Section for Cybersecurity Engineering

DTU Compute

Section Information

Cybersecurity engineering focuses on the methods, processes and tools for the design, development and analysis of secure computing systems that are accessible through a network, typically the Internet, which is often known as cyberspace.

We are particularly interested in these fields;

Cybersecurity in Pervasive/Ubiquitous Computing
Contacts: Nicola Dragoni, Christian D. Jensen, Weizhi Meng, Emmanouil Vasilomanolakis

Privacy and Privacy-Enhancing Technologies
Contacts: Christian D. Jensen, Weizhi Meng

Cryptography: Symmetric, Quantum and Post-Quantum
Contacts: Christian Majenz, Tyge Tiessen, Carsten Baum, Luisa Siniscalchi

How to implement secure voting.

Contact: Luisa Siniscalchi

Description: This project is focused on understanding and implementing how to realize secure voting between three users and what are the security requirements of the realized solution.

Study of threshold signature schemes

Contact: Luisa Siniscalchi

Description: This project is focused on understanding threshold signature schemes. At a high level, in threshold signature schemes, a new signature can only be generated cooperatively among a set of multiple users, but no user alone is able to generate a new signature. The project studies threshold signature schemes and their applications.

Password Authenticated Key Exchange

Contact: Carsten Baum

Prerequisites: a solid understanding of modular arithmetic and discrete mathematics in general

How the Signal app hides its memory access patterns

Contact: Carsten Baum

Prerequisites: a solid understanding of modular arithmetic and discrete mathematics in general

Estimating block cipher security with SAT-solvers

Contact: Tyge Tiessen

Description The difficulty of breaking block ciphers is expected to grow exponentially with the size of the key. In this project the goal is to give an estimate of the time that it would take a SAT-solver to break a block cipher by extrapolating from the time it takes to break reduced-key size variants.

Email Link Protection through Nudging

Contact: Christian D. Jensen

Description: Many workflow systems rely on emails to alert users about tasks that they need to complete; these emails often contain links to the local back-end system which the users click in order to complete their tasks. This clashes with the general advice to users that they should not click on links in emails or at least hover the mouse over the link to identify the destination before clicking it. Different approaches to URL rewriting or sandboxing have been proposed, but this project explores an approach that relies on nudging, to help users only click on links that they can safely click on. The idea is to write a filter for the email user agent, e.g. Thunderbird, Outlook or Chrome, that rewrites the emails to change the colour of links in the following way. Links to resources inside the organisation should be coloured green, links to resources that have been evaluated as "trustworthy", e.g. they appear on an Allow List, should be coloured yellow and links to resources outside the organisation that have not previously been put on the Allow List should be coloured red — the actual colours can be changed if the simple traffic light metaphor appears inadequate. The project therefore has three main components, a prototype implementation of a plug-in to Thunderbird, Outlook or Chrome, which implements the URL rewriting, definition of a metric to measure the trustworthiness of links in emails, and an evaluation of the proposed metric in the implemented prototype.

It is a condition for this project, that all developed code and policies is released under an Open Source Software License.

6G Connection Strategy with Blockchain

Contact: Weizhi Meng

Description: 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.

Blockchain-based Enterprise Resources Planning (BlockERP)

Contact: Weizhi Meng

Description: 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.

Supporting Zero Trust Architectures using the KeyNote Trust Management System

Contact: Christian D. Jensen

Description: One of the central tenets in Zero Trust Architectures is: "Never Trust, Always Verify!", but there is a wide scope for interpretation and implementations of ZTA.

25 Years ago, the KeyNote system (defined in RFC 2704) was proposed as an assertion based access control mechanism, built on many of the principles that are today underpinning ZTA. The work that resulted in Keynote is described in a number of papers that are available at Columbia University (https://www.cs.columbia.edu/ angelos/keynote.html), where source code for a prototype can also be downloaded.

This project examines the specification of Zero Trust Access Control Policies as KeyNote assertions, and evaluating their use in a few self-defined prototype applications. The above mentioned source code has probably not been maintained for more than a decade, so the first few steps include updating the system to use modern APIs and/or porting it to a modern programming language, such as Rust. Secondly, the project must identify central concepts from access conrol in the current definitions of ZTA, in particular NIST SP800-207 (`https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf`) and the DoD ZTA Reference Architecture (`https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf`). Finally, the project must develop mappings from these concepts onto the assertions supported by KeyNote and demonstrate the applicability of the proposed mappings through a few simple reference implementations.

It is a condition for this project, that all developed code and policies is released under an Open Source Software License.