ACK 2024
논문집 Annual Conference of KIPS 2024

신진학자 워크숍

AI-based Intrusion Detection and App Identification for Security

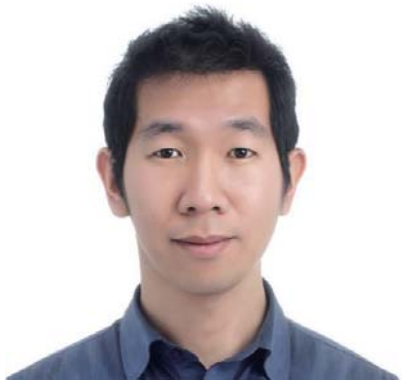
이현우 교수
(한국에너지공과대학교)

AI-based Intrusion Detection and App Identification for Security

Hyunwoo Lee
Korea Institute of Energy Technology (KENTECH)
email: hwlee@kentech.ac.kr / lab page: https://ess.kentech.ac.kr

KENTECH
한국에너지공과대학교
Korea Institute of Energy Technology

Introduction



Hyunwoo Lee

KENTECH
Korea Institute of Energy Technology

Assistant Professor

Career

Assistant Professor at KENTECH (2022.9 - present)
Energy System Security Lab. in Institute for Energy AI

Postdoc Research Associate at Purdue University (2020.8 - 2022.8)
Hosted by Prof. Elisa Bertino and Prof. Ninghui Li

Education

M.S./Ph D. at Seoul National University (2015-2020)
Advised by Prof. Taekyoung Kwon
Dissertation: TLS Extensions for Middleboxes and Edge Computing

B.S. at Seoul National University (2004-2011)

Selected Publications

maTLS: How to Make TLS middlebox-aware? (NDSS '19)
TLS 1.3 in Practice: How TLS 1.3 Contributes to the Internet (WWW '21)
VWAnalyzer: A Systematic Security Analysis Framework for the Voice over WiFi Protocol (ASIACCS '22)
An Infection-Identifying and Self-Evolving System for IoT Early Defense from Multi-Step Attacks (ESORICS '22)
AppSniffer: Towards Robust Mobile App Fingerprinting Against VPN (WWW '23)
ZTLS: A DNS-based Approach to Zero Round Trip in TLS handshake (WWW '23)
Towards Efficient Privacy-Preserving Deep Packet Inspection (ESORICS '23)
Sharing cyber threat intelligence: Does it really help? (NDSS '24)

Introduction

Welcome to Energy System Security Lab. at KENTECH

Energy System Security Lab. (esslab) aims to design and implement secure energy AI systems, and verify security of them!

Security by Design

We design and implement security building blocks for energy systems, including public key infrastructure (PKI) or security protocols (e.g., TLS or IPsec)

Security Verification

We verify security and privacy properties of energy AI systems based on specifications or implementations, leveraging formal or informal methods

AI-driven Security

We study machine-learning-based security building blocks such as intrusion detection systems (IDS) to make energy systems secure and trustworthy

Research Area

- **Security by Design:** Designing New Security Protocols
- **Security Verification:** Verifying Properties of Security Protocols
- **AI-driven Security:** Implementing AI-based Security Systems

Introduction

We are living in the era of the Internet of Things (IoT)

Introduction

We are living in the era of the Internet of Things (IoT)

- Power grids / plants
- Mobile devices / networks
- Vehicles
- …

Introduction

We are living in the era of the Internet of Things (IoT)

We are dreaming autonomous systems with Artificial Intelligence (AI)

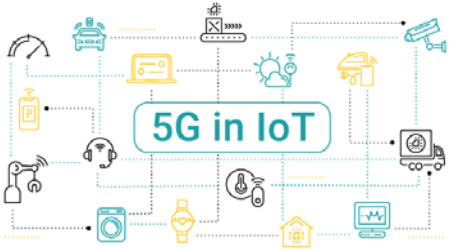
Introduction

We are living in the era of the Internet of Things (IoT)

We are dreaming autonomous systems with Artificial Intelligence (AI)

- Automated (Free from repetitive work)
- Energy/resource-efficient
- Cost-efficient

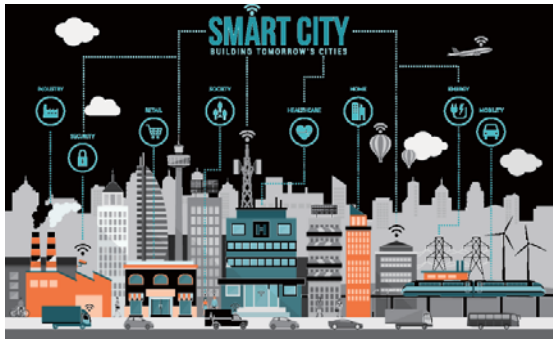
Introduction

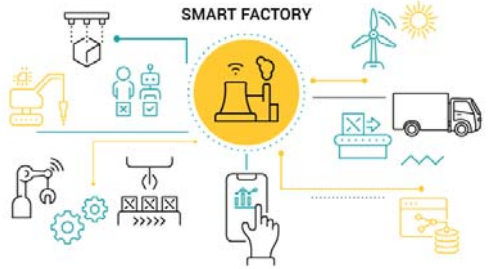


Diverse Networking Infrastructures

- Cloud/edge computing
- Innovative mobile networks

Introduction

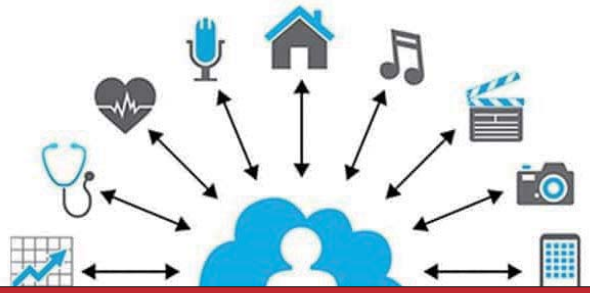


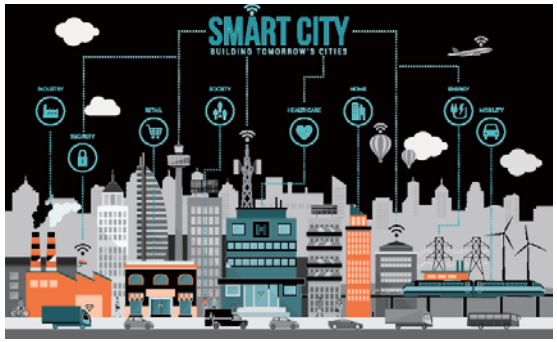


Value-added Services

- Smart grids
- Smart cities and smart factories

Introduction



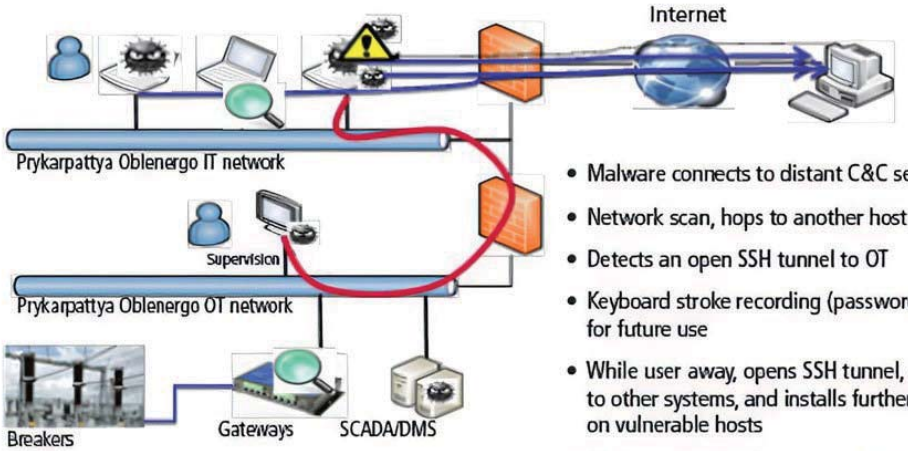


Network Security is Important!

Larger number of connected devices means larger attack surface

- Smart grids
- Smart cities and smart factories

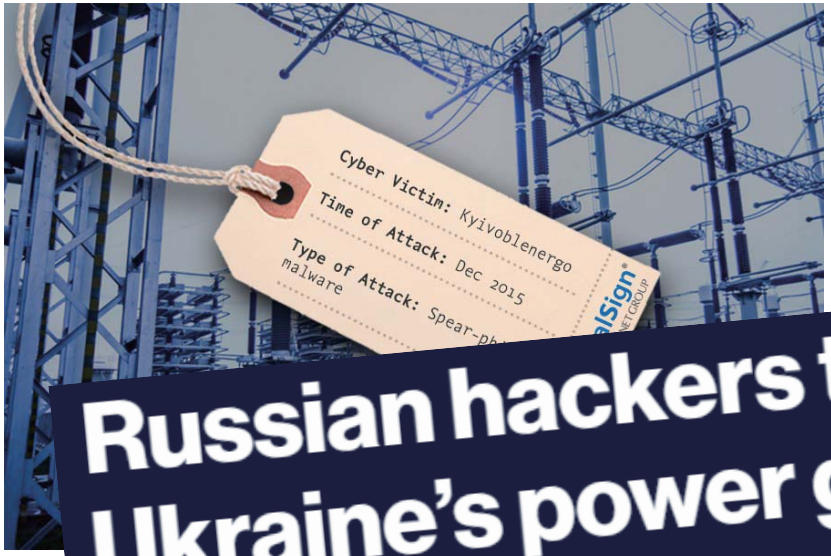
Introduction

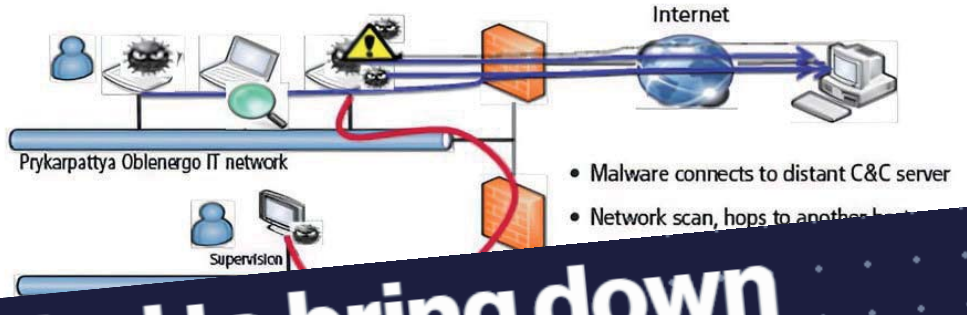


2015 Ukraine power grid hack

- Advanced Persistent Threat (APT) attack by a Russian group “Sandworm”
- Power outages for 230K consumers in Ukraine for 1-6 hours

Introduction





Russian hackers tried to bring down Ukraine's power grid to help the invasion

As Russia's ground war stalls, hackers attempted to cause a blackout for two million people.

April 12, 2022

201 ack

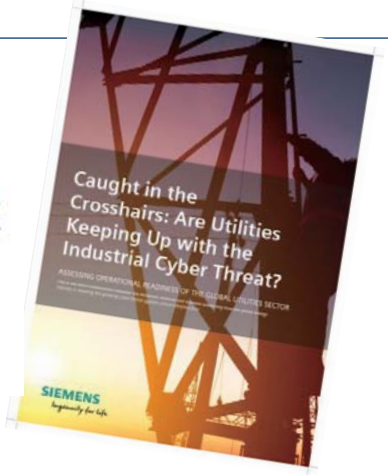
- Advanced Persistent Threat (APT) attack by a Russian group "Sandworm"
- Power outages for 230K consumers in Ukraine for 1-6 hours

Introduction

Survey: 56 percent of utilities have faced a cyberattack in the last year

Published on October 15, 2019 by Jaclyn Brandt

- Data loss
- Operations shutdown



Other Attacks on Infrastructures

- TRITON malware attack in 2017 toward a Saudi petrochemical plant, purposefully designed to cause loss of life
- Attack toward CPC Corp., Taiwan's state-owned energy company, causing the company's payment system into chaos

High Cost to Recover From

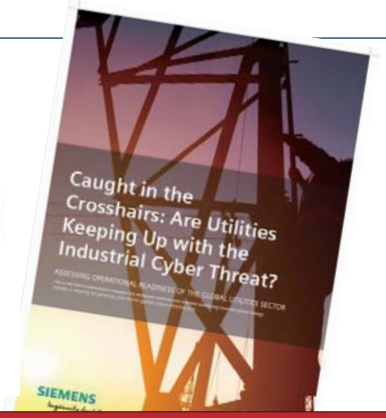
- The SolarWinds hack will cost an estimated $100 billion

Introduction

Survey: 56 percent of utilities have faced a cyberattack in the last year

Published on October 15, 2019 by Jaclyn Brandt

- Data loss
- Operations shutdown



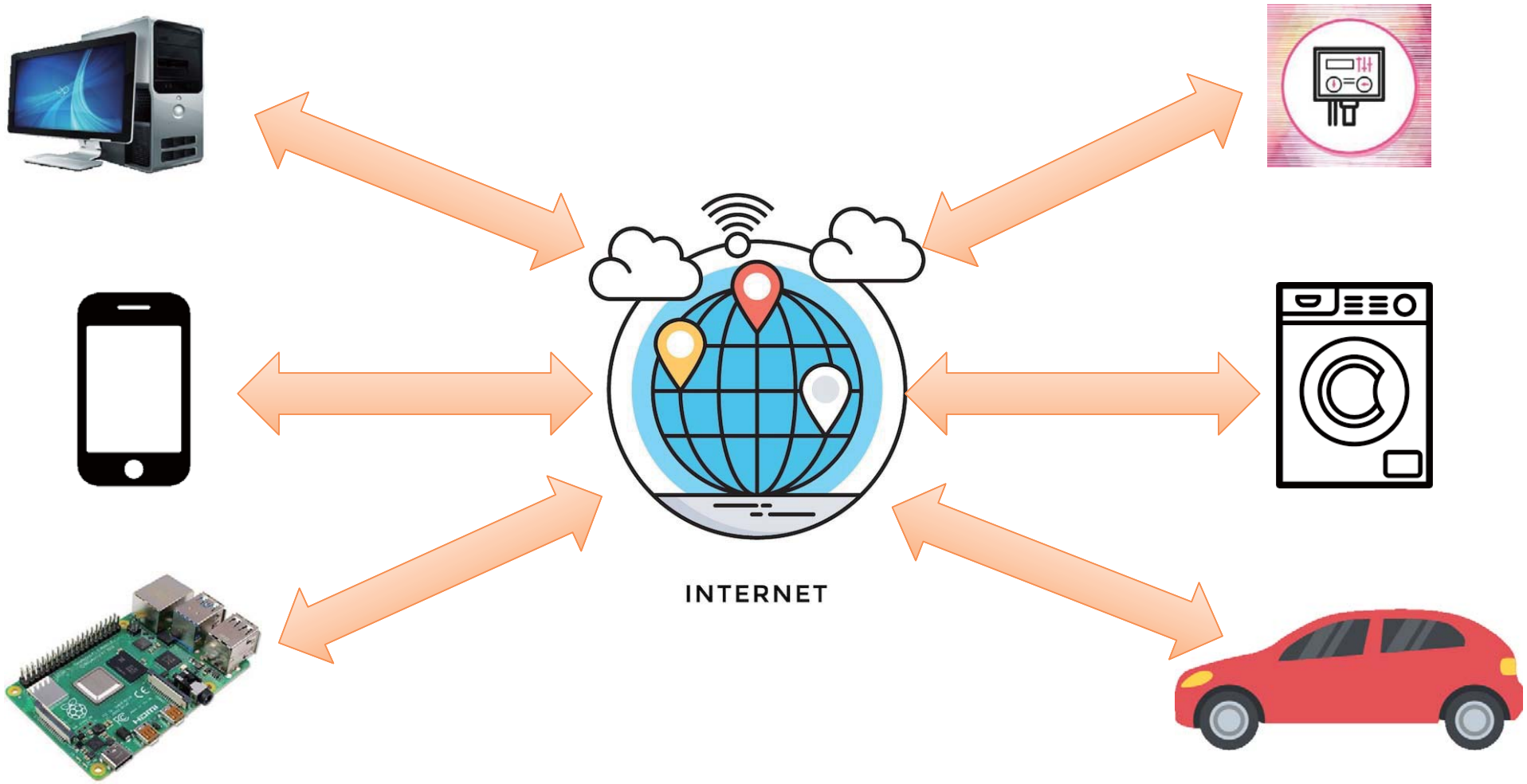
Again, Network Security is Important!

How can we Make the Infrastructures Trustworthy and Secure?

High Cost to Recover From

- The SolarWinds hack will cost an estimated $100 billion

End-to-end Communication



End-to-end Communication

Two Ways to Secure the Networking

Encryption Allows only authorized ones to read and write data

Middlebox Detect any malicious activities or data

- Web Application Firewalls
- Intrusion Detection System

Topic 1: Security by Design

1 Designing new security

[maTLS (NDSS'19), ZTLS (WWW'23), MT-DPI (ESORICS'23)]

Can we design a new protocol to address issues in practice?

2 Verifying properties of security protocols

[TLS 1.3 (WWW'21), TELEPORT (AsiaCCS'21), VWAnalyzer (AsiaCCS'22), CTI-Lense (NDSS'24)]

Are encryption protocols well designed or deployed?

Topic 3: AI-driven Security

Encryption

3 Implementing AI-driven security applications

[IoTEDef (ESORICS'22), AppSniffer (WWW'23)]

Middlebox

Can we improve security middleboxes with AI?

Identifying infection vectors from later step attacks

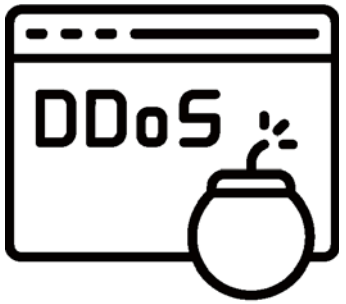
Paper **IoTEDef: An Infection-Identifying and Self-Evolving System for IoT Early Defense from Multi-Step Attacks** (ESORICS '22)

Lots of attacks include multi-steps: Advanced Persistence Threats (APTs)

The main purpose of APT attacks is to acquire persistence on target systems

Port Scanning

Zero-day or Stealthy Attacks



DDoS Attack

It is challenging to identify early-stage attacks

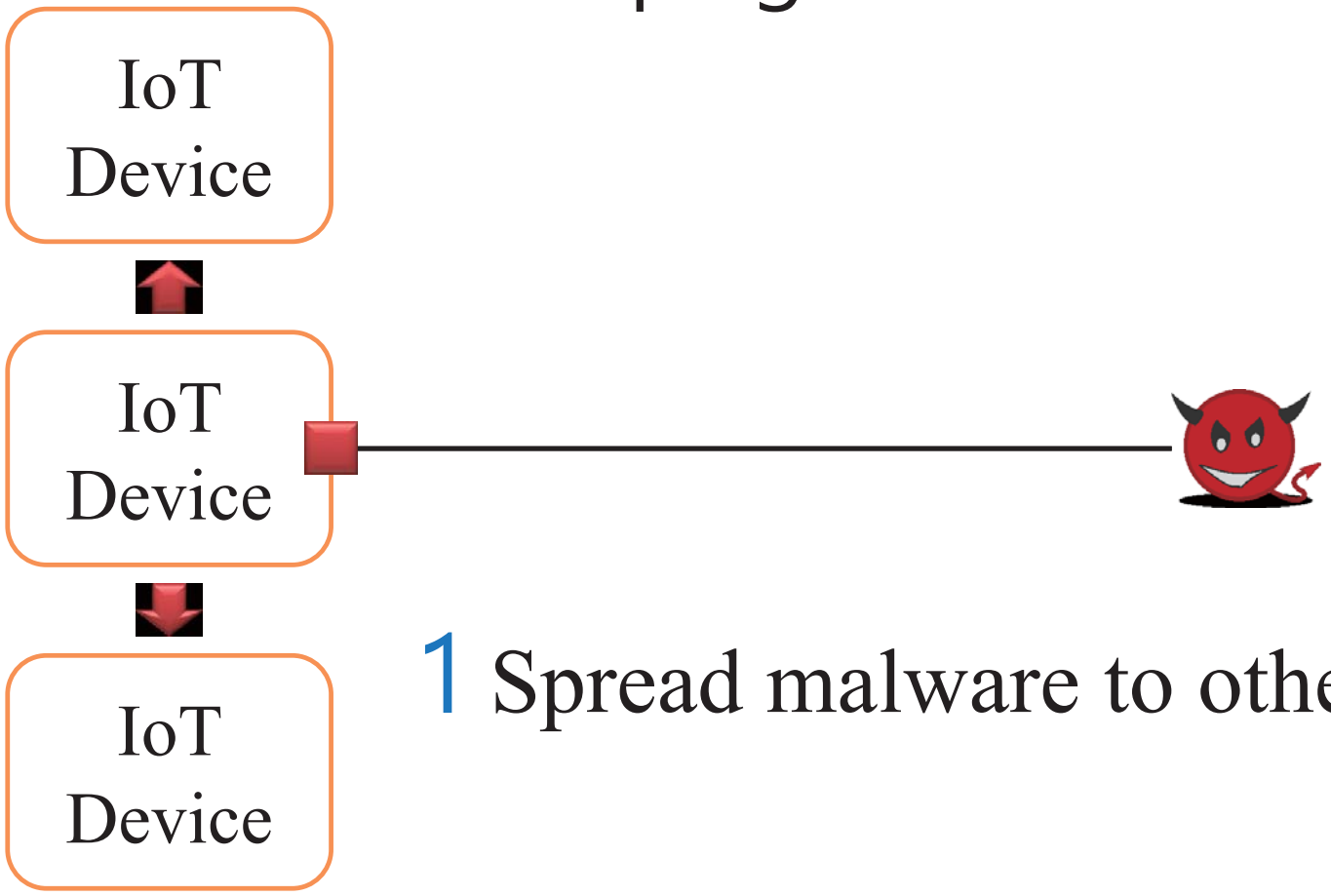
Persistent Attack Campaigns

IoT
Device

Persistent Attack Campaigns

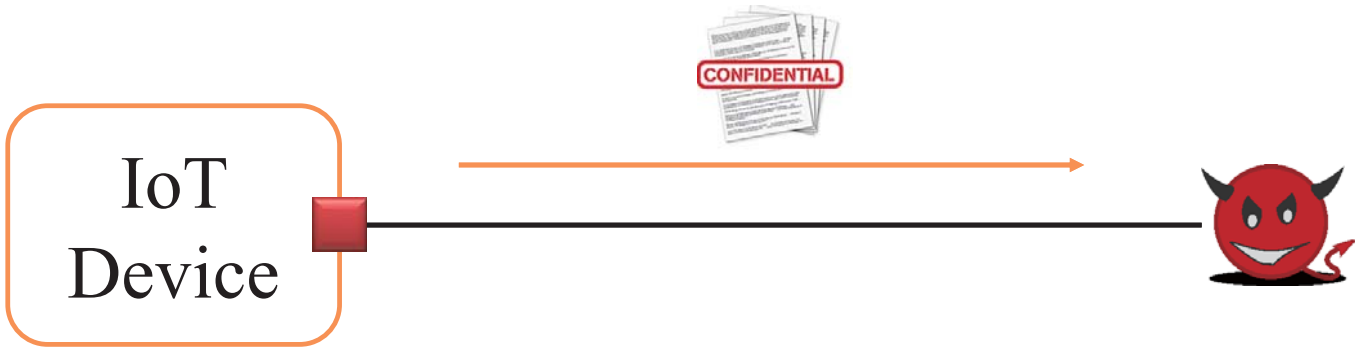
Persistent Attack Campaigns

Persistent Attack Campaigns



1 Spread malware to other devices

Persistent Attack Campaigns



1 Spread malware to other devices

2 Ex-filtrate confidential data

Detecting attacks at an early stage and identifying the infection vectors are critical

Early detection is **challenging**

Early detection is **challenging**

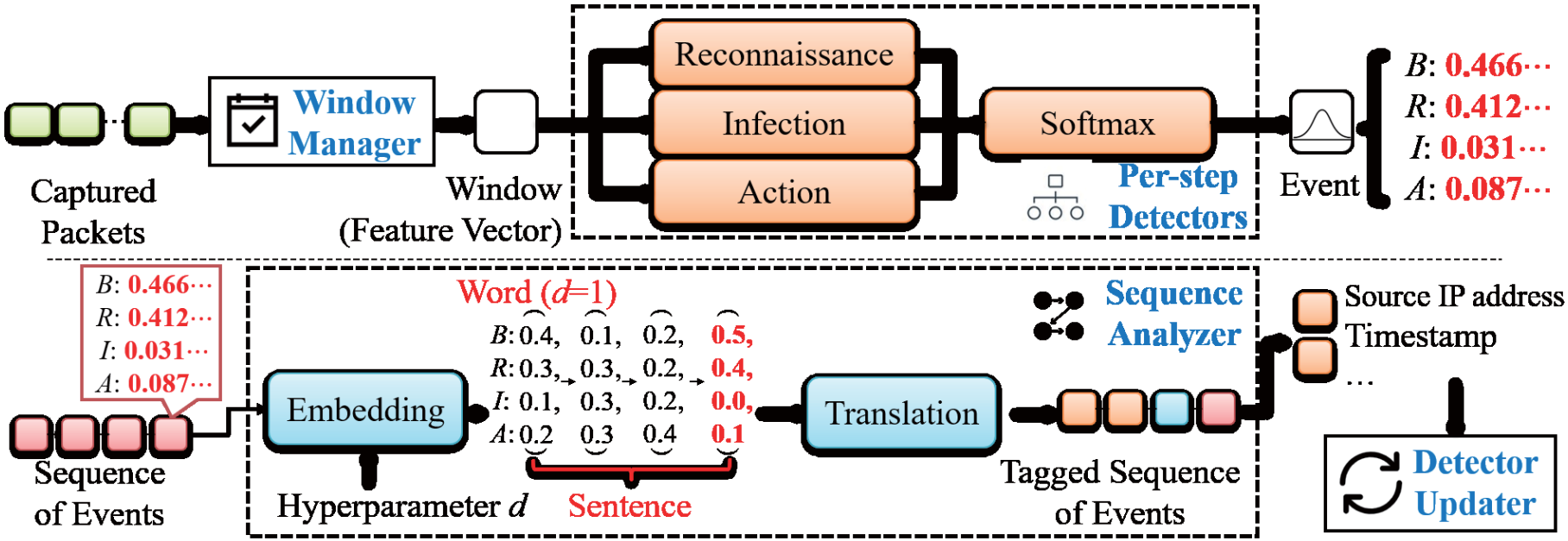
Zero-day attacks

Early detection is **challenging**

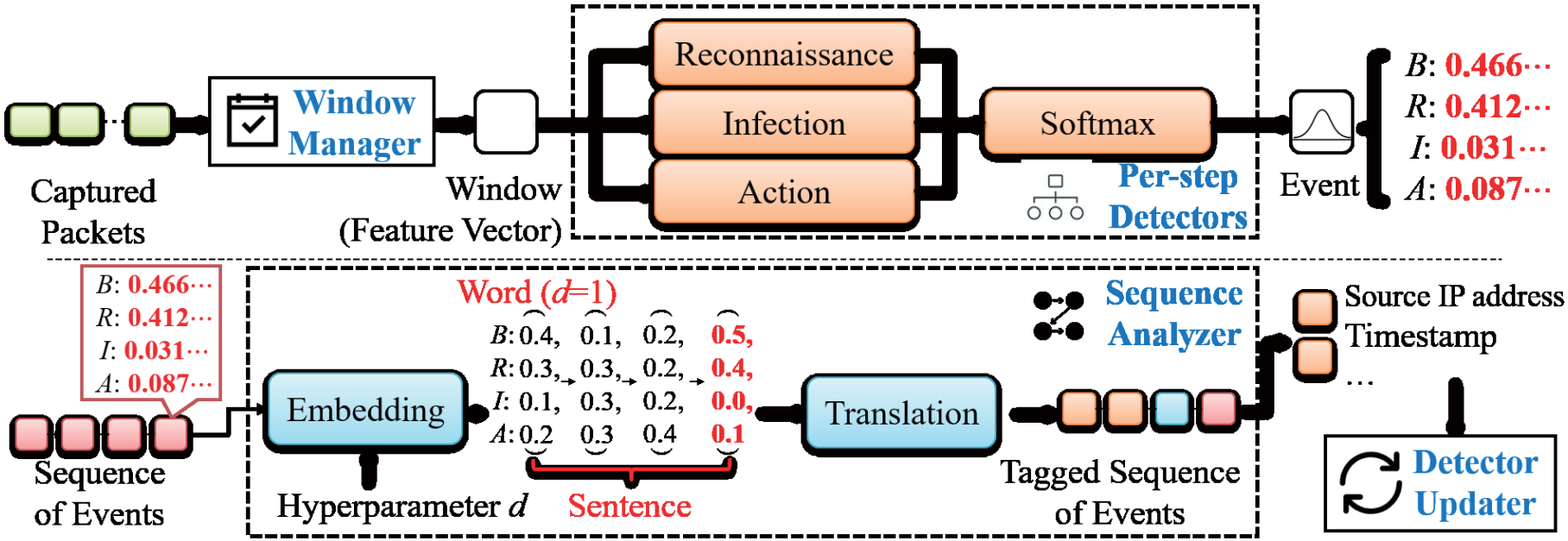
Zero-day attacks

High false positives

We propose IoTEDef,



We propose IoTEDef, an anomaly-based NIDS for IoT devices



We propose IoTEDef,
an anomaly-based NIDS for IoT devices

Main Goal

To detect multi-step attacks **at an early stage**
with high precision and high recall

Our Approach

Our Approach

1 IoTEDef **backward traverses** the log of the events upon detecting anomalies related to a later stage event

Our Approach

1 IoTEDef **backward traverses** the log of the events upon detecting anomalies related to a later stage event

2 IoTEDef **analyzes** these events to identify early stage events related to the later stage event

Our Approach

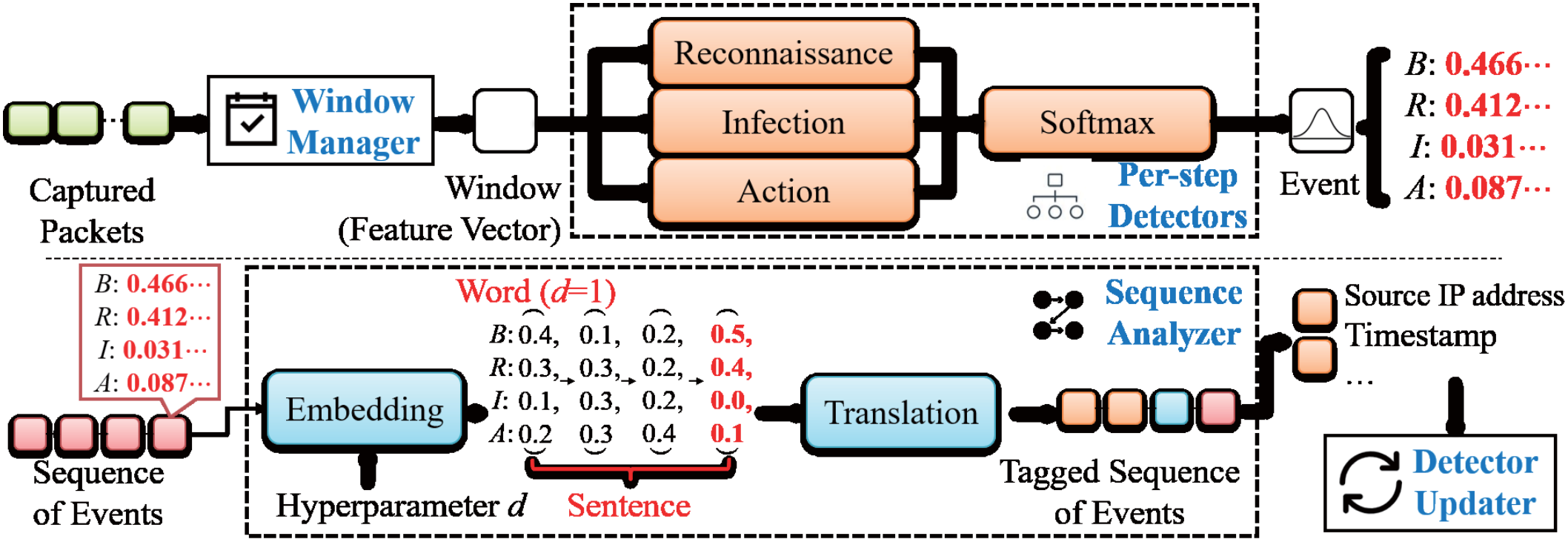
1 IoTEDef **backward traverses** the log of the events upon detecting anomalies related to a later stage event

2 IoTEDef **analyzes** these events to identify early stage events related to the later stage event

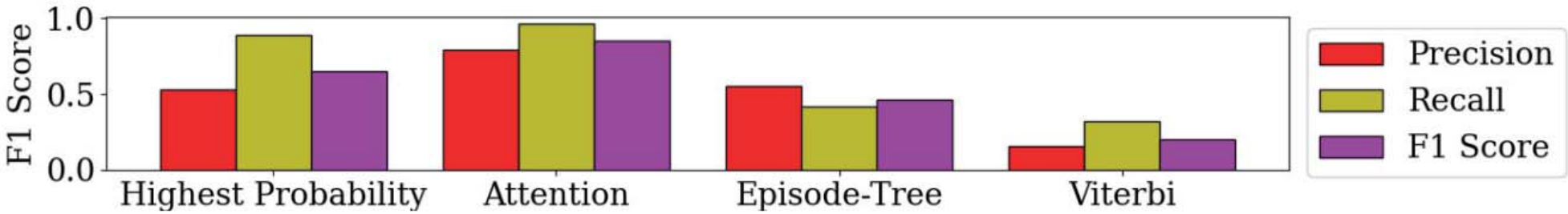
3 IoTEDef **updates** the system based on the identified events to improve the performance of detecting such early stage events

IoTEDef Architecture

An Infection-Identifying and Self-Evolving System for IoT Early Defense

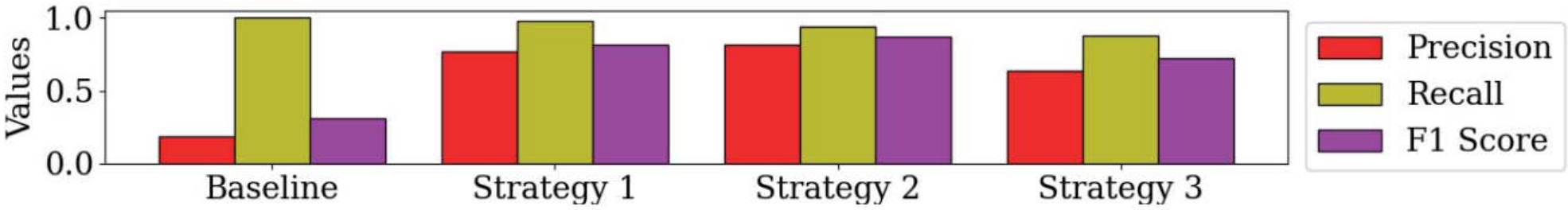


Infection Identification



Attention works best due to its support of the long-term dependency

Self-Evolving



Strategy 1: Update with infection-identified events and non-infection events
Strategy 2: Update with infection-identified events
Strategy 3: Update with non-infection identified events

Summary

Motivation

The early detection of the multi-step attack is important but challenging

Design of IoTEDef

An infection-identifying and self-evolving system for IoT early defense from multi-step attacks

Experiment Result

We show that our approach is feasible and effective

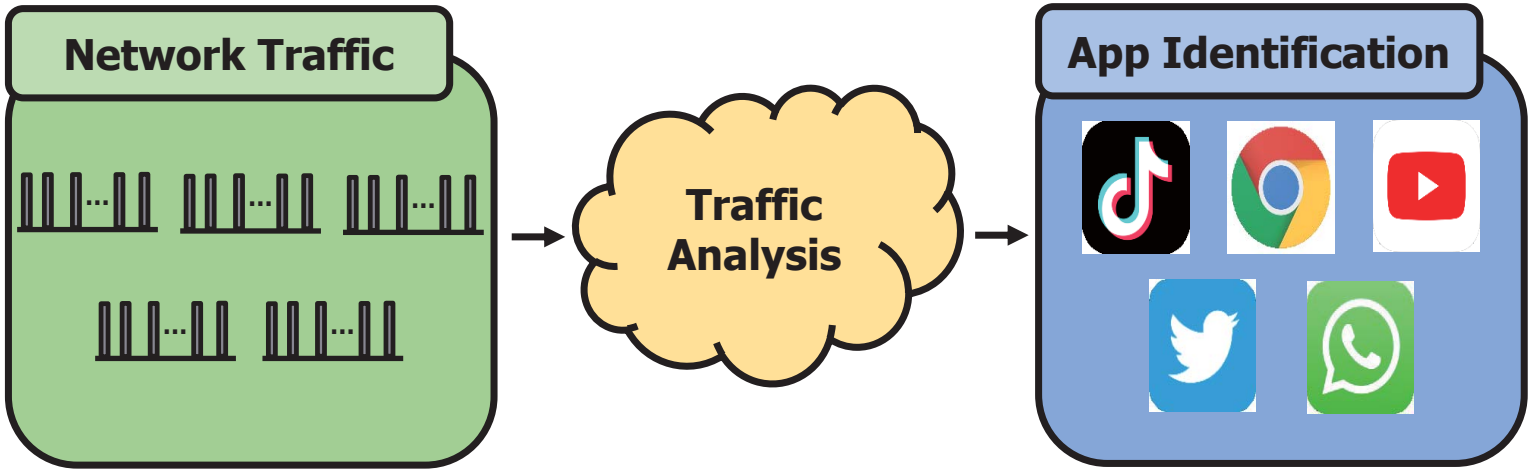
Identifying infection vectors from later step attacks

Paper

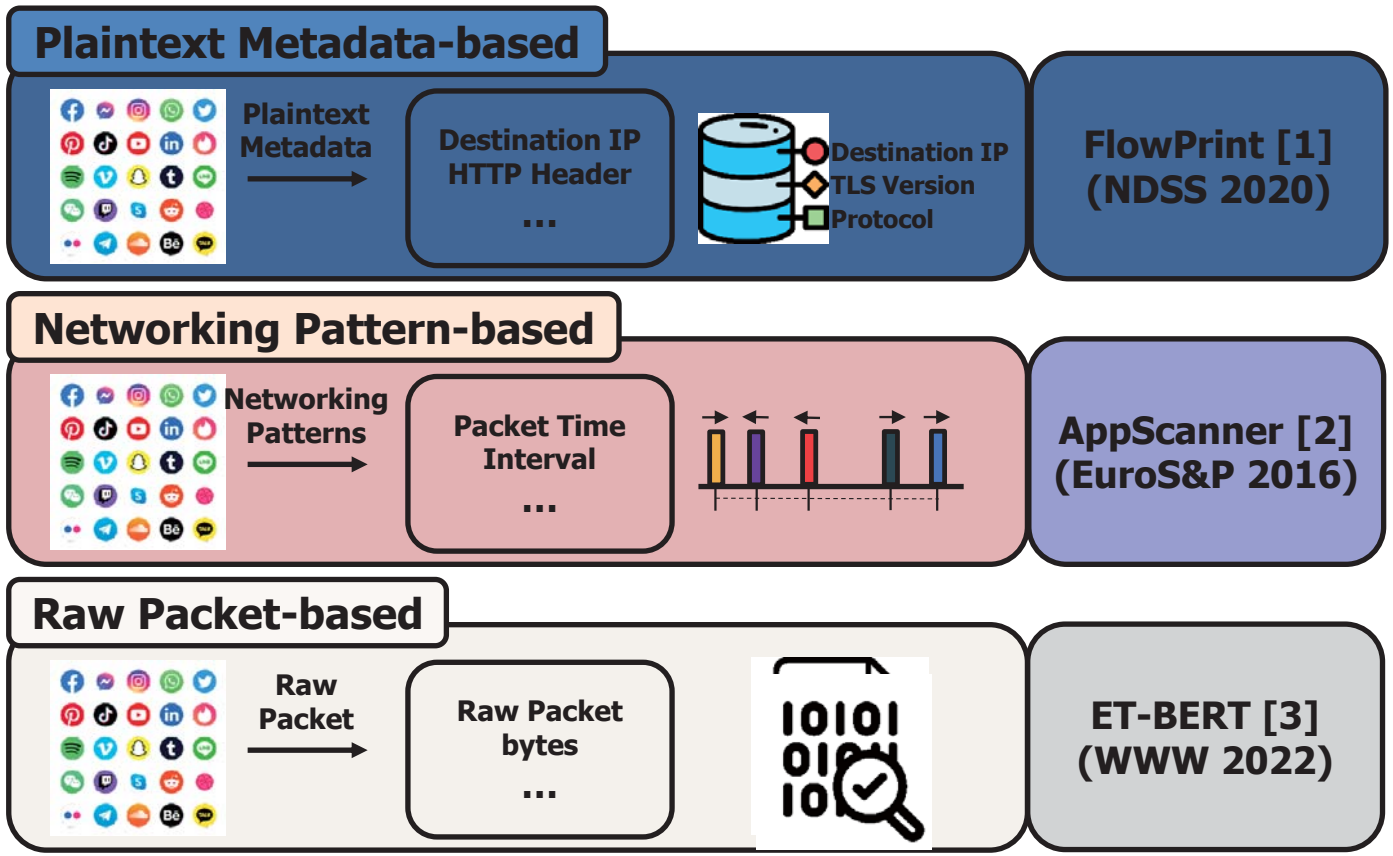
AppSniffer: Towards Robust Mobile App Fingerprinting Against VPN (WWW '23)

Mobile App Fingerprinting identifies mobile apps based on traffic analysis

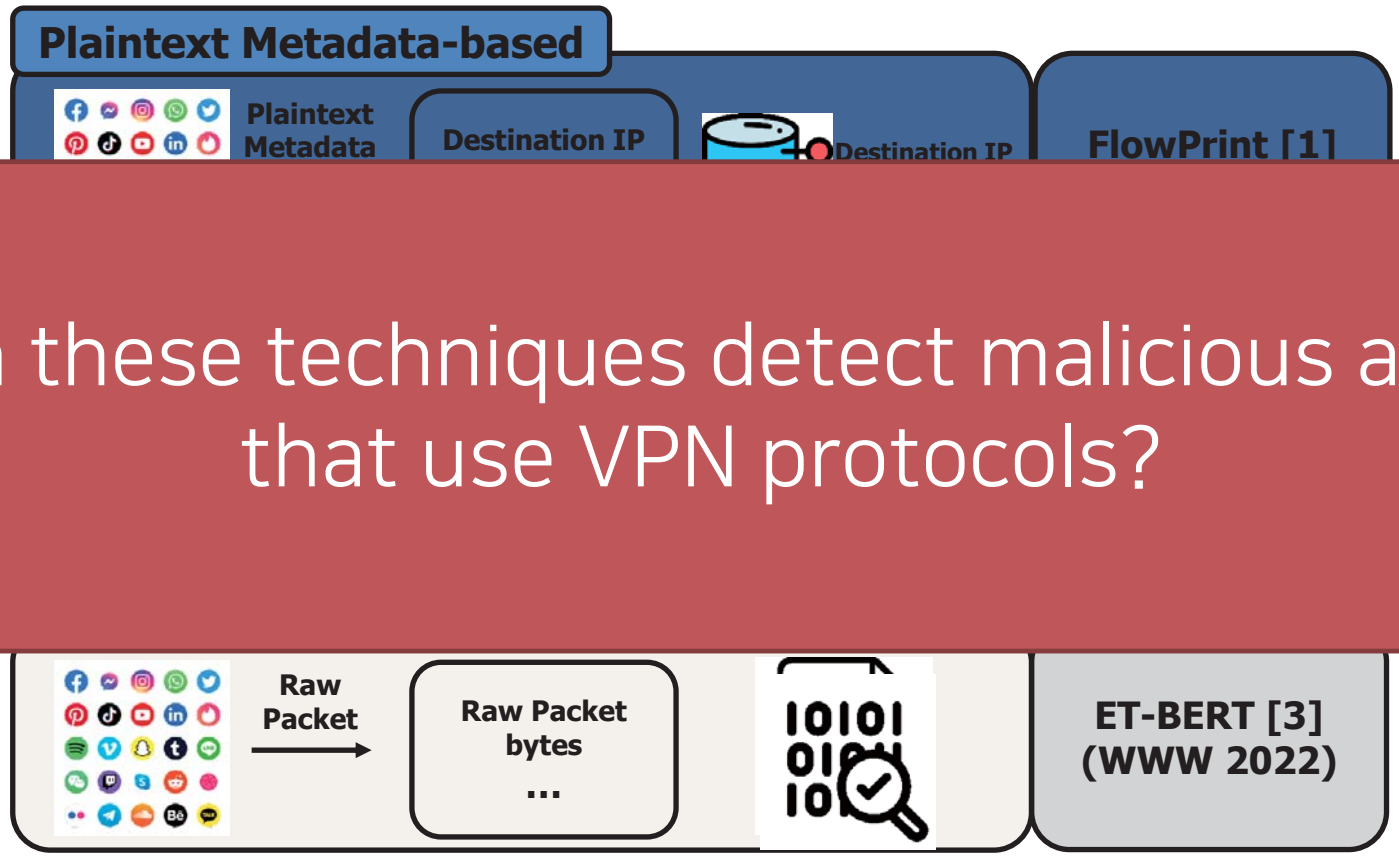
The technique can be used for blocking apps violating a company's policy or performing suspicious activities



Categories of Mobile App Fingerprinting

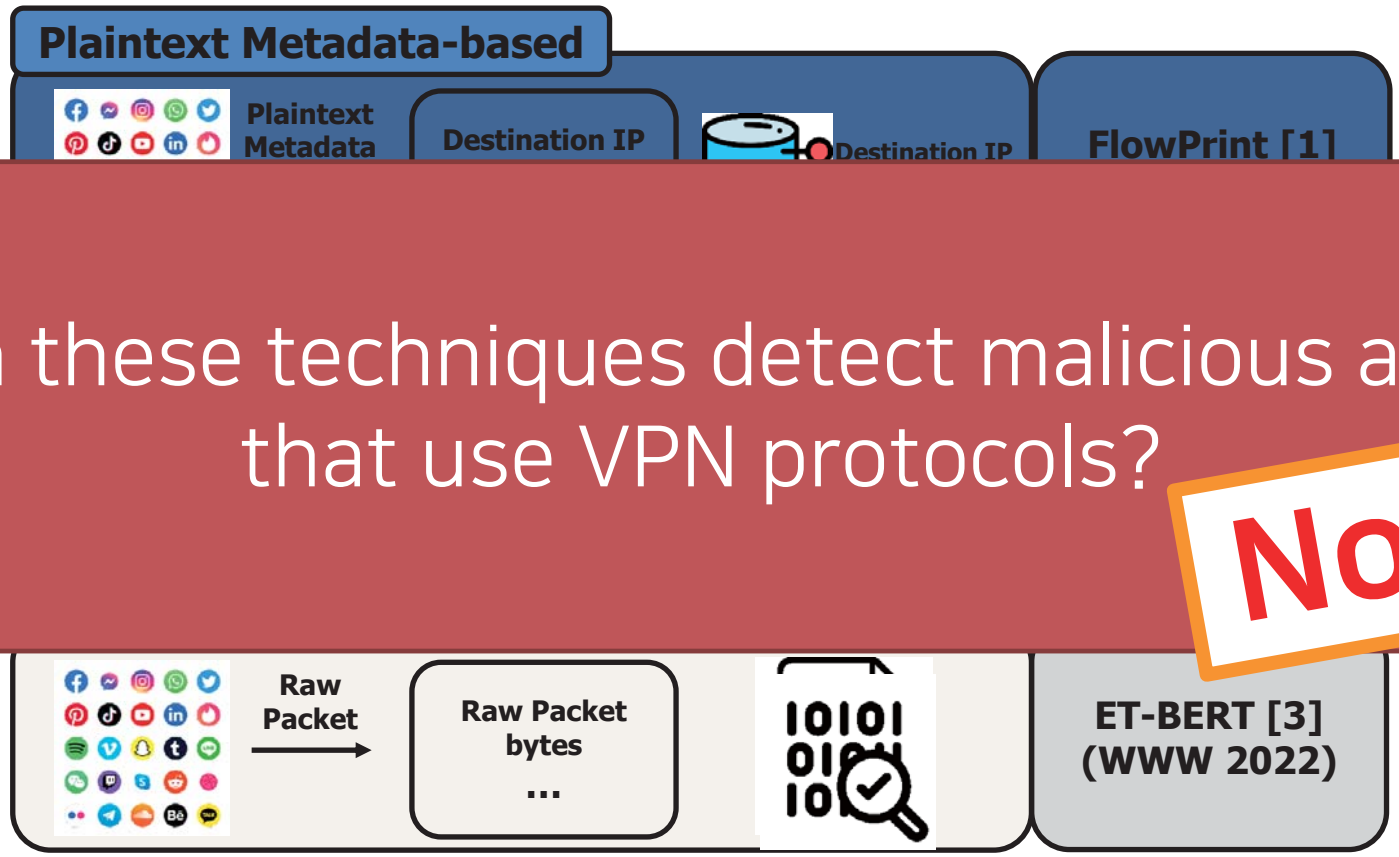


Categories of Mobile App Fingerprinting



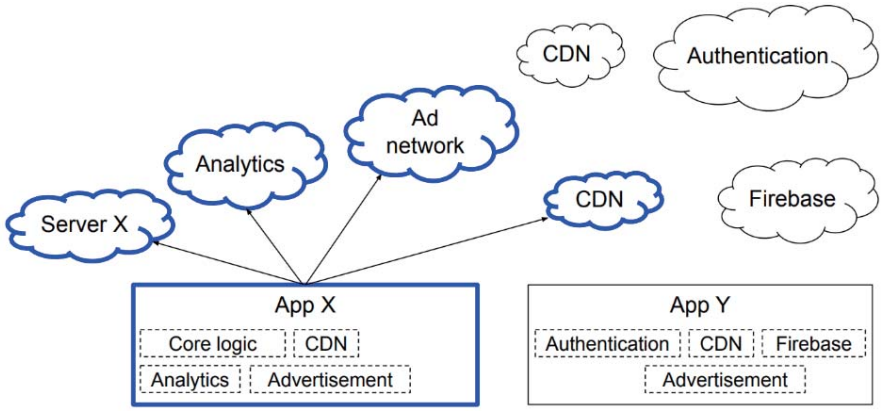
Can these techniques detect malicious apps that use VPN protocols?

Categories of Mobile App Fingerprinting



Limitation of FlowPrint

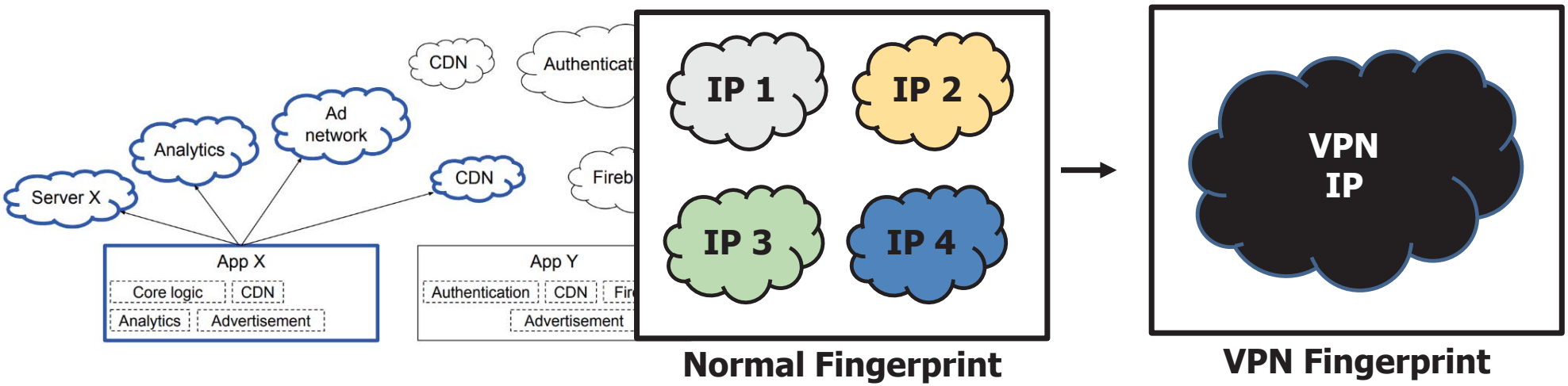
FlowPrint analyzes destination IP addresses of packets to identify mobile apps



***van Ede, Thijs, et al, "FlowPrint: Semi-Supervised Mobile-App Fingerprinting on Encrypted Network Traffic.", *Network and Distributed System Security Symposium (NDSS)*, 2020.**

Limitation of FlowPrint

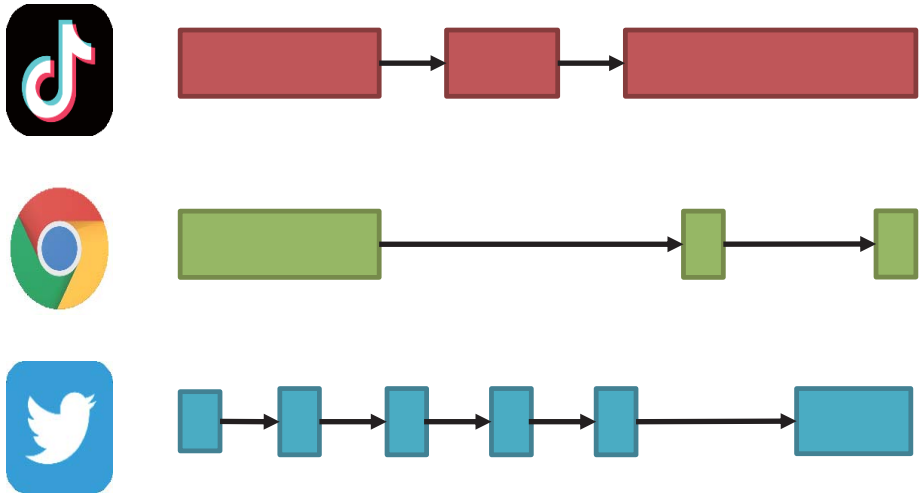
With VPN, destination IP addresses are changed; thus, they cannot be used to identify apps



*van Ede, Thijs, et al, "FlowPrint: Semi-Supervised Mobile-App Fingerprinting on Encrypted Network Traffic.", *Network and Distributed System Security Symposium (NDSS)*, 2020.

Limitation of AppScanner

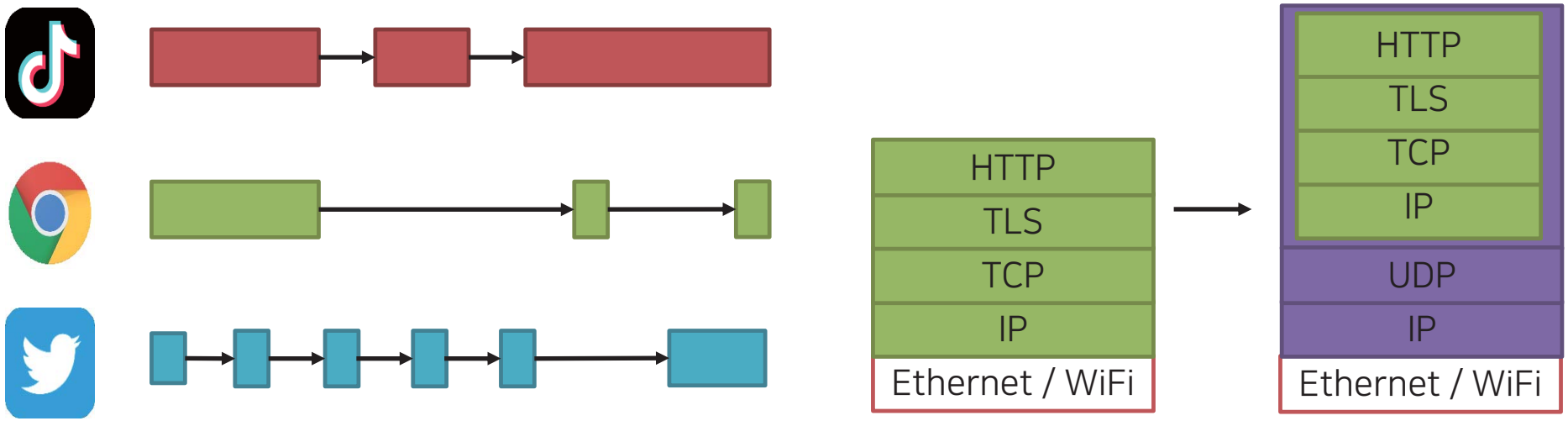
AppScanner analyzes a sequence of packet lengths to identify mobile apps



***Vincent F. Taylor et al, "AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic", *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016.**

Limitation of AppScanner

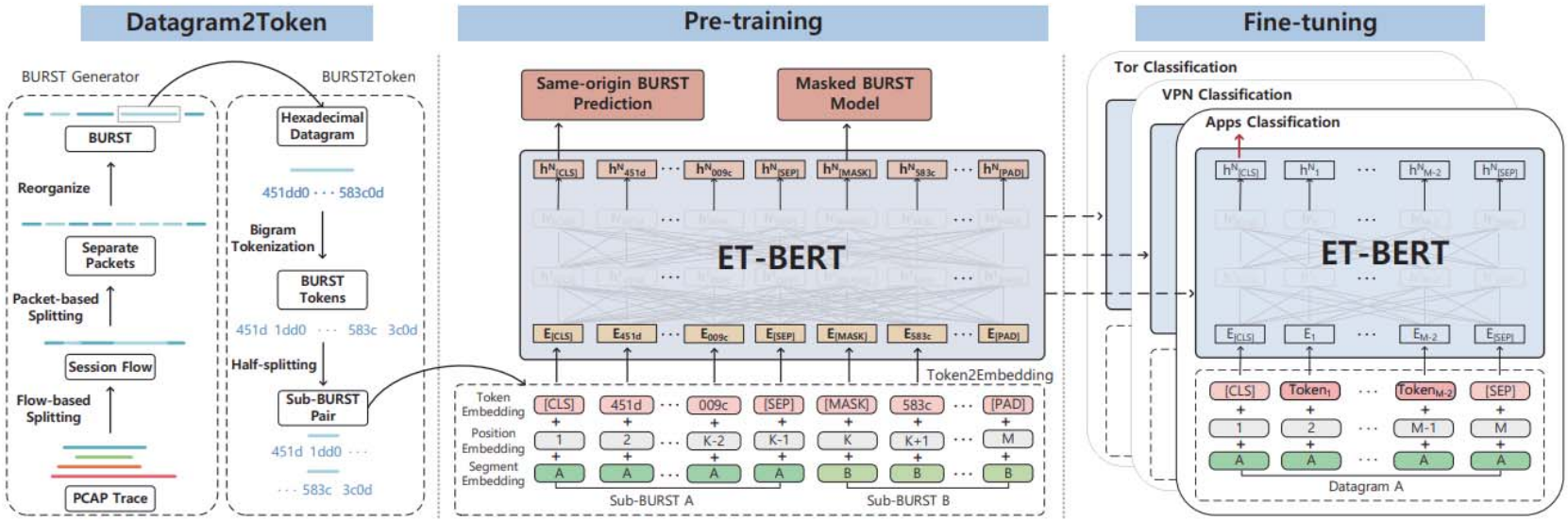
Due to VPN, packet lengths and underlying protocols are changed; thus, traffic patterns are changed



***Vincent F. Taylor et al, "AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic", *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016.**

Limitation of ET-BERT

ET-BERT is a traffic representation model with pre-trains deep contextualized datagram-level representation



***Lin, Xinjie, et al. "ET-BERT: A Contextualized Datagram Representation with Pre-training Transformers for Encrypted Traffic Classification." *ACM Web Conference (WWW)*, 2022.**

Limitation of ET-BERT

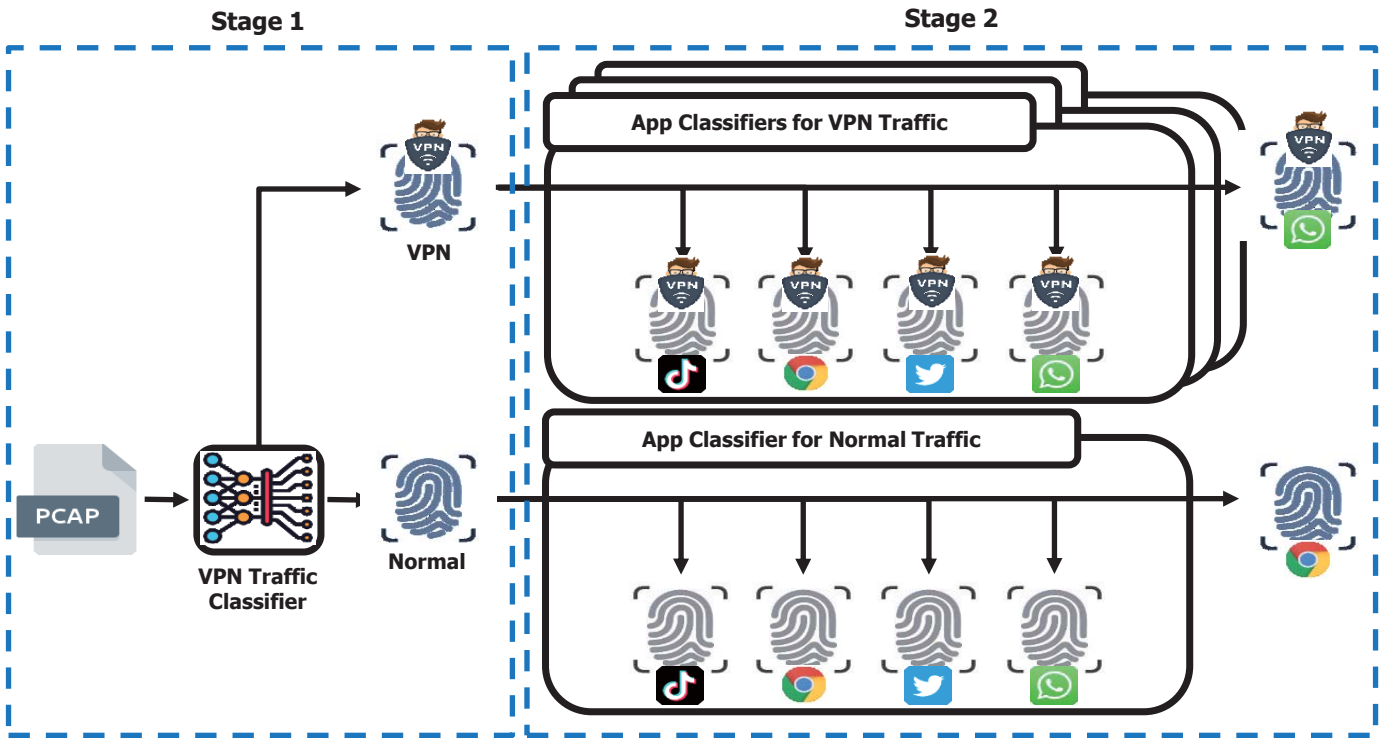
Our analysis shows that ET-BERT highly relies on plaintext features in TCP headers rather than encrypted payloads

TSval : time when the source sent the message
TSecr : time when the destination sent the message

***Lin, Xinjie, et al. "ET-BERT: A Contextualized Datagram Representation with Pre-training Transformers for Encrypted Traffic Classification." *ACM Web Conference (WWW)*, 2022.**

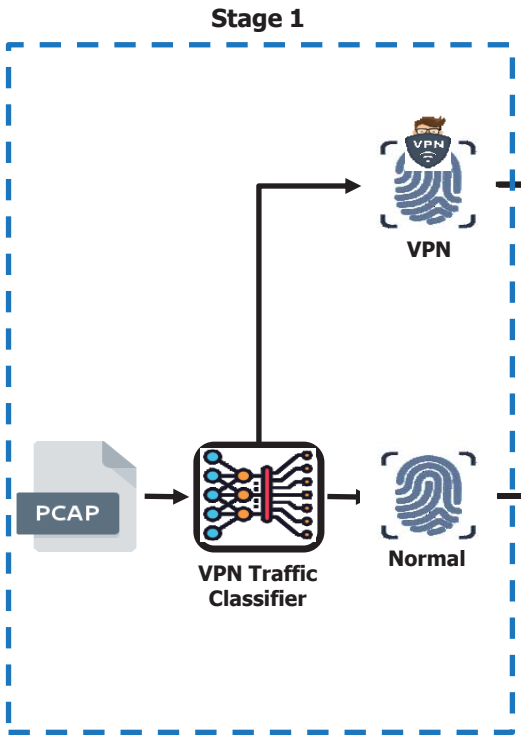
AppSniffer

Stage 1: Distinguish VPN traffic from normal traffic
Stage 2: Identify specific apps from VPN and normal traffic

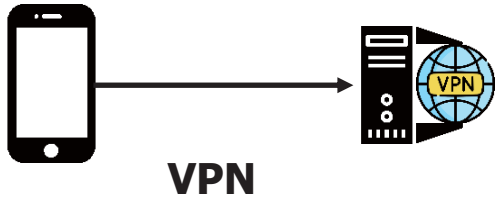


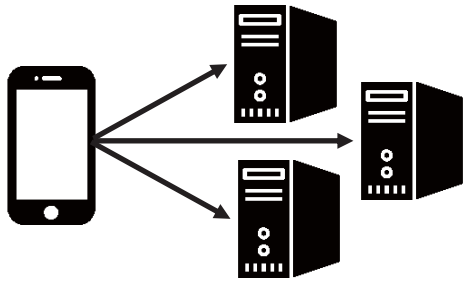
AppSniffer

Stage 1: Distinguish VPN traffic from normal traffic
Stage 2: Identify specific apps from VPN and normal traffic



Key Feature: Number of Flows



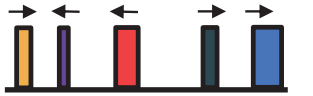


KENTECH
한국에너지공과대학교
Korea Institute of Energy Technology

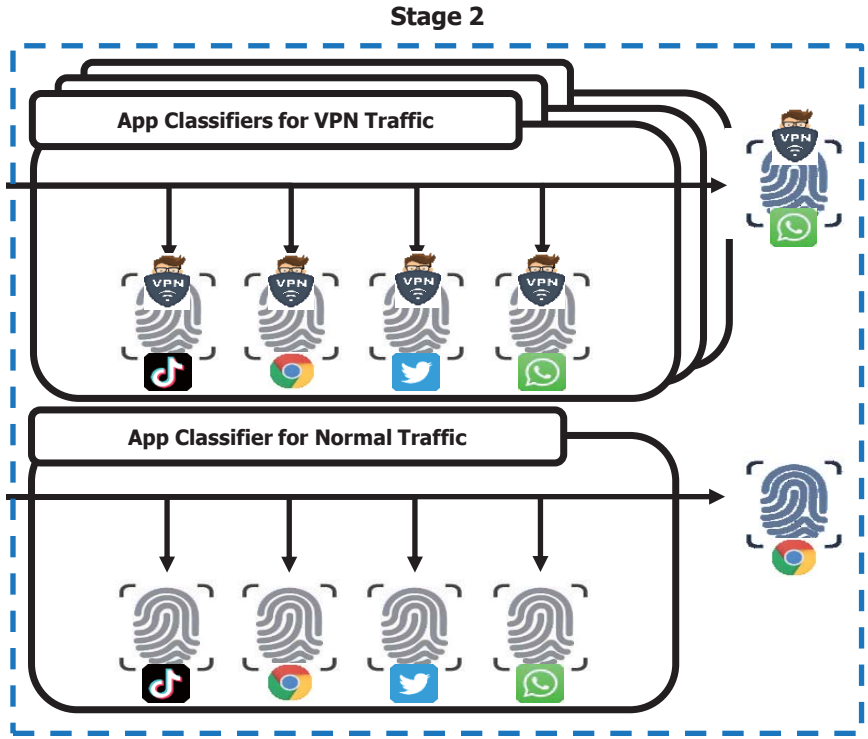
AppSniffer

Stage 1: Distinguish VPN traffic from normal traffic
Stage 2: Identify specific apps from VPN and normal traffic

Key Feature: Packet Length Sequences & Directions

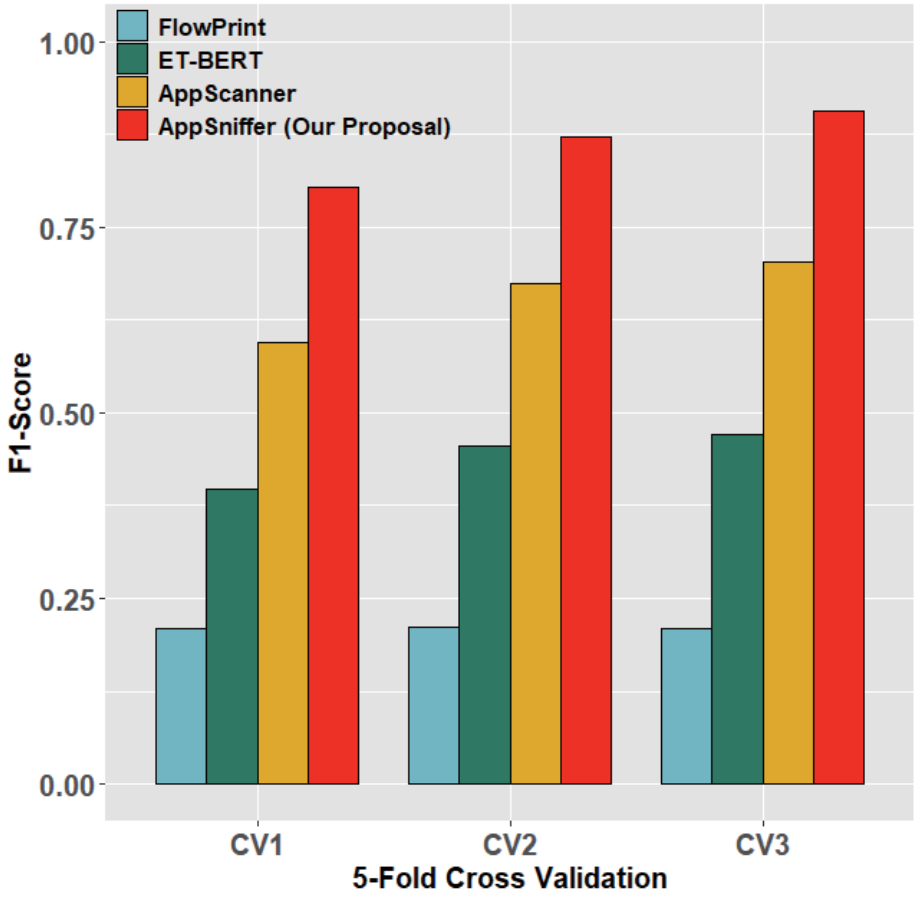


[+11, -5, -17, +13, +29]



Evaluation

AppSniffer achieves the best F1-score (90.63%), comparing with others



Summary

Motivation

The state-of-the-art mobile app fingerprinting techniques are ineffective in identifying apps that use VPN

Design of AppSniffer

A two-stage mobile app fingerprinting framework to identify apps regardless of whether a VPN is used

Experiment Result

We show that our approach is feasible and effective

Thank you!

KENTECH
한국에너지공과대학교
Korea Institute of Energy Technology

Hyunwoo Lee (Assistant professor)
E-mail: hwlee@kentech.ac.kr
Homepage: ess.kentech.ac.kr