DIGITAL FORENSICS SWEDEN

Inom nätverket Digital Forensics Sweden, arbetar vi med att lägga grunden till en nationell kraftsamling för att bygga ett svenskt kompetenscentrum för Digital Forensik. Vi vill samla människor och organisationer som verkar för det goda samhället

Nyhetsbrev #3/22

The Digital Forensics Competence Center of Sweden

DIGITAL-FORENSICS.SE

Nyhetsbrev #3/December 2022

Innehåll

1. Inledning

Svenskt nationellt cybersäkerhetsarbete har fått en skjuts framåt genom bildandet av det Nationella Cybersäkerhetscentret, och genom initiativet med ett CyberCampus genom bl a RISE och KTH. Ett flertal rapporter inom området är just nu aktuella, och innehåller många konkreta förslag på hur vi på ett samlat sätt ska stärka vårt försvar mot cyberattacker. Kriget i Ukraina har tydligt visat hur angrepp på samhällskritiska IT-system blivit en självklar del av nationella militära strategier, och hur sårbara samhällen kan vara. Sannolikt har vi här i Sverige, där vi lyckligtvis levt i fred under århundraden och där vi som ”early adopters” snabbt systematiserar och linjerar samhället och lika snabbt lämnar gamla teknologier bakom oss, ett idag mer sårbart samhälle än många av våra grannländer. I dagarna kom nyheten att bl a Försvarsmakten, Softronic och Norrköpings kommun blivit utsatta för större IT-attacker. Det här är en verklighet vi tyvärr kommer att få vänja oss vid.

Forensik handlar om att utreda händelser där brott misstänks vara begångna, och att ta fram välgrundade underlag för att finna och lagföra brottslingar. Forensiskt arbete bygger kunskap om samhällets skydd mot sina medborgare behöver utvecklas, synen på vad som är rätt och fel och hur vi i slutänden skapar ett tryggt och säkert rättssamhälle. Det är en uråldrig vetenskap, och som med digitaliseringen nu står inför en av de största transformationerna genom århundradena.

Digital Forensik är inte detsamma som Cybersäkerhet, men kan anses som en del av Cybersäkerhetsområdet i vid mening. Den digitala forensiken är en förutsättning för att utveckla bra cyberskydd, utan forensiska utredningar får vi inte svaren på hur en attack kunde ta sig förbi våra skydd. Forensiken lägger grund för ständiga förbättringar. Men vi vet också att cyberskydd och agerande för att skydda sina digitala tillgångar, sällan underlättar för forensiskt arbete.

Slutsatsen är självklar – de båda har ett ömsesidigt beroende och för att bygga ett starkt demokratiskt samhälle behöver vi satsa på dem båda. Tillsammans blir vi starkare.

Nätverket för Digital Forensik finansieras sedan september inte bara av Region Östergötland, Polisen, Stockholms universitet, Linköpings Universitet, Halmstad University och Sectra, utan nu också av AI Sweden, den nationella satsningen på tillämpad Artificiell Intelligens (ai.se). Genom AI Sweden har vi kunnat få tillgång till unga AI-talanger och under ledning av Lena Klasén starta upp ett flertal projekt som studerar teknik för digital forensik. Allt detta är vi förstås mycket tacksamma för.

I det nu pågående arbetet med vår större ansökan för att finansiera ett Nationellt Digitalt Forensiskt Kompetenscenter, räcker det dock inte – nu behöver vi er alla i nätverket!

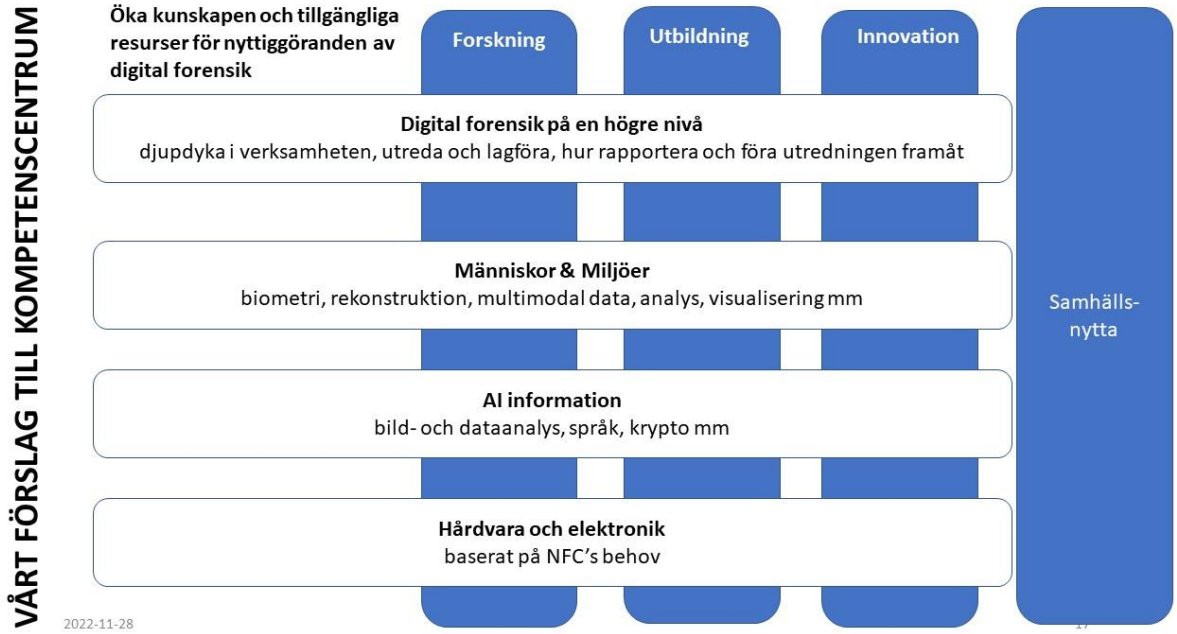
Vi behöver veta vilka av er partner som är beredda att ge ett konkret stöd i uppbyggnaden, i den händelse vi får medel från Vinnova.

Viktigast är ni som vill bli Core Partners i projektansökan, dvs ni som kan gå in med kontanta medel eller som i ert arbete kan gå in med timmar som blir ett tillskott i arbetet de kommande åren. Projektet sträcker sig över fem+fem år, och i den ansökan som nu ska in behövs ett Letter-of-Intent för att bidra under de fem första åren med start sen höst 2023 eller från och med januari 2024.

Från er som inte kan bidra på detta sätt, vill vi förstås ändå ha ett Letter-of-Support, som med en skrivning om vilket värde ni ser med centret, tydligt visar att ni står bakom satsningen.

Innehållsmässigt kommer vi att fokusera på Forskning, Utbildning och Innovation och knyta en tydlig kedja från samhällsbehov till stöd för Polis och andra behovsägande myndigheter, till konkret stöd i företagsforensiskt arbete (Corporate Forensics) och till uppbyggnad av nya affärsmodeller och nya kommersiella aktörer och startups.

Centret kommer att arbete med utveckling av policies, verktyg, metoder och teknik för att stärka det svenska ekosystemet. Omvärldsbevakning, utveckling av internationella relationer för att kunna vara en svensk kunskapshub gentemot er i nätverket blir en given del av centret.



- - -

Nyhetsbrevet denna innehåller en spännande gästkrönika av Stefan Axelsson, och information om vad som händer i vårt nätverk. Vi ber er alla bidra till innehåll och ta chans att dela sådant ni är angelägna om att nå ut med.

Nästa nätverksträff är för första gången enbart ett fysiskt möte, och samtidigt en öppen träff.
Läs mer i slutet av nyhetsbrevet och lägg den 23/1 på plats i Stockholm i era kalendrar.

Trevlig läsning!

Aktuellt från nätverket

På årets fjärde och sista nätverksträff hade vi förmånen att få lyssna till Fredrik Börjesson på MUST som presenterade NSCS, Sveriges nya nationella cybersäkerhetscenter. Därefter kom IVA's Staffan Eriksson som presenterade IVA's aktuella cybersäkerhetsrapport från projektet "Cybersäkerhet för ökad konkurrenskraft", följt av Pontus Johnson på KTH som berättade om CyberCampus. Avslutningen på dagen var Jan-Åke Larsson på LiU som gav oss en inblick i framtidens kryptoteknik, den dagen kvantkommunikation och kvantdatorer finns i full skala.

Nätverksledningen gör i januari och december sina första internationella besök, till Oslo och till Dakota/Louisiana för att bygga relation med ledande forensiska verksamheter och ta med oss intryck i formuleringen av vår ansökan om ett nationellt kompetenscenter.

Vi kan också glädjas åt ett nytt projekt genom Visual Sweden (https://visualsweden.se) där vi tillsammans med AI Sweden och EastSwedenGame (https://eastswedengame.se)kommer att utforska hur spelplattformar kan användas i visualisering av brottsplatser.

2. Forskningsnytt

Cybersäkerhet i centrum för nytt IVA-projekt

”Vår” doktorand Johnny Bengtsson på NFC rapporterar:

En av MSB finansierad fyra dagar lång cybersäkerhetsträning med it-forensiska inslag (se bilaga) ägde rum i slutet av november vid Crate hos FOI. De it-forensiska inslagen leddes av NFC och FOI. Träningen syftade till att stärka team hos medverkande organisationer i ökad förståelse för hot och tekniska plattformar för forensiskt arbete, och de medverkande fick träning i en simulerad miljö.

Bakgrund: I samband med ett FIDI-SCADA-möte arrangerat av MSB under december 2020, tog Johnny Bengtsson initiativet till att starta ett offentlig-privat samverkansnätverk kring cybersäkerhet och it-forensik, där grundidén från Johnnys sida framförallt syftade till att medvetandegöra it-forensikens roll inom både it- och ot-baserade driftsystem. I dagsläget utgör det löst sammansatta nätverk av ett flertal myndigheter, akademin och två stora kraftbolag, men att fler parter från olika samhällskritiska sektorer är välkomna att delta – t ex från nätverket inom Digital Forensics Sweden.

I våras slutförde KTH-studenten Rebecka Forsberg sitt examensarbete på mastersnivå. Hennes arbete handlade kortfattat om att genomföra intrång i en PLC och försöka finna forensiska artefakter. Här har flera av nätverkets medlemmar stöttat i det praktiska arbetet - ett gott exempel på nytta vi gör inom Digital Forensics Sweden och hur vi kan samverka för att stärka oss inom området och lyfta fram nya unga förmågor!

- - -

”Vår” andra doktorand på Stockholms Universitet och MSAB, Johannes Olegård berättar följande i ett mejl:

Ett lagförslag som tidigare i år röstats igenom och sedan i somras också trätt i kraft, ger nu bland annat laglig möjlighet till polisen att utföra "granskning på distans".

<https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/modernare-regler-for-anvandningen-av-tvangsmedel_H901JuU15>

Innebörden är att Polisen nu får använda misstänktas inloggningsuppgifter för att logga in i sociala medier och ladda ner bevis. Det gäller även om datan i sig ligger på en server i ett annat land. Man behöver alltså inte längre be molntjänst-ägaren snällt om lov eller fysiskt beslagta hela datacentret. För min del är detta intressant eftersom samma lag förmodligen kan tillämpas för att logga in i IoT-moln (både från appar och "bakvägen" från IoT-enheter). Dessutom får polisen nu möjlighet att om så krävs, tvinga fram biometrisk data, t ex fingeravtryck för att låsa upp mobiler.

3. ”Utblick” - Gästkrönikör, Stefan Axelsson, Professor Digital Forensik, Stockholms universitet

När jag arbetade på Ericsson för många år sedan, med bland annat kravhantering så fick jag många tillfällen att begrunda skillnaden mellan funktionella och icke-funktionella krav. De funktionella kraven är sådana som direkt rör produktens funktion; brukar ofta beskrivas i form av ett "use case". Icke-funktionella krav är således sådana som inte passar in i den första beskrivningen. Här döljer sig aspekter av systemet som inte enkelt kan beskrivas som ett funktionellt beteende men ändå mätas, exempelvis hastighet på ett nätverksinterface, eller routing-prestanda, till svårgripbara, och svårmätbara krav av typen "systemet skall vara enkelt att bygga ut", eller "systemet skall vara säkert". Även om vi idag fortfarande har problem med icke-funktionella krav så klarar vi dock av att möta de funktionella kraven bättre.

Eller gör vi det? En doktorand och undertecknad, Rune Nordvik, tillika lektor vid polishögskolan i Norge, har just publicerat en artikel som ställer även den observationen lite på ända. Rune har länge

intresserat sig för metadata av olika former, särskilt när det gäller filsystem. Han har också lett arbetet med att reverse-engineera Microsofts nya exFAT-filsystem, som idag är mycket spritt genom att bland annat minnesstickor ofta levereras med detta filsystem från fabrik. FAT-filsystemen är Microsofts äldsta filsystem, ursprungligen framtaget för 5,25" disketter. Det har uppdaterats många gånger genom åren främst för att möjliggöra större och större enheter. Men i och med uppdateringen till exFAT så införde man en ny egenskap som saknats hittills, nämligen den att knyta en tidsstämpel för en fil till absolut global tid.

Traditionellt så har filsystem som velat knyta tidsstämplar till jämförbar global tid lagrat alla tidsstämplar i GMT/UTC, och så har man översatt till lokal tidszon när man visar tiderna för användarna. Detta har många fördelar; alla tidsstämplar blir unikt knutna till en viss tidpunkt och oavhängiga sommartidsomställningar osv. FAT har från början bara lagrat tidsstämplar som lokal tid, dvs den tid som datorn har varit inställd på, och man har fått ta med det i beräkningen när man velat knyta en viss händelse till en tidpunkt. När man utvecklade exFAT så bestämde man sig dock för att rätta denna brist. För att äldre program/system inte skulle behöva hantera global tid så valde man istället att lagra lokal tid som förut, men också att lägga till ett ytterligare fält som beskriver hur lokal tid skiljer sig från global tid; alltså genom att lagra tidszonsinformation. Man har då valet att inte lagra någon sådan, och fortsätta bara lagra lokal tid, något som naturligtvis underlättar bakåtkompabilitet.

Så med Microsofts specifikation i hand bestämde sig Rune för att kontrollera hur denna nya egenskap hanteras av Windows, MacOS, och Linux.

Resultatet blev slående. Varken MacOS eller Linux implementerade specifikationen korrekt. Linux har dessutom två olika filsystemsdrivrutiner, en som kör som användarprogram (via FUSE) och en inbyggd i kärnan. Båda dessa implementerar specifikationen fel, men på olika sätt! Så Linux är inte ens internt konsistent... MacOS försöker följa specifikationen, men utvecklarna har missförstått tecknet på tidszonsangivelsen och anger alltså avvikelser västerut som om de vore österut, och tvärtom. Genom att flytta runt en USB-sticka mellan olika datorsystem så kan man enkelt få en situation där tidsstämplarna avviker flera timmar från vad de ursprungligen avsåg. Även om man inte öppnar filerna, eftersom bla MacOS uppdaterar tidsstämplar när man monterar filsystemet och visar innehållet.

När vi sedan kontrollerade hur populära forensiska verktyg hanterar denna situation så blev resultatet inte mycket bättre. Många av verktygen visar bara glatt den tid de tror avses, och varnar inte ens användare för att resultatet är opålitligt. De bättre varnar iaf användaren för att resultatet inte går att lita på.

Så här har man under utvecklingen helt klart inskränkt testningen och valideringen av sin filsystemsimplementation enbart till att skapa, öppna, skriva och läsa filer. Om man klarar det så har man ansett arbetet vara klart. Man har inte testat att implementationen av de nya tidszonerna interopererar med andra implementationer, eller ens Microsofts egen implementation.

Så, som alltid, när vi håller på med forensik, så använder vi ofta egenskaper som inte behandlats som ett funktionellt krav vid utvecklingen, eller ens testats, när man utvecklat de system vi undersöker. Vi mässar därför alltid att det krävs verifiering av de forensiska resultaten, och att man måste vara sunt skeptiskt inställd till de verktyg man använder. Handen på hjärtat så observerar vi väl mest den här regeln i att vi ignorerar den, men som det här resultaten visar så är och förblir det en riskabel strategi. Även ganska självklara och välspecificerade systemegenskaper blir fel vid utvecklingen, och det rejält. Våra forensiska verktygsmakare är inte alltid med på banan heller.

Så, avslutningsvis är det ju inte utan att man undrar vilka fler grynnor som döljer sig i sällan seglade forensiska vatten.

4. Aktuella event och länkar

Det som konferensmässigt kanske kan vara av visst intresse för nätverket är nästkommande IAFS-konferens (https://iafs2023.com.au/), en systerkonferens till EAFS (https://www.eafs2022.eu/) som i våras hölls i Stockholm, och där Emil Hjalmarson på NFC var huvudansvarig.

Beträffande IAFS 2023, så skriver Johnny Bengtsson på NFC i ett mejl att det kan finnas en poäng i att Digital Forensics Sweden direkt eller indirekt försöker att bevaka konferensens utkomst. Som det ser ut nu så kommer det finnas medverkande från NFC. Förhoppningsvis får vi inom Digital Forensics Sweden del av information genom NFC.

För mer information, kontakta Johnny Bengtsson: johnny.bengtsson@polisen.se

5. Nästa nätverksträff

Nästa nätverksträff är ett enbart fysiskt event, hos IVA på Grev Turegatan i Stockholm den 23 januari. Temat handlar om Digital Forensik – hur hotbilden ser ut idag och vad som är möjligt att göra. Vi har bjudit in talare och riksdagspolitiker för sätta ljuskäglan på ett samhällskritiskt område och förmå beslutande instanser på högsta nivå att reagera och inse att det är dags att agera.
Boka in redan nu – antalet platser är begränsat och eventet kommer att delas via en rad olika kanaler och samarbetsparter.

Den här gången är nätverksträffen publik och sker i samarbete mellan Digital Forensics Sweden, Kgl Ingenjörsvetenskapsakademien (IVA), AI Sweden och Visual Sweden, och kommer att vara på svenska.

Avslutningsvis - håll ögonen öppna efter nyheter och material som kan relatera till vårt område, värt att tipsa varandra om.

Vi ses i Stockholm den 23:e januari, och glöm inte att anmäla dig (länk här)

Till dess – ha en riktigt God Jul och tänk lite extra på Ukraina i vinter!

Om Nyhetsbrevet

Nyhetsbrevet har ambitionen att vara kort och koncist och är tänkt att (åtminstone i huvudsak) vara på svenska. Vi välkomnar gästskribenter bland er läsare, liksom tips om nyheter och viktiga händelser. Även det som händer på er egen horisont och som ni vill sprida kännedom om, har sin plats här, liksom länkar med tips på event eller texter om förestående produktlanseringar.

Redaktionen förbehåller sig rätten att redigera och förkorta texter liksom att välja vad som kommer med och inte sett till helhet och relevans. Vi tar förstås även gärna emot synpunkter på det som skrivs.

Nyhetsbrevet skickas till de som anmält att de vill vara mottagare av information från Digital Forensics Sweden, och det går bra att dela det vidare till kollegor i branschen. Önskar du inte längre ha nyhetsbrevet eller kallas till våra nätverksträffar, skicka ett meddelande till Niclas Fock (niclas.fock@ai.se) så stryker vi dina kontaktuppgifter ur vårt register.

Tipsa gärna kollegor i din organisation, eller kollegor i branschen så bygger vi ett större och starkare nätverk!

Fler länkar:

https://www.iva.se/event/nya-digitala-mojligheter-for-kriminella--vad-kravs-for-att-stoppa-dem/

https://www.ai.se/en/events/can-we-use-digital-tools-combat-digital-crimes

https://www.ai.se/en/digital-forensics-sweden

https://www.digital-forensics.se

https://dfcc.se

https://liu.se/nyhet/ai-ett-viktigt-verktyg-i-jakten-pa-digitala-brottslingar

https://www.ncsc.se/aktuellt/

https://www.ncsc.se/publikationer/

https://iafs2023.com.au/