Il lavoro di tesi proposto si incentra sullo sviluppo di SimSCADA, un security serious game creato per insegnare quali minacce informatiche sono presenti in un ambiente SCADA.
Nel primo capitolo vi è una breve introduzione riguardo le tematiche della sicurezza informatica e dei sistemi SCADA.
Nel secondo capitolo viene effettuata un'analisi dei Serious Game presenti attualmente sul mercato, incentrandosi su quelli che trattano il tema della sicurezza informatica.
Nel terzo viene offerta una panoramica sugli ambienti e le tecnologie SCADA: cosa sono, da quali elementi sono costituiti, quali differenze ci sono con altri sistemi simili.
Il quarto capitolo è incentrato nell'analisi dei rischi presenti in un sistema SCADA, quali differenze vi sono tra la sicurezza domestica e quella industriale e quali sono i punti di vulnerabilità che possono essere sfruttati. Viene poi proposto un elenco dei possibili attacchi effettuabili ai danni di un sistema SCADA.
Nel quinto capitolo viene esposto cosa ha portato allo sviluppo di SimSCADA, le ricerche effettuate nella fase iniziale e a quali risultati hanno portato.
Il sesto capitolo raccoglie tutte le informazioni necessarie per il manuale del programmatore, esponendo la logica ed il codice delle componenti fondamentali del gioco.
Nel settimo capitolo si espongono i dati raccolti dopo la fase di test finale.
l'ottavo ed ultimo capitolo contiene le conclusioni ed un'analisi sui possibili futuri sviluppi del gioco.