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 #1/23

The Digital Forensics Competence Center of Sweden

DIGITAL-FORENSICS.SE

Nyhetsbrev #1/April 2023

Innehåll

1. Inledning

Varmt välkomna till årets första nyhetsbrev från Digital Forensics Sweden!
Speciellt välkomna till er nya läsare och nya organisationer i sammanhanget.
Vi kan konstatera en synnerligen intensiv period sedan förra nyhetsbrevet, inklusive vårt nätverksmöte och event på IVA i januari.
- Vi har slutligen lämnat in vår ansökan till Vinnova om ett kompetenscenter, och väntar nu förstås med spänning på Vinnovas bedömningar. Besked kommer i Augusti, men med allt det stöd och alla de goda idéer och engagemang vi mött under arbetet med ansökan så vet vi att vi kommer att arbeta vidare med en stärkt grupp av partners och en större synlighet från samhällets sida. Ett stort tack till alla som bidrog och till er partners som gick in med insatser och värden i projektbudgeten!
- Inte minst fick vi en ökad synlighet genom vårt event tillsammans med IVA den 23/1 där vi fick möjlighet att bjuda in fler deltagare till nätverket, men framförallt att vi fick intresse från tre riksdagspolitiker - alla dessutom jurister - under dagen!
- Häromveckan fick vi chansen att synas i ViaPlay i ”Efterlyst” och prata AI och bedrägerier!
- Vi driver ett antal projekt med partners involverade. Ett av dessa är ett projekt tillsammans med NFC, AI Sweden, Linköpings Universitet, Visual Sweden och EastSwedenGame (regionalt gaming-bolag-kluster) där vi modellerar digitala brottsplatser med hjälp av studerar vi hur man kan använda gaming-plattformar för att effektivisera modellbygge och få bättre verktyg och kvalitet i arbetet samt att bättre förstå hur man under en brottsutredning kan använda sig av en digital modell.

2. Aktuellt från nätverket

På nätverksträffen den 23/1 samlades nätverket och en stor skara andra intresserade på IVA’s konferenscenter i Stockholm. Experter mötte politiker för att diskutera vad som måste göras för att komma till rätta med den ökande mängden cyberbrott och brott där digital forensik kan vara ett effektivt verktyg. Genom träffen har vi också kunnat knyta ett anta nya partners till nätverket.
Har kan du ta del av eventet i efterhand:
https://www.iva.se/event/nya-digitala-mojligheter-for-kriminella--vad-kravs-for-att-stoppa-dem/

3. Sprid budskapet

Digital transformation påverkar och förändrar dagligen hur vi lever våra liv. Som bekant är den digitala tekniken tyvärr inte begränsad till laglydiga organisationer och medborgare. Detta är grunden till varför vi samlar goda krafter för att skapa ett Digital Forensics Competence Center (DFCC). Genom er partners har vi i nätverket successivt skapat en lägesbild med behov, utmaningar och möjligheter. Så här motiverar vi ett kompetenscenter i den ansökan som nu gått till Vinnova:

- *Genom att exploatera och utveckla området digital forensik kommer DFCC att avsevärt öka Sveriges förmåga att möta den påfrestning på samhället som brottsligheten utvecklas under den digitala transformationstiden. DFCC samlar alla relevanta aktörer i ett nav med uppgift att möjliggöra, påverka och driva forskning, utbildning och innovation tillsammans med intressenter och slutanvändare. Forskningen och utbildningen kommer att genomföras av; Linköpings universitet (LiU), Stockholms universitet (SU), Högskolan i Halmstad (HH) och Blekinge Tekniska Högskola (BTH) tillsammans med AI Sweden, samordnar genom sin värdorganisation Santa Anna IT Research Institute (Sanna), och forskningsinstituten Defence Forskningsverket (FOI) och Sveriges Forskningsinstitut (RISE). Partners som representerar hela värdekedjan; regeringar Rikspolismyndigheten (SPA) inklusive Nationellt forensiskt centrum (NFC), Skatteverket (SKV), Ekobrottsmyndigheten (EBM), Östergötlands råd (RÖ); innovation hotspot Linköping Science Park (LiSP); industriella partners 2Secure, Intel, Maxar Technologies (Maxar), Medius, Micro Systemation (MSAB), Recorded Future (Inspelad), Saab, Sectra Communication (Sectra), Sylog Öst (Sylog) och Visage Technologies. Konsortiets befintliga forskningsbas ger en utmärkt plattform för forskning och introducerar nya verktyg och metoder för att utveckla typer av bevis som ska användas inom brottsbekämpning och företagens forensik. DFCC kommer att avsevärt stärka digital forensics (DF) i Sverige genom att förstärka och utöka internationell konkurrenskraftig digital forensics, för att bli mer agil och proaktiv, t.ex. upptäcka brott i tidigare skeden genom att observera förändringar eller anomalier, och utveckla nya teknologier och metoder som ska användas i hela den digitala utredningsprocessen.*
  Kriminella organisationer och individer är snabba att identifiera nya möjligheter med ny teknik, och digitala transformation förändrar dramatiskt karaktären på brott, terror och andra hot. Tekniker som AI, Internet of Things, drönare och kryptovalutor är katastrofala verktyg i händerna på brottslingar. Följaktligen behöver vårt samhälle mycket bättre kapacitet att förebygga och utreda kriminella handlingar för att skydda organisationer och medborgare. Det är därför viktigt att öka vår förståelse för hur dessa tekniker kan användas mot vårt samhälle och ständigt göra det svårare att effektivt använda digital teknik för kriminella aktiviteter, samtidigt som vi utnyttjar möjligheterna med digital teknik av de som drabbas, brottsbekämpande myndigheter, företag och företag. organisation. Till exempel att undersöka händelseförloppet vid cyberattacker, fjärrstyrd droghandel genom krypterad kommunikation, bedrägerier genom falska e-postmeddelanden och digitala transaktioner, sexuella övergrepp genom sociala medier och inte minst skurkstaters och extremisters förmåga att destabilisera samhällen, t.ex. krigsförbrytelser eller genom att påverka valresultaten. Brottsbekämpande myndigheter, banker, offentliga myndigheter och multinationella företag står inför enorma utmaningar när det gäller att hålla jämna steg med de innovativa tillämpningarna av ny teknik. Polisutredare och domstolar blir allt mer beroende av digitala experter. Svenska leverantörer av säkerhetslösningar och tjänster konkurrerar på enorma, komplexa marknader med svåra politiska och etiska överväganden. Andra sektorer, såsom läkemedel och livsmedel, har låg beredskap för digitala hot, vilket medför allvarliga risker för viktiga samhällsfunktioner. Infrastruktur och logistik är potentiella mål för digitala brottsliga handlingar som innebär ett enormt hot mot det civila samhället.

Dessutom lämnas allmänheten och mindre enheter i stort sett utan tydlig vägledning om hur man ska behandla känsliga uppgifter och hur man ska agera när incidenter inträffar.

Vi arbetar nu på att sprida budskapet om initiativet och ber er som partner i Digital Forensics Sweden att på olika vis, medverka i det arbetet. Vi kommer att jobba via nätverkande och lobbying, projektansökningar, event, kommunikation i media och artiklar.

Det handlar om att påvisa att brotten där digital teknik utnyttjas ökar dramatiskt, och skapa förståelse för vad som krävs av politik, myndigheter och företag för att bekämpa den nya typen av brottslighet. Och att samtidigt se vilka möjligheter som nya tekniska lösningar ger.

4. Forskningsnytt

Cybersäkerhet i centrum för nytt IVA-projekt

1) Johnny Bengtsson på NFC och ”DFCC-doktorand” på Linköpings Universitet, rapporterar:

Inom ramen för en nationellt myndighets- och privatsamverkan som syftar till att införa it-forensiken i samhällsviktig infrastruktur, sammanhållen av Johnny Bengtsson vid Nationellt forensiskt centrum (NFC), har NFC tillsammans med Totalförsvarets forskningsinstitut (FOI) genomfört en av Myndigheten för samhällsskydd och beredskap (MSB) finansierad cyber-säkerhetsträning med inslag av it-forensik vid FOI Linköpings cybersäkerhetsanläggning Crate. Övningsdeltagarna fick i fyra sammansatta grupper och i en fiktiv elproduktionsmiljö chansen att i tre olika scenarion parallellt träna på av FOI-personal utformade cyberangrepp med olika inspel från övningsledningen. Den fyra dagar långa träningen innefattade bland annat inledande it-forensisk genomgång och observationer av forensiskt agerande under varje övningsmoment och en uppföljande frågestund som bland annat innefattade forensiska moment och hur träningen forensiskt kan förbättras ur ett praktiskt och handgripligt perspektiv. I januari 2023 genomfördes en uppföljande utvärdering, vilket slutligen har resulterat i det publika memot:
FOI Memo 8115, ”Analys av observationer under EnergoNFC” av Martin Karresand.

Johnny Bengtsson, NFC

- - -

2) Johannes Olegård, ”DFCC-doktorand” på Stockholms Universitet och MSAB, berättar följande i ett mejl:

Min forskning fokuserar just nu på att hämta artefakter ur IoT-molntjänster med hjälp av tjänsternas egna APIer. Tanken är att många enklare IoT-enheter inte lagrar särskilt mycket data av forensiskt värde, utan snarare skickare upp datan till molnet/edge. Så genom att undersöka kommunikation mellan IoT-enheten och molnet (alternativt mellan mobil-appar och molnet) så kan man härma anropen och på så sätt "jaga efter" datan upp i molnet.

Däremot, så är det klart att rättsväsendet ofta kan begära ut data från större moln-företag utan APIer, men genom att studera APIer kan man få bättre belägg för vad som faktiskt finns i molnet (och var). APIer är dessutom lättare att studera med en doktorands resurser.

Johannes Olegård, Stockholms Universitet / MSAB

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

Jag gav en kort presentation för Childhood foundation för några veckor sedan som jag tyckte är intressant nog att sprida. Den började i observationen att generativa algoritmer börjar bli riktigt bra. Det är snarare det som imponerar mig med de senaste framstegen; att algoritmer kan generera material med så pass (relativt sett) hög kvalitet, snarare än förstå. Alla talar om ChatGPT men jag är lika imponerad av bildgeneratorerna så som Dall-E och Stable Diffusion.

Så, eftersom pornografi är det första som nya medier alltid används till (sägs det) så väcktes frågan hur AI-utvecklingen ser ut inom det området. Och jodå, det rör på sig även där. Ett gäng grabbar startade till och med i slutet på förra året ett företag för att ta fram "Unstable diffusion" som alltså genererar pornografiska bilder på samma sätt som stable diffusion genererar icke-pornografiska dito. (De lyckades för övrigt med konststycket att bli utslängda av både Reddit och Patreon. det förra är ju lite av en bedrift, reddit censurerar inte sina deltagare i första taget.)

Om sådana här algoritmer kan generera pornografi så kan de naturligtvis också generera barnpornografi. (Som vi i branschen kallar "barnövergreppsmaterial"). Det finns en enkel porr-generator fritt tillgänglig på nätet (den verkar ha en begränsad träningsmängd och modifierar existerande foton snarare än att generera nya) som även om den inte är så imponerande visar vad som är möjligt med ganska enkla medel: http://pornpen.ai (Inte för känsliga, och inte säkert på arbetsplatsen, naturligtvis lite beroende på var ni arbetar...) Men man är uppenbarligen medveten om riskerna med generativa algoritmer, så för att undvika att generera olagliga bilder har de begränsat användargränssnittet: Man kan inte välja fritt utan kan bara göra en begränsad mängd fasta val. Vad som slår besökaren främst är dock hastigheten med vilken den kan generera material; man möts av en veritabel störtflod av bilder. Alla mer eller mindre olika.

Men det finns naturligtvis inget som hindrar att man tränar dylika algoritmer att generera barnpornografi. Det finns gott om material att träna på, både barn, pornografi, samt barnpornografi.

Det leder till en nära framtid där man kan generera en outsinlig mängd material som kommer att överstiga vår förmåga att klassificera och stoppa den. Idag så används faktiskt mest kryptografiska hash-summor, så som MD5 osv. för att stoppa sändningen av barnövergreppsmaterial. Den kommer självklart inte att fungera här. Dessutom så behöver man inte lagra material, man skulle lika gärna kunna generera on-demand.

Så ett beslag skulle i en nära framtid kunna bestå i bara en dator med två-tre grafikkort och en tränad porrmodell som, om man vet precis hur, kan fås att generera barnövergreppsmaterial. Detta blir naturligtvis svårt att utreda; man kan inte på ett enkelt sätt se vad en modell är kapabel att generera, de är ju notoriskt svåra att analysera, och även om polisen skulle lyckas få den att generera barnövergreppsmaterial så blir ju då svaret "Ja, men det har inte jag gjort! Jag har köpt en vanlig pornografigenerator. Att *ni* lyckas få den att göra olagligheter kan ju inte jag lastas för..."

Det blir dessutom juridiskt intressant. Kommer dylika generatorer ens att vara olagliga i alla jurisdiktioner? I USA så är man inte helt på det klara med att material där inget barn faktiskt kommit till skada är olagligt. Så skulle en maskin som potentiellt genererar material i så fall vara olaglig? Analogt: Även om teckningar kan vara olagliga i Sverige så har vi inte förbjudit papper och penna...

Om svaret blir "nej" i USA så är det enligt min bedömning kört. Där finns kunskapen, infrastrukturen, marknaden och så vidare. Så då kommer vi andra antagligen inte att kunna hålla emot. (Det var främst FBI som på 80-talet sånär lyckades rota ut traditionell barnpornografi. Utan dem så blir det svårt).

Och lagom som jag tänkt de här tankarna så visade det sig att det här redan har börjat hända. För en vecka sedan så tog polisen i Spanien en misstänkt som skall ha automatgenererat barnkroppar och sedan "deep-fakeat" ansikten från verkliga människor på de genererade modellerna. Men eftersom materialet sparades så är det fortfarande (i de flesta jurisdiktioner) olagligt. (Artikel från Daily Mail:

https://www.dailymail.co.uk/news/crime/article-11665797/Paedophiles-using-AI-art-generators-create-child-porn.html)

Det lär vara en skröna att Kineserna förbannar varandra med orden "may you live in interesting times", men det är inte utan att de orden i det här fallet klingar lite sant...

Stefan Axelsson

6. Aktuella event och länkar

Ett av de projekt som Digital Forensics Sweden drivit under vintern har skett i samverkan med East Sweden Game, NFC, AI Sweden och LiU och finansierats av Visual Sweden. Projektet har syftat till att studera integration av etablerade spelplattformar som Unity och Unreal Engine med data från brottsplatser i syfte att automatisera flödet och skapa bättre digitalisering och visualisering av brottsplatser, och verktyg för att arbeta med sådana digitala modeller. Projektet hade en avslutande välbesökt workshop i Linköping den 28/3 och planerar fler liknande event bl a i Norrköping framöver.

Här är en länk till eventet:

https://www.eventbrite.se/e/exploiting-game-technology-biljetter-566485773197

Vi påminner om nästkommande IAFS-konferens (https://iafs2023.com.au/). För mer information, kontakta Johnny Bengtsson: johnny.bengtsson@polisen.se

Lena Klasén delar en länk till ett kommande event med koppling till digitala brottsplatser (Smart Twins):
https://www.youtube.com/watch?v=tibBOONDz0U

7. Nästa nätverksträff

Nästa nätverksträff blir ett fysiskt event innan sommaren, vi återkommer om plats men hoppas på en ny partner i sydöstra Sverige! Fokus kommer att ligga på …

Avslutningsvis - håll ögonen öppna efter nyheter och material som kan relatera till vårt område, värt att tipsa varandra om. Skicka gärna tips till oss i nätverket så delar vi dessa.

Om Nyhetsbrevet

Nyhetsbrevet har ambitionen att vara kort och koncist och är tänkt att (i huvudsak) vara på svenska.
Vi välkomnar gästskribenter bland er läsare och partners, 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:

Digital Forensik och AI i ViaPlay ”Efterlyst” 2023-03-09 (kräver inlogg på ViaPlay)
https://viaplay.se/player/default/serier/efterlyst/sasong-61/avsnitt-5

Video-inspelning från IVA-eventet
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

Artikel från Linköpings Science Park om IVA-eventet
https://linkopingsciencepark.se/nya-digitala-mojligheter-for-kriminella-vad-kravs-for-att-stoppa-dem/

Om det strategiska initiativet kring Digital Forensik inom AI Sweden
https://www.ai.se/en/digital-forensics-sweden

Digital Forensics Sweden, vår egna siter:
https://www.digital-forensics.se
https://dfcc.se

Digital Forensics Sweden, Artikel av Linköpings Universitet
https://liu.se/nyhet/ai-ett-viktigt-verktyg-i-jakten-pa-digitala-brottslingar

DFCC på Almedalen via EastSweden:
https://www.youtube.com/watch?v=vx4I7oQZ5bA

Länkar till Nationellt Cybersäkerhetscentrum
https://www.ncsc.se/aktuellt/

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

Tips på kommande konferenser
https://iafs2023.com.au/