Resumé över IG Programvarusäkerhets verksamhet under år 2003

Temat för det första mötet inom SESAM-gruppen i Programvarusäkerhet hösten 2002 var ’OS i säkerhetskritiska tillämpningar’. Under mötet drogs riktlinjerna för den fortsatta verksamheten upp och en prioritering av föreslagna delområden gjordes. Högst på listan placerades Operativsystem följt av Metoder, Verktyg, Återanvändning, Arkitekturer, Design, Utbildning samt Verifiering & Validering. Till tema för nästföljande möten valdes ’Provning av verktyg för systemsäkerhetsanalys av programvara’. Detta kom att bli styrande för de totalt 8 heldagsaktiviteter som genomfördes under 2003.

Som modell för gruppverksamheten stod det under 2002 avslutade projektet FoTA P12, ’Överföring till industrin av programvaruteknik för säkerhetskritiska system.
De teknikprov som där utförts avrapporterades i februari under 2003 års första möte, där deltagarna även redovisade sina erfarenheter av medlemsföretagens systemsäkerhetsmetoder o -verktyg. Beslut fattades att undersöka möjligheterna att utan kostnad få prova ett nytt metodhjälpmedel, **SpecTRM,** vilket då skulle bli ett passande mikroprojekt för årets tema. Detta verktyg, utvecklat av prof Nancy G Leveson, ger stöd vid modellering och uppbyggnad av säkerhetskritiska system, bl a genom avsiktsspecificeringar, spårbara motiveringar o beskrivningar av systemmålsättningar samt dokumentation av designbeslut, riskkällor, systemsäkerhetsrestriktioner. Två av Levesons doktorander inbjöds i mars för en tvådagars presentation av verktyget, dess tillämpning inom ett NASA-finansierat forskningsprojekt för bygge av återanvändbara rymdmodeller samt en avslutande demo. Bland åhörarna ingick gruppens medlemsföretag, de exjobbare som några av dessa engagerat för provning o utvärdering inom mikroprojektet samt den lokala högskolan (LiTH).
Ytterligare ett tillfälle till introduktion i SpecTRM arrangerades i augusti som del av en tvådagarskurs i ’*System Safety for Software-Intensive Systems’*, ett seminarium öppet även för icke SESAM-medlemmar. Denna gång var det prof Leveson som lockats över – en karismatisk talare, som fängslade drygt 120 personer. Även deltagare utanför försvarssektorn ingick och många återkom senare med förfrågan om att ordna fler, liknande Leveson-evenemang (det skulle dock dröja 5 år).
Vid höstens möten ventilerades o avrapporterades de teoretiska o praktiska erfarenheter som exjobbare o gruppmedlemmar gjort – ett givande utbyte för båda parter. Att SESAM kan spela en viktig roll i bryggan mellan industri-myndighet-universitet visades här. Sex år senare – efter utträde i arbetslivet – sökte f ö en av exjobbarna medlemskap i gruppen Programvarusäkerhet.

Ett annat tema under hösten var ’Tidsstyrd programmering’, där talare från universitet (KTH, CTH) och industri (Arcticus, Volvo CE) deltog i ett _-dagsseminarium inom gruppmötets ramar. ’Kommersiella operativsystem i säkerhetskritiska system’ blev en uppföljning av gruppens allra första möte – nu presenterat i en vidare SESAM-krets av två inbjudna talare.

Till de diskussionspunkter som avhandlades under olika gruppmöten hörde: B Myers teknik ’Design by Contract’: ett sätt att m h a invarianter, *constraints* samt *pre-/postconditions* specificera – för att efteråt kontrollera – vad ett system ej får göra. ’Riskinformation integrerad i företags kravdatabaser’ samt ’Återanvändning o interoperabilitet mellan konceptuella modeller för simulering’ är ytterligare några exempel.

Bland de nyheter på verktygsfronten som presenterades för gruppen var: NRLs SCR (*Software Cost Reduction*), en uppsättning verktyg, som bl a möjliggör specning i en tabellorienterad notation (jfr SpecTRMs logiska and-or-tabeller). En första presentation av Leveson-hjälpmedlet STAMP, en systemövergripande säkerhetsanalys baserad på styrflöden, gjordes också. Fyra år senare skulle gruppen visa sig redo för prov av detta.

Ett ytterst intensivt första år m a o, där alla aktiviteter finns dokumenterade på SESAMs hemsida!