Corso di Laurea Magistrale in Sicurezza Informatica: Fondamenti e applicazioni
Corso di Sviluppo di Software Sicuro
Progetto d'esame a.a. 2009/10

Il testo del progetto proposto dal corso parallelo di Fondamenti di Sicurezza recita, tra l'altro: "Il programma del concentratore viene sviluppato da un fornitore esterno alla MACA perchè essa non possiede le competenze adeguate."

Immaginando che, per aumentare l'appetibilità del prodotto, MACA richieda al fornitore che il nucleo del programma del concentratore, ossia la parte che esegue i conti e controlla le periferiche wireless (denominato MACA-C), sia certificato corretto secondo l'approccio SPARK, si ottiene il progetto di S3.

Progettare in INFORMED e realizzare in SPARK il concentratore del sistema MACA-C, le cui specifiche sono estraibili dal progetto di FS come segue.

Il sistema prevede che per ogni termosifone dell'edificio sia installato un dispositivo che misura la temperatura e la trasmette, ad ogni ora, mediante un collegamento wireless ad un sistema concentratore nell'edificio che calcola il consumo orario e lo trasmette mediante un collegamento ADSL ad un sistema nella sede di MACA. Alla caldaia viene collegato un ulteriore dispositivo che trasmette al concentratore il consumo orario.

La spesa per il riscaldamento di ogni appartamento viene calcolata sommando la spesa oraria per l'appartamento stesso. La spesa oraria per appartamento viene calcolata dal concentratore stimando il consumo orario del singolo appartamento, moltiplicando tale consumo per un parametro Cost. Il consumo orario viene calcolato sommando i consumi dei singoli termosifoni nell'appartamento. Il consumo del singolo termosifone viene calcolato moltiplicando la temperatura rilevata in quell'ora per un parametro theta. Inoltre, in ogni appartamento esiste un dispositivo (valvola) collegato anch'esso via wireless al concentratore che permette di bloccare l'erogazione del riscaldamento. La spesa oraria per appartamento viene inviata dal concentratore ad un sistema della rete informatica nella sede di MACA.

Per promuovere una coscienza ecologica, ogni utente può ottenere un forte sconto se si impegna a limitare il consumo giornaliero. Minore è il limite stabilito, maggiore è lo sconto. Al raggiungimento del limite giornaliero il concentratore esclude l'erogazione del riscaldamento nell'appartamento che viene riattivata il giorno seguente. Il limite per ogni utente è ~~comunicato dal sistema centrale al concentratore.~~ una costante.

Esiste una porta wireless sul PC che permette di caricare nuove versioni del programma. Il programma viene caricato criptato mediante una chiave K memorizzata nel concentratore; il valore iniziale di questa chiave viene registrato nel concentratore dal fornitore del PC. La lista di tali chiavi viene comunicata a MACA associando la chiave alla matricola del concentratore.

Norme tecniche

Scopo del progetto è quello di impadronirsi delle tecniche di progetto e verifica del software trattate nel corso. Quindi dovrà dapprima essere presentato il progetto INFORMED, corredato della verifica del flusso informativo. In seconda battuta, la certificazione deve avvenire consegnando il codice annotato accompagnato dal file .sum generato da POGS, corredato dalle regole di semplificazione (file .rlu) e dalle giustificazioni informali (file .prv) fornite dal produttore.

Norme gestionali

Il progetto può essere svolto in gruppo (al più tre studenti).

Mi deve essere data comunincazione della costituzione di ciascun gruppo, e dell’inizio delle attività. A fini statistici, ciascun componente del gruppo deve tener conto del lavoro svolto (in termini di ore dedicate al progetto) su un apposito registro (da consegnarsi in busta chiusa al momento del giudizio, dato che questa informazione non lo influenzerà: mi interessa solo che sia veritiera).

Sono ammesse ed incoraggiate le discussioni e lo scambio di informazioni tra gruppi diversi ma ogni gruppo deve presentare un progetto originale.

Ogni prodotto verrà valutato in base ai risultati dell'ispezione condotta dal docente. L'ispezione avverrà in due passi: valutazione del progetto INFORMED, valutazione della realizzazione. La realizzazione può iniziare solo dopo l'approvazione del progetto.

Eventuali domande e richieste di appuntamenti per chiarimenti, così come la consegna dei prodotti vanno fatte per posta elettronica (documentazione in pdf, codice come progetto GPS zippato), con “Progetto S3” nel campo oggetto.

Se si accumulerà materiale adatto, creerò una FAQ sulla pagina del corso.

Durante il mese di Agosto non sarò disponibile.