Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Biztonsági követelmények minta alapú formalizálása

Bártfay György, I. évf, (MSc) mérnökinformatikus szakos hallgató
Konzulens: dr. Majzik István egyetemi docens, MIT
Kritikus rendszerek főspecializáció
Önálló laboratórium 1. összefoglaló
2014/15. II. félév

A biztonsági követelmények helyes megfogalmazása igen fontos kérdés a szoftverfejlesztésben, különösképpen a biztonságkritikus alkalmazások esetén. Ám ez egy komplex feladat, mert a helyes és érthető kifejezés megalkotása specifikus tudást és gyakorlatot igényel.

A megfogalmazás folyamatát érdemes lenne egyszerűbbé, könnyebbé tenni, miközben a helyesség és precizitás nem csökken. Ebben lehet segítségünkre, hogy a tapasztalatok szerint a biztonsági követelmények jellemzően sémákra épülnek. Ezeket a mintákat sablonként használva, azok paraméterezésével és komponálásával a fenti célok elérhetőnek tűnnek.

A feladatom, hogy ezt az elképzelést egy gyakorlatban jól használható eszköz formájában realizáljam. Első lépésként a félév folyamán megismerkedtem a területre jellemző mintakészletekkel, illetve a témához kapcsolódó eddigi eredményekkel. A kutatás igazolta a korábbi feltételezést, miszerint a használt követelmények a gyakorlatban kisszámú mintába besorolhatóak. Ezeket a mintákat kiegészítettem kontextus- és időfüggő kifejezésekkel, melyek a biztonsági követelmények esetén szintén szükségesek.

Következő lépésben a mintákhoz definiáltam egy absztrakt és egy konkrét (grafikus) szintaxist. Az absztrakt szintaxis egy metamodell a minták leírásra. Erre alapozva elkészítettem a grafikus szintaxist is, mely definiálja, hogy hogyan fog majd egy kifejezés kinézni az eszközben. Ennek a célja nem a konkrét grafikus elemek meghatározása volt, hanem a magasabb szintű megfontolások megjelenítése.

A verifikációhoz szükséges egy formalizmus, amelyre leképezve a fenti mintákból komponált kifejezéseket megvalósítható a tényleges verifikáció. Erre a célra a Horányi Gergő által definiált Context-aware Timed Propositional Linear Temporal Logic (CaTL) [1] formalizmust választottam, mely a tanszéken már jelenleg is használatban van és vannak felhasználható eszközök az ebben megírt követelmények verifikációjához. A CaTL egy temporális logika kiegészítve időzítés és kontextus kifejezésekkel, tehát alkalmas a biztonsági követelmények leírására.

Következő lépésként meghatároztam a tervezett eszköz funkcióit. Ezek specifikációjakor fontos szempont volt a könnyű, intuitív használat és a jó áttekinthetőség összetettebb kifejezések esetén is. Implementációs technológiának két Eclipse alapú technológiát választottam. Az absztrakt szintaxishoz EMF, míg a grafikus reprezentáció Sirius segítségével lesz megvalósítva. Ezeknek köszönhetően a tervezett eszköz a fejlesztőként már ismert Eclipse környezethez fog illeszkedni.

A továbbiakban a megtervezett eszköz implementációját fogom elvégezni. Az elkészült eszköz a későbbiekben továbbfejleszthető további funkciókkal, például kontrollált természetes nyelvi reprezentációval.

[1] Horányi Gergő: Monitor synthesis for runtime checking of context-aware applications (2014)