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 #2/24

The Digital Forensics Competence Center of Sweden

DIGITAL-FORENSICS.SE

NO.2

NOVEMBER 2024

Innehåll

Lägg till i din kalender

Nätverksträff: den 12e december
kl. 10.00 - 12.00

1. Inledning

Välkomna till ett färskt nyhetsbrev från Digital Forensics Sweden!

I skrivande stund har Donald Trump återtagit makten i Vita huset, något som många tror kan innebära början på en ny världsordning, detta i en värld där det idag inte råder brist på oroligheter. Osäkerheten kring ny politisk riktning är förstås stor, och vilken påverkan det ska få för maktbalanser och konflikter globalt. Mycket återstår att se, men det lär bli ett drama att följa noga och där koll på verkliga fakta blir allt viktigare.

Digital Forensics Sweden har under hösten besökt Afrikanska kontinenten och där haft möjlighet att både möta en allt mindre stabil demokrati i Sydafrika, drastiskt utöka vårt nätverk av internationella kontakter, och också fått chans att visa upp svensk förmåga på den internationella forensic science-konferensen AFSA2024 (African Forensic Science Academy) i Rwanda. Bland många intryck och reflektioner är en sak slående; våra erfarenheter av att bygga ett nationellt digitalforensiskt ekosystem är unika, och det vi gör i våra projekt skapar stort internationellt intresse.

Vi verkar ha blivit synliga på den globala arenan! Efter att ha mött forensiker från hela världen, slås man också av en insikt; Forensiker som yrkesmänniskor liksom forskare inom område delar som kollektiv mycket mer med varandra än bara forensiken. Det är människor som brinner för vad som är rätt, vad som är verklig sanning, som söker transparens och klarhet, som delar ett inre driv att finna information och förklaring på händelser som inte borde inträffa, och som innebär skada på individer och samhälle. Det är inte sällan integritetsstarka människor med starkt rättspatos som vill bygga det goda samhället där grundläggande mänskliga rättigheter respekteras, där lag och rättvisa inte får grumlas av korruption eller slarvigt gjorda utredningar. Det vi talar om är egentligen rättssäkerhet, som ju utgör grunden för alla demokratiska samhällen. Det faktum att man delar dessa värderingar skapar en stark gemenskap i möten yrkesmänniskor emellan.

I Rwanda fick vi möta många av dessa, och kunde känna en stolthet i det vi gör och samlas kring. Vid ett tillfälle lyssnade vi på en polisutredare från Israel som delade med sig av sina erfarenheter från 7:e oktober (2023) och hur man under pågående attack arbetade under skydd för att samla in kroppar, skadade människor och bevismaterial. Här möter vi en yrkesmänniska som gör sitt jobb, frikopplat från politik och åsiktsmotsättningar. Det går inte att låta bli att känna en stor respekt.

Linköpings Universitet har kommit till andra året av det nya Masterprogrammet inom Cybersäkerhet, och det betyder att kursen i ”digital forensics & incident response” startat upp med gästföreläsningar av Polisen /NFC och avancerade labbar med case att lösa för att hitta ledtrådar i hårddiskar och servrar mm. Ett väldigt kvalificerat upplägg, och väldigt rätt i tiden. Parallellt skapas nu en forskningsgrupp inom Digital Forensics, inom avdelningen Informationskodning på Institutionen för systemteknik (isy).

Här hemma har vi också dragit igång det stora projektet ”Interactive Digital Twin for multimodal AI” tillsammans med flera av er partners, och kommer att kunna berätta mer om det inom kort – just nu skapas nya fiktiva brottsscenarior där vi kommer att få möjlighet att koppla in forskningsfronten och så småningom kunna demonstrera nya framtida digital-forensiska metoder.

I vårt nätverk, Digital Forensics Sweden, har vi fångat upp ett antal nya partners, och vi kommer att börja ge några av dessa möjlighet att presentera sig på kommande nätverksträff den 12/12.

Som vanligt bjuder vi på en krönika av Professor Stefan Axelsson, liksom lite information, tips och tankar från våra två doktorander, Johnny Bengtsson och Johannes Olegård.

Önskar er trevlig läsning!
Niclas Fock, redaktör

2. Rapport från en Afrika-tour med digitalforensiskt perspektiv

Digital Forensics Sweden genom Niclas Fock och Lena Klasén, är nyss hemkomna från Afrikanska kontinenten. Här följer några korta reflektioner.
Forensik-konferensen AFSA2024 avslutades nyligen i Rwandas huvudstad, Kigali. En välbesökt konferens med hög vetenskaplig nivå och delegater från runtom hela världen, bjöd på insikter och en överblick kring var området befinner sig forsknings och tillämpningsmässigt.

Själva bjöd vi från Digital Forensics Sweden på såväl en Keynote-föreläsning (Lena Klasén), en 4-timmars workshop på temat digital forensik, och kunde också bistå med lite moderering på stora scenen.

Här är följer ett axplock av våra intryck:

- Konferensen kretsade en hel del kring The Sydney Declaration (se t ex https://www.dfrws.org/presentation/sydney_declaration_path_ahead/
- vi hade ämnet uppe på vår nätverksträff den 13 juni i år), som presenterades på konferensen IAFS i Sydney i december 2023, inte minst med bäring på digital forensik in i framtiden. Man gör bedömningen att dokumentet blir en utgångspunkt för begrepp och arbetssätt från och med nu.

- Kompetensen på det digitala området är generellt hög, och inom många delar av Afrika bedrivs ledande forskning. Intresset för det som sker på kontinenten inom forensik är stort från andra delar av världen. Bl a investerar Indien i att bygga upp forensisk kompetens och infrastruktur i Uganda (exempelvis ett digitalforensiskt labb), med målet att utbilda och kunna lämna över till lokal personal inom en femårsperiod.

- Digitala spår och AI kommer in i allt mer av forensiken, oavsett om det gäller kemi, dna etc och liksom metoderna får allt mer stöd av digitala verktyg, digitala data och (därmed) AI. Liksom digital forensik är AI ”cross-disciplinary”. En majoritet av föredragen berörde på något sätt digital-forensiska aspekter, varav några uppenbarligen för att ”visa” att man inte missat att ta med det… Ett exempel är brandutredningar som i många fall löses med betydligt mindre resurser och med högre informationsvärde genom att samla in data från hus-sensorer, elförbrukningsdata, mobiltelefondata eller pulsarmband etc.

- Stora språkmodeller i Afrika har flera utmaningar; det finns över 3000 olika språk, varav vissa saknar skriftspråk, och det saknas stora beräkningsresurser för AI av det slag som nu snabbt byggs ut i många delar av världen.

- Vi var ensamma om att ha ”digital forensik” som topic på konferensen, vilket gjorde att det vi presenterade rönte stort intresse, och ledde till många inbjudningar till internationella konferenser framöver.

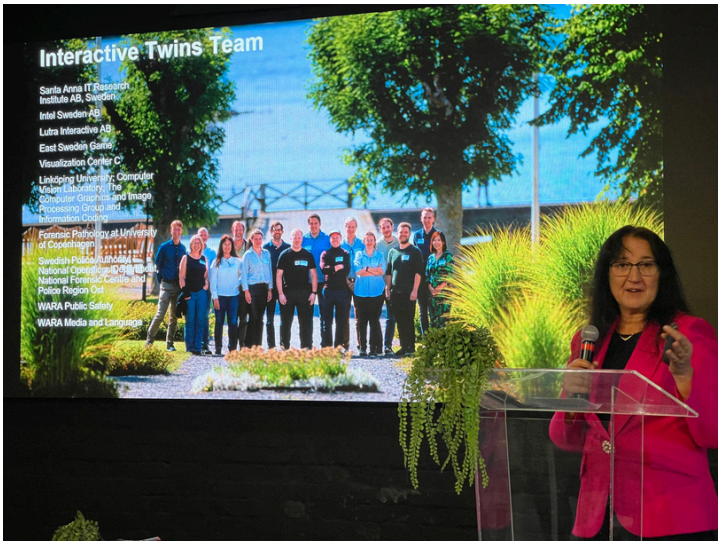
- Flera tankar om möjliga projekt för Digital Forensics Sweden föddes; t ex projekt kring byggnads-/fastighetsdata och data från personer som vistas i byggnader, exempelvis för att underlätta räddningsinsatser och utredningar i samband med naturkatastrofer eller terrorattentat etc, projekt där man tränar narrativ för påverkansoperationer och snabbare kan identifiera och spåra sådana.

På plats i Rwanda mötte vi också landets justitieminister som ville hälsa på den svenska ”delegationen”…man kunde önska att det aktiva intressen nu kunde vakna här hemma! Vi kan också konstatera att många av de forensiska labbchefer vi mötte från alla delar av världen, undrade om vi kunde ge kurser i digital forensik, något vi förstås tar med oss hem att fundera på hur vi skulle kunna lösa, och samtidigt skapa något av värde för er i nätverket här i Sverige.

Vidare i Sydafrika var vi under den efterföljande veckan inbjudna genom AI Sweden (Tack Ewa Thorslund!) till en vecka med AI-tema arrangerad av svenska ambassaden, under ledning av ambassadör Håkan Juholt. Lena Klasén var personligen inbjuden av Svenska Ambassaden som expert inom forensik under denna sk ”AI Week”, och teamet besökte bl a University of Pretoria på temat LLM:er (generativa språkmodeller) med fokus speciellt på Sydafrikas utmaningar. Lena Klasén besökte, tillsammans med AI Sweden och Peace Parks Foundation Sweden, även US Embassy Cyber Task Team där hon träffade representatnet för Secret Service och US Department of Homeland Security och fick en inblick i deras arbete.

Lenas grupp var dessutom inbjuden till Botswana för en workshop om AI och digital forensik tillsammans med representanter från Botswanas regering, Botswana Police, turistorganisationer och företag. Det betydde viktiga steg framåt i arbetet med att försöka skapa ett gemensamt projekt för övervakning av stora naturområden, i syfte att både förebygga och utreda brott med digital teknik och AI. Efter själva resan har det också varit ytterligare möten med Peace Parks för att forma gemensamma strategier och en tydligare projektidé och stärkt konsortium, ka rätt finansiering mm. Vi får anledning att återkomma med mer information om projektet när det blivit lite tydligare.

Klart är i alla fall att intresset från svensk försvarsmakt är stort, genom att resultaten förväntas kunna vara mycket användbara inte bara i Afrika, utan även här hemma i Sverige.



3. Forskningsnytt #1

Forensik, it-forensik och additiv tillverkning

NFC har sedan en tid tillbaka avslutat ett projekt som syftar till att ta fram en forensisk process inom 3D-utskrivna vapendelar, där jag och min it-forensiske kollega Janne K. fått möjlighet att bidra med våra kunskaper inom additiva utskrifter, it-forensik och tankar inom 3D-visualisering.

Utan att gå in på speficika detaljer och förmågor, så är den samlade bedömningen att det under vissa förutsättningar går att knyta en utskrift till en specifik skrivarmodell.

I vissa fall kan även en enskild skrivarindivid kunna tänkas identifieras tillsammans en forensisk spårjämförelse. Här är it-forensiken en av nyckelfaktorerna i kombination med användandet av en skiktröntgenutrustning. Med en sådan går det att icke-invasivt, alltså på ett icke-förstörande sätt, skapa en volymrekonstruktion.

En volymrekonstruktion är en 3D-volym som algoritmiskt har framräknats utifrån en tillräcklig stor mängd radiografiska 2D-bilder, alltå röntgenbilder som individuellt är tagna ur olika vinklar. i volymrekonstruktionen går det också göra utföra fotogrammetriska beräkningar, avståndsberäkningar mellan olika voxlar, tredimensionella pixlar.

Jag har med haft en dialog med ett par andra forensiska labb och forskare inom Europa. Främst finns behovet av forensisk forskning och metodutveckling inom additiv tillverkning av 3D-vapen. Här har jag emellertid föreslagit att både additiv och subtraktiv tillverkning skulle kunna bilda ett gemensamt och övergripande forensiskt forskningsområde.

Med additiv tillverkning menas att material tillförs för att bygga upp en struktur, medan subtraktiv tillverkning baseras på idén om att avlägsna material för att skapa en slutprodukt. Här ser jag att även it-forensiken har en naturlig hemvist jämte traditionella forensiska undersökningar som verktygsspår, biospår, fotografering, kemi- och materialanalys.

Nästa gång kanske jag författar ett par ord om brandplatsundersökningar och hur it- och IoT-forensik kan vara till stöd för sådana platsundersökningar, vilket var en av de avgörande faktorerna i en mordbrand i Sandviken.

Mer om detta finns också i podden Aftonbladets podd "Djävulen finns i detaljerna", 3. Detaljerna som avslöjade mordbranden.

källa:https://www.aftonbladet.se/podcasts/ab/program/1363

Johnny Bengtsson
doktorand på LiU och från NFC

Bilden från Aftonbladet

3. Forskningsnytt #2

Att tala med bönder på bönders vis - perspektiv från olika verkligheter

Tala med bönder på bönders vis är ett välbekant talesätt. Eller här, skriva till bönder på bönders vis.

Jag har under snart två decennier putsat på mina färdigheter att, i samband med forensiska undersökningar, både skriva arbetsblad och författa korta och koncisa sakkunnigutlåtanden som ett resultat av undersökningen.
Det sistnämnda är något som förhoppningsvis når en mottagare utan tekniska förkunskaper.

När du skriver ett arbetsblad -- eller när du tekniskt, forensiskt och språkligt granskar en undersökning som någon kollega har gjort -- förtväntas det av både dig och din kollega att ni båda besitter adekvata domänkunskaper samt har kännedom om relevanta facktermer som är gällande för den specifika undersökningen eller undersökningstypen. Språket i sådana arbetslad kan vara stundtals vara väldigt kompakt, men i gengäld informationseffektivt; mätvärden, tabeller, grafer, loggdata, utskrivter av terminalkommunikation och bilder kan mer än väl kompensera för språkliga tillkortakommanden, liksom bruket av facktermer och begrepp.

Ni som har genomgått en forskarutbildning, eller är produktiva skribenter av akademiska publikationer, vet att det kan ta väldigt lång tid att författa ett ynkaste textstycke -- även om det går fortare ju mer du skriver.I mitt parallella yrkesliv, rollen som forskarstuderande, har mitt skrivande till delar ställts på ända. Det är inte förrän nu jag har insett hur mycket tid jag måste ägna åt att textreflektioner; varje ord i varje mening avvägs noggrant, där ledstjärnan är att det ska vara så tydligt, precist och informativt som möjligt, utan att för den sakens skull krångla till det. Läsarens uppmärksamhet får helst inte tappas.

Korta meningar och valet av ett enkelt språkbruk tycks många gånger vara att föredra framför effektiv användning av fackterminologi. Om sådan terminologi ändå används, måste detta på något vis deklareras, varpå ännu mer tid försvinner från det du egentligen skulle skriva om.

Det jag har också har reflekterat över är hur friskt det i akademiska texter gödslas med övergångsord, som moreover, furthermore, additionally, consequently, accordingly och så vidare.

Det är inte riktigt så vi uttrycker oss på svenska, men något som ibland kan underlätta för läsaren. Det jag däremot inte känner mig bekväm med är användningen av första person plural: we demonstrate, we conclude, we propose... Vilka är förresten vi? Är det enbart författarna som har bidragit? Har de suttit instängda i en bunker och tänkt -- eller har det förekommit interaktion med andra personer i deras närhet och som möjligen kan ha bidragit till tankeverksamheten, vilket i sin tur har lett arbetet framåt?

För egen del kommer jag även forsättningsvis hålla fast vid tredje person; this study demonstrates, it was concluded that, this work proposes. Det ser i mina ögen lite mer objektivt ut. Dessutom är det bara jag som har skrivit mina manuskript, så det skulle ännu konstigare ut om jag tog på mig vi-titeln. Det är är ju helt ointressant vem som gjorde vad, snarare vad som har undersökts, på vilket sätt och vad resultat blev. Och det är precis så som NFC:s sakkunnigutlåtanden kan se ut. Neutralt. Objektivt. Byråkratiskt och formellt.

Slutligen, språket och språkbruket är något som i många situationer endast är ämnat en viss målgrupp. Vill jag nå ut till it-forensiska akademin, som jag till stora delar upplever saknar praktisk erfarenhet av it-forensiska undersökningar och tillämpad it-forensisk metodutveckling, då får jag ta på mig min akademiska hatt. Vill jag nå ut till utredare och åklagare, då kanske jag väljer att helt eller till stora delar utelämna tekniska detaljer som budskapsmässigt ändå går till spillo.

Om jag däremot vill utbyta tankar och idéer med tekniskt likasinnade lekkamrater; då kan jag bre på med facktermer som för utomstående verkar vara rena grekiskan - såvida du inte själv pratar avartsgrekiska. Detsamma gäller när jag tar på mig min foliehatt, när jag vill prata med konspirationsteoretiker som står i den vetenskapliga radioskuggan.
Eller ja. Kanske inte. Men ni fattar.

Tala med bönder på bönder vis. Då når kanske ut med budskapet på ett bättre sätt.

Johnny Bengtsson
Doktorand på LiU och från NFC

3. Forskningsnytt #3

Kanske inte nytt, men jag snubblade nyligen över denna artikel [1], där författarna inte bara bygger ett intrångsdetekteringsdataset, utan också delar med sig av den testbed [2] som användes för att bygga datasettet (vilket är sorgligt sällsynt).

Inom IT-forensik-forskningen pratas det en del om problematiken runt att bygga realistiska dataset---och vad jag tycker man ofta missar (i strävan att försöka härma andra ämnesområden) är: hur centralt mellansteg i orskan-verkan-kedjan (chain-of-events) är för forensisk forskning och hur ett "vanliga" dataset därför är väldigt begränsande.

Visst kan man använda dataset för att testa att ett forensiskt verktyg kan käka upp en fil och spottar ut rätt information, men mer intressant är ju vilken information som är tillförlitlig och relevant till att börja med (dvs. värd att spotta ut).

Ett dataset är ju (oftast) ett orsakan-verkan-experiment som redan gjorts åt dig, så det är både viktigt att ett (helst flera) bra experiment gjorts och att tillräckligt med information om orsakan-verkan-kedjan finns beskriven i tillräcklig detalj.
(Liknande kritik kan riktas mot AI-forskning där fokus ofta läggs på att svara rätt på frågor snarare än att förstå underliggande fenomen.)

Bilden från Wikipedia

Jag skickade nyligen in en artikel till en konferens (vi får se om den går genom peer review).

Den handlar om hur man kan i loggar kan lagra svaret på frågan "varför?" i form av "orskande" event IDn---för att på så sätt enkelt koppla ihop händelser (events) från olika loggfiler (event A orskar event B) utan att förlita sig på fuzzy metoder (t.ex. jämföra tidsstämplar). Typ "dynamic taint tracking" och "provenance graphs" [3], men på steroider.
Min förhoppning är att detta kan bland annat (i en senare artikel) fungera som ett bättre sätt att lagra "groundtruth" för IT-forensiska dataset.

Det vill säga, att hela orskan-verkan-kedjan för ett experiment sparas (på billigt vis) och inte bara slutresultatet (endstate).
På så sätt kan man forska på hela kedjan händelseförlopp--slutresultat--tolkning, och inte bara det sista steget.

[1] https://doi.org/10.1109/TDSC.2022.3201582
[2] https://github.com/ait-aecid/kyoushi-environment
[3] https://doi.org/10.1145/2508859.2516731

P.S. I andra "old news" rekommenderar jag starkt podden "Darknet Diaries"---som har nästan inget alls att göra med "darknet" och mycket mer att göra med intervjuer med IT-forensiker och hackers om riktiga incidenter. Podden "DFIRL" (av Magnet forensics) är också bra, och har fokus på riktiga fall (snarare än tekniska detaljer---som de flesta DF-poddar lätt snöar in sig på, vilket gör sig dåligt i ljud-format).

Johannes Olegård
Doktoranden Stockholm s universitet

AI-hypen fortsätter oförtrutet

Vi har ju nu levt med stora språkmodeller ett tag så har våra initiala farhågor besannats eller kommit på skam?

Vi var ju många som gissade att stora språkmodeller och annan generativ AI skulle påverka säkerhetslandskapet både på gott och ont, men när journalisterna frågar så är det främst domedagsprofetior som efterfrågas. Så hur ser det ut nu när vi börjat få lite facit?
Kan generativ AI i allmänhet, och stora språkmodeller i synnerhet, hjälpa en angripare på traven, och hur mycket hjälp kan vederbörande få?

Jag och många andra har siat i medierna att även om de inte nödvändigtvis skulle vara bättre än en mänsklig angripare så har de åtminstone fördelen att de skulle kunna automatisera stora delar av angreppet och på så sätt göra det billigare. Det verkar som om de faktiskt skulle kunna göra precis det.

På KTH så ställde sig Fredrik Heiding just den frågan och angrep den från två håll i sin nyligen försvarade doktorsavhandling, där jag hade förmånen att sitta med i betygs-kommitten. Han undersökte dels hur språkmodellerna kan hjälpa till med att skriva phishing-mail och dels hur de kan hjälpa en angripare att knäcka IoT-enheter av den typ man skulle kunna hitta i hemmet.

Tillsammans med forskare vid Harvard i USA och här hemma så sjösatte Fredrik en phishing-kampanj där försökspersonerna delades in i tre olika grupper (plus en kontrollgrupp). En grupp fick mail som skrevs manuellt med hjälp av V-triad-teorin om hur man skriver bra phishing-mail, en fick mail genererade av ChatGPT 4.0, och en fick mail som genererats med en kombination av ChatGPT och V-triaden.

V-triaden går i korthet ut på att man riktar in sig på de tre faktorerna Credibility/Trovärdighet, Compatibility (Relevancy)/Relevans, och Customizability/Anpassning. Trovärdigheten kan man öka genom att till exempel använda ett välkänt företagsnamn eller logotyp, inkludera namnet på mottagaren, namnet på en välkänd avsändare, använda välkända fonter, färger och så vidare på samma sätt som kända varumärken.

Kompatibiliteten hänvisar till hur väl mailet stämmer med vad mottagaren förväntar sig, det vill säga om det är rimligt att få ett sådant mail.
Om man till exempel skickar ett mail med en länk till schemat för KTH till en Chalmersstudent så lär inte det mailet övertyga särskilt väl, oavsett hur väl man kopierats KTHs logotyp. Den sista, anpassning handlar om hur väl websidan man kommer till, eller emailet för den delen, uppför sig. Kan man kopiera länkar utan att det havererar, uppför sig loginsidor och så vidare som man förväntar sig etc.

Sedan så skickade man olika mail till försökerspersonerna. De i kontrollgruppen fick ett redan existerande mail som riktade sig mot Starbuckskunder.

En annan grupp fick motsvarande mail men genererat av ChatGPT 4.0. Nu ska ju LLM:er innehålla skydd mot att generera sådana mail, dvs de ska inte hjälpa en angripare hur enkelt som helst, men det visade sig. trivialt att kringgå dessa skydd genom att enkelt be ChatGPT att. generera "informativa" mail i stället för rena phishing-mail. Med detta lilla fikonlöv applicerat så genererade ChatGPT snällt phishing-mail så det stod härliga till.

Man skrev vidare personliga brev baserade på V-triaden på samma tema, dvs fortfarande från Starbucks, men riktat till de enskilda studenterna.

Till sist så slog man ihop de två metoderna och bad ChatGPT att generera ett phishing-mail genom att använda V-triaden, dvs inkludera information om mottagarens person, att de studerade vid Harvard etc.

Resultatet blev intressant i det att kontrollgruppen (när man sållat bort de respondenter som aldrig svarade) klarade sig bäst. Bara 25% klickade på länken. För ChatGPT ensamt så låg siffran runt 50% och för både V-triaden samt V-triaden+ChatGPT så fick man cirka 75% träff.

Med andra ord så är inte ChatGPT som sådant nödvändigtvis bättre än de som kompetent gör jobbet manuellt, men den är i stort sett lika bra, det vill säga om man sparkar lite på den och säger till den att. använda rätt metod i form av V-triaden. Den gör det dock automatiskt. och mycket billigare. Den intresserade av konstnadsberäkningen hänvisas till avhandligen/artikeln.

När det kom till angrepp mot IoT-enheter så baserades den på tidigare arbete där man undersökt en mängd enheter och hittat angrepp mot dem manuellt. Man lät sedan ChatGPT (3.5 och 4.0 beroende på) försöka. upprepa angreppet genom att berätta för en medhjälpare, steg för steg hur denne skulle gå tillväga. Totalt så genfördes 32 olika angrepp på fem olika enheter.

Man analyserade även hur väl ChatGPT hjälpte till, dvs graden av framgång i detalj, men i korthet så gjorde ChatGPT mycket väl ifrån sig. Den var inte bättre än en mänsklig angripare i det att den misslyckades med några av de mest avancerade attackerna, främst för att den verkade sakna up-to-date information om de senaste metoderna och verktygen, men de enkla, och medelsvåra angreppen klarade den av minst lika bra som en insatt mänsklig pen-testare, och den jobbar som sagt gratis och utan någon vidare utbildning.

Jag tycker personligen att det här är spännande resultat. Det är imponerande att ChatGPT, som inte tagits fram specifikt för informationsäkerhet, datorsäkerhet eller forensik, lyckas så väl på två så vitt skilda uppgifter. Även om den inte är bättre än en människa så jobbar den oförtrutet på utan rast, utbildning, eller lön.

Så om det inte kommer en AI-vinter snart, så är det inte utan att jag undrar om man kommer att kunna hänga med och vara konkurrenskraftig tills pension. Bäva mände universitetsprofessorerna...

Avhandling: Mitigating AI-Enabled Cyber Attacks on Hardware, Software, and System Users, Fredrik Heiding, Doctoral thesis in Computer Science, TRITA-EECS-AVL-2024:68, Division of Network and Systems Engineering, KTH Royal Institute of Technology, SE-100 44 Stockholm

Länk:https://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1898666&dswid=-4261
tyvärr ingår inte artiklarna; de får man söka separat.

5. Nästa Nätverksträff

Nästa nätverksträff blir den 12/12 kl 10:00 -12:00 och det är årets sista träff.
Det kommer bl a att handla om hur man kan bli Quantum Safe, och varför det blir allt viktigare.

Preliminär agenda

10:00 Välkomna
10:15 Key Note presentation: The concept of Quantum Safe Information
Konsta Rönkkö, CTO, IBM Finland
11:00 Partner presentation: (Possible partner presentations: ForensiqOne, Siemens, Eon, Vattenfall, Tekniska verken Linköping, Defentry, Försvarshögskolan – anmäl gärna intresse att hålla en kort presentation)
11:30 Nätverksinformation;
12:00 Slut

Senaste nytt

Vi har fått frågan från DFRWS, om vi vill vara värdar för deras internationella konferens 2026, och har tackat ja till detta. Det betyder att 2026 års konferens i Digital Forensik kommer att äga rum i Linköping i mars!

Flera länkar

AFSA2024: https://afsa2024.afsa.africa/
DFRWS: https://dfrws.org/

Aftonbladets podd "Djävulen finns i detaljerna", 3. Detaljerna som avslöjade mordbranden.
https://www.aftonbladet.se/podcasts/ab/program/1363

Från Jonas Olegårds “forskningsnytt #3”
1] https://doi.org/10.1109/TDSC.2022.3201582
[2] https://github.com/ait-aecid/kyoushi-environment
[3] https://doi.org/10.1145/2508859.2516731

Mitigating AI-Enabled Cyber Attacks on Hardware, Software, and System Users
https://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1898666&dswid=-9831

Digital Forensics Sweden, vår egen site: https://www.digital-forensics.se

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!