112 年度 TACC 期末審查暨成果發表會
中研院資安中心：未來人工智慧與後量子密碼的資安研究(1/2)

計畫編號： 112-2634-F-001-001-MBK

計畫主持人：黃彥男 中研院資安專題研究中心執行長

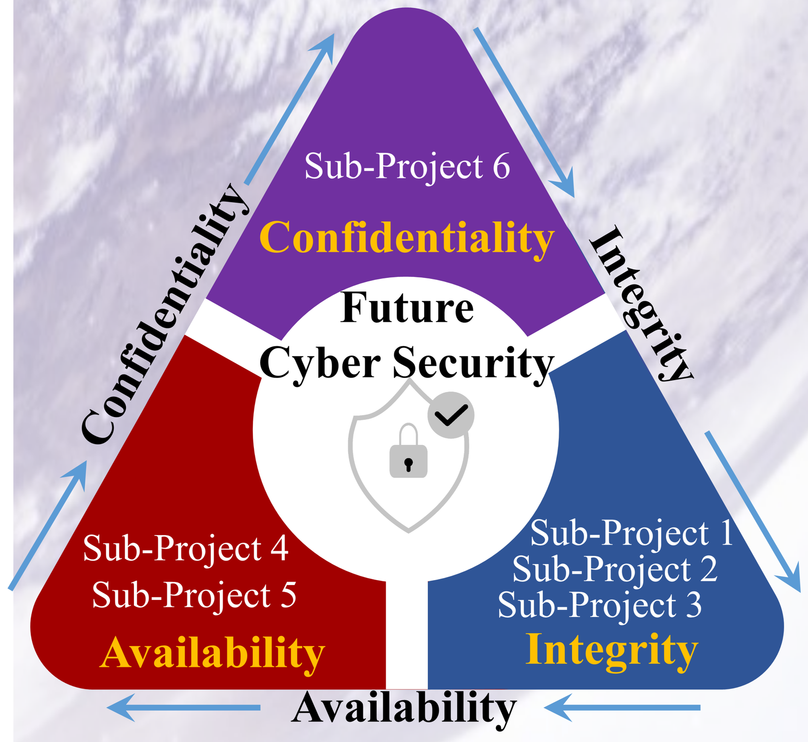
共同主持人：楊柏因研究員、陳孟彰研究員、李育杰研究員、
陳駿丞副研究員、黃意婷助理教授

執行機構：中央研究院、國立臺灣科技大學

Introduction

In light of escalating information security threats that pose risks to national security and societal well-being, the 'Future Network Security' project is paramount. This initiative aims to bolster AI network security and post-quantum cryptography while enhancing national information security and fostering academic research. Comprising six sub-projects, it holds immense potential for impact and benefits, ranging from fortifying national information security to advancing scholarly endeavors. Emphasizing confidentiality, integrity, and availability, the project offers holistic protection, fostering the sustainable growth of the network security sector and contributing to the establishment of an intelligent and secure nation.

CIA Triad for Future Cybersecurity



Confidentiality:

- Post-quantum cryptography serves as a defense mechanism for conventional computers against malicious adversaries armed with quantum computers

Integrity:

- The protection of a system from malware, attacks, and intrusions

Availability:

- Data should be accessible when it is needed for authorized use, without causing unnecessary risk

Sub-Project 1 (PI: Yennun Haung)
Stealth Cyber Attack Discovery via Data Correlation and Provenance Analysis

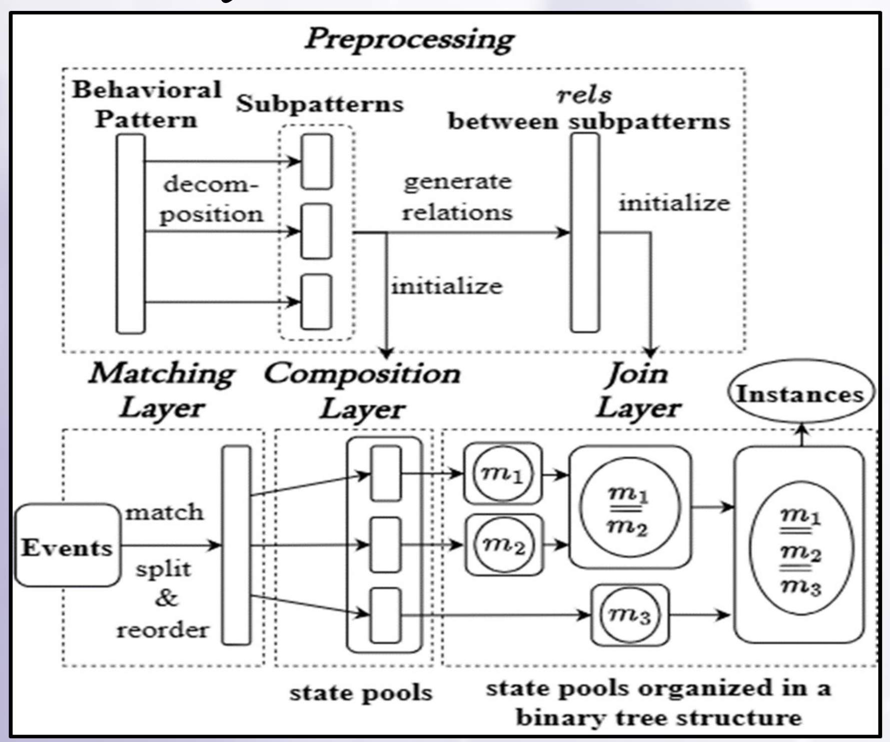
IPMES: A Tool for Incremental TTP Detection over the System Audit Event Stream

Motivation:

- Graph-based TTP patterns is hard to incrementally matched

Contribution:

- Can handle events with same timestamps and interval timestamps
- More efficient than practical tools



Hong-Wei Li, Ping-Ting Liu, Bo-Wei Lin, Yi-Chun Liao, Yennun Huang, "IPMES: A Tool for Incremental TTP Detection over the System Audit Event Stream", DSN 2014, Accepted

Sub-Project 2 (PI: Yi-Ting Huang)
Enhancing Malicious Behavior Discovery with Cyber Threat Intelligence and Generated Malware

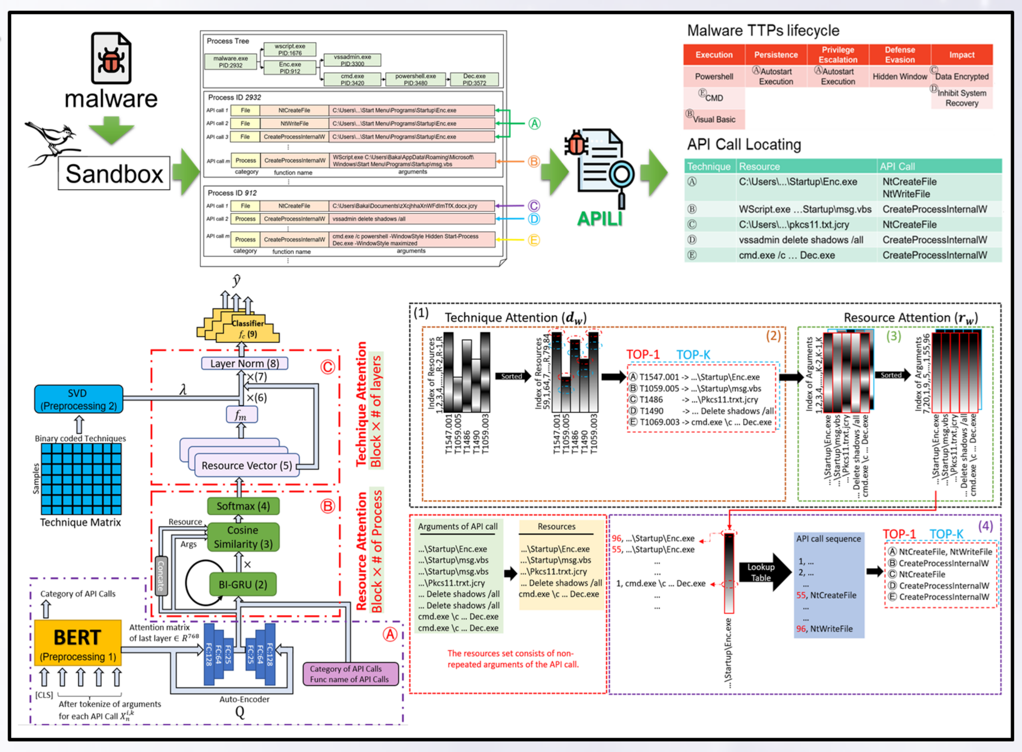
Attention-Based API Locating for Malware Techniques

Motivation:

- Traditional dynamic malware analysis requires significant human effort for analyzing malware behavior.

Contribution:

- Lessen analyst workload by detecting malicious behavior.
- locating API calls matching high-level behavior.



Wong, G. W., Huang, Y. T., Guo, Y. R., Sun, Y., & Chen, M. C. (2023). Attention-Based API Locating for Malware Techniques. *IEEE TIFS.*

Sub-Project 3 (PI: Meng Chang Chen)
Adversarial Cyber Attack Practice, Theory and Defense

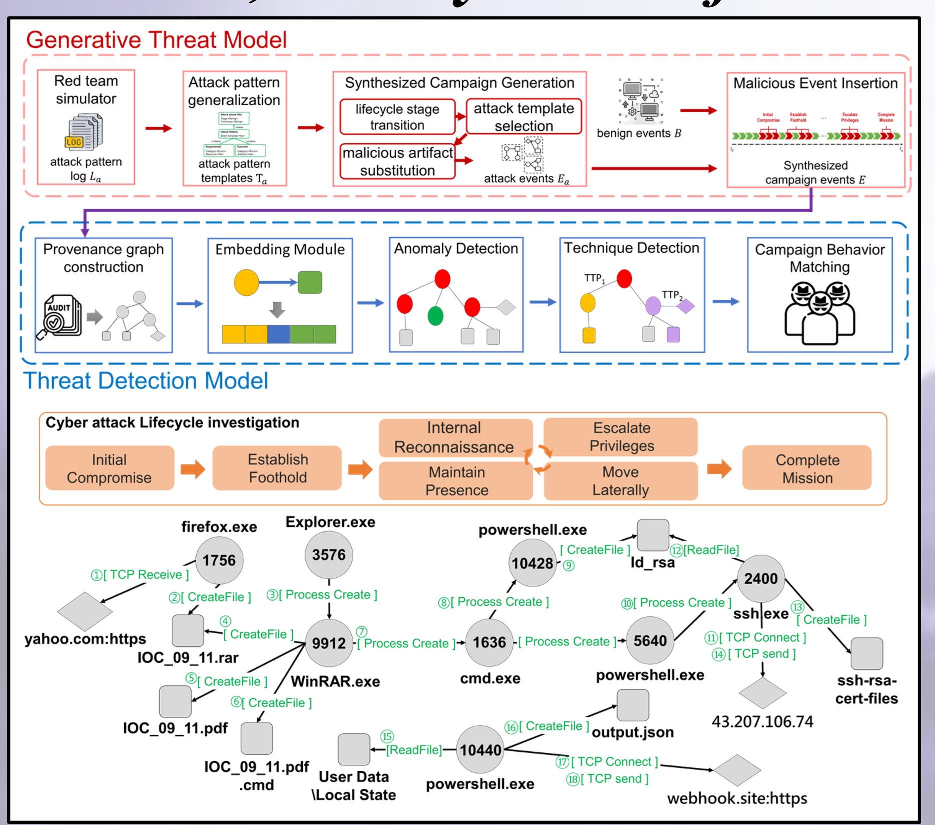
Synthetic Audit Log Generation for Embedded APT Campaign Detection

Motivation:

- Lack of a comprehensive benchmark dataset hampers APT attack detection from audit logs.

Contribution:

- A configurable synthetic audit log generation facilitated by adopting a red-team emulator
- A two-way approach aiming to detect attack patterns



Y. T. Huang, Y. R. Guo, Y. S. Yang, G. W. Wong, Y. Z. Jheng, Y. Sun, Timothy Lynar and M. C. Chen (2024). Synthetic Audit Log Generation for Embedded APT Campaign Detection . USENIX 2024 [rejected]

Sub-Project 4 (PI: Jun-Cheng Chen)
Robust Multi-modal Deepfake Detection and Suppression

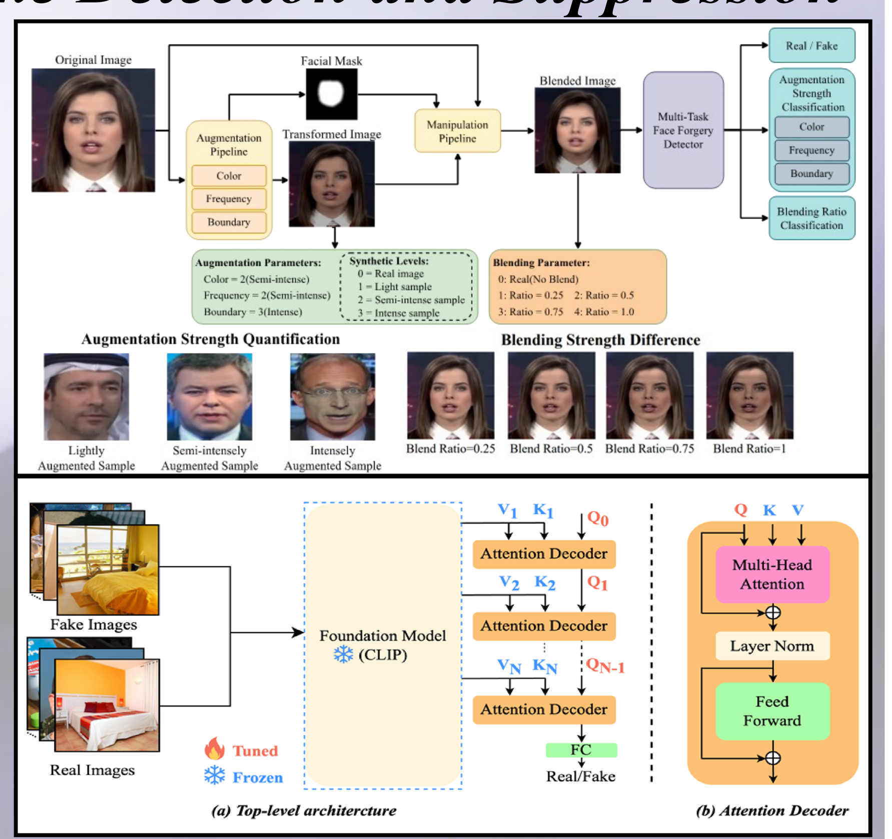
Multi-Task Self-Blended Images for Face Forgery Detection

Motivation:

- The Deepfake data collection and annotation are time-consuming and costly.
- The existing detectors usually have a significant performance drop for new and unseen Deepfakes.

Contribution:

- We develop a novel self-supervised learning approach to effectively simulate fake samples with simple data augmentation.
- We further develop a new detector with a side-network-based adapter upon the OpenAI's foundation model, CLIP, for improved detection performance and generalization. More efficient than practical tools



Po-Han Huang, Yue-Hua Han, Ernie Chu, Jun-Cheng Chen, Kai-Lung Hua, "Multi-Task Self-Blended Images for Face Forgery Detection," ACM Multimedia Asia, December 2023.

Sub-Project 5 (PI: Yuh-Jye Lee)
Zero-Trust Federated Learning

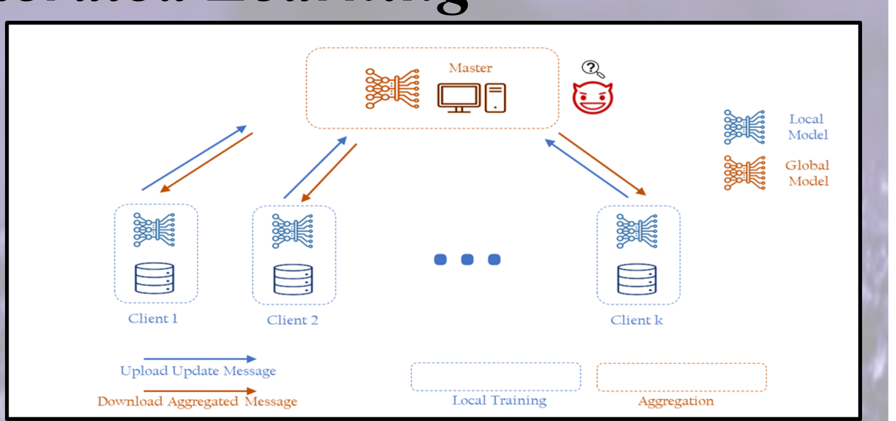
Federated Learning with ZTA

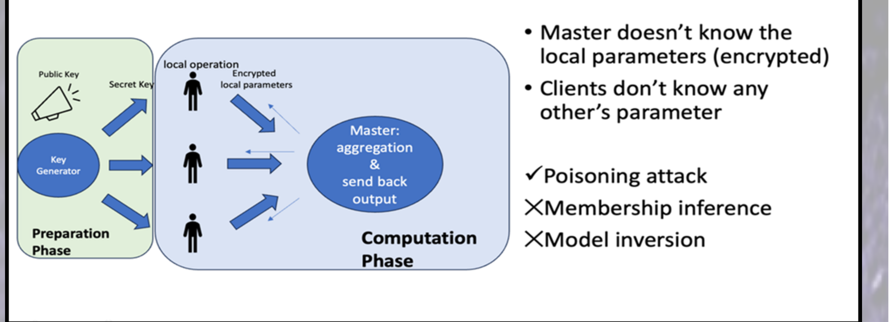
Motivation:

- Federated learning, a methodology preserving data on client devices, mitigates concerns regarding data leakage. Nevertheless, within this framework, security challenges persist due to potential attacks like membership inference, model inversion, Byzantine, and backdoor attacks.

Contribution:

- Zero Trust Architecture (ZTA) addresses FL security concerns with the principle of "never trust, always verify". Leveraging the ADMM distributed optimization framework, we simplify server-side computation and partially homomorphically encrypt client-side model parameters to reduce the computational burden of fully homomorphic encryption. Additionally, we will incorporate identity authentication and introduce anomaly detection to realize zero-trust federated learning.





Sin Cheng Ciou, Pin Jui Chen, Elvin Y. Tseng, **Yuh-Jye Lee**, "Federated Learning for Sparse Principal Component", 2023 IEEE International Conference on Big Data (Big Data), Sorrento, Italy, December 15-18, 2023.

Sub-Project 6 (PI: Bo-Yin Yang)
Post-quantum Cryptography

Algorithmic Views of Vectorized Polynomial Multipliers–NTRU
Algorithmic Views of Vectorized Polynomial Multipliers–NTRU Prime

- Lattice-based crypto records (on ARM Neon) with Number Theoretic Transforms or TMVP (Toeplitz Matrix Vector Product)

Prior:

- Toom (maybe with TMVP) when " no suitable NTT "

Our Innovations:

- Truncated Rader's Transform, for NTRU Prime 4591761.
- New Toom-5 (÷8 not ÷16) for NTRU HRSS701, HPS2048677

Key Achievements: Generating efficient code

- NIST (National Institute of Standards and Technology) competition speed records including NTRU and NTRU Prime

Quantitative Results :

- Improvements to NTRU and NTRU Prime
  - NTRU 2.18×/2.23× for ntruhps2048677 / ntruhrsss701.
  - polymul in sntrup 4591677 6×fast, enc/dec ~ 2.8×/3.0×

Future Goals :

- Formally verifiable NTT program generator
  - Variable moduli; in different rings; on different HW platforms
- Automatic selection of suitable programming techniques
  - Good's FFTvs Incomplete NTT; layer Merge/Twists in NTT;
  - Schönhage / Nussbaumer FFT

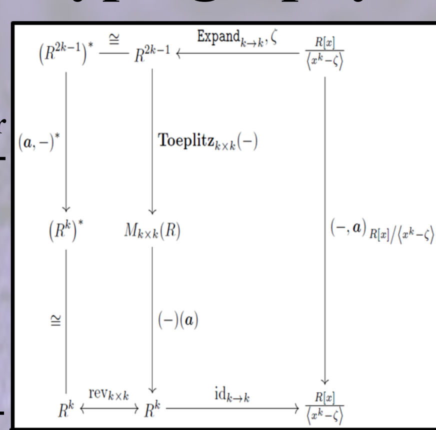


Table 5: Detailed performance numbers of ntruhps2048677 and ntruhrss701 with Toeplitz-TC. Only performance-critical subroutines are shown.

ntruhps2048677		ntruhrss701	
Operation	Cycles	Operation	Cycles
crypto_kem_keypair	1 002 187	crypto_kem_keypair	1 076 810
owcpa_keypair	990 579	owcpa_keypair	1 069 128
poly_S3_inv	482 005	poly_S3_inv	503 590
poly_Rq_mul(×5)	5× 26 784	poly_Rq_mul(×5)	5× 31 478
poly_Rq_inv	341 482	poly_Rq_inv	392 478
poly_R2_inv	136 776	poly_R2_inv	140 290
poly_Rq_mul(×8)	8× 26 784	poly_Rq_mul(×8)	8× 31 478
sort	17 819		
randombytes	12 054	randombytes	6 294
crypto_kem_enc	79 213	crypto_kem_enc	59 625
owcpa_enc	32 501	owcpa_enc	41 559
poly_Rq_mul	26 784	poly_Rq_mul	31 478
randombytes	13 023	randombytes	6 202
sort	18 040		
sha3	5 148	sha3	5 296
crypto_kem_dec	120 208	crypto_kem_dec	142 174
owcpa_dec	100 842	owcpa_dec	120 485
poly_Rq_mul(×2)	2× 26 784	poly_Rq_mul(×2)	2× 31 478
poly_S3_mul	28 341	poly_S3_mul	33 319
sha3	18 867	sha3	21 342

Table 7: Overall cycles of sntrup761/ntrulpr761.

sntrup761			
Operation	Key generation	Encapsulation	Decapsulation
Ref	273 598 470	29 750 035	89 968 342
Good--Rader--Bruun	6 333 403	147 977	158 233
Good--Thomas	6 340 758	153 465	182 271
Good--Schönhage--Bruun	6 345 787	163 305	193 626

ntrulpr761			
Operation	Key generation	Encapsulation	Decapsulation
Ref	29 853 635	59 572 637	89 185 030
[Haa21]	775 472	1 150 294	1 417 394
Good--Rader--Bruun	260 606	412 629	461 250
Good--Thomas	269 590	422 102	471 014
Good--Schönhage--Bruun	272 738	436 965	499 559

※ *Han-Ting Chen, Yi-Hua Chung, Vincent Hwang and Bo-Yin Yang, "Algorithmic Views of Vectorized Polynomial Multipliers – NTRU," Indocrypt 2023*
※ *Vincent Hwang, Chi-Ting Liu and Bo-Yin Yang, "Algorithmic Views of Vectorized Polynomial Multipliers – NTRU Prime," ACNS 2024*