Resumé över IG Programvarusäkerhets verksamhet under år 2007

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 det saknas lösningar, finns olika angrepps-sätt eller kanske motstridiga åsikter om lämpligt förfaringssätt.

Under 2006 startades ett nytt mikroprojekt, ’**SäkAnalysMetoder**’. Detta projekt har som syfte, att studera olika analysmetoder inom systemsäkerhetsområdet, för att utreda vilka av dessa, som lämpar sig för programvarusystem samt under vilka analysfaser. Under 6 analysmöten provades de klassiska metoderna HAZOP, FMECA, FTA. Som typexempel valdes ’Ejection System’, ett hypotetiskt system för utskjutning av raketstolar, tänkt att undersökas under analysfaserna PHL-analys, PHA, SHA, SSHA.

Under 2007 genomfördes (p g a hälsoproblem) hälften så många möten; två SESAM-redovisningar och ett gruppmöte, där provningen inriktades mot en ny analysmetod: STAMP/STPA. Inför varje nytt prov sammanställs ett underlag, som distribueras ut till medlemmarna före analysmötet. Detta utgörs bl a av komprimerade faktablad, mallar till metoden samt beskrivningar av det tillämpnings-exempel metoden skall provas på. Den första STAMP/STPA-analysen provades på ett adaptivt farthållningssystem. Gruppen fann, att detta exempel inte helt kunde lyfta fram metodens styrkor och särdrag: bl a finns flera varianter av metoden, som inte passade att testa under provet. Därför beslutades att provningen skulle fortsätta vid ett senare möte, denna gång på ett annat tillämpnings-exempel. Underlag till detta togs fram, men p g a svårigheter att finna lämpligt datum, har detta prov skjutits upp till februari 2008. Det tillämpningsexempel, som valts ut är flygolyckan över Überlingen i juli 2002.
En hel del arbete har på detta sätt investerats i framtagning av underlag inför analyserna. Detta har bidragit till att det – trots begränsade insatser under själva analysmötet – har gått att få en relativt god bild av provad teknik samt att dra vissa slutsatser angående dess användbarhet på programvarusystem. Detta har i sin tur blivit sporren till att lägga ned ytterligare tid på att sammanställa slutsatser och analysresultat. På SESAM:s hemsida finns dessa utlagda, både i form av mötesanteckningar samt som självstudiematerial. Därigenom kan även de, som inte kunnat närvara vid proven, ta del av dragna erfarenheter.

Gruppmötena har förutom dessa prov i vanlig ordning även ägnats åt nyheter från konferenser, kurser och andra redovisningar. Dessutom har, inför SESAM:s 20-årsjubileum år 2008, två semina-riedagar planerats in den 21-22 maj med prof. Nancy Leveson – den person, som byggt upp området Programvarusäkerhet. Hon har därvid ombetts att som tillämpningsexempel välja just flygolyckan över Überlingen, något som gruppmedlemmarna kommer att vara väl förtrogna med till dess.