Project Profile

ENTA

Uncovering encrypted network traffic

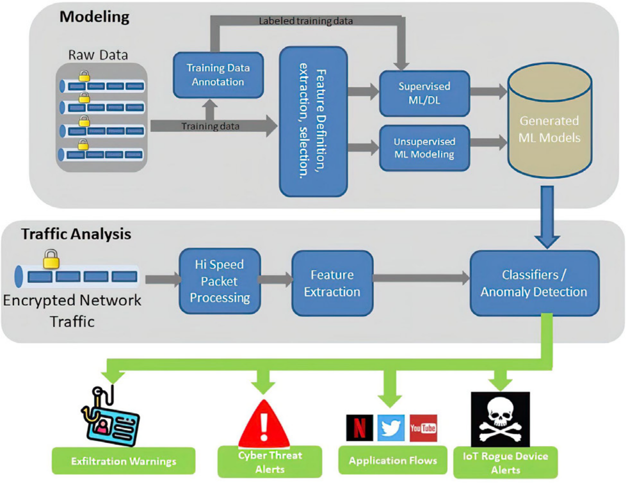
The ITEA project ENTA (Encrypted Network Traffic Analysis for Cyber Security) will provide visibility into encrypted network traffic as well as detect network threats. In doing so, public safety can be improved, the costs of cybercrime can be reduced, and new AI-based cybersecurity business opportunities can be created.

Addressing the challenge

While the growth of Internet traffic encryption is beneficial to the data privacy of end-users and organisations, it renders many existing cybersecurity toolchains useless due to their inability to examine traffic content. This makes it harder for IT security analysts to distinguish between legitimate and illegitimate traffic, preventing operators from blocking illegal applications, enforcing policies, and detecting threats. Additionally, extensive Internet of Things (IoT) deployment has created a new attack surface that increases the opportunity and ease of such threats.

Proposed solutions

To meet the need for tools which can detect cyberattacks within encrypted traffic, the ENTA project will explore two Encrypted Network Traffic Analysis use-cases: 1) the identification of encrypted applications and associated traffic classes and 2) support for the automated discovery of encrypted IoT devices and detection of rogue IoT devices. These will be centred around a platform which will integrate network traffic analysis services on encrypted traffic and will allow life-cycle management of the machine learning development process. Analytics are built on the platform using machine/deep learning techniques that leverage temporal and spatial traffic characteristics. The approach does not inspect payload data i.e., it preserves end-user privacy and complies with GDPR regulations. The platform will also support a number of basic building blocks for machine/deep learning-based network traffic analysis to enable near-product quality prototyping with a focus on scalability, flexibility and near real-time performance.



< ENTA solution diagram

Projected results and impact

Although some existing tools can carry out anomaly detection or TLS fingerprinting with coverage for encryption, these scale to traffic rates of just 1 Gbps. In creating real-time solutions for up to 100 Gbps, ENTA aims to detect at least 90% of encrypted traffic classes accurately. In addition, threats generated due to compromised and rogue IoT devices will be detected with high accuracy and low false positives. This enhanced corporate security and general network availability will reduce the costs of cyberattacks, providing a strong return on investment while also reducing the risk of dangerous accidents in some industries. Overall, cybercrime costs over USD 600 billion per year – a 14% 'tax' on the worldwide Internet economy – which is driving a compound annual growth rate of 10% in the cybersecurity market, expected to be worth USD 248 billion in 2023. ENTA has identified three primary exploitation routes for project outputs: deployment as standalone products, integration into managed security service provider (MSSP) software, and licensing as part of larger security vendor products. This results in a broad potential userbase, from IT security departments to law enforcement agencies working on public safety, through which ENTA intends to make a sizeable contribution to reducing cybercrime. In addition, Network Operation Centres will obtain better visibility to encrypted traffic enabling more effective management (e.g., QoS, Policy enforcement) of benign traffic.

Project partners

ENTA
20020

Canada

DALHOUSIE UNIVERSITY

SOLANA NETWORKS

Switzerland

Together ahead. RUAG

Austria

Beia CONSULT INTERNATIONAL

Türkiye

KAREL

United Kingdom

C4FF Developing the Future

Spain

mtp DIGITAL BUSINESS ASSURANCE

Project start
October 2021

Project end
March 2025

Project leader
Biswajit Nandy, Solana Networks

Project email
bnandy@solananetworks.com

Project website
https://project-enta.com/