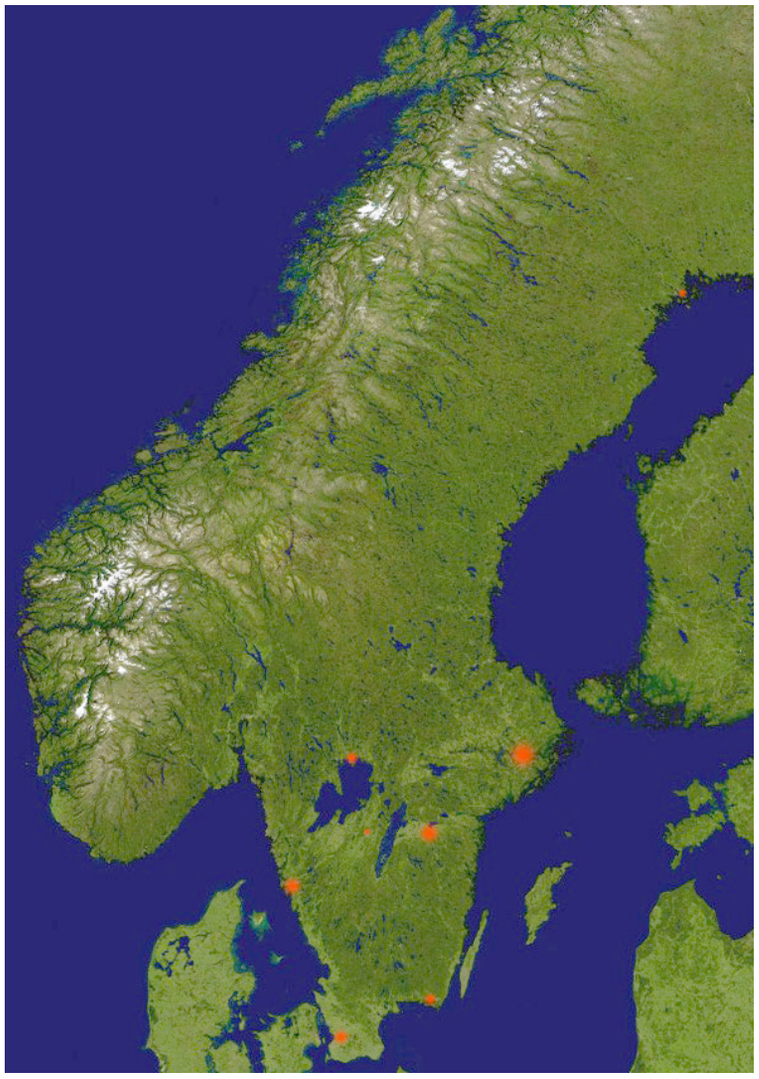
En översikt över IT-säkerhetsforskning i Sverige

November 2010

JACOB LÖFVENBERG



FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R--3069--SE
ISSN 1650-1942

Underlagsrapport
November 2010

Informationssystem

Jacob Löfvenberg

En översikt över IT-säkerhetsforskning i Sverige

November 2010

Titel	En översikt över IT-säkerhetsforskning i Sverige November 2010
Title	An overview of IT security research in Sweden November 2010
Rapportnr / Report No.	FOI-R--3069--SE
Rapporttyp	Base data report
Report Type	Underlagsrapport
Månad / Month	November / November
Utgivningsår / Year	2010
Antal sidor / Pages	17
ISSN	1650-1942
Kund / Customer	FM
Kompetenskloss	IT-säkerhet
Projektnr / Project No.	E53251
Godkänd av / Approved by	Anders Törne

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för informationssystem
Box 1165
581 11 LINKÖPING

FOI, Swedish Defence Research Agency
Information Systems
P.O. Box 1165
SE-581 11 LINKÖPING

Sammanfattning

En översikt över aktuell IT-säkerhetsforskning i Sverige presenteras. Översikten har sammanställts genom telefonintervjuer och några redan existerande, liknande översikter. Huvudfokus har legat på universitetsanknuten forskning, men några institut har också tagits med.

Nyckelord: IT-säkerhet, informationssäkerhet, forskning

Abstract

An overview of current Swedish IT security related research is presented. The overview is based on telephone interviews and some already existing, similar overviews. The main focus has been reseach at universities, but some institutes have also been considered.

Keywords: IT security, information security, research

Innehåll

1 Inledning

IT-säkerhetsrelaterad forskning bedrivs idag av ett relativt stort antal aktörer i Sverige. I de flesta fall är det universitet och högskolor, men även forskningsinstitut och näringsliv är aktiva inom området. Denna rapport innehåller en beskrivning av vilka grupper som finns och vilka områden varje grupp intresserar sig för. Tonvikten ligger på vad som görs av universitet och högskolor, men två forskningsinstitut behandlas också.

2 Andra liknande undersökningar

De senaste tio åren har det gjorts ett antal ansatser att göra en inventering av vilka forskningsgrupper som finns och vilken forskning som bedrivs inom IT-säkerhetsområdet. Den senaste publicerade genomgången som vi hittat är från 2002 [2], där Bilaga 4 innehåller resultatet av en kartläggning av IT-säkerhetsforskning i Sverige. Undersökningen gjordes i form av enkäter som besvarades av ett relativt stort antal forskningsinriktade och kommersiella aktörer. Förutom en projektlista och basfakta om antalet anställa hos varje aktör så gjordes en grafisk bild där de olika gruppernas intresseområden placerades in.

En enklare genomgång gjordes i början av 2010 av SICS, vilket resulterade i ett powerpointdokument där svenska forskningsgrupper inom IT-säkerhetsområdet presenteras med en sida per grupp. Dessutom redovisades en lista med företag och en lista med forskningsfinansiärer.

Även Forsknings- och Utvecklingskommittén inom ISACA påbörjade en liknande undersökning [3] under 2009, men den har inte avslutats.

3 Avgränsningar

Vi har i vår undersökning huvudsakligen varit intresserade av forskning om IT-säkerhet och inte det bredare begreppet informationssäkerhet. Vad IT-säkerhet är är förstås inte helt väldefinierat. Det vi har letat efter är forskning som handlar om teknik eller åtminstone är ganska nära de teknika frågorna.

Vi har också sökt grupper som har IT-säkerhet som huvudintresse. Det finns ett ett större antal enskilda forskare som huvudsakligen har andra intressen än IT-säkerhet, men som ägnar en mindre del av sin tid åt forskning som berör IT-säkerhet. Dessa forskare har inte inkluderats i genomgången.

Avgränsningarna har handlat om urvalet av personer vi kontaktat. I den mån någon under intervjun synts vara utanför avgränsningarna har resultatet ändå tagits med i sammanställningen.

4 Metod

Vi har använt telefonintervjuer med representanter för de olika forskningsgrupperna för att få information om grupperna och deras verksamhet. Den information som efterfrågades var gruppens storlek och sammansättning samt vilken verksamhet de bedrev. Vad gällde verksamheten ombads respondenterna att inte redogöra för enskilda projekt utan att istället beskriva intresseområden eller forskningsintriktningar som gruppen har. Detta för att undvika allt för detaljerade beskrivningar med endast kort aktualitet.

De anteckningar som gjorts vid intervjuerna har i efterhand i samtliga fall sänts till respondenterna för att ge möjlighet till invändningar och kompletteringar. I några fall har dessa svarat med ytterligare information, som då bifogats till intervjuanteckningarna.

Ett fåtal personer och grupper som vi känner till inom universitetsvärlden har vi inte lyckats nå och dessa har utelämnats i genomgångarna. Vårt fokus har vidare varit den akademiska forskningen, varför vi inte gjort några breda försök att kontakta representanter inom företagssfären.

5 Grundläggande information om forskningsgrupperna

I det här avsnittet ges i form av en tabell en översikt över de grupper vi hittat och hur stora de är. Vid beräkningen av antalet medarbetare har hänsyn tagits endast till forskande personer. Namnen på grupperna har i första hand givits på svenska. I de fall vi inte känner till något svenskt namn så har vi nyttjat det engelska namnet.

Det vi efterfrågat är hur många som *huvudsakligen* ägnar sig åt forskningsverksamhet. Antalet som ges är alltså fysiska personer, inte personår som gruppen ägnar åt forskning. Flera av respondenterna har påtalat att antalet personer som forskar inom ett visst område varierar över tiden, varför antalen som ges nedan bör ses som ungefärliga värden.

Beroende på den administrativa indelningen i forskningsorganisationerna har i några fall flera skilda forskningsgrupper samma namn i tabellen. Det rör sig i de fallen om grupperingar som inte är administrativt formella och som sorterar under en och samma, större, formella grupp (t.ex. forskningsgrupper inom samma storinstitution på ett universitet).

Vidare kan det finnas personer som varken är disputerade eller doktorander, varför antalet medarbetare i några fall är större än summan av disputerade och doktorander.

Forskningsgrupp	**Antal medarbetare**	**Antal disputerade**	**Antal doktorander**
Security Group, Blekinge Tekniska Högskola	10	6	4
Computer Security, Data- och informationsteknik, Chalmers	7	4	3

Forskningsgrupp	Antal medarbetare	Antal disputerade	Antal doktorander
ProSec, Computer Security, Data- och informationsteknik, Chalmers	10	4	6
Distributed Computing and Systems, Data- och informationsteknik, Chalmers	5	2	3
Privacy and Security, Datavetenskap, Karlstads Universitet	8	3	5
Network communications, Datavetenskap, Karlstads Universitet	3	2	0
Teoretisk datalogi, Skolan för datavetenskap och kommunikation, Kungliga Tekniska Högskolan	11	5	6
Skolan för elektro- och systemteknik, Kungliga Tekniska Högskolan	1	1	0
Skolan för elektro- och systemteknik, Kungliga Tekniska Högskolan	4	3	1
Industriella informations- och styrsystem, Skolan för elektro- och systemteknik, Kungliga Tekniska Högskolan	4	1	3
Computer Science, Space and Electronics, Systemtekni, Luleå tekniska universitet	4	3	1
SECLAB, Dator- och systemvetenskap, Stockholms universitet	24	10	14
Secure Systems, Swedish Institute of Computer Science	4	2	2
Networked, Embedded Systems Group, Computer Systems Lab, Swedish Institute of Computer Science	3	2	1
Informationskodning, Institutionen för systemteknik, Linköpings universitet	2	1	1
Laboratory for Intelligent Information Systems, Institutionen för datavetenskap, Linköpings universitet	9	2	6
Real-Time Systems Laboratory, Institutionen för datavetenskap, Linköpings universitet	4	2	2
Crypto and Security, Elektro- och informationsteknik, Lunds tekniska högskola	8	3	4

Forskningsgrupp	Antal medarbetare	Antal disputerade	Antal doktorander
Information Systems, Skövde högskola	3	3	0
IT-säkerhet, IT-infrastruktur, Informationssystem, Totalförsvarets forskningsinstitut	14	2	0
Product and services development, Product development, Products and production, Mobility services, TeliaSonera	10	1	0

6 Gruppernas forskningsområden

I det här avsnittet ges i form av en tabell en översikt över de olika gruppernas verksamhet. Det vi efterfrågat är intresseområden och forskningsinriktningar snarare än enskilda projekt. Beskrivningarna är tagna från intervjuerna och är inte tolkade eller verifierade mot någon annan källa. Däremot har en viss layoutmässig redigering gjorts och en del referenser till enskilda projekt tagits bort.

Beroende på den administrativa indelningen i forskningsorganisationerna har i några fall flera skilda forskningsgrupper samma namn i tabellen. Det rör sig i de fallen om grupperingar som inte är administrativt formella och som sorterar under en och samma, större, formella grupp (t.ex. forskningsgrupper inom samma storinstitution på ett universitet).

Namnen på grupperna har givits i första hand givits på svenska. I de fall vi inte känner till något svenskt namn så har vi nyttjat det engelska namnet. På samma sätt har forskningsbeskrivningar på svenska eftersträvats, men i de fall någon sådan inte varit tillgänglig, antingen för enskilda termer eller hela beskrivningar, så har engelska använts.

Forskningsgrupp	Forskningsområden
Security Group, Blekinge Tekniska Högskola	• Maritim säkerhet-få ut information om t.ex. fartyg via nätet. • Forensics, avvikelsedetektion i informationsmaterial, bearbeta material för att hitta avvikelser. • Malware–hur den kan bekämpas. Görs tillsammans med Internetfonden och i samarbete med några antivirusföretag. Har tillgång till deras databaser. • EULA-studier (EULA–End User License Agreement) kring program i den legala gråzonen. • Analysera programvara och utveckla säkrare program–tillsammans med Ericsson. Hur blir det med säkerhet vid agil utveckling? • Använder sig av machine learningtekniker i verksamheten, t.ex. vid EULA-studier. Forskar kring hur detta kan fungera som verktyg. Det finns också personer på BTH som tittar på nätsäkerhet
Computer Security, Data- och informationsteknik, Chalmers	Det överordnade temat är samhällets krisberedskap (finansierat av MSB). Vitbok om Emergent Cyber Threats (FORWARD) http://www.ict-forward.eu/whitebook/ • Intrångsdetektering och intrångstolerans. • Säkerhetsmetrik. • Säker bilelektronik (specialfall av secure software download)–samarbete med Volvo om hur man kan se till att det är säkert när bilen är en nod i ett nätverk–t.ex. vid remote diagnostics. • Mätningar på infrastruktur (Sunet backbone) för att se t.ex. spamnivå och andel elakartad trafik. Kopplade till Security Arena på Lindholmen http://www.lindholmen.se/sv/vad-vi-gor/security-arena

Forskningsgrupp	Forskningsområden
ProSec, Computer Security, Data- och informationsteknik, Chalmers	• Programspråk och programanalys. • Hur bygga teknik och verktyg som kan hjälpa oss att bygga in säkerhet i mjukvara. Kontroll av informationsflöden. • Websäkerhet–hur bygga webapplikationer som är säkra. • Design av ett nytt programspråk med säkerhet i fokus, där krav och policys kan specificeras. Med en avancerad kompilator kan det verifieras att detta uppfylls. • Både web och moln är i fokus.
Distributed Computing and Systems, Data- och informationsteknik, Chalmers	• Security on network protocols for sensor networks. • Basic protocols for sensor networks. How to secure such protocols, e.g. routing. • How implement symmetric cryptography and ECC in sensor networks. • Distributed denial of service attacks and how to mitigate them. • Using traces from SUNET to analyze and find DDOS attacks. • Identifying spam activities. • Project upstart on smartgrids with EON, partly on security.

Forskningsgrupp	Forskningsområden
Privacy and Security, Datavetenskap, Karlstads Universitet	• Privacy och identity management. • Transparancy enhancing tools–dvs göra det möjligt för enskilda att se vad uppgifter används till. • Användargränssnitt för usable security och usable privacy. • VoIP security and privacy, t.ex. skydd mot denial of service och anonym kommunikation. Möjliga attacker och vägar att förbättra VoIP. • Security och privacy metrics. • Nätverkssäkerhet. • Intrångsdetektering. • Säkerhet i trådlösa nät. • Anpassningsbar/adaptiv säkerhet. • Loggtransport och prioritering av olika typer av meddelanden. • Gjort en utökning av SCTP map säkerhet.
Network communications, Datavetenskap, Karlstads Universitet	• Computer forensics–specifikt med tillämpning för polisen. • Hårddiskanalys med avseende på filfragmentsmatchning av olagliga mediafiler.

Forskningsgrupp	Forskningsområden
Teoretisk datalogi, Skolan för datavetenskap och kommunikation, Kungliga Tekniska Högskolan	• Network security. • Crypto. • Security and privacy in social networks. • E-Voting. • Security protocols. • Security logics. • Secure virtualization. • Security monitoring. • Software security (information flow control, secure compilation).
Skolan för elektro- och systemteknik, Kungliga Tekniska Högskolan	• System security with a focus on protocol design and rigourous analysis from a security point of view. • Proving security of protocols. The work is done from a applied point of view. The problems are inspired by the real world.
Skolan för elektro- och systemteknik, Kungliga Tekniska Högskolan	Säkerhet i SCADA-system: • IT-mässigt med fokus på feldetektering i larmcentraler i SCADA-system. • Känslighet för manipulering.

Forskningsgrupp	Forskningsområden
Industriella informations- och styrsystem, Skolan för elektro- och systemteknik, Kungliga Tekniska Högskolan	• Akademiskt område: system- och programvaruarkitektur. • Tillämpning: kraftindustri. • Försöker bygga systemarkitekturmodeller för SCADA-system. Arkitekturmodellerande ur ett förvaltningsperspektiv snarare än ett utvecklingsperspektiv. Bland annat ur ett säkerhetsperspektiv. • Hur kan man anpassa modellerna beroende på syftet med dem. • Går det att säga något om när olika säkerhetsmetoder är gynnsamma. Säkerhetsanalyser ur ett helhetsperspektiv. • Probabilistiska analysmetoder.
Computer Science, Space and Electronics, Systemteknik, Luleå tekniska universitet	• Inte utveckling av teknisk säkerhet utan mer managementrelaterat som policies och strategier. • Beteendeaspekter, användaraspekter och relationer mellan management och användning av säkerhetskontroller och informationssystem.

Forskningsgrupp	Forskningsområden
SECLAB, Dator- och systemvetenskap, Stockholms universitet	• Ledning och styrning av informationssäkerhet i IT-miljöer: governence, compliance, risk och säkerhet, metriker och key performance indicators. • Förståelse och lärande: datorspel, interaktiva kunskapsformer, komparativa studier av etik och kulturmönster, nya paradigmer och ramverk • Informationssäkerhetsfunktionalitet i IT-miljöer: revision, assurance och forensik. • Security metrics, security management och standarder–särskilt för ledningssystem. • Security in e-government. • Utveckling av ett forensiklabb pågår.
Secure Systems, Swedish Institute of Computer Science	• Plattformssäkerhet med tonvikt på säkerhetsfrågor kring virtualisering, särskilt för större system, t.ex. telekomsystem. • Säkerhet för inbyggda system (hypervisor). • Hur skapar man tillit i virtualiserade system. Trusted computing-metoder i virtualiserade system.
Networked, Embedded Systems Group, Computer Systems Lab, Swedish Institute of Computer Science	Security in standard-based wireless networked embedded systems.
Informationskodning, Institutionen för systemteknik, Linköpings universitet	• Säkerhet hos de klassiska delarna av kvantkryptoprotokoll. • Teknik för kvantmekanikdelarna i kvantkryptoprotokoll. Hur gör man det säkert? • Användarautenticering med hjälp av mobiltelefoner.

Forskningsgrupp	Forskningsområden
Laboratory for Intelligent Information Systems, Institutionen för datavetenskap, Linköpings universitet	• Software security. • Network security. • Communications security. • E-service security. • User-centred security. • Cybercrime prevention.
Real-Time Systems Laboratory, Institutionen för datavetenskap, Linköpings universitet	• Intrångsdetektering, särskilt anomalidetektering. • Kritisk infrastruktur.
Crypto and Security, Elektro- och informationsteknik, Lunds tekniska högskola	• Kryptologi. • Trusted computing. • Virtualisering. • Sidokanaler i inbyggda system både hård- och mjukvara.
Information Systems, Skövde högskola	• Informationssäkerhet snarare än IT-säkerhet. Studerar informationssäkerhet i vården. • Patientsäkerhet och patientintegritet. • Trust. • Administrativ säkerhet. • Strategier, policies osv. • Riskhantering i små- och medelstora företag. • Social engineering

Forskningsgrupp	Forskningsområden
IT-säkerhet, IT-infrastruktur, Informationssystem, Totalförsvarets forskningsinstitut	• Försvar av IT-system. • Övning av försvar av IT-system. • IT-säkerhet i industriella kontrollsystem. • Värdering av IT-säkerhet. • Riskanalyser avseende IT-system. • Objektbaserad säkerhet.
Product and services development, Product development, Products and production, Mobility services, TeliaSonera	Produktsäkerhet, både telefoni och IP-baserat (med produkter menas tjänster riktade mot kunder).

Referenser

[1] C. Gehrmann, ”ICT Security in Sweden”, februari 2010, powerpointpresentation tillhandahållen av Christian Gehrmann, SICS.

[2] Post&Telestyrelsen, ”Tillit till IT vid internetanvändning”, rapportnr PTS-ER-2002:24, ISSN 1650-9862, november 2002.

[3] ISACA Sweden Chapter, 2009, arbetsmaterial tillhandahållet av Teodor Sommestad, KTH.