DV1620: Kravspecifikation

Antivirus i C++

Samir Jamehdar & Mathias Carlshjelm
DVGHI20
Blekinge Institute of Technology

2020-01-19

Beskrivning

Projektet innefattar skapandet av ett förenklat antivirusprogram skrivet i programmeringsspråket C++. Programmet ska med hjälp av en virusdatabas hitta och identifiera infektera filer i en given filkatalog.

Kundens krav

De krav som är satta av kunden är följande:

Kravnr	Krav	Omfattar
1	Filtraversering	- Programmet ska gå genom en katalog i filsystemet samt alla dess underkataloger, och dess underkataloger
2	Filidentifiering	- För varje fil som programmet hittar ska det kontrollera om filen matchar någon av beskrivningarna i virusdatabasen - Om filen matchar med ett virus i databasen ska detta rapporteras till en loggfil
3	Felhantering	- Kontrollera syntaxfel i virusdatabasen - Virusdatabasen ska inte behöva ligga i samma katalog som programmet när det startar
4	Operativsystem	- Programmet ska kompilera och exekvera korrekt under Ubuntu 18.04
5	Makefil	- Verktyg för automatisk kompilering och sammansättning av applikationsfiler

Funktionella krav

Fördjupade krav

Kravnr	Krav	Omfattar
1	Filtraversering	- Söka genom filkatalog och kartlägga dess filer. Detta görs med en rekursiv funktion. - Bibliotek eller mjukvara från tredje part får inte användas för detta ändamål.
2	Filläsning	- Läsa in filer som ASCII. - Börja med att läsa från början av varje fil, antalet bytes som ska läsas in motsvarar antalet bytes från virussignaturen.
3	Virusdatabas	- Virussignaturer kommer att vara skrivna i hexadecimal notation. - Funktion för översättning från hexadecimal till ASCII. - Identifiering av virussignatur och virusnamn. - Kontrollerar att virusnamnen är max 32 tecken inkl. NULL-terminering.
4	Filidentifiering	- För varje fil som stämmer överens med en virussignatur ska information om filen loggas i en logfil med namnet dv1620. - Informationen ska innehålla filnamn, filens sökväg och namnet på det virus som infekterat filen. - Även dolda filer & kataloger ska identifieras
5	Operativsystem	- Programmet ska fungera korrekt i operativsystemet Ubuntu.
6	Felhantering	- Undantagshantering för syntaxfel i virusdatabasen: Ge en varning för de virussignaturer som har syntaxfel och fortsätt exekveringen. - Om filkatalogen och virusdatabasen inte finns i samma katalog som antivirusprogrammet bör användaren mata in absoluta sökvägar. - Om filnamnet inte finns ger programmet en varning - Sökväg till enstaka filer ska accepteras
7	Gränssnitt	- Förväntas att kunna köras direkt från Ubuntu terminalen. - Användaren ska kunna mata in absolut- och relativsökväg till filkataloger eller filer, som ska undersökas
8	Sammanställning	En Makefil ska skrivas för att automatisera och effektivisera kompilering av applikationsfilerna där funktionaliteten innefattar: - Kompilering och sammansättning till körbar fil med kommandot make. - Borttagning av körbar och objektfiler med kommandot makeclean.

Ytterligare två krav har lagts till efter risk- och sårbarhetsanalysen och är markerade med gult i tabellen ovan. De nya kraven är: Identifiering och skanning av dolda filer och att programmet även accepterar sökvägen till enskilda filer. I Ubuntu är dolda filer egentligen bara filer med en punkt i början av filnamnet. Det är därför mycket viktigt att också hantera dolda filer där det finns en stor säkerhetsrisk att utesluta dessa från genomsökningen. De andra kravet utgör inte någon större säkerhetsrisk men är en bekvämlighet för användaren om den bara önskar att genomsöka enstaka filer mot en virusdatabas.

Mailadresser

samirjamehdar@hotmail.com
mathias.c256400@gmail.com