AsiaCCS2022
Best Poster Awards

(17:20-17:40 JST)

Poster Co-Chairs:

Naoto Yanai (Osaka University)

Jason Paul Cruz (Osaka University)

Slack channel: #531-poster-session

Poster Session

- 18 posters (in-person:7, online:11)

Separated Formats for In-Person and Online

(but you can vote both independently of your registration)

In-Person Presentations *

- "IoT System Trustworthiness Assurance," Razvan Beuran, Sian En Ooi, Abbie Barbir and Yasuo Tan
- "TTP-Aided Secure Computation using Secret Sharing With Only One Computing Server," Keiichi Iwamura, Ahmad Akmal Aminuddin Mohd Kamal and Masaki Inamura
- "Towards Polyvalent Adversarial Attacks on URL classification engines," Fabien Charmet, Tomohiro Mo... Harry Chandra Tanuwidjaja ... Takeshi Takahashi
- "Decentralized Federated ...arnin... fo... nter... f ...ing ...Ar... ...aly Dete... o... Z...uot... Lian and Chunhua Su
- "Autonomous Network Defence using Reinforcement Learning," Myles Foley, Chris Hicks, Kate Highnam and Vasilios Mavroudis
- "Developing Secured Android Applications by Mitigating Code Vulnerabilities with Machine Learning," Janaka Senanayake, Harsha Kalutarage, Mhd Omar Al Kadri, Andrei Petrovski and Luca Piras
- "Decentralized and Collaborative Tracing for Group Signatures," Maharage Perera, Toru Nakamura, Masayuki Hashimoto, Hiroyuki Yokoyama, Chen-Mou Cheng and Kouichi Sakurai
- Nothing

Online Presentations *

- "Depth, Breadth, and Complexity: Ways to Attack and Defend Deep Learning Models," Firuz Juraev, Eldor Abdukhamidov, Mohammed Abuhamad and Tamer Abuhmed
- "Privacy Guarantees of BLE Contact Tracing for COVID-19 and Beyond: A Case Study on COVIDWISE," Salman Ahmed, Ya Xiao, Taejoong Chung, Carol Fung, Moti Yung and Danfeng Yao
- "A Systematic Study of Bulletin Board and Its Application," Misni Suwito, Bayu Tama, Bagus Santo... Sa...yas... Du... Ho...wan Tan, U...hi...e Yoshifumi and Kouichi ...ak...ai
- "Black-box and Target-specific Attack Against In...rp...able Deep Learning Systems," Eldor Abdukhamidov, Firuz Juraev, Mohammed Abuhamad and Tamer Abuhmed
- "Base64 Malleability in Practice," Konstantinos Chalkias and Panagiotis Chatzigiannis
- "Vulnerability Detection via Multimodal Learning: Datasets and Analysis," Xin Zhou and Rakesh Verma
- "RBMon: Real Time System Behavior Monitoring Tool," Nitesh Kumar, Anand Handa and Sandeep K. Shukla
- "The Personalities of Social Media Posts and Photos," Anne Wagner, Anna Bakas, Daisy Reyes, Shelia Kennison and Eric Chan-Tin

Thank you for Voting

Slack channel: #531-poster-session

Selection of Poster Awards

- We selected **3** posters in total as awards from in-person and online
- Based on your voting scores

- To the presenters:

  please prepare one-minute comments for your award winner

Base64 Malleability in Practice

Panagiotis Chatzigiannis, Konstantinos Chalkias

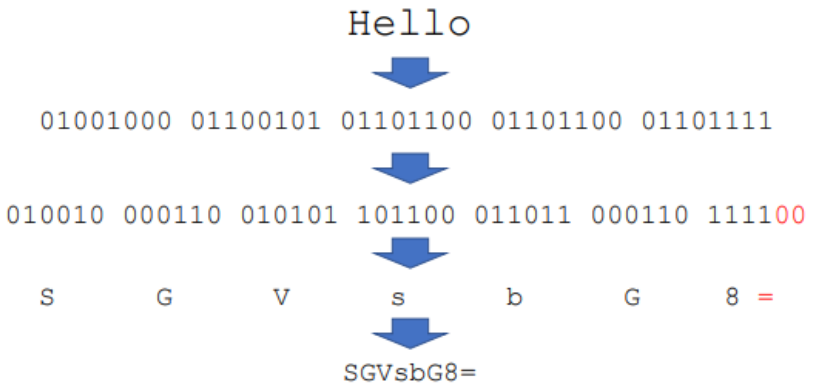
ACM AsiaCCS 2022

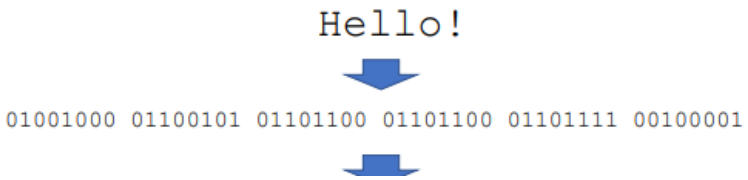
Motivation

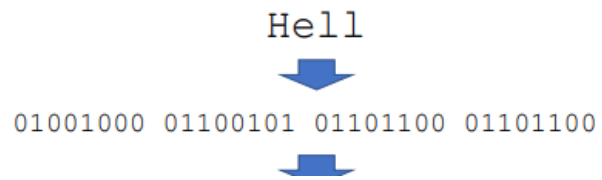
Base64 is a popular method to encode binary data into printable ASCII characters. This method is commonly used in web pages, when exchanging files over email, when representing binary data in JSON data structures, etc. Base64 is a mapping between 64 chosen ASCII characters to groups of 6 bits.

The input data might not always be a multiple of 6. For instance, for the ASCII string `Hello`, by grouping the binary data into 6-bit groups, 2 extra bits are needed to get an exact multiple of 6. Base64 then utilizes padding by adding the necessary number of zeroes in the end. The added padding is represented with extra '=' characters for each two added zeroes.

000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/







Decentralized and Collaborative Tracing for Group Signatures

Maharage Nisansala Sevwandi Perera[1], *Toru Nakamura*[2], *Masayuki Hashimoto*[2], *Hiroyuki Yokoyama*[1], *Chen – Mou Cheng*[3], *and Kouichi Sakurai*[4]

1: Advanced Telecommunications Research Institute International (ATR), Kyoto, Japan
2: KDDI Research, Inc., Saitama, Japan 3: Kanazawa University, Kanazawa, Japan 4: Kyushu University, Fukuoka, Japan

Abstract

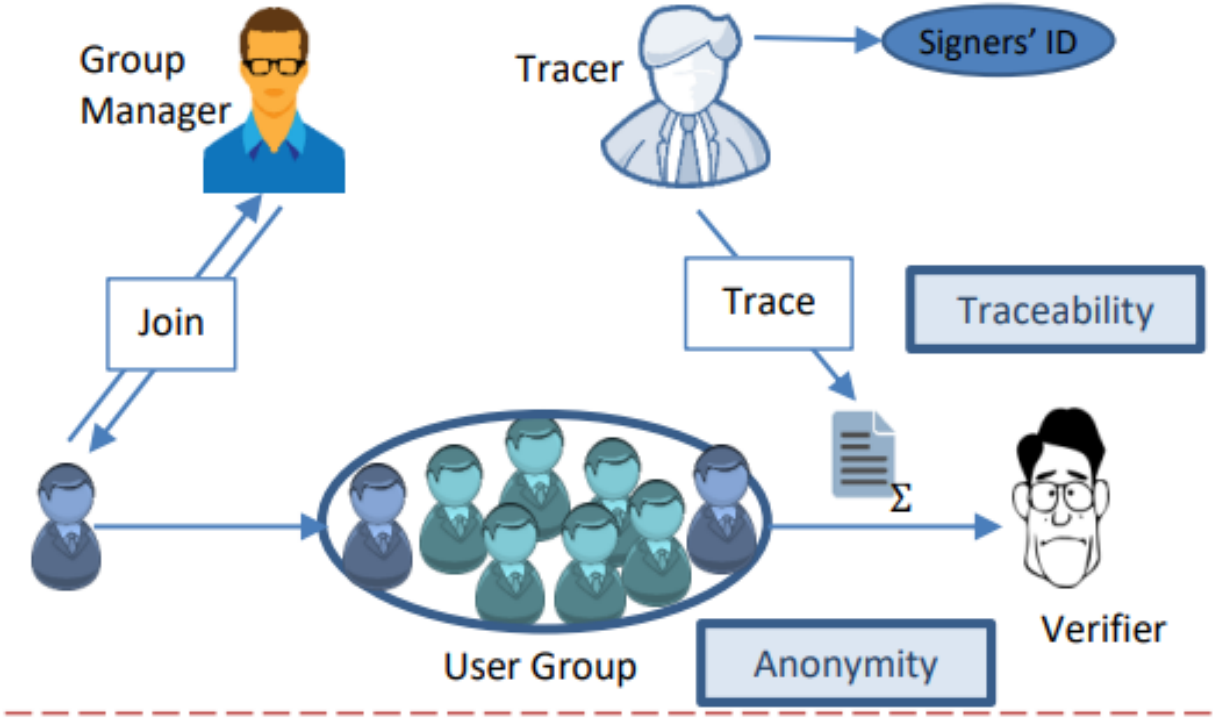
We propose a decentralized but collaborative tracing mechanism (a signer-identifying mechanism) for group signatures using attribute-based encryption mechanism.

Group Signatures

- Group Signatures preserve the privacy of users.
- Group Signatures allow group users to generate a signature while hiding his identity in the group [1].
- Tracing authority can cancel the user anonymity [1].
- User anonymity is depended on tracer's honesty.

Research Problems

- Tracer can identify any user and any signature.
- If tracer is corrupted all users are in danger.
- **Tracer Uncontrolled and Centralized.**



Imperial College London

The Alan Turing Institute

Autonomous Network Defence using Reinforcement Learning

Myles Foley, Chris Hicks, Kate Highnam, Vasilios Mavroudis
mindrake@turing.ac.uk

In the network security arms race, the defender is significantly disadvantaged as they need to successfully detect and counter every malicious attack. In contrast, the attacker needs to succeed only once. To level the playing field, we investigate the effectiveness of **autonomous agents in a realistic network defence scenario**. Using a network environment simulation, with **13 hosts spanning 3 subnets**, we train a **novel reinforcement learning agent and show that it can reliably defend continual attacks by two advanced persistent threat (APT) red agents**: one with complete knowledge of the network layout and another which must discover resources through exploration but is more general.

Objectives

- Design and implement a reinforcement learning agent that can defend a realistic network.
- Demonstrate that the agent can defend the network from attackers with different strategies.
- Compete and outperform competitors in the CAGE Challenge.

The Network Defence Agent

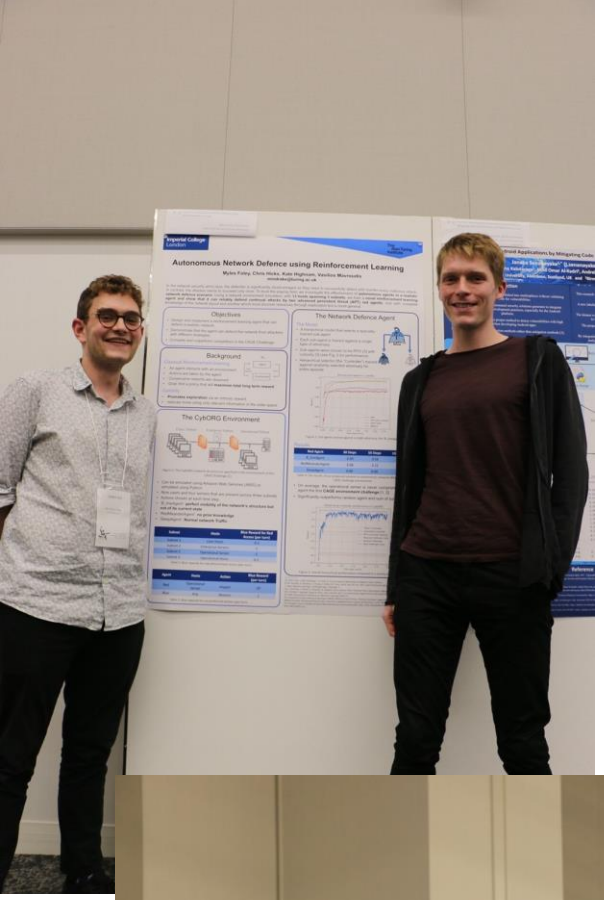
The Model

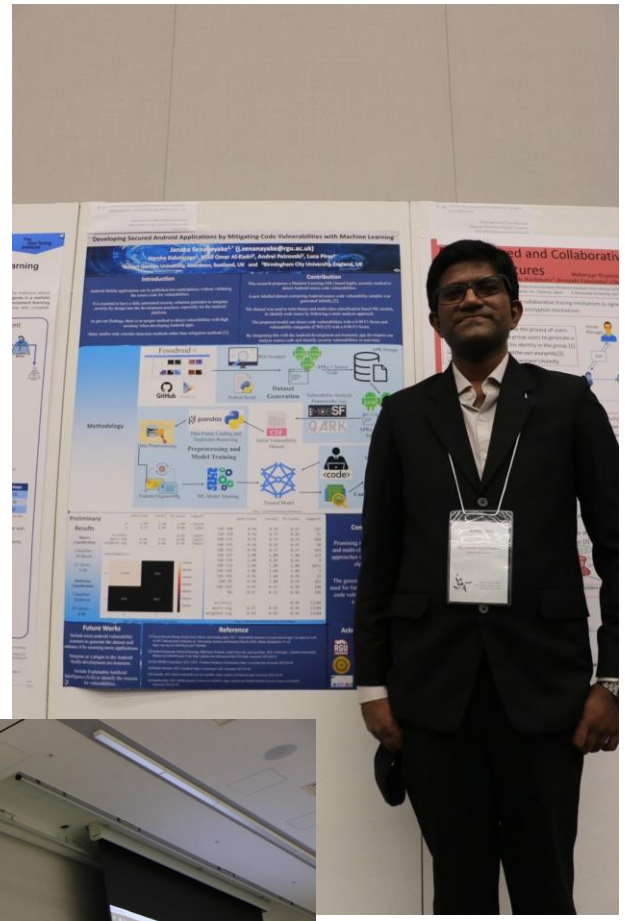
- A hierarchical model that selects a specially-trained sub-agent
- Each sub-agent is trained against a single type of adversary
- Sub-agents were chosen to be PPO [3] with

- *Base64 Malleability in Practice,*
  Konstantinos Chalkias and Panagiotis Chatzigiannis

- *Decentralized and Collaborative Tracing for Group Signatures,*
  Maharage Perera, Toru Nakamura, Masayuki Hashimoto, Hiroyuki Yokoyama, Chen-Mou Cheng and Kouichi Sakurai

- *Autonomous Network Defence using Reinforcement Learning,*
  Myles Foley, Chris Hicks, Kate Highnam and Vasilios Mavroudis


Autonomous Network Defence using Reinforcement Learning
Objectives
Background
The CybORG Environment
The Network Defence Agent


Developing Secured Android Applications by Mitigating Code Vulnerabilities with Machine Learning
Introduction
Contribution
Methodology
Preprocessing and Model Training
Results
Future Works
Reference


Speaker (Room B)
Whiteboards
Leave