Resumé över IG Programvarusäkerhets verksamhet under år 2008

SESAM:s grupp i Programvarusäkerhet studerar frågeställningar aktuella för säkerhetskritiska programvarusystem. Arbetet är organiserat i olika teman (med ett eller flera mikroprojekt) samt ett antal diskussionsuppgifter – vart och ett med en utsedd inledare (’*coach*’), vilken lägger fram sin frågeställning samt stimulerar till vidare diskussioner och utredningar inom gruppen.
Idén med att definiera olika diskussionsuppgifter inom programvarusäkerhet har varit, att kunna ta upp problemområden, som deltagarna finner värdefulla att diskutera i en vidare krets, för att få dem belysta från olika synvinklar. Det kan t ex gälla fall, där inga lösningar tycks föreligga, där det finns olika angreppssätt eller motstridiga uppfattningar om lämpligt förfaringssätt.

Uppgiften inom mikroprojektet ’**SäkAnalysMetoder**’, som startade under 2006, var att studera olika analysmetoder inom systemsäkerhetsområdet, för att utreda vilka av dessa, som lämpar sig för programvarusystem samt under vilka analysfaser. Under inledningsåret provades de klassiska metoderna HAZOP, FMECA, FTA. Provningarna forsatte 2007 med en relativt ny analysmetod, STAMP/STPA, vilken inriktar sig mot riskkällor förknippade med de olika typer av styr- och reglermekanismer, som förekommer såväl på programvarunivå i tekniska realtidssystem som på organisatorisk/personell nivå (med styrning i form av reglementen/ordergivning och återmatning via bekräftelser). Som tillämpningsexempel valdes ett adaptivt farthållningssystem, vilket analyserades m h a den proaktiva varianten STPA (en riskskälleanalysmetod baserad på STAMP).

Under 2008 övergick provningen till basvarianten STAMP (en haveriutredningsmetod, *root cause analysis*). Som tillämpning valdes ett fall med omfattande dokumentation på nätet: flygolyckan över Überlingen juli 2002. Detta material komprimerades, grafer över analysobjektets statiska o dynamiska styrstrukturer och dynamiska förändringsprocesser togs fram tillsammans med faktablad över metoden, vilka fick bilda underlag inför gruppanalyserna. Väl kända tillämpningsexempel och noggrant förberedda analyssessioner är en förutsättning, för att deltagarna på en dag skall hinna sätta sig in i både analysmetod o applikation samt utföra själva analysen. Denna STAMP-analys visade sig dock kräva två möten. Underlag, analysresultat o slutsatser dokumenterades i mötesnotiser och sammanfattades i ett självstudiematerial (se http://sesam.smart-lab.se: Ig programvarusäkerhet).
Som del i detta mikroprojekt inbjöds prof Nancy G Leveson, upphovsman till STAMP/STPA, att hålla en 2-dagars kurs i systemsäkerhet för programvaruintensiva system. Detta blev en mycket välbesökt och uppskattad tillställning. Seminariet var öppet även för icke SESAMmedlemmar och ca 100 personer deltog. Första dagen ägnades åt STAMP. Leveson, som blivit ombedd att inkludera Überlingen-olyckan bland sina fallbeskrivningar, illustrerade elegant hur de olika graftyperna som ingår i STAMP kan användas för att påvisa defekter i interaktionsflödena mellan flygledningscentral o cockpit samt inom dessa: ett mycket givande komplement till o avslut av såväl STAMP-prov som mikroprojekt!

Årets sista gruppmöte ägnades åt diskussioner om framtida ledarskap och verksamhetsinriktning samt till att lägga upp riktlinjerna för nästföljande års inledande mikroprojekt, ’FAQ’, upprättandet av en Frågor&Svar-svit på hemsidan. En bas för detta förelåg redan i frågeställningar utredda genom gruppens diskussionsuppgifter o mikroprojekt samt ordförandens introduktionspapper, kurser o sparade mailförfrågningar. En inledande uppgift inför 2009 för samtliga gruppmedlemmar blev därför, att sända runt kompletterande frågor/svar (egna o andras) – ett sätt att även ge den, som har svårt frigöra tid för möten, möjlighet att bidra till sviten.

Ett innehållsrikt år med ett program omfattande totalt 5 träffar var därmed till ända.