programmare i movimenti di un robot in modo da risolvere un labirinto, mettendo nel giusto ordine alcuni blocchi di pseudo-codice.

Password. Sono una serie di duelli con un hacker, in cui il giocatore, seguendo alcune regole, deve ideare delle password abbastanza complesse da non poter essere scoperte dall'hacker; allo stesso tempo si deve indovinare la password ideata da quest'ultimo, basandosi sugli indizi forniti.

Social engineering. Sono presentate coppie di mail o pagine internet delle quali una è affidabile mentre l'altra è un tentativo di phishing. Il giocatore deve identificare le differenze tra le due e decidere quale ritiene essere il tentativo di phishing.

Attacchi alla rete. Il giocatore deve difendere la start-up da alcuni attacchi, investendo ciò che ha guadagnato nei minigiochi precedenti nell'acquisto di difese adeguate.

Al termine della partita (se si utilizza un account) viene generato un report che indica il grado di completamento del gioco. Sono inoltre disponibili alcuni video in cui vengono spiegati concetti di sicurezza, ai quali seguono alcuni quiz a risposta multipla, in modo da verificare quanto gli argomenti siano stati compresi e appresi.

2.2.12 STIX and Stones

STIX and Stones [43][44] è un serious game realizzato con lo scopo di insegnare agli sviluppatori poco esperti di sicurezza informatica come difendersi in modo efficace dagli attacchi più diffusi. Si tratta di un gioco di tipo "difendi la torre" in cui il giocatore deve difendere 3 punti di ingresso (client, network e server) dagli attacchi nemici. In base al tipo di attacco il giocatore deve dispiegare la difesa adatta a neutralizzarlo, perché solo determinate difese sono efficaci nel fermare un attacco. Questo aspetto si rispecchia nel gameplay, dove determinate torrette (le difese) sono in grado di colpire solo determinati nemici (gli attacchi informatici).

Si tratta in generale di un gioco abbastanza complesso e in cui ci vuole del tempo per comprendere appieno le meccaniche. Il numero e la varietà di potenziamenti e attacchi rendono il gioco abbastanza vasto, anche se questo può provocare smarrimento ai giocatori meno esperti; inoltre alcuni aspetti del gameplay risultano inizialmente poco chiari e non adeguatamente spiegati.

2.2.13 NetSim

NetSim [45] è stato realizzato con lo scopo di mostrare il funzionamento delle reti informatiche, ponendo particolare enfasi sugli aspetti che riguardano la sicurezza. Il gioco ha la struttura di un simulatore di rete informatica, in cui è possibile inviare e ricevere pacchetti all'interno della rete.

All'inizio di ogni livello vengono mostrati alcuni consigli e indicazioni sulle operazioni da adottare per terminare con successo il livello. In questo modo il giocatore può comprendere il

senso delle azioni che va a compiere, ricevendo delle spiegazioni esaustive ma non invadenti. I livelli sono strutturati in modo incrementale e mostrano possibili attacchi che si possono perpetrare in rete, ponendo il giocatore nei panni dell'hacker.

2.2.14 Permission Impossible

Permission Impossible [46] è un serious game disponibile online [47] realizzato per insegnare ai meno esperti di sicurezza informatica i principi di funzionamento di un firewall. Il gioco è molto semplice ed è suddiviso in una serie di livelli in cui il giocatore deve costruire le regole di input e output di un firewall, seguendo le richieste indicate. Per fare ciò si devono trascinare e mettere in fila dei mattoncini fino a formare le suddette regole.

Il gameplay e la difficoltà sono molto semplici, dato che viene richiesto di formulare delle regole abbastanza comuni, in un ambiente guidato. Per questo il gioco risulta utile a chi non possiede delle basi solide sull'argomento ed è, al contrario, poco incisivo per chi conosce già a grandi linee il funzionamento di un firewall.

2.2.15 The Weakest Link

The Weakest Link [48] è un serious game realizzato dalla compagnia Is Decisions, che si occupa di sicurezza informatica nell'ambito di accesso e autorizzazione degli utenti. Lo scopo del gioco è mostrare ai potenziali acquirenti l'ambito in cui opera l'azienda, sensibilizzando inoltre sull'importanza delle scelte dei dipendenti, che condizionano la sicurezza di un'azienda e spesso rappresentano "l'anello debole" della sicurezza, come indica il titolo.

Il protagonista è stato appena assunto dall'azienda in cui le vicende si svolgono. Al giocatore viene proposta una domanda a risposta multipla ogni giorno di lavoro per un mese. Ad ogni risposta viene comunicato se quella selezionata è corretta o no, con una breve spiegazione delle sue implicazioni e dell'impatto sulla sicurezza aziendale (Fig. 2.5).

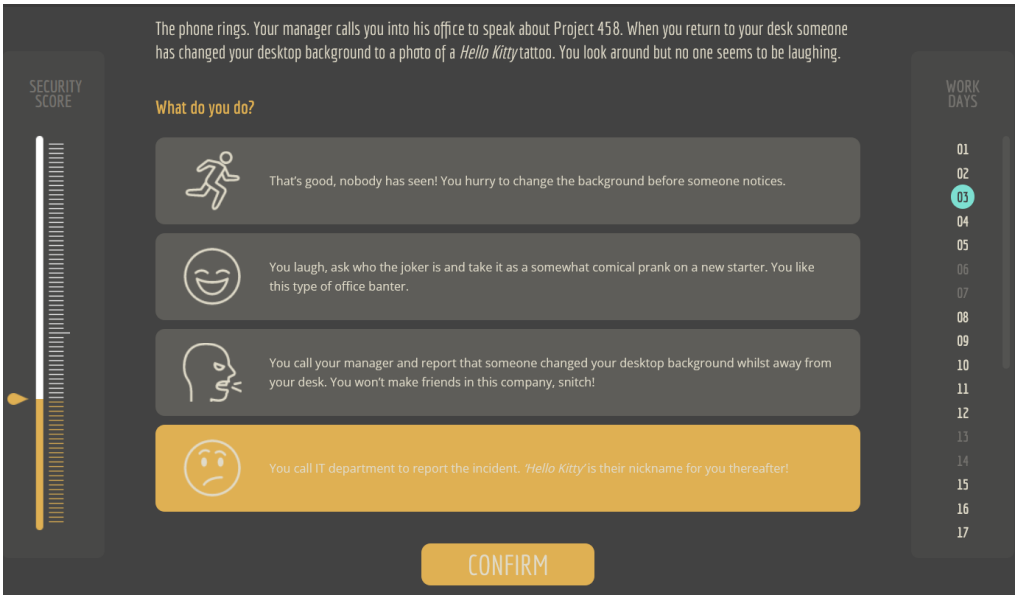

Figura 2.5. Un esempio di domanda sottoposta al giocatore in The Weakest Link.

Capitolo 3

Open Banking e Sicurezza

Dall'analisi dello stato dell'arte dei Security Serious Games (Sez. 2.2) emerge che nessun gioco si è concentrato sull'ambito dell'open banking, che ha recentemente visto una forte espansione e crescita. Per questo motivo si è deciso di approfondire le minacce alla sicurezza presenti in questo ambiente, in vista di sviluppare Fintech Tycoon in questo contesto. Dopo l'introduzione iniziale verranno considerati gli aspetti di sicurezza informatica relativi a questo nuovo paradigma. Verranno inoltre analizzate normative, tecniche e proposte introdotte per regolamentare e rendere più sicuro il suo funzionamento.

3.1 Open banking

Con il termine "open banking" si indica un modello collaborativo di business che si basa sulla condivisione di dati bancari tra diverse parti, con l'obiettivo di fornire un servizio di maggiore qualità all'utente [49]. In particolare questo termine fa riferimento all'innovazione tecnologica dei servizi finanziari, che consiste concretamente nell'utilizzo di open APIs (Application Programming Interfaces) che consentono maggiori possibilità di trasparenza finanziaria.

Il principio che guida il paradigma dell'open banking è quello di permettere ai clienti di fruire liberamente delle informazioni riguardanti le transazioni finanziarie. Questo può essere visto come un'applicazione di Open Innovation, un modello proposto da Henry Chesbrough [50]. Questo modello predilige le innovazioni che il mercato offre all'esterno rispetto ad un approccio tradizionale, basato su segreti industriali e reciproca chiusura tra le aziende.

L'adozione del paradigma open banking è avvenuta con le modifiche nelle disposizioni relative al trattamento dei dati personali, come il GDPR; essa è stata incentivata anche dall'introduzione di nuove normative (come la PSD2), che con le nuove regole imposte mirano a promuovere lo sviluppo e l'innovazione del settore dei pagamenti online, nel rispetto del cliente e della sicurezza dei suoi dati.

3.2 Sicurezza dell'open banking

L'introduzione del modello open banking porta inevitabilmente con sé anche aspetti negativi: dato che più attori accedono ai dati bancari le opportunità di attacco aumentano notevolmente. A questo si aggiunge che queste nuove compagnie potrebbero non essere sottoposte alle normative stringenti cui devono aderire gli istituti bancari [51]. Le principali aree di suscettibilità a possibili attacchi sono:

- le API pubblicamente accessibili di banche e aziende FinTech;
- le applicazioni di banche e aziende FinTech;

- nuovi moduli di sicurezza che potrebbero introdurre attacchi non considerati in fase di design;
- misure di sicurezza non implementate correttamente;
- tecniche obsolete (e poco sicure) per lo scambio di dati bancari.

3.2.1 Banking APIs

Le banking APIs sono lo strumento essenziale da cui è possibile recuperare le informazioni bancarie e rendono quindi possibile il modello open banking. Tuttavia il fatto che siano aperte al pubblico le rende molto vulnerabili e, per questo motivo, è necessario che siano estremamente robuste dal punto di vista della sicurezza. Purtroppo non tutte le API vengono protette in modo adeguato ed esistono vulnerabilità diffuse.

Un aspetto fondamentale per la sicurezza delle API è la confidenzialità dei dati personali del cliente. In molti sistemi di banche e aziende FinTech (e addirittura banche centrali) vengono esposti alcuni dati sensibili dei clienti all'interno dell'URL. Anche se l'utilizzo di protocolli di sicurezza (come SSL) garantisce l'illeggibilità del traffico intercettato grazie alla crittografia messa in campo, inserire dati di autenticazione o riguardanti una transazione nel percorso URL non è una buona idea. Queste informazioni potrebbero essere memorizzate nei file di log o nella cronologia di navigazione, oltre che essere visibili all'interno del browser.

3.2.2 Applicazioni di open banking

È comune che le banche e le aziende FinTech offrano i propri servizi anche attraverso applicazioni mobile, soprattutto per il fatto che viene spesso richiesta al cliente un'autenticazione multi-fattore, i cui elementi coinvolgono parzialmente (e in alcuni casi completamente) lo smartphone. Questa soluzione viene adottata anche per sostituire il sistema precedente: spesso venivano condivisi codici OTP tramite SMS, ma questa procedura è stata progressivamente accantonata per i costi operazionali e il livello di sicurezza poco soddisfacente.

Molte applicazioni di open banking si affidano a Software Development Kits (SDKs) di terze parti per implementare funzionalità utili al loro servizio (come attività di crash report e misurazione delle performance). Queste funzionalità aggiuntive estendono la superficie di attacco e possono costituire delle vulnerabilità se non vengono adeguatamente protette.

3.2.3 Open Financial Exchange

Open Financial Exchange (OFX) è un protocollo la cui introduzione risale al 1997. Si tratta di uno standard open-source che permette alle applicazioni di interagire con istituti bancari e aziende FinTech. OFX si è diffuso tra le istituzioni finanziare nel tempo come mezzo per lo scambio di dati e ne sono state rilasciate versioni aggiornate più recenti (l'ultima è OFX v2.2.0, risalente al 2016 [52]).

Molti istituti non utilizzano la versione più recente del protocollo e questo rappresenta un evidente rischio per la sicurezza. Nonostante ciò non sono stati riportati data breaches causati da un abuso di OFX. Probabilmente il motivo è che si tratta di un protocollo in declino utilizzato sempre meno; inoltre raramente le banche offrono gratuitamente il servizio di OFX ai propri clienti, limitando ulteriormente l'uso che ne viene fatto.

3.2.4 Screen scraping

Nonostante sia una tecnica abbastanza datata, alcune aziende FinTech utilizzano ancora lo "screen scraping". Si tratta di utilizzare le credenziali del cliente per accedere al sito della sua banca ed

estrarre i suoi dati finanziari dall'interfaccia (di solito dal contenuto HTML della pagina web). Nonostante sia una tecnica rischiosa, dato che prevede la condivisione con terze parti delle credenziali di accesso a dati molto sensibili, non è considerata illegale di per sé.

Lo screen scraping è una tecnica abbastanza sensibile: per via del modo in cui i dati vengono ottenuti, può accadere che una modifica del layout grafico del sito della banca non permetta più di ricavare le informazioni, costringendo la FinTech a scusarsi con i propri clienti per la temporanea indisponibilità dei loro dati bancari. Inoltre con l'adozione sempre più diffusa di procedure di autenticazione multi-fattore (ad esempio per via delle regole imposte dalla normativa PSD2) è molto più complesso mettere in pratica questa tecnica, dato che per la FinTech risulta impossibile accedere al sito bancario.

3.2.5 Considerazioni complessive

Tralasciando i rischi legati alle frodi online, i dati finanziari contengono al proprio interno informazioni personali che descrivono le abitudini di vita dei clienti e costituiscono di per sé una risorsa di valore agli occhi dei malintenzionati. Il fatto che ora questi dati transitino anche attraverso le FinTech offre loro possibilità maggiori rispetto al passato: queste nuove realtà aziendali sono spesso da poco tempo sul mercato e non hanno avuto il tempo e le risorse per mettere in campo sistemi di sicurezza paragonabili a quelli delle banche. Eventuali attacchi alle aziende di terze parti sono anche più difficili da individuare da parte dei sofisticati sistemi anti-frode delle banche.

Un altro attacco, più sottile, può consistere nella creazione di false FinTech. Uno o più malintenzionati possono fondare un'azienda di copertura per convincere le banche a fornire loro accesso ai dati degli utenti. Con l'introduzione della PSD2 le terze parti possono ottenere fino a 2 anni di storico contenente le transazioni del cliente.

Come mostrato in precedenza (in 3.2.1 e 3.2.2) l'introduzione di API e applicazioni mobile porta con sé la possibilità di nuovi attacchi: ad esempio, individuando i loro punti deboli, è possibile effettuare attacchi di Distributed Denial of Service (DDoS). Oppure un malintenzionato potrebbe sfruttare dei bug per ottenere accesso ad un account e utilizzarlo per effettuare delle transazioni.

In ultimo gli attacchi possono essere rivolti direttamente al cliente. Da molto tempo sono diffuse tecniche di phishing e social engineering per raggirare gli utenti di un servizio. In questo caso per i malintenzionati può risultare più efficace impersonare una FinTech; gli utenti possono avere la tendenza a porre più attenzione quando si tratta di banche, rispetto ad una azienda di terze parti.

3.3 Revised Payment Services Directive

La Revised Payment Services Directive (PSD2) è una direttiva emanata nel 2015 dal Consiglio Europeo [53] per regolare i servizi di pagamento online all'interno dell'Unione e dell'Area Economica Europea (EEA). La principale necessità di formulare una nuova normativa si deve al fatto che la PDS1 (la direttiva precedentemente vigente che risale al 2007) è risultata molto datata a causa della veloce innovazione tecnologica e della conseguente nascita di realtà non ancora regolamentate [54].

Le frodi online. Durante il periodo 2011-2016 la Banca Centrale Europea (ECB) ha registrato un aumento del 66% del numero di frodi CNP (Card Not Present), che avvengono quando un malintenzionato entra in possesso dei dati riservati di una carta di credito e li utilizza per effettuare pagamenti non autorizzati dal possessore della carta. Nello stesso periodo di tempo la quantità di frodi che si verificano online è passata dal 60% al 73% del numero di frodi totali [55].

Ruolo delle API. L'utilizzo delle API per facilitare la comunicazione tra sistemi differenti è diventato nel tempo un requisito fondamentale per il successo economico delle aziende che offrono servizi online. Allo stesso tempo hanno provocato l'ascesa di attori prima inesistenti, anche in campo finanziario.

Nuovi modelli di business. Il progresso tecnologico e l'adozione di nuove tecniche, come le API, ha permesso lo sviluppo di nuovi modelli di business non ancora regolamentati. La PSD2 fornisce standard e norme a cui adeguarsi, soprattutto per quanto riguarda il trattamento dei dati personali dei clienti e il loro livello di protezione.

3.3.1 Obiettivi

Come accennato in precedenza, la direttiva PSD2 mira principalmente all'espansione dell'ecosistema finanziario ponendo particolare enfasi sulla sicurezza dei pagamenti digitali. In quest'ottica gli obiettivi sono così riassumibili:

- aumentare integrazione ed efficienza del mercato dei pagamenti online in Europa;
- migliorare la parità di condizioni tra i fornitori dei servizi di pagamento;
- rendere i pagamenti più sicuri;
- proteggere gli utenti dalle frodi.

3.3.2 Le parti coinvolte

All'interno della PSD2 vengono identificate le parti che hanno un ruolo nello schema di una transazione digitale [56], e vengono descritte le relazioni che si configurano tra di esse (Fig. 3.1). In particolare vengono distinti diversi tipi di Payment Service Providers (PSP).

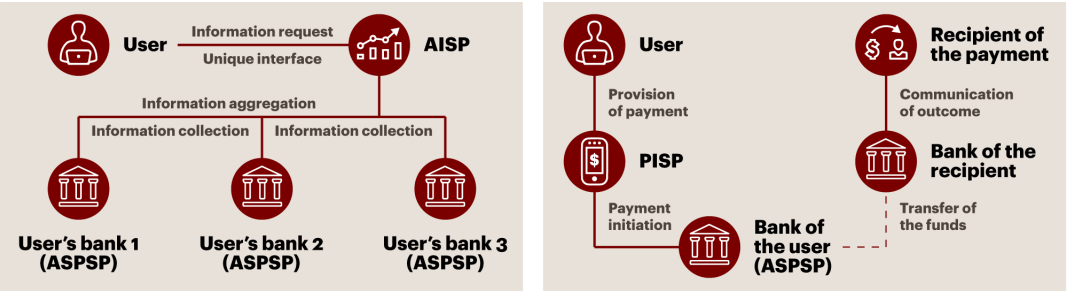

Figura 3.1. Principali relazioni tra i PSP (fonte: Kearney).

AISP. Un Account Information Service Provider è un PSP che si occupa di ottenere informazioni relative al conto di un utente. In questo modo permette al cliente di avere tutte le informazioni di conti diversi su una singola piattaforma, offrendogli così una panoramica generale della sua situazione finanziaria e dei pagamenti effettuati. Può fornire le informazioni direttamente al cliente oppure può recuperarle per conto di un altro PSP.

PISP. Un Payment Initiation Service Provider è un PSP che costituisce il tramite tra il cliente e il suo conto online. In particolare si occupa di iniziare una transazione su richiesta del cliente, generalmente inoltrando la transazione all'ASPSP, che detiene il conto del cliente. Un PISP non entra mai in possesso del denaro che il cliente utilizza per il pagamento, ma il suo servizio è di offrirgli una buona flessibilità, occupandosi di trattare con l'ASPSP.

ASPSP. Un Account Servicing Payment Service Provider è un PSP che controlla e gestisce direttamente un account di online banking per un cliente. Solitamente si occupa di fornire le informazioni richieste dagli AISP e soprattutto riceve e attua gli ordini di pagamento ricevuti dal cliente tramite un PISP.

3.3.3 Strong Customer Authentication

Una delle principali novità introdotte con la PSD2 è l'obbligo di implementare una politica di Strong Customer Authentication (SCA) rivolto ai fornitori dei servizi di pagamento online [57]. Questa richiede di utilizzare la Multi-Factor Authentication (MFA) per ogni pagamento effettuato dal cliente. La European Banking Authority (EBA) si è espressa in modo rigoroso [58] su ciò che viene considerato conforme allo standard. Una procedura di autenticazione per essere considerata MFA richiede il coinvolgimento di almeno 2 dei seguenti elementi:

- inherence: qualcosa che l'utente è, come i dati biometrici dell'impronta digitale;
- possession: qualcosa che l'utente possiede, come un token per generare codici;
- knowledge: qualcosa che l'utente conosce, come una password.

Per garantire un adeguato livello di sicurezza è necessario che gli elementi coinvolti siano indipendenti, in modo che la compromissione di un elemento non influenzi l'affidabilità di un altro. Inoltre questi elementi devono collegare dinamicamente la transazione all'importo e al beneficiario, in modo che queste informazioni possano essere mostrate al momento in cui viene iniziata la transazione.

3.3.4 Regole di esenzione

Data la rigidità della SCA (considerando che deve essere applicata ad ogni singola transazione), l'industria dei pagamenti online ha presentato molte obiezioni a riguardo, temendo che l'inasprimento delle regole avrebbe portato ad un effetto negativo sul volume di transazioni effettuate. Preoccupazioni legittime se si considera che alcune aziende hanno registrato un crollo del 25% nelle vendite quando in India è stata introdotta una misura simile [59].

Per questo motivo l'EBA ha preso in carico le richieste dei fornitori dei servizi di pagamento e ha stilato una lista di casi in cui è possibile chiedere l'esenzione della SCA per una transazione. È importante sottolineare che l'esenzione può essere richiesta solo dal fornitore del servizio di pagamento (e non dal venditore) e spetta alla banca, che detiene il metodo di pagamento, prendere la decisione di accettare o meno la richiesta.

Venditore fidato. Il cliente può decidere di accordare lo status di "venditore fidato", in modo che non sia necessario applicare la SCA ad ogni acquisto. Con questo metodo è il cliente a decidere e il venditore deve lavorare sulla comunicazione per garantirsi la sua fiducia.

Pagamento ricorrente. Se un pagamento viene reiterato nel tempo non è necessario applicare la SCA tutte le volte, ma questa viene richiesta solo al primo pagamento della serie. Si tratta di un'esenzione che si rivolge ai servizi in abbonamento, ma non copre il caso in cui l'importo subisca una variazione.

Pagamento modesto. Questa esenzione permette di evitare l'applicazione della SCA per i pagamenti inferiori ai 30€. Tuttavia ci sono alcune limitazioni: la banca può richiedere la SCA quando si supera la soglia cumulativa di 100€, oppure dopo 5 pagamenti effettuati applicando l'esenzione.

Pagamento a basso rischio. Se il fornitore del servizio di pagamento ha dei tassi di frode sufficientemente bassi può applicare un'analisi di rischio in tempo reale e applicare l'esenzione da SCA (solo per pagamenti inferiori a 500€). Questo meccanismo rappresenta un incentivo a investire in tecniche anti-frode: dato che ai fornitori di servizi di pagamento conviene mantenere bassi i tassi di frode, le richieste di esenzione dei venditori che si impegnano maggiormente nel ridurre il rischio risultano più appetibili.

È importante sottolineare che l'utilizzo di un'esenzione corrisponde ad un'assunzione di responsabilità legale in caso di frode. In questo modo è interesse dei fornitori di servizi di pagamento minimizzare il rischio di frode e non abusare delle esenzioni.

3.3.5 Criticità introdotte

Alcune considerazioni di sicurezza sulla normativa PSD2.

Social engineering. La presenza di terze parti che si frappongono tra gli ASPSPs e gli utenti favorisce un nuovo tipo di attacco di social engineering, in cui il truffatore contatta l'utente pretendendo di rappresentare la parte terza. Una vulnerabilità importante è rappresentata dall'utilizzo delle applicazioni mobile, che non consentono di avere 2 elementi di esecuzione dell'accesso separati. Non importa che i dispositivi in questione dimostrino un adeguato livello di sicurezza, perché rimane il problema che questo tipo di attacchi risulta lo stesso efficace e le banche non riescono a individuarlo facilmente.

Attacchi malware. Gli istituti bancari nel tempo hanno messo in campo strumenti di analisi sempre più efficaci per identificare e prevedere il comportamento tenuto dagli utenti nell'accedere al proprio account. Ciò ha permesso di identificare, intercettare e neutralizzare gli attacchi malware con molta precisione. Tuttavia con l'introduzione della PSD2 i PISP possono accedere in vece degli utenti, contribuendo a confondere i sistemi di prevenzione dei malware. Una soluzione a questo problema può venire dall'applicazione di machine learning, per riconoscere nuovamente i pattern legittimi.

Verifica dei certificati. Gli ASPSP non sono in grado di verificare i certificati digitali degli AISP, perché manca un sistema standard a livello europeo per lo scambio di informazioni tra le varie Certification Authorities.

Conflitti con il GDPR. Secondo la PSD2 le terze parti possono accedere, una volta ottenuto il consenso, ai dati finanziari del cliente e devono garantirne la portabilità come stabilito dal GDPR. Tuttavia il GDPR stabilisce anche la responsabilità dell'ASPSP nel trattamento dei dati personali. Questi due aspetti rendono complicato capire di chi sia effettivamente il compito di ottenere il consenso dal cliente, e di conseguenza la responsabilità in caso di data breach.

Vulnerabilità delle API. I PISP e gli ASPSP possono utilizzare API diverse e quindi possono utilizzare delle forme di mediazione che introducono vulnerabilità non considerate nella PSD2. Inoltre non esistono motivazioni che costringano le terze parti a non fare più uso dello screen scraping: l'identificazione dei trasgressori e le restrizioni di accesso sono molto difficili da mettere in campo.

Fiducia tra le parti. Non è chiaro come possano fare le banche a verificare che le policies delle terze parti con cui operano siano compatibili. Più in generale occorrerebbe poter creare un "circle of trust" tra gli attori in gioco, ma per farlo occorre prima individuare un modo di autenticare i vari partner.

3.4 Proposte per la sicurezza delle transazioni online

Nel corso del tempo sono state proposte numerose misure e protocolli per migliorare la sicurezza delle transazioni online. Con la progressiva regolamentazione dell'ambiente digitale attraverso normative più stringenti (come GDPR e PSD2) sono nate ulteriori proposte che puntano al rispetto dei nuovi requisiti in materia di sicurezza e protezione dei dati personali. Anche i vecchi protocolli hanno cercato di tenere il passo con l'evoluzione legislativa. Di seguito vengono descritti e analizzati alcuni protocolli per la sicurezza delle transazioni online.

3.4.1 3-D Secure

3-D Secure (3DS) è un protocollo ideato nel 1999 da Celo Communications AB per la società Visa; successivamente il progetto è stato portato avanti da EMVCo [60] e il protocollo è stato adottato da altre società finanziarie (come MasterCard e American Express). Il funzionamento si basa sull'utilizzo di messaggi XML inviati tramite connessioni SSL con autenticazione del client. La procedura consiste nel richiedere al pagante una password, collegata al metodo di pagamento, per autorizzare la transazione. In questo modo la responsabilità legale in caso di frode è di chi ha emesso la carta di credito.

Nonostante ciò 3DS viene utilizzato dai venditori solo per le transazioni più rischiose. Il motivo principale è che si tratta di un controllo che può far desistere il cliente dal portare a termine la transazione, dato che la sua interfaccia (Fig.3.2) risulta poco curata sui dispositivi più recenti (come quelli mobile). L'aspetto antiquato è anche il motivo per cui alcuni utenti la percepiscono come una procedura poco sicura o addirittura sospettano si tratti di un tentativo di phishing [61]. Inoltre il fatto che sia poco utilizzata comporta i clienti dimentichino spesso la password da inserire, prolungando ulteriormente il processo di pagamento.

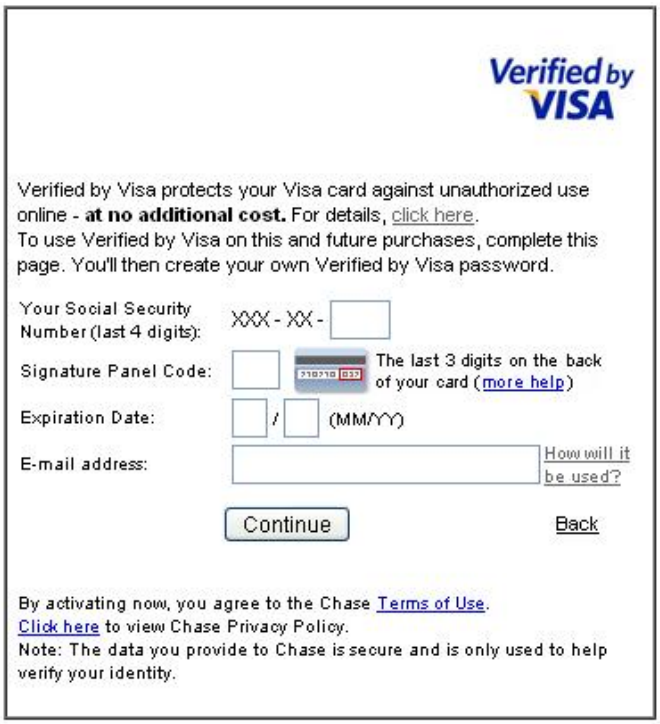

Figura 3.2. Un esempio di interfaccia della procedura 3DS (fonte: Customer Think).

3.4.2 3-D Secure 2.0

Considerati i problemi del protocollo, nel 2017 è stato introdotto 3DS2 [62]. Il motivo principale di questa scelta è stata l'emanazione della PSD2, che ha reso incompatibile 3DS con i requisiti della SCA. Questa versione più recente del protocollo permette ai fornitori dei servizi di pagamento di inviare dati sull'analisi del rischio alle banche. Anche l'aspetto grafico è migliore, perché permette una buona personalizzazione anche in ambienti mobile, con risultati più chiari nella navigazione dell'interfaccia.

Nonostante i miglioramenti anche l'adozione di 3DS2 potrebbe causare dei problemi. Una novità introdotta con la nuova versione del protocollo è la possibilità di accettare nuovi metodi di autenticazione oltre le password (come dati biometrici e OTP). Ciò consente un miglioramento dell'esperienza utente, ma allo stesso tempo rende i pagamenti strettamente dipendenti dal device utilizzato per l'autenticazione (spesso lo smartphone, su cui sono memorizzati i dati biometrici o si ricevono gli OTP). Inoltre le migliorie non eliminano completamente il problema alla radice: l'applicazione del 3DS2 consiste in un controllo aggiuntivo, che può non andare a buon fine e può quindi portare il cliente a desistere e non completare la transazione.

Authentication Enrichment. Appurato che la problematica principale del protocollo 3DS consiste nell'obbligare il cliente a superare un passaggio aggiuntivo per completare la transazione, la soluzione più efficace offerta da 3DS2 è la tecnica di "authentication enrichment". Questa consiste nell'arricchire la richiesta di autenticazione con alcune informazioni utili, come dati sul venditore e di analisi del rischio, in modo che sia molto più probabile che la banca conceda un'esenzione dalla SCA per la transazione.

3.4.3 Financial Grade API

Financial Grade API (FAPI) è un protocollo di sicurezza progettato per essere applicato a scenari di alto rischio, sviluppato dalla OpenID Foundation e dalla U.K. Open Banking Implementation Entity [63]. FAPI è stato pensato per essere una versione più sicura di OAuth 2.0, un protocollo ampiamente utilizzato che permette di accedere ad un servizio senza bisogno di credenziali. Al loro posto viene utilizzato un token generato da una terza parte presso cui ci si è registrati in precedenza. In generale si tratta di un protocollo sicuro, che però si presta comunque ad attacchi di tipo social engineering.

OAuth 2.0 risulta particolarmente utile nel contesto open banking, perché rimpiazza i metodi datati e poco sicuri (come OFX 3.2.3 e screen scraping 3.2.4) tuttora utilizzati dalle aziende FinTech per fornire i propri servizi. FAPI propone diversi moduli per aggiungere funzioni non presenti in OAuth 2.0.

mutual TLS. Solitamente in una sessione HTTPS è il server che si autentica con un certificato presso il client. Con mTLS anche il client deve autenticarsi presso il server, dimostrando di possedere una chiave privata. Nel constesto open banking il ruolo di client viene interpretato da un'applicazione dedicata o da un sito appartenenti a un'azienda FinTech.

JSON Web Signature Client Assertion. Lo scopo di JSW Client Assertion è di assicurare che solo uno specifico client possa utilizzare un access token presso il server di una banca. Ciò può essere implementato dimostrando di possedere un token che può garantire l'accesso a dati che possono essere utilizzati solo dal server della FinTech.

Proof Key for Code Exchange. La procedura PKCE serve a prevenire che un malintenzionato utilizzi un token sottratto al client, tenendo conto che questo può mantenere una chiave per un breve periodo di tempo. Per evitare ciò l'applicazione del client deve inviare una conferma aggiuntiva al server di autenticazione, per confermare che si tratta del cliente legittimo e non di un malintenzionato.

3.4.4 Attacco al protocollo FAPI

Nonostante i propositi di sicurezza del protocollo alcuni ricercatori hanno pubblicato un'analisi che mostra che FAPI potrebbe non essere abbastanza sicuro negli scenari per cui è stato progettato, cioè quelli ad alto rischio [64]. Per meglio comprendere l'attacco che è stato teorizzato è bene descrivere il funzionamento generale del protocollo (Fig. 3.3):

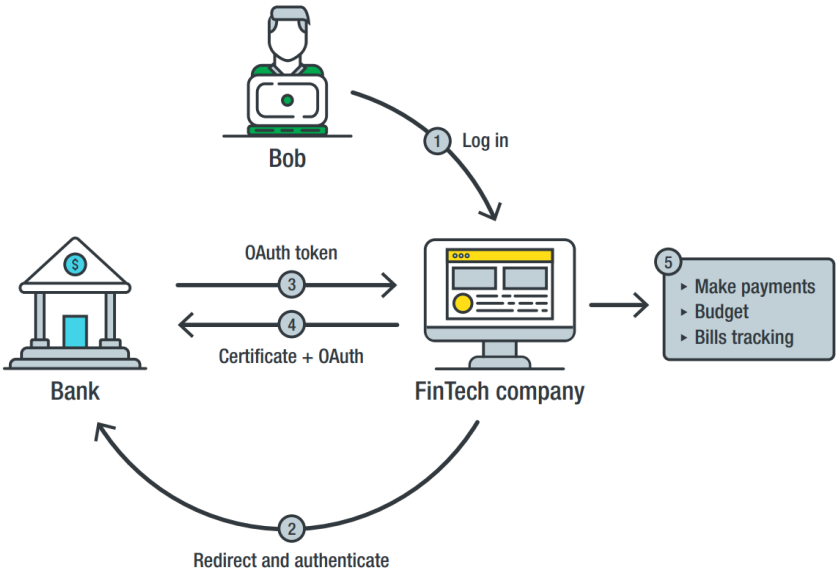

Figura 3.3. Schema dell'attacco al protocollo FAPI [51]).

1. un cliente (che chiameremo Bob) utilizza un servizio offerto da una FinTech per gestire i propri account bancari. Per utilizzare il servizio Bob deve autenticarsi presso la FinTech;
2. la FinTech chiede a Bob di autenticarsi anche presso la sua banca;
3. dopo che Bob si è autenticato presso la banca la FinTech riceve un token OAuth dalla banca, insieme all'URL a cui richiedere i dati bancari di Bob;
4. la FinTech deve mostrare il proprio certificato alla banca (come specificato dal modulo mTLS);
5. la FinTech utilizza il token per accedere alle informazioni bancarie di Bob e le mette a sua disposizione.

Ora consideriamo uno scenario di attacco: utilizzando delle tecniche di phishing la malintenzionata Eve è riuscita a prendere possesso del token di Bob, con l'obiettivo di accedere ai suoi dati bancari. Con il protocollo FAPI non dovrebbe essere in grado di utilizzare il token perché non riesce a superare l'autenticazione richiesta da mTLS. Tuttavia Eve può agire in modo subdolo e riuscire ugualmente nel suo intento (Fig. 3.4). Per prima cosa Eve decide di creare una finta banca e stipulare un contratto con la FinTech di cui Bob è cliente. Successivamente:

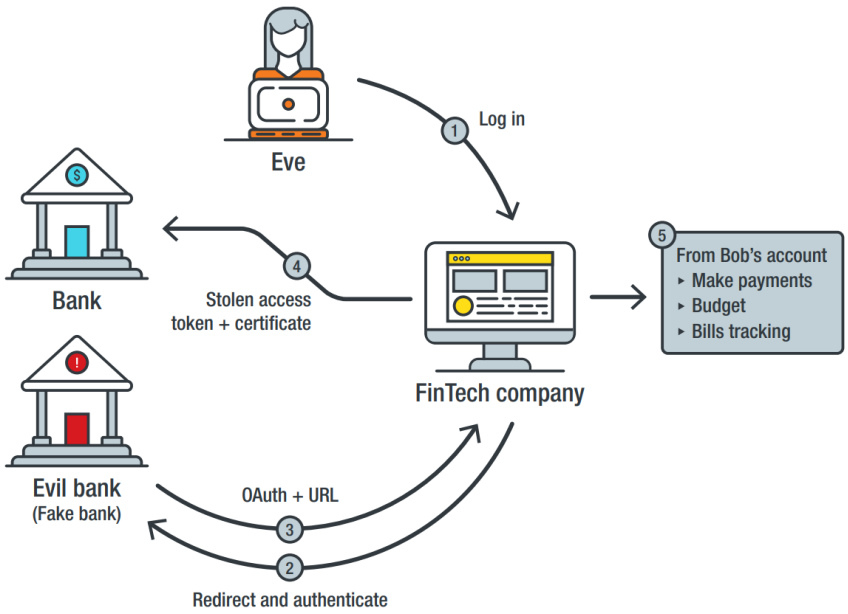

Figura 3.4. Schema dell'attacco al protocollo FAPI [51].

1. Eve si autentica presso la FinTech e chiede di visualizzare i propri dati bancari presso la finta banca;
2. la FinTech chiede ad Eve di autenticarsi anche presso la sua finta banca;
3. Eve si è autenticata presso la finta banca, che controlla, e modifica la risposta alla FinTech, inviandole il token sottratto ad Bob, insieme all'URL manipolato, che indica di rivolgersi alla banca di Bob;
4. la FinTech mostra il proprio certificato alla banca e accede con il token ai dati di Bob;
5. la FinTech restituisce i dati bancari di Bob a Eve.

Come si può notare l'utilizzo di mTLS non garantisce alcuna sicurezza aggiuntiva in questo scenario perché viene bypassato dalla finta banca, che sfrutta la FinTech per recuperare i dati da quella

reale. È chiaro che si tratta di una situazione complessa e di un attacco non banale; tuttavia l'obiettivo rivendicato da FAPI è di garantire la sicurezza anche negli scenari a più alto rischio con i propri moduli aggiuntivi (come mTLS) e da questo esempio emergono delle problematiche a riguardo.

3.5 Scenari per la sicurezza dell'open banking

CyberSec4Europe è un progetto di ricerca finanziato dall'Unione Europea che ha dedicato parte del proprio lavoro alla realizzazione di alcuni scenari riguardanti l'open banking. Le preoccupazioni per la sicurezza di questo ambito sono sorte in seguito alla sua repentina trasformazione negli ultimi anni, conseguente all'adozione di nuovi regolamenti come il GDPR e la PSD2. Al centro di queste normative vi è l'utilizzo che viene fatto dei dati e infatti gli scenari proposti da CyberSec4Europe analizzano, in un modo o nell'altro, la protezione di dati sensibili come quelli finanziari [65].

3.5.1 Cyber Threat Intelligence and Information Sharing (CYTILIS)

L'obiettivo di questo scenario è consentire alle banche e ai CERT (Computer Emergency Response Team) di reagire prontamente in caso di attacco informatico o di tentativo di frode. Per effettuare tutto ciò in maniera efficace è necessario condividere e processare le informazioni in maniera automatica e sicura. Le banche europee hanno un interesse economico nella condivisione di tutte le informazioni utili a prevenire le minacce informatiche alla sicurezza.

Per raggiungere l'obiettivo la proposta è di creare una rete trust-minimized che garantisca privacy, che sia basata su una rete MISP (Malware Information Sharing Platform) e che utilizzi tecnologia blockchain. La condivisione di informazioni sensibili porta a problemi di sicurezza e privacy, dovuti principalmente alla divulgazione di PII (Personal Identifiable Information) contenute negli account bancari (come IBAN e numeri di telefono). Nonostante il rischio maggiore sia la compromissione della confidenzialità di questi dati è importante anche impedire la loro manipolazione in fase di scambio.

3.5.2 Open Banking Sensitive Data Sharing Network (OBSIDIAN)

L'obiettivo di questo scenario è permettere alle banche di condividere informazioni critiche che riguardano le frodi, facendo sì che possano fronteggiare in tempo reale i casi che vengono segnalati. L'interesse delle banche in questo campo è duplice: da una parte ridurre l'impatto economico delle frodi e dall'altra accrescere la fiducia del propri clienti proteggendoli in maniera più efficace. Nonostante esistano già servizi a riguardo, questi mostrano alcuni limiti: spesso si tratta di servizi specifici che non includono tutti i tipi di frode e le soluzioni proposte sono di tipo black-box, per proteggere la propria competitività.

Per fornire alle banche i canali per comunicare le informazioni sulle frodi è stata proposta la realizzazione di una trusted network. Questa rete deve garantire privacy dei dati bancari e sicurezza generale della rete, dato che davanti ad una potenziale frode la banca deve fare una richiesta sulla rete inviando i dati della transazione sospetta. Le operazioni che possono essere operate sulla rete sono:

- preparazione dei dati da spedire (anonimizzazione e certificazione dei dati);
- riportare i dati della frode sulla rete;
- richiedere alla rete di valutare i dati relativi ad una transazione;
- gestire una nuova frode, incorporando i dati relativi ad essa in OBSIDIAN;
- gestire un falso positivo dopo aver ricevuto indicazioni erronee da OBSIDIAN.

Un altro aspetto da considerare è l'esperienza dell'utente, che deve essere di qualità: di conseguenza anche le prestazioni della rete devono essere adeguate. Per fare si che ciò avvenga gli utenti devono possedere il controllo delle proprie credenziali e deve valere il principio least privilege, cioè l'utente deve fornire solamente i dati strettamente necessari.

3.5.3 Privacy Preserving Verifiable Credentials

L'obiettivo di questo scenario è di identificare e autenticare i clienti delle banche presso AISP e PISP in modo sicuro e affidabile, rendendoli consapevoli dell'utilizzo che viene fatto dei loro dati personali. Viene preso in considerazione l'utilizzo del meccanismo di single-sign-on che permette di centralizzare tutti gli attributi di identità autenticandosi presso un IdP (Identity Provider) ed evita di doversi autenticare presso più SP (Service Provider). Nel contesto Open Banking il ruolo di IdP può essere implementato da ASPSP, AISP e PISP, costruendo un circle of trust e realizzando un sistema FIM (Federated Identity Management). Tuttavia mettendo l'IdP al centro del sistema sorgono alcuni problemi:

- l'IdP deve fidarsi del fatto che i SP preservino la privacy degli utenti;
- il SP deve fidarsi delle informazioni ricevute dall'IdP, in quanto unica autorità nel campo;
- essendo al centro del sistema, l'IdP può potenzialmente tracciare i movimenti degli utenti basandosi sulle richieste dei vari SP.

Dato che si tratta di problemi notevoli, soprattutto per gli standard di privacy dettati con il GDPR, si è presa in considerazione l'opzione di utilizzare le Verifiable Credentials (VC). Si tratta dell'equivalente dei documenti d'identità fisici, con la differenza che quelli digitali sono protetti con la crittografia e sono memorizzati sui dispositivi degli utenti. Questo approccio presenta alcuni vantaggi rispetto ad un sistema FIM:

- gli utenti sono in possesso delle proprie credenziali e quindi possono mostrarle a qualunque verificatore intenda accettarle;
- le credenziali verificabili permettono all'utente di presentare credenziali multiple in base alle richieste del verificatore, senza bisogno di un id univoco globale (come avviene in un sistema FIM);
- le credenziali verificabili applicano il principio di least privilege perché l'utente è tenuto a rivelare solo gli attributi strettamente necessari per accedere al servizio;
- le credenziali verificabili proteggono meglio la privacy dell'utente, in accordo con le norme dettate dal GDPR;
- credenziali verificabili sono immuni ad attacchi di phishing, perché non necessitano dell'intervento di un'autorità terza (come l'IdP) per l'autenticazione.

3.5.4 Open Banking API Architecture

L'obiettivo di questo scenario è definire un'architettura per organizzare lo sviluppo delle API in un contesto di open banking. Per questo motivo è stato realizzato uno schema in cui sono definiti i macro-componenti che andranno a comporre l'ecosistema delle API. In particolare sono state identificate 5 aree in cui dividere questi componenti:

- API Security: comprende le componenti che garantiscono il livello di sicurezza necessario nell'interazione con l'OBA (Open Banking Architecture);
- API Platform: ne fanno parte le componenti per il monitoraggio e il policy enforcement (API Gateway, API Manager, API Portal);

- Knowledge Base: l'area per la raccolta, organizzazione e distribuzione delle informazioni sulle specifiche (attraverso API Catalogue e Documentation Management);
- Baseline: comprende le componenti che costituiscono il punto di riferimento per l'implementazione delle funzionalità di open bnking;
- Ecosystem: racchiude le componenti realizzate da terze parti esterne alla banca.

Lo sviluppo delle API deve soprattutto fronteggiare le principali minacce alla sicurezza:

- accesso illegale al sistema: occorre prevenire attacchi (come identity spoofing o Man-In-The-Middle) a danno di IdP, API Manager o API Portal, mirati a ottenere accesso illegale al sistema;
- modifiche non autorizzate: è necessario prevenire attacchi a API Gateway o API Manager, mirati ad apportare modifiche non autorizzate ai dati, compromettendone l'integrità;
- privilege escalation: occorre prevenire attacchi a API Gateway, API Manager o API Portal, mirati a utilizzare il sistema di autorizzazione per consentire accessi non autorizzati a funzioni e informazioni sensibili.

3.6 Considerazioni

Questi scenari, per quanto interessanti e utili per il profilo della sicurezza nel mondo dell'online banking, sono anche molto ambiziosi e complessi da realizzare. Al momento solo il progetto OBSIDIAN viene supportato attivamente [66] con la realizzazione di demo e strumenti sperimentali per la condivisione dei dati riguardanti le frodi bancarie. In futuro anche lo scenario che prevede l'introduzione di Privacy Preserving Verifiable Credentials potrebbe essere oggetto di implementazioni, basandosi su tecnologie già presenti come FIDO e W3C VC.

Capitolo 4

Fintech Tycoon: design e implementazione

Ora verranno trattate nel dettaglio le caratteristiche di Fintech Tycoon e il modo con cui è stato progettato e implementato. Per provare il gioco e ottenere il codice del progetto occorre fare riferimento al manuale apposito (Sez. A.1).

4.1 Contesto di sviluppo

4.1.1 Piattaforma di destinazione

Fin dalle fasi iniziali del progetto è stata considerata la questione della piattaforma a cui destinare il gioco. La decisione è stata di utilizzare le API WebGL per rendere il serious game accessibile dal browser, in seguito ad alcune considerazioni. La migliore alternativa a questa scelta era quella di sviluppare un gioco per Windows, per permettere di accedere al gioco senza dover essere collegati alla rete. Tuttavia, per quanto sia diffuso, il sistema operativo di Microsoft non è il solo, e una decisione del genere avrebbe tagliato fuori gli utilizzatori di Mac OS e di Linux.

Inoltre si deve tenere conto del processo di installazione, inevitabile per una piattaforma di quel tipo, che potrebbe far desistere alcuni utenti dal provare il gioco. Da questo punto di vista l'utilizzo della tecnologia WebGL garantisce un certo grado di immediatezza, dato che nella pratica si tratta di attendere il caricamento di una pagina nel browser prima di iniziare a giocare. Oltre a garantire un'accessibilità maggiore al gioco, la struttura di WebGL permette di raccogliere e aggregare i dati di gioco in maniera più semplice.

Per rendere disponibile il gioco al pubblico si è deciso inizialmente di utilizzare `Heroku`, una piattaforma cloud che offre gratuitamente uno spazio di 512 MB e garantisce una quota di 550 ore mensili di accesso all'applicazione. Inoltre è compatibile con un buon numero di linguaggi, tra cui Node.js che è stato utilizzato per eseguire il gioco. Tuttavia questa soluzione non permette di raccogliere i dati per la valutazione dell'esperienza di gioco, dato che non presenta nessuna possibilità di memorizzazione permanente integrata nella piattaforma. A causa di questa problematica è stata applicata una soluzione di compromesso basata sull'utilizzo di una macchina virtuale collegata alla rete, fornita dal Politecnico di Torino. Da un lato è una soluzione meno efficiente, dato che richiede l'utilizzo di una macchina dedicata 24 ore su 24; d'altro canto permette di recuperare i dati prodotti dai giocatori in maniera relativamente semplice.

4.1.2 Motore di gioco

La scelta del motore di gioco è ricaduta su `Unity`, un motore grafico multi-piattaforma, che permette la creazione di applicazioni grafiche sia 2D che 3D. Le motivazioni che hanno portato a questa decisione sono molteplici:

Semplicità. `Unity` è un motore relativamente semplice ed è consigliato per chi non ha esperienze pregresse nello sviluppo di videogiochi (come lo sviluppatore di Fintech Tycoon). Questo aspetto è utile anche in vista del futuro del gioco, dato che sarà più semplice per uno sviluppatore apportarvi delle modifiche.

Supporto. Un grande vantaggio di utilizzare `Unity` sta nel fatto che si tratta di un motore di gioco molto utilizzato e che viene quindi supportato con continuità. Vengono rilasciati aggiornamenti e nuove versioni in maniera frequente, per garantire una migliore esperienza agli sviluppatori. Inoltre `Unity` è accompagnato da una documentazione completa e anch'essa aggiornata, corredata da un grande numero di tutorial disponibili online per imparare da zero ad utilizzarlo.

Integrazione. L'ambiente di sviluppo di `Unity` è ricco di funzionalità: è possibile generare codice per diversi tipi di piattaforme e sistemi operativi, permettendo una buona portabilità dei progetti su diversi dispositivi. Un ulteriore vantaggio consiste nell'integrazione di `Unity` con l'IDE Visual Studio, che permette di sviluppare il codice `C#` necessario al funzionamento del gioco in modo interattivo e funzionale.

4.2 Struttura del gioco

4.2.1 Tipologia e contesto

Il genere del gioco può essere definito gestionale o tycoon. Il giocatore infatti si trova a capo di una realtà economica (il dipartimento per la sicurezza della FinTech) e deve intraprendere delle decisioni per far fronte ai problemi presentati lungo la partita. La componente gestionale, come è stato notato all'interno di giochi come CyberCIEGE (Sez. 2.2.2), permette di conservare una certa verosimiglianza con la realtà, con una struttura che allo stesso tempo consente di incanalare il giocatore nel flusso del gameplay. Per farlo l'idea è di rendere il gioco ritmato, come avviene all'interno di un tycoon, in modo che il giocatore non abbia tempo per distrarsi e possa rimanere concentrato sulla componente di sfida. A tal proposito ci si è ispirati a ciò che avviene in giochi come SimSCADA (Sez. 2.2.5) e DropIt! (Sez. 2.2.6).

I serious games individuati durante l'analisi iniziale (Sez. 2.2) hanno mostrato come al momento, dato che si tratta di una materia di studio recente, non esistano giochi che trattano l'argomento della sicurezza informatica in ambito finanziario. Considerando la rilevanza dell'open banking nella società a nel quotidiano si è deciso di realizzare un gioco per coprire questa tematica.

Si è scelto di ambientare il serious game in una FinTech, dato che si tratta dell'elemento distintivo dell'online banking e rappresenta l'attore che più preoccupa in vista della sicurezza dei dati finanziari degli utenti (Sez. 3.2.5). Inoltre questo ambiente si presta bene a realizzare uno scenario gestionale in cui occorre gestire le risorse a disposizione nel miglior modo possibile per crescere e offrire servizi sempre più sicuri.

4.2.2 Gameplay

Il gioco è ambientato all'interno di un'azienda FinTech in cui il giocatore è stato appena assunto (Fig. 4.1). Il suo compito è quello di gestire i vari aspetti legati alla sicurezza, senza tralasciare la sostenibilità economica delle proprie scelte. L'obiettivo principale del gioco è accrescere la platea di utenti che utilizzano i servizi dell'azienda, che saranno condizionati dalla qualità di questi ultimi e dalla reputazione della FinTech. Una scarsa reputazione e servizi poco affidabili spingeranno molti potenziali clienti a diffidare dell'azienda, limitandone la crescita.

Al crescere del numero di clienti, la FinTech potrà espandere il proprio business assumendo dei nuovi dipendenti e destinando più fondi alla sicurezza. Un ulteriore compito del giocatore è quello di gestire i dipendenti impiegandoli nell'implementazione di nuove contromisure difensive, nella riparazione dei danni provocati da un attacco e nella prevenzione di attacchi futuri (Fig. 4.2). Gli impiegati hanno abilità differenti nei vari campi dell'informatica e queste influiscono

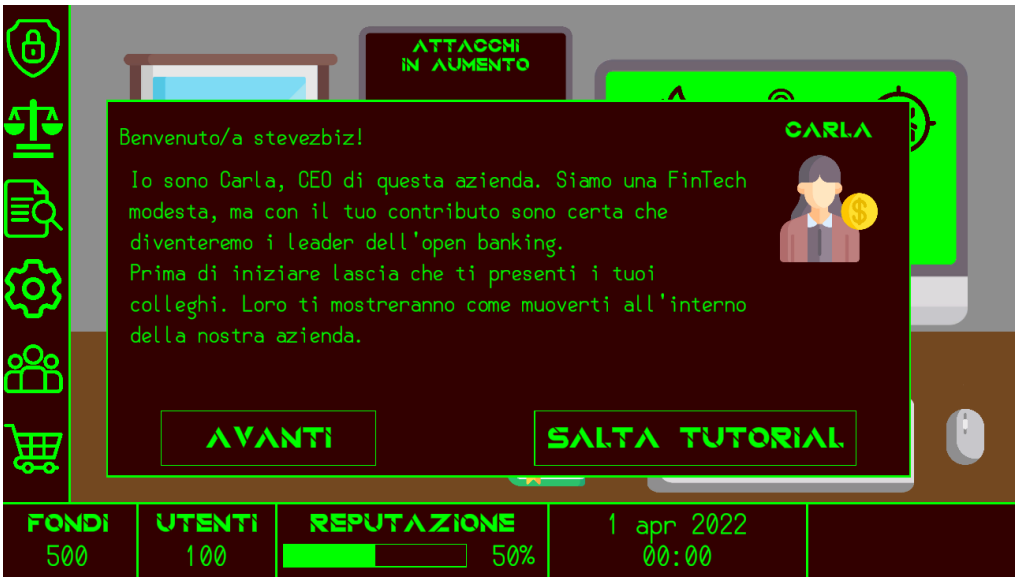

Figura 4.1. Schermata introduttiva di una nuova partita.

sull'efficacia del loro operato. Quindi è compito del giocatore considerare questo ulteriore aspetto nella gestione dell'azienda, mettendo in atto le strategie più adatte.

Figura 4.2. Vista degli impiegati.

Durante il gameplay il protagonista interagisce con le altre figure aziendali (come il CEO, il direttore marketing, etc.), che di volta in volta gli comunicheranno informazioni utili ai compiti che deve svolgere oppure segnaleranno problemi da risolvere. Inoltre di tanto in tanto questi personaggi faranno delle richieste o domanderanno consigli che riguardano la sicurezza informatica al giocatore, che dovrà aiutarli. Le risposte del protagonista avranno conseguenze dirette (economiche e di sicurezza) sulla FinTech.

Per introdurre il giocatore a queste meccaniche e guidarlo nelle prime fasi di gioco è stato realizzato e integrato un tutorial. Data la scarsa efficacia di suggerimenti composti da muri di testo, la sequenza del tutorial è stata presentata come l'incontro con i vari personaggi del gioco che spiegano al nuovo arrivato come è strutturata l'azienda. Inoltre in alcuni punti del tutorial

viene chiesto al giocatore di interagire in modo da aumentare il suo coinvolgimento e contrastare la noia che potrebbero generare le numerose spiegazioni testuali.

4.3 Aspetti didattici

4.3.1 Concetti di sicurezza nel gioco

In questa sezione vengono analizzati gli aspetti di sicurezza trattati nel gioco e il loro inserimento all'interno del gameplay.

Guida e descrizioni All'interno del gioco è presente una guida, consultabile in ogni momento, in cui sono riportate le spiegazioni e descrizioni dei principali concetti di sicurezza affrontati nel gioco (come attacchi e tecniche di cybersecurity). Nonostante ciò anche all'interno del gameplay sono stati integrati contenuti simili: ad esempio quando viene subito o sventato un attacco viene anche fornita una spiegazione che riassume le principali motivazioni dell'avvenimento. Da questi messaggi il giocatore può capire quali lacune nella sicurezza hanno permesso all'attacco di andare a segno, o, al contrario, quali contromisure si sono rivelate efficaci nel contrastarlo e neutralizzarlo.

Attacchi e contromisure Nel negozio è possibile acquistare varie contromisure per mitigare gli attacchi che affliggono la FinTech (Fig. 4.3). Ognuna di esse ha una descrizione che ne indica brevemente le caratteristiche e gli attacchi che il suo impiego può contrastare. Un attacco può essere contrastato in 3 modi:

- rendere più complesso elaborare gli attacchi, che nel gioco ha l'effetto di aumentare il tempo che intercorre tra 2 tentativi di attacco consecutivi;
- organizzare la riparazione dei danni dopo un attacco, che nel gioco ha l'effetto di ridurre il tempo necessario a riparare i danni provocati da un attacco andato a segno;
- individuare un tentativo di attacco, che nel gioco ha l'effetto di sventare più facilmente gli attacchi.

L'obiettivo didattico di questa parte del gioco è fornire una conoscenza schematica che metta in relazione le contromisure con le minacce da esse contrastate, in maniera simile a come avviene in CyberCraft (Sez. 2.2.4), fornendo al contempo descrizioni utili a capire il funzionamento delle difese stesse.

Figura 4.3. Schermata del negozio.

Sicurezza nel tempo Le contromisure acquistabili in negozio possiedono un sistema di livelli: in questo modo è possibile migliorarle con il progredire della partita. Questa meccanica è stata implementata sia per garantire maggiori opzioni d'acquisto al giocatore (e quindi un gameplay più vario), sia per emulare l'invecchiamento delle difese nel tempo. Questo ultimo aspetto è rafforzato da un'ulteriore meccanica: con il progredire della partita i valori di difesa delle contromisure diminuiscono progressivamente, rendendo necessario potenziarle per tenere il passo con gli attacchi che si perfezionano con il passare del tempo.

Quiz di valutazione Per far interagire maggiormente il giocatore con i vari aspetti della sicurezza informatica nel gameplay sono stati introdotti anche alcuni quiz a risposta multipla (Fig. 4.4). Si tratta di domande poste dai vari personaggi del gioco volte a far riflettere sui comportamenti e le tecniche da adottare per promuovere la sicurezza nell'ambiente lavorativo della FinTech, in maniera simile a ciò che avviene nel gioco The Weakest Link (Sez. 2.2.15).

Figura 4.4. Messaggio contenente un quiz.

4.3.2 Attacchi

In questa sezione sono elencati gli attacchi presenti all'interno del gioco, accompagnati da una breve descrizione dei loro effetti sul gameplay.

Denial of Service Si tratta di un attacco volto a colpire i servizi offerti dalla FinTech, con lo scopo di impedire ai clienti di usufruire di tali servizi. Sovraccaricando di richieste la rete e i server dell'azienda, l'attacco DoS procura danni economici in base alla propria durata e di conseguenza al numero di clienti che non possono essere serviti; inoltre ciò peggiora la qualità del servizio e spinge alcuni utenti ad abbandonare il servizio.

Man-In-The-Middle Questo attacco ha lo scopo di ottenere accesso non autorizzato ad informazioni sensibili appartenenti alla FinTech (come dati personali dei clienti). Per farlo sfrutta le vulnerabilità di autenticazione e integrità delle comunicazioni della FinTech. Un attacco MITM andato a segno provoca dei danni economici (oltre che reputazionali).

Brute-force Si tratta di un attacco rivolto contro l'autenticazione via password dei clienti della FinTech. Il suo scopo è di sfruttare le vulnerabilità nella definizione delle password (ad es. scarsa varietà di caratteri utilizzati, lunghezza inadeguata, etc.) per ottenere un accesso non autorizzato al profilo della vittima e sottrarre dati personali e denaro. Ciò risulta nel peggioramento della reputazione dell'azienda.

Dictionary Attack Sfruttando un dizionario di password e relativi hash questo attacco ha l'obiettivo di accedere all'account della vittima e sottrarre dati personali e denaro. Per riuscirci

questa tecnica sfrutta le vulnerabilità nella definizione delle password, spesso troppo semplici e intuibili. Un dictionary attack andato a segno ha come conseguenza principale il peggioramento della reputazione dell'azienda.

Rainbow Table Attack Un attacco di questo tipo è molto simile al dictionary attack, con la differenza che il numero di password e hash calcolati è considerevolmente maggiore. In modo simile all'attacco precedente, il rainbow table attack sfrutta le vulnerabilità nella definizione delle password per individuare quella corretta, accedere all'account della vittima e sottrarre dati personali e denaro, con analoghe conseguenze per la reputazione della FinTech.

Attacco alle Open Banking API Questo attacco sfrutta le vulnerabilità presenti nelle API (ad es. bugs nel software, dati personali nell'URL - Sez. 3.2.1 -, etc.) per ottenere accesso ai dati personali dei clienti dell'azienda. Nel caso che l'attacco vada a segno l'azienda riceverà una sanzione economica dovuta al data breach avvenuto.

Social Engineering Si tratta di una tipologia di attacco che può colpire i clienti della FinTech, con l'obiettivo di raggirarli e ottenere i loro dati personali o sottrarre il loro denaro. Non essendo un attacco diretto contro l'azienda non provoca danni diretti, però influisce negativamente sulla sicurezza percepita che i clienti hanno del servizio, portando alcuni di essi ad abbandonarlo.

Phishing Questo attacco all'interno del gioco può colpire i lavoratori della FinTech con lo scopo di accedere al sistema e trafugare informazioni personali dei clienti utilizzando comunicazioni contraffatte. Le conseguenze sono un danno economico per l'azienda accompagnato da un danno reputazionale.

Worm Questo attacco malware mira a diffondersi velocemente attraverso i sistemi infetti, replicandosi autonomamente, in modo da esaurire le risorse computazionali del sistema aziendale. Di conseguenza nel gioco i clienti troveranno difficoltà ad utilizzare i servizi offerti dalla FinTech, decretando quindi una perdita economica e anche un malus per il numero di utenti.

Virus Si tratta di un attacco malware abbastanza generico che all'interno di Fintech Tycoon ha lo scopo di danneggiare il sistema infetto e renderlo inutilizzabile. Ciò ha delle conseguenze economiche per l'azienda, dovute al tempo necessario per riparare i danni procurati dall'attacco.

Spyware Questo attacco malware si concentra in modo specifico sulla raccolta di informazioni dalla vittima infetta. All'interno del gioco un attacco di questo tipo è riconducibile ad un tentativo di spionaggio industriale da parte di un'azienda concorrente; per questo, nel caso in cui lo spyware riesca ad infiltrarsi nel sistema, ci sono delle ricadute sul numero di utenti, molti dei quali abbandonano il servizio della FinTech per utilizzare quello dell'azienda concorrente.

Ransomware Si tratta di un attacco malware specifico che ha lo scopo di accedere ai dati del sistema vittima, renderli inaccessibili (utilizzando la crittografia) e infine chiedere un riscatto alla vittima in cambio della restituzione dell'accesso ai dati. I danni di un attacco del genere sono economici ma influenzano negativamente anche il numero di utenti, dato che il servizio è reso inaccessibile ai clienti.

4.3.3 Contromisure

In questa sezione sono elencate le contromisure presenti nel negozio del gioco, accompagnate da una breve descrizione dei loro effetti sugli attacchi.

Sicurezza di rete Raccoglie diverse tecniche per il rafforzamento della sicurezza di rete, dalle semplici configurazioni per mitigare attacchi DoS fino a tecniche complesse come l'utilizzo di penetration test per identificare e correggere le vulnerabilità riscontrate.

Firewall Riguarda l'utilizzo di diverse tecnologie per rafforzare il firewall, dal semplice packet filter fino a tecniche più complesse come l'utilizzo di reverse proxy e stealth firewall. Garantisce un livello di protezione contro gli attacchi DoS e la connessione a siti malevoli che possono portare ad attacchi malware.

Sicurezza DNS Raccoglie alcune misure per aumentare la sicurezza del protocollo DNS, in particolare diminuendo l'efficacia di attacchi Man-In-The-Middle e tentativi di phishing.

Sicurezza delle password Si occupa di definire strategie e regole per la creazione, l'utilizzo e il mantenimento delle password. Sono comprese al suo interno regole per la creazione di password complesse e strategie per il loro rinnovo; tutti meccanismi volti a contrastare gli attacchi brute-force, dictionary attack e rainbow table attack.

Autenticazione Multi-Fattore Raccoglie alcune tecniche di autenticazione rafforzata (sia per i dipendenti che per i clienti) volte al contrasto di attacchi Man-In-The-Middle, attacchi alle password e tentativi di phishing.

Hashing delle password Prevede l'applicazione di tecniche per incrementare la sicurezza nella gestione delle password e in generale delle procedure di accesso. In particolare si occupa di definire l'applicazione di algoritmi di hash e l'utilizzo di salt nella memorizzazione delle password, per contrastare dictionary attack e rainbow table attack.

Intrusion Detection System Questa contromisura prevede l'installazione e l'utilizzo di diversi componenti di un Intrusion Detection System con lo scopo di contrastare principalmente gli attacchi malware e i tentativi di accesso non autorizzato.

Sicurezza del sistema informatico Raccoglie alcune regole e impostazioni che consolidano la sicurezza all'interno dell'ambiente di lavoro della FinTech, in particolare contrastando la diffusione dei malware.

Antivirus Questa contromisura prevede l'installazione e l'utilizzo di un antivirus, partendo dall'utilizzo di tecniche comuni come l'analisi delle firme del software eseguito, fino a raggiungere tecniche più complesse come la realizzazione di un ambiente sandbox in cui eseguire software sospetto. Tutto ciò con il fine di contrastare gli attacchi malware.

Sensibilizzare gli utenti Raccoglie una serie di iniziative indirizzate ai clienti della FinTech che hanno lo scopo di ridurre l'impatto degli attacchi di social engineering a danno degli utenti. Tra queste misure ce ne sono di tradizionali, come una campagna di sensibilizzazione, e di più innovative, come lo sviluppo di un serious game per trasmettere agli utenti alcuni concetti di sicurezza.

Assistenza clienti Si tratta di un insieme di servizi che, una volta implementati, migliorano l'esperienza dell'utente e contribuiscono al contrasto degli attacchi di social engineering rivolti ai clienti.

Prestazioni del sistema Raccoglie una serie di miglioramenti che riguardano il numero e le prestazioni delle macchina dell'azienda. Queste possono risultare utili a migliorare la qualità del servizio e anche a mitigare gli attacchi DoS.

Training di sicurezza Prevede l'organizzazione di seminari per i dipendenti sulla sicurezza informatica, che variano per livello di approfondimento ed efficacia. L'obiettivo è di contrastare la diffusione di tentativi di phishing e attacchi malware all'interno dell'ambiente di lavoro.

Backup Raccoglie alcune tecniche di backup, da quelle molto semplici e poco sicure fino a quelle più solide e complesse. Lo scopo del backup è fornire la possibilità di ripristinare in modo veloce ed efficiente i dati del sistema in seguito, ad esempio, alla diffusione di un virus o un ransomware.

4.4 Sistema di valutazione

4.4.1 Modelli e tecniche

Molti serious games utilizzano tecniche di data science, che variano per complessità e qualità dei risultati, con il fine di analizzare i dati collezionati lungo l'esperienza di gioco [67]. Queste possono essere suddivise in 3 categorie:

- supervised algorithms: si tratta di algoritmi di machine learning che necessitano di essere addestrati con dati precedentemente raccolti ed etichettati per poter essere impiegati effettivamente in tempo reale (come logistic regression, decision trees, etc.);

- unsupervised algorithms: si tratta di algoritmi di machine learning che necessitano di dati non etichettati per essere addestrati, per riuscire così a riconoscere pattern una volta impiegati (come clustering, neural networks, etc.);
- visualization techniques: si tratta di tecniche di aggregazione statistica dei dati, che non prevedono un impiego di machine learning (come curve di apprendimento, correlazioni, etc.).

In generale le tecniche più utilizzate sono modelli lineari e correlazioni, probabilmente perché si tratta delle più semplici da applicare. Tecniche più moderne e complesse, come ad esempio le reti neurali, sono poco utilizzate in questo ambito, probabilmente anche per via della difficoltà nell'interpretare i risultati ottenuti con il loro utilizzo. Sicuramente una causa di queste preferenze risiede nella raccolta dati: in molti casi è difficile raccogliere una quantità di dati sufficiente ad addestrare una rete complessa e per questo si utilizzano sistemi di valutazione che ne richiedono meno per fornire risultati accettabili.

Un esempio di applicazione di supervised learning è lo studio condotto da Cheng et al. sul serious game "The Radix Endeavor" [68]. Nell'analisi viene presa in considerazione la missione "Bake me a cake", che tratta la genetica mendeliana. In questa fase il giocatore deve servirsi di alcuni strumenti per raggiungere l'obiettivo della missione. Il modello mette in correlazione l'utilizzo degli strumenti messi a disposizione e l'esito della missione. Con i dati ottenuti è stato addestrato un classification tree per predire l'esito della missione a partire dagli strumenti utilizzati dal giocatore. In questo modo è stato possibile identificare le difficoltà incontrate dai giocatori analizzando i pattern errati.

In un altro studio Baker et al. analizzano l'acquisizione di conoscenza nel gioco "Zombie Division" [69]. L'argomento trattato dal serious game sono le divisioni matematiche: al giocatore è richiesto di decidere quale arma (contrassegnata da un numero) utilizzare per attaccare il nemico (contrassegnato anch'esso da un numero). Se il valore del nemico è divisibile per quello dell'arma esso viene colpito, altrimenti ad essere colpito è il giocatore. Il modello consiste in alcune semplici curve di apprendimento, ottenute aggregando i dati di tutti i partecipanti per stabilire quanto il gioco si rivela efficace nel tempo. La semplicità di questo modello tuttavia presenta il limite di non poter considerare l'apprendimento dei singoli giocatori separatamente.

4.4.2 BKT Model

Il Bayesian Knowledge Tracing (BKT) Model è un modello per la valutazione dell'apprendimento ideato nel 1994 da Corbett e Anderson [70]. Il BKT Model è apprezzato e utilizzato per la sua buona accuratezza combinata alla semplicità della sua implementazione. Per applicare il modello è necessario identificare i Knowledge Components (KC) (Fig. 4.5): ognuno di essi rappresenta una competenza o un pezzo di informazione che può essere appreso ed è considerato indipendente dagli altri. Ogni KC possiede uno stato che indica se esso è considerato appreso o meno. Inoltre un Knowledge Component può solo passare dallo stato di "non imparato" a quello di "imparato"; in pratica viene modellato solo l'atto di apprendere e non quello di disimparare concetti. Il modello prevede una sequenza di test da sottoporre al soggetto, che deve formulare una risposta; l'esito del test, in base ai valori assunti dalla risposta, può essere solamente un risultato di tipo binario (risposta "corretta" o "errata"). Durante ognuno di questi test il modello, in base ai parametri che verranno descritti di seguito, può modificare lo stato del KC.

Il parametro di maggiore rilevanza del BKT Model è $p(L_n)$ che rappresenta la probabilità che il KC sia stato appreso in seguito al test n. Per il calcolo di questa probabilità il modello è influenzato da 4 parametri:

- $p(L_0)$ indica la probabilità che il KC sia stato appreso prima di iniziare i test;
- $p(T)$ indica la probabilità che un KC passi dallo stato "non imparato" a quello di "imparato" in seguito ad un test;
- $p(S)$ indica la probabilità di sbagliare un test nonostante il KC sia stato appreso;
- $p(G)$ indica la probabilità di indovinare un test nonostante il KC non sia stato appreso.

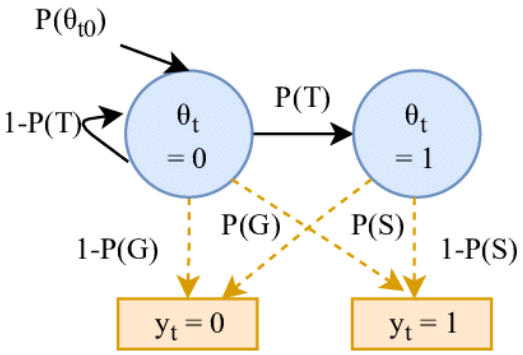

Figura 4.5. Modello di Knowledge Component (fonte: ResearchGate).

A queste se ne aggiungono altre 2 complementari:

- $1 - p(G)$ indica la probabilità di sbagliare un test non avendo appreso il KC;
- $1 - p(S)$ indica la probabilità di rispondere correttamente ad un test avendo appreso il KC.

Applicando le definizioni di questi parametri è possibile individuare le probabilità di ottenere un determinato risultato per un test n:

$$p(corretto_n) = p(L_n) \cdot (1 - p(S)) + (1 - p(L_n)) \cdot p(G)$$

$$p(errato_n) = p(L_n) \cdot p(S) + (1 - p(L_n)) \cdot (1 - p(G))$$

Applicando il teorema di Bayes è possibile definire la probabilità che un KC fosse appreso prima di effettuare il test n, considerando il risultato del test stesso:

$$p(L_{n-1}|corretto_n) = \frac{p(L_{n-1}) \cdot (1 - p(S))}{p(L_{n-1}) \cdot (1 - p(S)) + (1 - p(L_{n-1})) \cdot p(G)}$$

$$p(L_{n-1}|errato_n) = \frac{p(L_{n-1}) \cdot p(S)}{p(L_{n-1}) \cdot p(S) + (1 - p(L_{n-1})) \cdot (1 - p(G))}$$

Utilizzando queste probabilità è possibile calcolare la probabilità che un KC sia appreso dopo il test n:

$$p(L_n) = p(L_{n-1}|risultato_n) + (1 - p(L_{n-1}|risultato_n)) \cdot p(T)$$

Quando il valore di $p(L_n)$ ha raggiunto una determinata soglia (identificata generalmente con il valore 0.95) si considera raggiunta la "skill mastery", che significa che il KC è ritenuto completamente appreso.

4.4.3 Implementazione nel gioco

All'interno del gioco è stato implementato un BKT Model, in quanto si tratta di un modello abbastanza semplice che produce risultati sufficientemente accurati. Si è deciso di rendere la componente di valutazione modulare, in modo che in futuro sia possibile sostituirla con metodi differenti senza troppe difficoltà.

Una parte rilevante nella realizzazione del modello è stata l'inizializzazione dei parametri. In uno studio condotto da Gey-Hong Gweon et al. [71] viene analizzato il significato dei parametri del BKT Model, per descrivere come questi influenzano la valutazione dell'apprendimento. Da questo emerge che $p(T)$ è il principale responsabile della velocità con cui avanza il processo di apprendimento: al diminuire del suo valore aumenta il numero di test necessari a raggiungere la "skill mastery". Inoltre viene considerato il valore $A = (1 - p(S) - p(G)) \cdot (1 - p(L_0))$, che risulta essere un buon indicatore dello stato dell'apprendimento nel modello:

- se $A > 0.3$ il processo di apprendimento procede;
- se $-0.3 < A < 0.3$ il processo di apprendimento è in stallo;
- se $A < -0.3$ il processo di apprendimento regredisce.

Ne consegue che per ottenere il processo di apprendimento desiderato i parametri coinvolti non devono essere in generale troppo elevati. Questo ha un significato specifico in base al parametro considerato:

- un $p(L_0)$ poco elevato implica che il KC non deve essere un concetto eccessivamente semplice o scontato e quindi già appreso prima di effettuare i test;
- un $p(S)$ poco elevato implica che i test devono essere posti con chiarezza e non devono risultare troppo difficili, per limitare l'eventualità di un errore di incomprensione;
- un $p(G)$ poco elevato implica che i test non devono risultare troppo semplici e devono essere posti con un buon numero di alternative, per limitare l'eventualità che la risposta corretta possa essere indovinata.

Un altro aspetto da considerare nell'inizializzazione dei parametri è la possibile degenerazione del modello. Lo studio condotto da Baker et al. [72] mostra che esistono diverse tecniche d'inizializzazione dei parametri, che variano per complessità e qualità dei risultati. Queste tecniche inoltre si occupano di evitare la degenerazione del BKT Model, che può verificarsi in modalità differenti, come mostrato di seguito.

Theoretical degeneration. Il principio teorico che garantisce il corretto funzionamento del BKT Model è che una migliore conoscenza implica una maggiore correttezza dei risultati dei test effettuati. Quando questo principio non viene più rispettato si dice che il modello è degenerato perché non fornisce più alcuna indicazione utile. In particolare ciò si verifica quando il modello implica che la casualità ha un impatto matematicamente maggiore rispetto alla conoscenza nella valutazione generale dell'apprendimento:

1. $p(S) > 0.5$: significa che avendo appreso un KC è più probabile sbagliare un test rispetto a rispondere correttamente;
2. $p(G) > 0.5$: significa che non avendo appreso un KC è più probabile rispondere correttamente ad un test rispetto a sbagliare;

Empirical degeneration. In base al valore assunto dai parametri del modello potrebbe verificarsi un'eventualità in cui rispondere correttamente ai test non implica un aumento del livello di conoscenza all'interno del BKT model. Se ciò avviene si considera il modello degenerato perché non fornisce più alcuna indicazione utile. In particolare Baker et al. propongono 2 test che devono essere superati dal modello per garantire l'assenza di degenerazione:

1. se i primi N test sono corretti deve valere la relazione $p(L_N) > p(L_0)$, cioè deve verificarsi un effettivo incremento dell'apprendimento all'interno del modello;
2. se M test consecutivi sono corretti deve essere garantito dal modello il raggiungimento della "skill mastery".

Gli effettivi valori di N e M sono arbitrari e al loro crescere aumenta la tolleranza del modello alla degenerazione. Nello studio vengono indicati $N = 3$ e $M = 10$ come cifre ragionevoli da adottare e sono questi i valori utilizzati per implementare il BKT Model all'interno del progetto di gioco. Il valore adottato per definire la soglia di raggiungimento della "skill mastery" è 0.95. Per quanto riguarda l'inizializzazione di $p(S)$ e $p(G)$ si è utilizzato il "bounded guess and slip approach" [72], che si basa sull'ipotesi che generalmente valgono gli assunti $p(S) < 0.1$ e $p(G) < 0.3$. Per questo motivo $p(S)$ e $p(G)$ sono stati inizializzati a questi valori di soglia.

Capitolo 5

Risultati

5.1 Questionario preliminare

Per testare in modo oggettivo l'efficacia del gioco è stato realizzato un questionario da compilare prima di iniziare a giocare. Le domande a risposta multipla al suo interno (disponibili alla Sez. B.4) trattano la sicurezza informatica; in particolare esse sono relative alle contromisure e agli attacchi contenuti nel gioco. Principalmente i contenuti del test sono categorizzabili in:

- domande sulla sicurezza di rete: verificano la conoscenza delle tecniche di difesa e delle configurazioni atte a contrastare gli attacchi che la minacciano;
- domande sulla sicurezza dell'accesso: trattano i comportamenti virtuosi da adottare per contrastare i tentativi di accesso illegale al sistema;
- domande sulla sicurezza del software: verificano sia la conoscenza delle tecniche di prevenzione e contrasto degli attacchi, sia la conoscenza degli attacchi stessi (in particolare malware);
- domande sull'usabilità della sicurezza: trattano il tema dell'esperienza dell'utente applicato a diverse contromisure.

Stimare la conoscenza preliminare del giocatore ha anche lo scopo di inizializzare al meglio il modello di valutazione interno al gioco: infatti uno dei parametri da inizializzare nel BKT Model è $p(L_0)$ (Sez. 4.4.2), ovvero la probabilità che un Knowledge Component sia appreso prima di iniziare i test. Purtroppo il gioco non è stato testato da una quantità di utenti sufficiente a rendere significativi i dati raccolti ed è per questo motivo che non vengono qui riportati i risultati del questionario confrontati al modello nel gioco. Tuttavia questi giocatori hanno condiviso alcuni feedback che suggeriscono le criticità e i punti di forza di Fintech Tycoon.

5.2 Feedback sull'esperienza di gioco

Vengono qui riassunti i principali aspetti commentati dai giocatori.

Utilità didattica Il punto maggiormente apprezzato sono stati gli elementi descrittivi all'interno del gioco. A tal proposito sono risultate particolarmente utili e dettagliate le descrizioni dei livelli dei vari oggetti in negozio, perché permettono di trasmettere concetti di sicurezza in modo integrato con il gameplay. A rafforzare questo aspetto è risultata utile la guida (soprattutto per i giocatori con una conoscenza preliminare non nulla della sicurezza informatica).

Realismo e profondità Le descrizioni degli oggetti in negozio favoriscono anche il realismo e la profondità del gameplay. A contribuire a quest'ultimo aspetto sono anche la gestione dei fondi e degli impiegati, che mostrano come non sia sufficiente individuare le contromisure adatte

a contrastare un attacco; al contrario il gioco suggerisce che sia necessario implementare con efficienza queste tecniche, considerando anche l'aspetto economico e organizzativo.

Quiz I quiz sono risultati utili a spezzare in determinati punti il ritmo del gioco, che altrimenti sarebbe risultato troppo monotono. Tuttavia i giocatori hanno riportato come alcuni di essi tendano a ripetersi, dato che il numero di domande non è molto elevato. Questo rovina l'esperienza di gioco, introducendo un fattore di ripetitività che non stimola la curiosità del giocatore.

Chiarezza delle meccaniche Alcuni giocatori hanno riportato come il tutorial possa risultare prolisso e, per questo, poco efficace. Tuttavia certi aspetti del gioco, come le gestione dei fondi e la riparazione degli attacchi, sono risultati poco chiari, proprio perché non approfonditi dal tutorial iniziale. La soluzione potrebbe essere di accorciarlo e allo stesso tempo renderlo più denso, per concentrarsi maggiormente sulle meccaniche meno chiare e tralasciare aspetti più facilmente intuibili dal giocatore.

Capitolo 6

Conclusioni

6.1 Stato dei Serious Games

In questa tesi l'analisi si è concentrata sui serious games videoludici, ma occorre sottolineare che sono stati proposti e sviluppati giochi che utilizzano un medium diverso. Sono diffusi, anche nell'ambito della sicurezza informatica, giochi da tavolo e anche giochi basati su mazzi di carte che si prefiggono obiettivi simili ai serious games analizzati in precedenza. Alcuni esempi sono i giochi da tavolo Control-Alt-Hack [73] e D0x3d! [74], che godono di una buona popolarità, oppure il gioco di carte realizzato di recente Riskio [75].

Per quanto riguarda l'analisi dello stato dell'arte dei Security Serious Games si può concludere che l'offerta è in continuo ampliamento ed è già discretamente vasta. La varietà dei progetti non si riscontra solamente negli argomenti trattati dai giochi, ma anche dalle differenze sostanziali tra i vari gameplay, che suggeriscono enormi potenzialità: si può spaziare da serious games con un approccio simulativo come CyberCIEGE (Sez. 2.2.2), ad altri come CyberCraft (Sez. 2.2.4) che presentano delle componenti ludiche e tattiche più marcate, fino ad avere giochi come Targeted Attacks (Sez. 2.2.10), che sono in pratica delle storie interattive.

Nonostante ciò l'offerta non è ancora esaustiva: la stessa proposta di Fintech Tycoon ha come motivazione principale il fatto che non siano stati individuati Serious Games che si occupano della sicurezza informatica in ambito open banking. Tuttavia lo sviluppo di giochi come The Weakest Link (Sez. 2.2.15) e lo stesso Targeted Attacks si può interpretare come un segnale di maggiore interesse delle compagnie nei confronti di questo mezzo, visto come un metodo efficace nel veicolare nuove conoscenze.

6.2 Fintech Tycoon: sviluppi futuri

In generale Fintech Tycoon è un gioco abbastanza semplice (anche dal punto di vista della grafica utilizzata) e che presenta per questo dei margini di miglioramento. In questa sezione sono indicati i punti principali che possono essere migliorati o aggiunti.

6.2.1 Storia

Il gioco non presenta una storia vera e propria, ma solamente un contesto (quello della FinTech) in cui avvengono alcuni eventi isolati (come i quiz) e dove il giocatore deve perseguire l'obiettivo di ottenere un numero di clienti sempre maggiore, gestendo la sicurezza dell'azienda. Ciò è dovuto anche dal fatto che si tratta di un gioco tycoon, in cui spesso la storia gioca un ruolo secondario. Tuttavia la realizzazione di una trama, anche semplice, può aumentare l'immersività del gioco, rafforzando il coinvolgimento e la curiosità del giocatore.

6.2.2 Elementi da migliorare

Alcuni elementi già presenti nel gioco possono essere migliorati.

Quiz I quiz che vengono sottoposti al giocatore tendono a ripetersi durante la partita (Sez. 5.2). Per evitare che ciò accada sarebbe utile aggiungerne di ulteriori, andando ad ampliarne anche la quantità di argomenti trattati. In questo modo si possono fornire informazioni maggiori e più accurate anche al sistema di valutazione.

Guida La guida presente nel gioco può essere arricchita sia nelle descrizioni che nel numero di nozioni trattate. Inoltre in alcuni punti risulta eccessivamente testuale e si può ovviare a questo problema corredandola di immagini e schemi, per rendere più chiare le spiegazioni.

Impiegati Ogni impiegato possiede delle abilità specifiche, che attualmente sono fisse. Una miglioria potrebbe essere quella di introdurre un sistema di esperienza per i dipendenti, in modo che, lavorando ai vari incarichi, possano migliorare le loro abilità. Questo permetterebbe al giocatore una maggiore personalizzazione della partita e una maggiore possibilità di scelta.

Tutorial Rendere il tutorial più appetibile è un altro possibile miglioramento, anche richiesto in alcuni feedback (Sez. 5.2). Si potrebbe lavorare per renderlo meno prolisso e allo stesso tempo più denso di informazioni, concentrandosi maggiormente sulle meccaniche meno chiare al giocatore e tralasciando gli aspetti più intuibili del gioco.

6.2.3 Attacchi ed eventi imprevisti

Per rendere l'esperienza di gioco più avvincente e sollecitare la curiosità del giocatore si può pensare di aggiungere elementi a sorpresa lungo la partita. In particolare si potrebbero introdurre degli eventi imprevisti a cui il giocatore deve far fronte (ad es. un dipendente si ammala e non può lavorare per un periodo di tempo). Allo stesso modo durante la partita si potrebbero pianificare degli attacchi complessi spezzandoli in più fasi: in questo modo le decisioni del giocatore potrebbero determinare se l'attacco verrà individuato e bloccato in tempo o se, al contrario, colpirà l'azienda a causa della sua mancata accortezza.

6.2.4 Accessibilità

Ulteriori miglioramenti possono essere applicati al contesto dell'accessibilità al gioco.

Compatibilità mobile La tecnologia WebGL utilizzata permette di giocare tramite un browser, ma allo stesso tempo essa presenta delle incompatibilità con l'ambiente mobile. Rendere il serious game compatibile anche per queste piattaforme permetterebbe di raggiungere un numero maggiore di giocatori.

Localizzazione I contenuti del gioco sono in lingua italiana e questo limita di molto il bacino di utenza. Sarebbe utile poter presentare una versione del gioco che utilizza la lingua inglese.

6.3 Considerazioni finali

L'interesse per i Serious Games è sempre maggiore, come anche il riconoscimento della loro efficacia. Con questo lavoro si è analizzato nel particolare lo stato dell'arte di tali giochi nell'ambito della sicurezza informatica, mostrando che, per quanto in rapido aumento, l'offerta dei Security Serious Games non è esaustiva, ma è anzi lontana dal potersi definire completa.

Per favorire l'inserimento di questi strumenti nell'ambito educativo è necessario vincere alcune diffidenze che ancora identificano il giocare (e soprattutto il videogiocare) unicamente come un'attività frivola. D'altro canto uno sforzo è richiesto anche agli sviluppatori di questi strumenti, che sono chiamati a realizzare dei prodotti solidi che si possano diffondere nei campi didattici più disparati.

Bibliografia

[1] S. Morgan, "Cybersecurity market report, q4 2015", Mar 2018, https://cybersecurityventures.com/cybersecurity-market-report-q4-2015/

[2] S. Morgan, "Cybercrime to cost the world $10.5 trillion annually by 2025", Nov 2020, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[3] D. Braue, "Global cybersecurity spending to exceed $1.75 trillion from 2021-2025", Set 2021, https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

[4] B. Schneier, "The process of security", Apr 2000, https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

[5] C. Abt, "Serious games", The Viking Press, 1970

[6] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: Defining gamification", MindTrek '11: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, Set 2011, p. 9–15, DOI 10.1145/2181037.2181040

[7] Serious Games Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026), Nov 2021, https://www.researchandmarkets.com/reports/4897252/serious-games-market-growth-trends-covid-19

[8] Serious Game Initiative, https://www.wilsoncenter.org/program/serious-games-initiative

[9] America's Army, https://www.americasarmy.com/

[10] D. Michael e S. Chen, "Serious games: Games that educate, train, and inform", Course Technology PTR, Ott 2005, ISBN: 978-1-592-00622-9

[11] K. Corti, "Games-based learning; a serious business application", Feb 2006, https://www.cs.auckland.ac.nz/courses/compsci777s2c/lectures/Ian/serious%20games%20business%20applications.pdf

[12] B. Sawyer and P. Smith, "Serious games taxonomy", San Francisco Game Developer Conference 2008, 19 Feb 2008. https://thedigitalentertainmentalliance.files.wordpress.com/2011/08/serious-games-taxonomy.pdf

[13] D. Djaouti, J. Alvarez, and J.-P. Jessel, "Classifying serious games: The g/p/s model", Handbook of Research on Improving Learning and Motivation through Educational Games: Multidisciplinary Approaches (P. Felicia, ed.), ch. 6, pp. 118–136, IGI Global, Apr 2011, DOI 10.4018/978-1-60960-495-0.ch006

[14] Serious Game Classification, http://serious.gameclassification.com/EN/index.html

[15] K. Subrahmanyam and P. M. Greenfield, "Effect of video game practice on spatial skills in girls and boys", Journal of Applied Developmental Psychology, vol. 15, no. 1, Gen 1994, pp. 13–32, DOI 10.1016/0193-3973(94)90004-3

[16] K. Lohse, N. Shirzad, A. Verster, N. Hodges, and M. Van der Loos, "Video games and rehabilitation", Journal of Neurologic Physical Therapy, vol. 37, no. 4, Dec 2013, pp. 166–175, DOI 10.1097/NPT.0000000000000017

[17] P. Bonato, "Advances in wearable technology and applications in physical medicine and rehabilitation", Journal of NeuroEngineering and Rehabilitation, vol. 2, no. 2, Feb 2005, DOI 10.1186/1743-0003-2-2

[18] L. Elliott, A. Golub, M. Price, and A. Bennett, "More than just a game? combat-themed gaming among recent veterans with posttraumatic stress disorder", Games for Health Journal, vol. 4, no. 4, Ago 2015, p. 271–277, DOI 10.1089/g4h.2014.0104

[19] T. Saraiva, P. Gamito, J. Oliveira, D. Morais, M. Pombal, L. Gamito, and M. Anastácio, "The use of vr exposure in the treatment of motor vehicle ptsd: A case-report", Annual

Review of CyberTherapy and Telemedicine, vol. 5, 2007, p. 199–205. https://psycnet.apa.org/record/2008-04694-027

[20] R. Kulman, "Video games can help kids with adhd - if you choose wisely", 20 Mag 2021, https://www.additudemag.com/video-games-help-adhd

[21] C. A. Anderson, A. Shibuya, N. Ihori, E. L. Swing, B. J. Bushman, A. Sakamoto, H. R. Rothstein, and M. Saleem, "Violent video game effects on aggression, empathy, and prosocial behavior in eastern and western countries: A meta-analytic review", Psychological Bulletin, vol. 136, no. 2, 2010, pp. 151–173, DOI 10.1037/a0018251

[22] World Health Organization, "Icd-11 for mortality and morbidity statistics", Feb 2022, https://icd.who.int/browse11/l-m/en

[23] E. Aarseth, A. M. Bean, H. Boonen, M. C. Carras, M. Coulson, D. Das, J. Deleuze, E. Dunkels, J. Edman, C. J. Ferguson, M. C. Haagsma, K. H. Bergmark, Z. Hussain, J. Jansz, D. Kardefelt-Winther, L. Kutner, P. Markey, R. K. L. Nielsen, N. Prause, A. Przybylski, T. Quandt, A. Schimmenti, V. Starcevic, G. Stutman, J. V. Looy, and A. J. V. Rooij, "Scholars'open debate paper on the world health organization icd-11 gaming disorder proposal", Journal of Behavioral Addictions, vol. 6, no. 3, Set 2017, pp. 267–270, DOI 10.1556/2006.5.2016.088

[24] M. Csikszentmihalyi, "Flow: The psychology of optimal experience", HarperCollins Publishers, 1991, ISBN: 9780060920777

[25] M. Csikszentmihalyi and I. S. Csikszentmihalyi, "Optimal experience: Psychological studies of flow in consciousness", Cambridge University Press, Ago 1988, DOI 10.1017/CBO9780511621956

[26] J. Lave and E. Wenger, "Situated learning: Legitimate peripheral participation", 1991, DOI 10.1017/cbo9780511815355

[27] J. Herrington and R. Oliver, "An instructional design framework for authentic learning environments", Educational Technology Research and Development, vol. 48, no. 3, Set 2000, pp. 23–48, DOI 10.1007/bf02319856

[28] D. W. Shaffer, K. R. Squire, R. Halverson, and J. P. Gee, "Video games and the future of learning", Phi Delta Kappan, vol. 87, no. 2, Ott 2005, pp. 105–111, DOI 10.1177/003172170508700205

[29] Cryptoclub Project, https://cryptoclubproject.uchicago.edu/

[30] CryptoClub.org, https://www.cryptoclub.org/

[31] V.O.R.T.E.X., https://www.cryptoclub.org/index.html#vGames

[32] CyberCIEGE, https://nps.edu/web/c3o/cyberciege

[33] A. L. Krassmann, A. Falcade, L. E. G. D. Silva, and R. D. Medina, "Serious games to computer networks learning with cyberciege: A case study in brazilian higher education", 23º WEI - Workshop sobre Educação em Computação, Luglio 2015, DOI 10.5753/wei.2015.10219

[34] BigBro, https://bitbucket.org/BlackDavid/securityseriousgame/src/master/gaetano/BigBro/

[35] CyberCraft, https://github.com/luyangshang/CyberCraft

[36] SimSCADA, https://github.com/serranda/SecuritySeriousGame

[37] DropIt!, https://bitbucket.org/alexander_doni/dropit-a-personal-firewall-sec...

[38] Insector, https://github.com/davidpereza7/InSecTorv1

[39] Game-based Interactive Simulator for Training Professionals in Cybersecurity Vulnerabilities, https://imprint-india.org/knowledge-portal-7804-game-based-interactive-sim...

[40] Targeted Attack: The Game, http://targetedattacks.trendmicro.com/

[41] Data Center Attack: The Game, https://resources.trendmicro.com/datacenter-attack.html

[42] Cybersecurity Lab, https://www.pbs.org/wgbh/nova/labs/lab/cyber/

[43] D. E. H. Løvgren, J. Li, and T. D. Oyetoyan, "A data-driven security game to facilitate information security education", 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), 2019, pp. 256–257, DOI 10.1109/ICSE-Companion.2019.00102

[44] Data-driven Security Game, https://github.com/dagerikhl/ddsg

[45] NetSim, https://netsim.erinn.io/

[46] S. K. Sehl, "Permission impossible - the design and evaluation of a video game that teaches beginners about firewalls", 2017

[47] Permission Impossible, https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/

[48] The Weakest Link, https://www.isdecisions.com/user-security-awareness-game/

[49] L. Brodsky, L. Oakes, "Data sharing and open banking", 5 Set 2017, https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

[50] H. Chesbrough, "Open innovation: The new imperative for creating and profiting from technology", Harvard Business Press, Gen 2003, ISBN: 9781578518371

[51] F. Hacquebord, R. McArdle, F. Mercês, Da. Sancho, "Ready or not for psd2: The risks of open banking", 17 Set 2019, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2

[52] OFX Work Group, https://financialdataexchange.org/ofx

[53] R. P. S. Directive, https://eur-lex.europa.eu/eli/dir/2015/2366/oj/ita

[54] Ravelin, "Psd2 and strong customer authentication." https://www.ravelin.com/insights/ultimate-guide-psd2-strong-customer-authentication

[55] European Central Bank, "Fifth report on card fraud", Set 2018, https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html

[56] Tech Specifications of the PSD2 services exposed to the Third Party Providers, https://www.cbiglobe.com/Wiki/index.php/2._Actors_and_definitions

[57] Regulatory Technical Standards on Strong Customer Authentication, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC

[58] European Banking Authority, "Opinion of the european banking authority on the implementation of the rts on sca and csc", 13 Giu 2018, https://www.eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-...

[59] I. Lunden, "Stripe acquires touchtech, updates apis to prep for strong customer authentication in europe", 17 Apr 2019, https://techcrunch.com/2019/04/17/stripe-acquires-touchtech-updates-apis-...

[60] 3-D Secure, https://www.emvco.com/emv-technologies/3d-secure/

[61] S. J. Murdoch and R. Anderson, "Verified by visa and mastercard securecode: Or, how not to design authentication", FC 2010: Financial Cryptography and Data Security (R. Sion, ed.), pp. 336–342, Springer, Berlin, Heidelberg, 2010, DOI 10.1007/978-3-642-14577-3_27

[62] 3-D Secure 2.0, https://3dsecure2.com/

[63] Financial Grade API Work Group, https://openid.net/wg/fapi/

[64] D. Fett, P. Hosseyni, and R. Küsters, "An extensive formal security analysis of the openid financial-grade api", 2019 IEEE Symposium on Security and Privacy, Mag 2019, pp. 453–471, DOI 10.1109/SP.2019.00067

[65] CyberSec4Europe, "D5.4 requirements analysis of demonstration cases phase 2." https://cybersec4europe.eu/wp-content/uploads/2021/05/D5.4-Requirements-Analysis-of-Demonstration-Cases-Phase-2-v1.0-submitted.pdf

[66] OBSIDIAN project, https://obsidian-project.eu/

[67] C. Alonso-Fernández, A. Calvo-Morata, M. Freire, I. Martínez-Ortiz, and B. Fernández-Manjón, "Applications of data science to game learning analytics data: A systematic literature review", Computers & Education, vol. 141, Nov 2019, DOI 10.1016/j.compedu.2019.103612

[68] M.-T. Cheng, L. Rosenheck, C.-Y. Lin, and E. Klopfer, "Analyzing gameplay data to inform feedback loops in the radix endeavor", Computers & Education, vol. 111, 2017, pp. 60–73, DOI 10.1016/j.compedu.2017.03.015

[69] R. S. J. D. Baker, M. P. J. Habgood, S. E. Ainsworth, and A. T. Corbett, "Modeling the acquisition of fluent skill in educational action games", UM 2007: User Modeling 2007 (C. Conati, K. McCoy, and G. Paliouras, eds.), pp. 17–26, Springer, Berlin, Heidelberg, 2007, DOI 10.1007/978-3-540-73078-1_5

[70] A. T. Corbett and J. R. Anderson, "Knowledge tracing: Modeling the acquisition of procedural knowledge", User Model User-Adap Inter, vol. 4, 1994, pp. 253–278, DOI 10.1007/BF01099821

[71] G.-H. Gweon, H.-S. Lee, C. Dorsey, R. Tinker, W. Finzer, and D. Damelin, "Tracking student progress in a game-like learning environment with a monte carlo bayesian knowledge tracing model", LAK '15: Proceedings of the Fifth International Conference on Learning Analytics And Knowledge, March 2015, p. 166–170, DOI 10.1145/2723576.2723608

[72] R. S. J. d. Baker, A. T. Corbett, and V. Aleven, "More accurate student modeling through contextual estimation of slip and guess probabilities in bayesian knowledge tracing", ITS 2008: Intelligent Tutoring Systems (B. Woolf, E. Aïmeur, R. Nkambou, and S. Lajoie, eds.), pp. 406–415, Springer, Berlin, Heidelberg, 2008, DOI 10.1007/978-3-540-69132-7_44

[73] Control-Alt-Hack, http://www.controlalthack.com/

[74] D0x3d!, https://d0x3d.com/d0x3d/welcome.html

[75] Riskio, https://www.riskio.co.uk/

Appendice A

Manuale di installazione

A.1 Installazione

Al momento della stesura di questo documento non è necessario installare il gioco per poterlo provare, dato che è possibile giocarci a questo indirizzo. Tuttavia nel caso il gioco non sia disponibile online è possibile giocarlo anche dal proprio computer utilizzando un web server. Di seguito vengono illustrati i passaggi da seguire.

A.1.1 Installazione del server di gioco

Per poter eseguire il gioco è necessario avere un web server Apache installato sul proprio computer. Una soluzione per questo punto è utilizzare il software gratuito `XAMPP`[1], disponibile per Windows, MacOS e Linux. Dopo aver completato l'installazione occorre individuare la cartella in cui sono stati salvati i file di `XAMPP`, che generalmente è:

- su Windows: `C:/xampp`
- su Linux: `/opt/xampp`
- su MacOS: `/Applications/XAMPP/xamppfiles`

Al suo interno occorre aprire la cartella `htdocs` e qui creare una nuova cartella `fintech-tycoon`, in cui andranno posizionati i file del gioco.

A.1.2 Ottenimento della build

Dopo aver impostato il web server è necessario ottenere i file di gioco, scaricando il repository GitHub all'indirizzo `https://github.com/Stevezbiz/SecuritySeriousGame` (utilizzando il comando `git clone https://github.com/Stevezbiz/SecuritySeriousGame` o semplicemente scaricando il progetto in formato .zip). Ora è necessario copiare il contenuto della cartella `SeriousGame/Build` (appartenente al progetto appena scaricato) all'interno della cartella `htdocs/fintech-tycoon` creata in precedenza. Inoltre, per permettere al server di funzionare correttamente, è anche necessario copiare la cartella `SeriousGame/WebScripts` nella cartella `htdocs/fintech-tycoon`.

In alternativa è possibile generare un build utilizzando direttamente Unity. Dopo aver installato `Unity Hub`[2] (occorre, al momento dell'installazione, selezionare il modulo WebGL) sarà

[1] scaricabile alla pagina `https://www.apachefriends.org/it/download.html`

[2] scaricabile alla pagina `https://unity3d.com/get-unity/download`

possibile aprire all'interno dell'ambiente di sviluppo il progetto appena scaricato, selezionando la cartella `SeriousGame`. A questo punto occorre generare una nuova build WebGL. Selezionando dal menu `File` la voce `Build Settings` si aprirà la schermata di build. Bisogna selezionare la piattaforma WebGL dal menu a sisnistra e premere sul tasto build, selezionando come destinazione la cartella `htdocs/fintech-tycoon` (oppure selezionando una cartella a scelta e copiando i file generati in seguito).

A.1.3 Avvio del server e del gioco

Dopo aver effettuato tutti i passaggi descritti finora è necessario avviare il server Apache dal pannello di controllo `XAMPP`. Per iniziare a giocare occorre collegarsi dal browser alla pagina `http://localhost/fintech-tycoon`.

Appendice B

Manuale del programmatore

Il progetto Unity di Fintech Tycoon è disponibile su GitHub all'indirizzo https://github.com/Stevezbiz/SecuritySeriousGame. Una volta scaricato è sufficiente aprire il progetto contenuto nella cartella `SeriousGame` all'interno dell'editor Unity. La versione utilizzata per la realizzazione del gioco è `Unity 2020.3.16.f1`.

B.1 Contenuti senza codice

Per caricare la maggior parte dei dati di gioco sono stati utilizzati file di configurazione in formato `json`, con l'obiettivo di rendere più semplice l'aggiunta e la modifica dei dati stessi. L'interazione del motore di gioco con i suddetti file avviene tramite l'utilizzo della classe `JsonUtility` (contenuta nelle API di Unity), che mette a disposizione i metodi `FromJson` e `ToJson` per trasformare stringhe `json` in oggetti e viceversa.

B.1.1 Strutture dati e file di configurazione

In questa sezione viene spiegato a cosa servono i vari file utilizzati e viene anche descritta la struttura dei file di configurazione che si trovano nella cartella `SeriousGame/Assets/Config`.

Dipendenti Gli impiegati disponibili all'interno del gioco sono definiti all'interno del file `employees.json` e presentano la struttura della classe `EmployeeInfo` mostrata in Fig. B.1. Per aggiungere un nuovo dipendente è sufficiente inserire nel file un nuovo oggetto con un `id` non ancora utilizzato (da aggiungere nell'`enum EmployeeCode` all'interno del file `EmployeeUtils.cs`).

```
"id": (enum) id univoco per riconoscere l'impiegato
"name": (string) nome dell'impiegato
"description": (string) breve descrizione delle caratteristiche
"moneyGain": (int) guadagno ottenuto dal lavoro dell'impiegato
"owned": (bool) indica se l'impiegato e' assunto
"status": (enum) indica lo stato dell'impiegato (al lavoro, prevenzione, ...)
"abilities": (array) indica le abilita' dell'impiegato nei vari ambiti
    {"category": (enum) id per riconoscere la categoria
    "level": (int) livello dell'abilita'}
```

Figura B.1. Struttura dati di un impiegato in `employees.json`

Attacchi Gli attacchi utilizzati all'interno del gioco sono ottenuti dal file `attacks.json` e presentano la struttura della classe `AttackInfo` mostrata in Fig. B.2. Per aggiungere un attacco

è sufficiente inserire nel file un nuovo oggetto con un `id` non ancora utilizzato (da aggiungere nell'`enum AttackCode` all'interno del file `AttackUtils.cs`).

```
"id": (enum) id univoco per riconoscere l'attacco
"category": (enum) indica la categoria di appartenenza
"name": (string) il nome dell'attacco
"description": (string) descrizione dell'attacco e delle sue conseguenze
"moneyLoss": (int) ricaduta economica istantanea
"usersLoss": (int) perdita di utenti istantanea
"moneyMalus": (float) malus economico per la durata dell'attacco
"usersMalus": (float) ricaduta sul numero di utenti per la durata
"reputationMalus": (float) perdita di reputazione istantanea
"maxTime": (int) tempo massimo tra due tentativi consecutivi di attacco
"duration": (int) durata dell'attacco in ore
```

Figura B.2. Struttura dati di un attacco in `attacks.json`

Negozio Gli oggetti che popolano il negozio sono ottenuti dal file `shop.json` e presentano la struttura della classe `ShopItemInfo` mostrata in Fig. B.3. Per aggiungere un oggetto al negozio è sufficiente inserire nel file un nuovo oggetto con un `id` non ancora utilizzato (da aggiungere nell'`enum ShopItemCode` all'interno del file `ShopUtils.cs`).

```
"id": (enum) id univoco per riconoscere l'oggetto
"category": (enum) id per riconoscere la categoria
"name": (string) il nome dell'oggetto
"description": (string[]) ogni elemento contiene la descrizione del livello
    del potenziamento (es. description[1] contiene la descrizione del livello
    2)
"cost": (int[]) i costi per acquistare i vari livelli
"moneyMalus": (float[]) costo di mantenimento all'ora
"usersMod": (float[]) eventuali malus o bonus all'usabilita' del servizio (<0
    malus, >0 bonus)
"status": (enum) stato dell'oggetto (acquistato, attivo, ...)
"locked": (bool[]) indica se il livello dell'oggetto e' bloccato e non puo'
    essere ancora acquistato
"upgradeTime": (int[]) tempi necessari all'installazione e al potenziamento
"resArray": (array) resistenze agli attacchi in base al livello
    {"resistances": (array) resistenze agli attacchi per un livello
        {"id": (enum) id univoco dell'attacco
        "duration": (float) diminuzione della durata dell'attacco
        "miss": (float) umento della probabilita' di evitare l'attacco
        "endurance": (float) aumento del tempo massimo tra due tentativi
            consecutivi di attacco}}
"reqArray": (array) elenco dei requisiti in base al livello
    {"requirements": (enum[]) indica eventuali requisiti necessari
        all'acquisto del livello corrispondente}
"maxLevel": (int) il numero di livelli dell'oggetto
"level": (int) livello attuale dell'oggetto
```

Figura B.3. Struttura dati di un oggetto del negozio in `shop.json`

Configurazione della partita Le variabili utilizzate per creare una nuova partita sono ottenute dal file `game_config.json` e presentano la struttura della classe `GameConfig` mostrata in

Fig. B.4. In questo modo è possibile modificare i parametri principali di una partita senza andare a modificare il codice del progetto. Inoltre questo insieme di variabili viene utilizzato per generare anche i salvataggi.

```
"totalTime": (int) ore di gioco trascorse dall'inizio della partita
"endTime": (int) ore di gioco totali per terminare la partita
"negativeTime": (int) ore di gioco consecutive in cui il bilancio e' in
    negativo
"maxNegative":(int) massimo numero di "negativeTime" prima del game over
"evaluationTime": (int) numero di ore di gioco per una nuova valutazione
"quizTime": (int) numero di ore di gioco per un nuovo quiz
"actualQuiz": (enum) id del prossimo quiz
"quizTimer": (int) ore di gioco rimaste per mostrare il prossimo quiz
"attackTrendTime": (int) durata in ore di gioco per un trend di attacchi
"actualAttackTrend": (enum) attacco attualmente in trend
"attackTrendTimer": (int) ore di gioco rimaste al trend attuale
"resistanceModStep": (int) numero di ore di gioco per un nuovo invecchiamento
    delle difese
"actualResistanceMod": (int) livello attuale di invecchiamento delle difese
"noAttackTime": (int) ore di gioco consecutive senza attacchi in corso
"noAttackStep": (int) numero di ore di gioco consecutive senza attacchi per
    ottenere un bonus di reputazione
"ongoingAttacks": (int) numero di attacchi in corso
"userLevel": (int) livello del numero di utenti
"employeeLevel": (int) indice per selezionare l'obiettivo di utenti da
    raggiungere per assumere un nuovo dipendente
"abilityOffset": (float) offset per il calcolo delle abilita'
"abilityFactor": (float) coefficiente per il calcolo delle abilita'
"money": (float) denaro disponibile
"users": (float) utenti
"reputation": (float) reputazione
"duration": (float[]) modificatori della durata degli attacchi
    (invecchiamento)
"endurance": (float[]) modificatori della complessita' degli attacchi
    (invecchiamento)
"miss": (float[]) modificatori della difesa contro gli attacchi
    (invecchiamento)
"usersGain": (float[]) coefficienti per il guadagno di utenti
"usersGoals": (float[]) obiettivi per stabilire il guadagno di utenti
"employeeGoals": (float[]) obiettivi per assumere personale
"date": (string) data all'interno del gioco
"musicVolume": (float) volume della musica in gioco
"musicMute": (bool) indica se la musica e' mutata
"effectsVolume": (float) volume degli effetti sonori in gioco
"effectsMute": (bool) indica se gli effetti sonori sono mutati
"firstNegative": (bool) indica se il bilancio non e' ancora andato in negativo
```

Figura B.4. Struttura dati delle variabili di configurazione in `game_config.json`

B.1.2 Assets utilizzati

In questa sezione viene riassunto brevemente da dove sono stati recuperati gli assets utilizzati nel progetto.

Grafica Tutti gli assets grafici utilizzati (come gli sprite e le immagini del gioco) sono stati realizzati da Freepik[1] e sono stati presi dal sito Flaticon (all'indirizzo https://www.flaticon.com/authors/freepik). Alcuni di essi sono stati modificati con il software GIMP[2] per migliorarne l'integrazione con gli altri elementi del gioco.

Musiche e suoni La musica del gioco è il brano Funky Deep realizzato da fourstones, ottenuta dal sito ccMixter all'indirizzo http://dig.ccmixter.org/files/victor/52194. Gli effetti sonori sono stati realizzati e forniti dal sito ZapSplat all'indirizzo https://www.zapsplat.com.

Font Sono stati utilizzati dei font forniti dal sito DaFont (all'indirizzo https://www.dafont.com/it/), in particolare:

- Alarm Clock, realizzato da David J. Patterson;
- Quantum, realizzato da Sesohq;
- Semi Coder, realizzato da Walter E. Stewart.

B.2 Classi e scripts

In questa sezione vengono descritte le componenti responsabili del funzionamento vero e proprio del gioco. Vengono anche descritti i metodi più significativi.

B.2.1 Gestione della partita

Il file `GameManager.cs` contiene il codice responsabile della gestione generale del gioco. Nella classe `GameManager` sono contenute tutte le principali strutture dati (liste di impiegati, attacchi, difese...) e tutti i metodi principali su cui sono basati gli eventi del gioco. All'interno del metodo `Update` è presente una funzione che ogni secondo si occupa di aggiornare lo stato del gioco, chiamando i suddetti metodi. Segue una descrizione delle principali operazioni che vengono effettuate.

Attacchi Il funzionamento degli attacchi in Fintech Tycoon è temporizzato: ogni attacco viene programmato calcolando un timer che, una volta scaduto, provoca il lancio dell'attacco stesso (che può avere esito positivo o negativo). In particolare:

- il metodo `ScheduleAttack` programma un attacco calcolando il timer relativo;
- il metodo `ActivateAttacks` si occupa di introdurre nuovi attacchi durante la partita;
- il metodo `UpdateAttacks` gestisce lo stato degli attacchi in corso, decrementando i timer e occupandosi di rilanciarli ciclicamente.

Messaggi Il sistema di messaggistica viene gestito tramite il metodo `UpdateMessages` che si occupa di mostrare i messaggi al giocatore. In particolare tutti i messaggi vengono inseriti in una coda e ogni volta che questo metodo viene eseguito essi vengono mostrati uno dopo l'altro, fino a svuotare la coda.

Incarichi I vari tasks assegnati agli impiegati vengono gestiti tramite il metodo `UpdateTasks`. In particolare questo metodo si occupa di decrementare i timer degli incarichi e gestire la loro conclusione.

La classe `GameManager` si occupa inoltre di fornire i dati alle varie viste che compongono il gioco. Ognuna di queste (contenute nei files `*View.cs`) presenta graficamente i dati ottenuti e quando il giocatore intraprende un'azione chiama i metodi contenuti in `GameManager`.

[1] https://www.freepik.com

[2] scaricabile all'indirizzo https://www.gimp.org/downloads/

B.2.2 Gestione del salvataggio

All'interno del gioco è prevista la possibilità di salvare la partita, in modo da interromperla e continuarla in un secondo momento. Il salvataggio e il caricamento di dati salvati vengono gestiti in modo asincrono all'interno del codice, dato che prevedono di comunicare con il server, dove i dati vengono effettivamente memorizzati. Il salvataggio viene effettuato all'interno di una cartella creata per ogni giocatore in formato `json` (utilizzando nuovamente la classe di Unity `JsonUtility`). In particolare viene creato un oggetto di classe `GameSave` (la cui struttura è mostrata in Fig. B.5) che verrà salvato nel file `game_save.data`.

```
"gc": configurazione del gioco (classe GameConfig)
"sir": stato degli oggetti nel negozio
"er": stato degli impiegati
"logs": logs di gioco
"aStats": statistiche degli attacchi
"aSchedule": stato degli attacchi programmati
"waitingAttacks": tasks non assegnati
"assignedTasks": stato dei tasks assegnati
"res": stato delle resistenze attive
```

Figura B.5. Struttura dati della classe di salvataggio `GameSave`

Il file `SaveSystem.cs` contiene l'omonima classe e i metodi che si occupano di comunicare con il server al fine di salvare o caricare i dati di una partita. Per farlo vengono utilizzate le `Coroutine` messe a disposizione dall'ambiente Unity. Si tratta di funzioni asincrone non bloccanti che vengono lanciate in parallelo all'esecuzione del gioco. Al loro interno vengono utilizzate delle `UnityWebRequest` per formulare le richieste al server. Una volta giunte al server le richieste vengono gestite da alcuni script in linguaggio `php` contenuti nella cartella `WebScripts`, che si occupano di attuare modifiche sul server (salvataggio) oppure di restituire i dati richiesti (caricamento).

B.3 Sistema di valutazione

Il sistema di valutazione è stato implementato in maniera modulare, nel tentativo di mantenerlo il più distinto possibile dal codice del gioco. In particolare la sua implementazione di trova all'interno del file `BKTModel.cs` e viene inizializzato dalla classe `ModelConfig` (la cui struttura è mostrata in Fig. B.6). Il modello viene utilizzato aggiungendo i test effettuati tramite il metodo `AddTestResult`, che provoca l'aggiornamento delle variabili del modello stesso. Per mantenere minima l'interazione tra il codice del modello e del gioco, il sistema di valutazione viene aggiornato solo dalla classe `GameManager`, che contiene vari metodi (rinominati nella forma `Evaluate*`) che si occupano di valutare le decisioni del giocatore.

Per comunicare al server i dati generati dal modello si utilizza un approccio analogo a quello descritto precedentemente (Sez. B.2.2), con la differenza che viene utilizzata la classe `ModelSave` (mostrata in B.7) per generare il salvataggio. I dati vengono salvati nel file `model_save.data`, sempre utilizzando script `php` appositi.

B.4 Questionario di valutazione

Prima di iniziare a giocare viene proposto ai giocatori un questionario per valutare il loro livello di conoscenza della sicurezza informatica, in vista di una valutazione dell'efficacia del gioco. Vengono riportate di seguito le domande utilizzate al suo interno (tutte le domande hanno come risposta corretta la prima opzione tra le quattro proposte).

```
"COGNITIVE_MASTERY": (float) soglia di raggiungimento della skill mastery
"N_FIRST_EMPIRICAL_TEST": (int) numero di tests per il primo test empirico
"M_SECOND_EMPIRICAL_TEST": (int) numero di tests per il secondo test empirico
"baseTransit": (float) probabilita' di transizione p(T)
"baseSlip": (float) probabilita' di slip p(S)
"baseGuess": (float) probabilita' di guess p(G)
"baseLearned": (float) probabilita' di conoscenza gia' appresa p(L0)
"actualTimeSlot": (int) indice per decretare i requisiti attuali
"timeSlots": (int[]) intervalli di tempo per modificare i requisiti
"kcs": (array) elenco dei vari Knowledge Components del modello
    {"id": (enum) id della skill
    "name": (string) nome della skill}
"requirements": (array) elenco dei requisiti di difesa dagli attacchi
    {"id": (enum) id dell'attacco
    "durationL": (float[]) soglie minime del valore della resistenza "durata"
    "durationH": (float[]) soglie massime del valore della resistenza "durata"
    "missL": (float[]) soglie minime del valore della resistenza "difesa"
    "missH": (float[]) soglie massime del valore della resistenza "difesa"
    "enduranceL": (float[]) soglie minime del valore della resistenza
        "complessita'"
    "enduranceH": (float[]) soglie massime del valore della resistenza
        "complessita'"}
```

Figura B.6. Struttura dati delle variabili di configurazione in `bkt_model.json`

```
"records": (array)
    {"id": (enum) id della skill
    "name": (string) nome della skill
    "transitionPos": (int) numero del test in cui si stima sia avvenuta
        l'acquisizione della conoscenza
    "tests": (bool[]) elenco dei tests effettuati}
"actualTimeSlot": (int) indice per decretare i requisiti attuali
```

Figura B.7. Struttura dati della classe di salvataggio `ModelSave`

1. Qual è lo scopo principale di un firewall?
   - scartare connessioni pericolose in ingresso e uscita da una rete
   - scartare connessioni pericolose solo in ingresso ad una rete
   - impedire gli attacchi malware
   - proteggere le credenziali di chi accede alla rete
2. Perché un attacco Man-In-The-Middle è pericoloso?
   - può intercettare informazioni riservate (come le credenziali di accesso)
   - aggira controlli di accesso deboli (come password brevi)
   - raggira le vittime con e-mail false
   - danneggia il backup di una compagnia
3. Quale di queste contromisure è inefficace nel contrastare un attacco DoS?
   - aumentare la lunghezza delle password

- utilizzare server più performanti
- rimuovere dalla coda di connessioni quelle non completate dopo un limite di tempo
- utilizzare un firewall

4. Quale tra le seguenti è la maggiore minaccia alla sicurezza del DNS (Domain Name System)?
   - attacco Man-In-The-Middle
   - attaco brute-force
   - attacco malware
   - attacco rainbow table
5. Quale di queste contromisure danneggia maggiormente l'esperienza dell'utente?
   - rimuovere dalla coda di connessioni quelle non completate dopo un limite di tempo
   - utilizzare il protocollo DNSSEC
   - utilizzare uno stealth firewall
   - utilizzare funzioni di hash per memorizzare le password degli utenti
6. Quale di queste contromisure è inefficace nel contrastare un brute-force attack?
   - utilizzare funzioni di hash per memorizzare le password degli utenti
   - aumentare la lunghezza delle password
   - obbligare ad includere nella password almeno 1 lettera maiuscola, 1 minuscola, 1 numero e 1 carattere speciale
   - introdurre un limite di tentativi errati nell'inserimento della password
7. Quale di questi attacchi non è volto a fornire un accesso illegale ad un sistema?
   - attacco DoS
   - dictionary attack
   - attacco brute-force
   - rainbow table attack
8. Quale contromisura tra le seguenti è la più efficace contro un dictionary attack?
   - adozione dell'Autenticazione Multi-Fattore
   - utilizzare la funzione di hash MD5 per memorizzare le password degli utenti
   - modificare periodicamente le password
   - utilizzare un firewall di tipo circuit-level gateway
9. Quale tra queste procedure di accesso consiste in un'Autenticazione Multi-Fattore?
   - richiedere una password di almeno 12 caratteri e un badge elettronico
   - richiedere 2 password diverse lunghe almeno 12 caratteri
   - richiedere una mail valida e una password di almeni 16 caratteri
   - richiedere l'impronta digitale e la scansione della retina
10. Quale di queste contromisure non impatta negativamente sull'esperienza dell'utente?
    - utilizzare la funzione di hash SHA3 per memorizzare le password degli utenti
    - utilizzare l'autenticazione a 2 fattori (con password e PIN ricevuto via mail)
    - modificare le password ogni 6 mesi
    - introduzione di una breve attesa dopo l'inserimento di una password errata
11. Qual è l'utilità principale di vietare l'installazione di software esterno sui computer di un'organizzazione?

- i programmi installati possono introdurre nuove vulnerabilità
- i programmi installati interferiscono con il firewall
- i programmi installati rallentano i computer
- i programmi installati non sono inclusi nel backup

12. Quali sono le caratteristiche peculiari di un worm?
    - sfrutta la vittima per autoreplicarsi e diffondersi ulteriormente
    - sfrutta i dispositivi esterni (come chiavette USB) per infettare nuove vittime
    - infetta un dispositivo e ne blocca i dati contenuti, chiedendo un riscatto alla vittima
    - cerca di ottenere informazioni sensibili dalla vittima infetta
13. Quale tra questi comportamenti non ha lo scopo di limitare la diffusione di malware?
    - utilizzare una password per accedere al computer aziendale
    - non collegare dispositivi personali ad un computer della rete aziendale
    - organizzare degli aggiornamenti periodici dei sistemi informatici
    - mantenere attivo e aggiornato l'antivirus
14. Quale tra queste strategie non può essere messa in atto da un antivirus?
    - rafforzare i controlli di accesso ai dati contenuti nel sistema
    - riconoscere i malware analizzando le firme dei programmi eseguiti
    - ricercare pattern sospetti all'interno del codice dei programmi
    - eseguire un programma sospetto all'interno di un ambiente protetto e isolato
15. Quale inconveniente può causare l'adozione di un Intrusion Prevention and Detection System (IPDS)?
    - un blocco di azioni legittime identificate come rischiose dal sistema
    - un conflitto con le attività svolte dal firewall
    - una maggiore efficacia degli attacchi di phishing via mail
    - una maggiore difficoltà nella compilazione dei log da parte del sistema
16. A cosa può servire mantenere un backup completo e aggiornato?
    - recupero dei dati in caso di attacco ransomware andato a segno
    - prevenzione degli attacchi malware
    - recupero dei dati in caso di attacco spyware andato a segno
    - facilita le operazioni di scansione dell'antivirus
17. Quale tra i seguenti messaggi non è un tentativo di phishing?
    - Sono stati aggiornati i termini di servizio di Amadron. Per saperne di più accedi al tuo profilo oppure vai a www.amadron.org/terms-of-service
    - Siamo la banca Secure Bank. Purtroppo il tuo conto è stato bloccato per errore. Ci servono subito le tue credenziali per risolvere il problema al più presto.
    - Il tuo abbonamento a SuperSoft Office sta per scadere. Se desideri puoi prolungarlo di 6 mesi GRATUITAMENTE a questo link www.scamsoft.xyz/DGHSjdjhfksHTeruFs84h. Attenzione, l'offerta scade tra poche ore, APPROFITTANE!
    - Sono Guido, il responsabile della sicurezza aziendale. Purtroppo abbiamo smarrito le tue credenziali per un problema tecnico. Ti prego di inviarmele urgentemente in risposta a questa mail.
18. Quali effetti ha un attacco di tipo ransomware?

- rende inaccessibile il sistema e viene richiesto un riscatto per potervi accedere
- sfrutta strategie di camuffamento e cerca di ottenere informazioni sensibili dalla vittima
- si replica fino ad esaurire le risorse della vittima infetta
- cerca di trarre in inganno un utente per impossessarsi delle sue credenziali

19. In cosa consiste il social engineering?

    - una tecnica per spingere l'utente a condividere informazioni sensibili
    - un percorso di training per migliorare le conoscenze di sicurezza informatica
    - un modo efficiente di strutturare l'ambiente lavorativo
    - una branca dell'ingegneria