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 #2/23

The Digital Forensics Competence Center of Sweden

DIGITAL-FORENSICS.SE

Nyhetsbrev #2/September 2023

Innehåll

1. *Inledning*
2. *Aktuellt från nätverket*
3. *Forskningsnytt*
4. *Projektrapporter*
5. *Gästkrönika*
6. *Aktuella event och länkar*
7. *Nästa nätverksträff*

1. Inledning

Sedan förra nyhetsbrevet från Digital Forensics, har vi (precis) hunnit ha två nätverksträffar!
Strax innan sommaren tog BHT generöst emot de som rest till Karlskrona.
Flera nya deltagare fanns på plats och vi fick möta engagerade och initierad forskare som gav oss en unik inblick i arbetet med att analysera cyberattacker från krigets Ukraina. Diskussionerna kommer att leda vidare till flera projektansökningar tillsammans med BTH. Vi fock också en partnerpresentation från PRV som anslutit som ny nätverkspartner. På plats fanns även Kustbevakningen som kommer att få tillfälle att presentera sig närmare innan årsskiftet.

Den 26/9 hade vi ytterligare nätverksträff, on-line, med en både skrämmande och synnerligen intressant dragning av Susanne Drakborg om sexuella övergrepp mot barn på nätet, och arbetet inom Stella Polaris, den AI-hub som drivs av World Childhood Foundation. Det är imponerande att se hur konkret arbetet bedrivs, och hur långt fram man är med användning av AI-verktyg i detta viktiga arbete. Intel och Bjärn Runåker presenterade Intels forskning och utveckling av tekniker för Deep Fake Caption, som kan fungera som en möjlig teknik för exempelvis Childhood, där man skulle kunna skilja AI-genererat videomaterial från äkta.

I Nyhetesbrevet denna gång, som vanligt en krönika av vår Svenska professor i Digital Forensik vid Stockholms universitet, Stefan Axelsson, som skriver om årets grej, ChatGPT. Och förstås lite uppdateringar från nätverkets doktorander.

2. Aktuellt från nätverket

För er som deltog berättade vi den 26/9 också att vår ansökan till Vinnova om ett kompetenscenter inte får finansiering. Det är förstås ett negativt besked, men vi har under tiden sedan mötet i Blekinge arbetat på en annan väg framåt, och det blir nu den huvudplan vi kommer att följa.

Som ett led i det arbetet kommer vi att kontakta samtliga partner för att dels samtala kring andra finansieringsmöjligheter och klargöra era önskade engagemangsnivåer, och dels genomföra en uppföljande intervju om ert nuvarande arbete och era behov inom Digital Forensik.

Vinnova har också kontaktat oss direkt och bett oss skicka in en intresseanmälan till NATO / Diana, vilket vi också har gjort.

Våra projekt med bl a med NFC, AI Sweden, Linköpings Universitet, VisualiseringscenterC, Visual Sweden och EastSwedenGame (Lutra Interactive) där vi modellerar digitala brottsplatser med hjälp av gaming-plattformar fortsätter och har gått raskt framåt. Vi kommer att presentera en första installation på NorrköpingsVisualiseringscenterC den 7 december (nästa nätverksträff). Boka upp en heldag i Norrköping alltså!

3. Forskningsnytt

Johnny Bengtsson på NFC och ”DFCC-doktorand” på Linköpings Universitet är nyss hemkommen från en kurs inom steganografi och steganalys och tipsar om projektet UNCOVER.

Kursen utgör en leverabel i det H2020-finansierade projektet UNCOVER (https://www.uncoverproject.eu/) och riktades till brottsbekämande myndigheter (eng. law enforcement agencies, LEA:s) inom konsortiet och där Polismyndigheten ingår, externa LEA:s samt doktorander.

Steganografi kan i den här kontexten beskrivas som ett samlingsnamn för olika tillvägagångssätt att dolt inbädda ett meddelande i digital filer genom exempelvis filmanipulation. Genom olika metoder går det dessutom att statistiskt försvåra detektion genom exempelvis steganalys.

Steganalys är samlingsnamnet för de olika tillvägagångssätten att detektera användandet av steganografi. I bästa fall går det att både påvisa förekomsten av ett dolt meddelande samt en metod för att avkoda detsamma. I sämsta fall har du kanske ett statistiskt mått med stor osäkerhet och avsaknad av reell lösning för att meddelandedechiffrering.

Steganografi och steganalys för filer är ingen ny företeelse. Ross J. Anderson [1] och Jessica J. Fridrich m.fl. [2] har exempelvis publicerat inom dessa områden redan för ett kvarts sekel sedan. Sett till den stora mängd publikationer inom dessa ämnesområden så tycks forskningen fortskrida. Min personliga fundering är om det endast är av akademiskt intresse – eller om det faktisk finns någon reell nytta med steganografi och steganalys inom forensiken, då det idag finns andra sätt att skicka stora mängder signalskyddad data på ett svårdetekterat vis – både 1:1 och 1:många i båda vägar. Problemet är att vi inom forensiken faktiskt inte vet – och därför kan det finnas en poäng med deltagandet i UNCOVER.

[1] Ross Anderson (1996), Stretching the Limits of Steganography. First International Workshop, Cambridge, U.K. (1996).

[2] Fridrich, J. et al. (2001). Reliable Detection of LSB Steganography in Color and Grayscale Images. MM&Sec '01, 2001 workshop on Multimedia and security new challenges

Johnny Bengtsson, NFC

- - -

Johannes Olegård, ”DFCC-doktorand” på Stockholms Universitet och MSAB, är inne i intensivt forskningsarbete och berättar att han försöker få sin API-forensik-artikel publicerad samtidigt som

han skissar på nästa artikel. Johannes meddelar också att Stockholms universitet också håller på att fräscha upp ena av sina forensik-kurser!

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

Även om den värsta uppståndelsen kring stora språkmodeller illustrerade av ChatGPT 4.0 lagt sig, så betyder det inte att de inte fortsatt visar en del imponerande egenskaper. Den senaste tiden så har vi sett allt fler kritiska röster, där det visar sig att ChatGPT t ex inte klarar av programmeringsuppgifter man ger studenter när dessa ökar i komplexitet. Å andra sidan så fick vi i dagarna veta att ChatGPT minsann klarade sig lika bra som en akutläkare när den fick symptom presenterade för sig. Så att resultaten varierar verkar tydligt.

Det är också undertecknads egen erfarenhet; ChatGPT kan ena stunden leverera korrekt C-kod för ett medelsvårt problem, eller klara tentamen i introduktionskursen i digital forensik här vid Stockholms universitet (den klarade t ex nio av tio flervalfrågor), för att sedan inte kunna summera poängen rätt, eller komma ihåg hur många frågor den svarade rätt på. Det är väl idag det största problemet. ChatGPT klarar förvånansvärt komplexa problem ena stunden, för att sedan snubbla på triviala dito den andra. Det är svårt att i förväg, eller ens med svaret i hand, se om svaret är korrekt, eller utsökt invecklat svammel. ChatGPT, antagligen pga sin arkitektur, argumenterar sig gärna fast i ett hörn som den inte tycks kunna komma ur.

Så en grupp mycket namnkunniga forskare med insyn tog på sig att göra en bredare utvärdering av vad ChatGPT 4.0 faktiskt klarar av och publicerade resultaten i en öppen artikel på arXiv [1]. Den har några månader på nacken vid det här laget, och området rör sig fort, men är ändå väl värd att läsa i sin helhet.

Vad har artikeln att säga som är relevant för digital forensik? Jo, som av en händelse så utsätter faktiskt forskarna ChatGPT för ett forensik-scenario, nämligen reverse engineering av en okänd binär. [1, appendix C] Man instruerar ChatGPT att använda användaren som ett verktyg och ge instruktioner steg-för-steg och i form av kommandon som användaren kan exekvera rakt av.

Problemet ChatGPT ställs inför är att användaren har en exekverbar fil vid namn easy_one på mac OS X som säger "Enter password:" när man kör det, och ChatGPT tillfrågas om hjälp att finna lösenordet.

ChatGPT börjar med att fråga om vad "file" kommandot ger, och får svaret att det är en Mach-O 64-bit körbar fil, arkitektur x86_64.

ChatGPT frågar sedan efter resultatet av "strings easy_one" och efter att ha sett svaret så ger den två strategier för att gå vidare; antingen gissa lösenordet rakt av, eller att använda en debugger för att inspektera det körda programmets minne och hitta lösenordet den vägen. Den förordar det senare alternativet och ber användare köra debuggern "lldb".

ChatGPT talar om för användaren hur man sätter en breakpoint i printf, kör programmet, läser och förklarar registerinnehåll, ber om och tolkar en disassembly (alltså listning av maskinkoden) av programmet och drar den korrekt slutsatsen att programmet easy_one har ett osäkert lösenord. Programmet kontrollerar bara att längden på lösenordet är tio tecken långt samt att första tecknet har ett visst (okänt) värde.

ChatGPT rekommenderar sedan att man knäcker lösenordet och på tillfrågan så genererar det ett pyton-program som genererar alla möjliga lösenord och kör programmet med dem som indata. Det tar 0,16s ungefär att knäcka lösenordet.

Jag kan inte tycka annat än att det här är ett imponerande resultat. Som student så måste man ha ganska många års studier på högskolenivå innan man kommit till den nivå av kunskap och färdigheter att man skulle kunna förväntas klara av det här som exv. Första uppgiften på en laboration. De som studerar malware reverse-engineering osv. i senare kurs når och klarar naturligtvis betydligt svårare uppgifter än den här och de som sitter på sin fritid, kan naturligtvis nå hit och längre på relativt kort tid, men det är långtifrån alla studenter som ens når den här nivån.

Om man betänker hur fort ChatGPT och liknande system nått den här nivån, egentligen bara genom att bli större och större, så kan man inte annat än tro att de kommer att bli kraftfulla verktyg att användas för både gott och ont. Efter varje AI-vår så kommer som bekant en AI-vinter, men jag undrar om det inte kommer att bli en ganska modern, dvs grön och kort vinter den här gången. "Attacks only get better, they never get worse" som det sägs inom krypto- och datasäkerhets-området.

P.S. Den här krönikan har jag faktiskt skrivit själv, men ChatGPT hade antagligen klarat av att göra det lika bra. Åtminstone nästan... Jag hoppas hinna gå i pension innan den kan ta över mitt jobb helt.

Stefan Axelsson

1) Sparks of Artificial General Intelligence: Early experiments with GPT-4 Sébastien Bubeck, Varun Chandrasekaran, Ronen Eldan, Johannes Gehrke, Eric Horvitz, Ece Kamar, Peter Lee, Yin Tat Lee, Yuanzhi Li, Scott Lundberg, Harsha Nori, Hamid Palangi, Marco Tulio Ribeiro, Yi Zhang, https://arxiv.org/abs/2303.12712, v5 Thu, 13 Apr 2023. ’

5. Aktuella event och länkar

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

Värt att notera är att två ansikten ur nätverkskretsen deltar som talare, Lena Klasén (LiU samt Polisen/NOA) och Jimmy Berggren (Polisen/NFC).

6. Nästa nätverksträff

Nästa nätverksträff blir ett fysiskt event den 7:e december kl 10-16 på Norrköpings VisualiseringscenterC.

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/

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