Cybersecurity Engineering Section

DTU Compute

Faculty

- Nicola Dragoni
- Christian D. Jensen
- Weizhi Meng
- Emmanouil Vasilomanolakis
- Luisa Siniscalchi
- Christian Majenz
- Carsten Baum
- Tyge Tiessen

Christian D. Jensen

1) Cybersecurity Roadshow
2) Nøglekopiering fra fotografier
3) Security Incident Simulations
4) Applikationsbaseret (trace-based) netværk trafik simulator

Cybersecurity Roadshow

Dette projekt definerer en ramme for flere bachelorprojekter der retter sig mod sikkerhedsawareness og sikkerhedsuddannelse af den bredere offentlighed; hvert projekt kan gennemføres af en til flere bachelorstuderende.

Projekterne skal indgå i et roadshow, som lærere og studerende fra DTU, eller andre uddannelsesinstitutioner, kan bruge til at illustrere et sikkerhedsproblem gennem en demonstration (også kaldet "stunt hacking") eller hands-on undervisning/øvelser til et publikum der ikke nødvendigvis kender meget til cybersikkerhed. Hands-on undervisningen kan rette sig mod almindelige softwareudviklere i virksomheder, studerende på gymnasiale uddannelser eller den brede offentlighed, så den skal kunne gennemføres med deltagernes eget udstyr og/eller med begrænset brug af specialiseret hardware, som i givet fald skal være billig at anskaffe.

Cybersecurity Roadshow

Projekter kan demonstrere kendte sårbarheder i eksisterende produkter eller systemer (vi har allerede demonstrationer af MouseJacking, falske WiFi Access Points, USB Rubber Ducky og en enkelt brug af Metasploit), men demonstrationer kan også fokusere på mere generelle problemstillinger, som f.eks. "Replay"- eller "Relay"-angreb eller værktøjer (f.eks. OpenVas eller flere øvelser med Metasploit).

Hvert projekt skal identificere et emne indenfor cybersikkerhed, som demonstrationen eller hands-on undervisningen skal fokusere på, gennemgå den bagvedliggende teori, samt udvikle det "hack" som skal demomstreres eller undervisningen skal omhandle og det materiale der skal bruges af Roadshowet (f.eks. en kort pædagogisk tekst der gennemgår den bagvedliggende teori og forklarer sikkerhedsproblemet, en præsentation der kan bruges til undervisningen, samt en drejebog der forklarer hvordan demonstrationen/øvelsen gennemføres i praksis.

Cybersecurity Roadshow

Eksempler på emner der kan inkluderes i roadshowøvelser er:

- trådløs kommunikation - både proprietære protokoller (f.eks. Logitech wireless keyboard eller alarmsystemer til hjemmet) eller standardprotokoller som LoRa og Bluetooth
- adgangskontrolsystemer, smarte låse og andre smartcard baserede systemer
- IP-baserede kameraovervågningssystemer
- biometriske sikkerhedsmekanismer
- sikkerhed i IoT konsumerelektronik
- fjernstyret legetøj o.lign.

I forbindelse med udvikling af demonstration/øvelse vil det ofte være nødvendigt at udvikle egne programmer, der demonstrerer problemstillingen (f.eks. en sårbarhed), samt konfigurere både forskellige klienter og eventuelle servere så demonstrationen/øvelsen kan gennemføres pålideligt.

Nøglekopiering fra fotografier

Det har længe været kendt at man med et billede med tilstrækkelig høj opløsning kan lave en fungerende kopi af den nøgle der ses på billedet (se f.eks. https://www.youtube.com/watch?v=pohVT1nKZig).

Målet med dette projekt er at afprøve undersøge hvor meget denne proces kan automatiseres, ved at udvikle software der konvertere et billede af en nøgle til en fungerende 3D printet kopi af denne nøgle.

Det udviklede software skal så bruges til at afprøve teknologiens grænser, f.eks. ved at undersøge om man kan tage et billede fra SoMe der indeholder en nøgle, som systemet så kopierer.

Security Incident Simulations

Undervisning of træning bliver ofte bedre med hands-on erfaringer, men det er sjældent ønskværdigt at forårsage en katastrofe, for at undervise i katastrofeplaner. Formålet med dette projekt er at udvikle en simulator (et "serious game") hvor studerende gennem gamification kan lære at håndtere sikkerhedshændelser. Simulatoren kan enten fokusere på et identificeret aspekt af håndtering af sikkeredshændelser, eller en type af hændelser hvor man så lærer hvilke roller og ansvar de forskellige teams i organisationen har.

Applikationsbaseret (trace-based) netværk trafik simulator

Træning af sikkerhedseksperter (både naturlig og kunstig intelligens) afhænger ofte af adgang til netværkstrafik, de studerende kan analysere for at identificere afvigende og muligvis ondsindet trafik.

Formålet med dette projekt er at undersøge eksisterende trafikmønstre på netværk og udvikle en netværkstrafikgenerator der kan generere en pcap fil der ligner den pcap fil man får ved at benytte Wireshark eller lign. til at optage trafikken på et rigtigt netværk.

Målgruppen for dette projekt vil dels være undervisere i cybersikkerhed, opgavestillere til forensicsopgaver til CTF'er og AI/ML eksperter der ønsker et realistisk baseline traffik mønster (trafik med kendt label "good") til træning af Neurale Netværk eller Deep Learning netværk.

Benjamin Larsen

1. We would like to find out exactly what kind of personal data that websites and newsletters of Danish political parties collect from visitors, members and/or users via cookies, tracking etc. (i.e. Facebook Pixel or other)

2. We would like to figure out if it is possible to develop a simple tool to scrape data from TikTok, since TikTok is more of a black box than most social media. We find TikTok especially interesting since the Danish election of 2022 is the first election where TikTok has played a pivotal role in reaching and affecting especially first-time and younger voters.

3. We would like to find out exactly what kind of personal data that websites and newsletters of Danish public hospitals, private hospitals and private practitioner collect from patients, users and visitors.

Carsten Baum

- (Cryptographic) Problems with the Bridgefy communication app
- Privacy-friendly machine learning with Homomorphic Encryption
- Computing on private data – the simplest MPC

Weizhi Meng

- Project 1: Blockchain-based Enterprise Resources Planning (BlockERP).
- Project 2: 6G Connection Strategy with Blockchain.

Blockchain-based Enterprise Resources Planning (BlockERP)

The core functionality of Enterprise Resources Planning is to automate the workflow in the Enterprise. Some requires further integration with multi-parties, which create a complicated joint-venture and information exchange network.

ERP requires its storing data with highest integrity and best traceability, in order to enhance decision support and cost estimation. Traditionally, ERP fully relies on the operational integrity of the core database, which is centralized in some manner.

Due to different format between systems, integration or information sharing due to joint-venture or cooperation can be hassle. Furthermore, integrity recognition can be questionable between party, as there might not be no consensus.

Blockchain not only provides the possibility to create different sizes of permission-chain, but also, the consensus algorithms ensure both parties not able to deny the input data on chain.

In this project, we aim to develop a prototype of blockchain-based ERP. This underlying securely decentralized database allows ERP to be more expandable and integrate-able between different parties, which creates a better business environment for the future.

6G Connection Strategy with Blockchain

Wireless Wire-Area Network (a.k.a. WWAN) has fulfilled our expectation of ubiquitous network access. As technology advances from GSM to NR, not only the access media moved from monogenous to heterogeneous, but the flexibility of the network also allows extensive coverage. As the basic bandwidth requirement has been pushed due to the underlying application, efficiency on infrastructures' usage and resources' distribution has gained unprecedented importance.

However, until now, most of the WWAN consumer premises equipment (CPE) still relies on simple decision of connection strategy – The stronger signal is, the better connection quality will be. Though, it might be true in rural areas, it may not be useful in crowded downtown – As the tower that's closes to you might be the most packed. As 6G provides its variety of access media from small low power indoor Femto-Cells to the off-ground satellite connection, connection strategy should no longer limited to the strength of the signals, but the overall connection quality.

Blockchain provides a decentralized database as a reference for telecom operators to define connection strategy and provide the experience sharing of connection quality reported from each device. This creates a flexible connection strategy for both end-users and telecom operators. Telecom operators can release its latest connection strategy on to the Blockchain, so that the CPE's follows and connect to the service endpoint in the optimized way.

In this project, we aim to develop a blockchain-based connection strategy in 6G.