跨雲安全原生之虛實情境感知零信任架構

Cloud-Agnostic Security Native Cyber-Physical Context Awareness-Based Zero Trust Architecture

計畫主持人　：范俊逸 特聘教授/中心主任

計畫共同主持人：陳嘉玫 教授、王智弘 教授、謝東佑 教授、蔡崇煒 副教授、徐瑞壕 助理教授、克拉迪 助理教授

國立中山大學資訊安全研究中心

資安三位一體

- 資訊工程學系 資訊安全博士班 (全臺灣第一個)
- 資訊工程學系 資訊安全碩士班 (全臺灣第一個)
- 學士班整合學程 資通安全學程

校一級研究中心

- 圖書與資訊處 資訊安全組 (全臺灣第一個)
- 資安社團

高屏澎區 TWAREN GigaPOP

TANet CERT 台灣學術網路危機處理中心

- 前瞻資安科技研究
- 資安Hub
- 培育資安人才
- 促進產學資安技術合作與交流
- 協助產官學強化資安防護
- 協助政府推廣/實施資安政策

學術拔尖
Academic Excellence

TOP 5 Journals
ranked by JCI or JCR

3 / 1
Accepted　Submitted

TOP 5 Conferences
ranked by h5-index

1 / 1
Accepted　Submitted

人才培育
Talent Development

人才培育

- 資訊安全博士班、資訊安全碩士班、資通安全學士班學程
- 資訊安全研究中心
- 國立中山大學資安社團
- ZTA或AI安全相關領域研討會
  - 跨雲原生零信任架構前瞻技術交流（高雄場）
  - 跨雲原生零信任暨後量子密碼技術交流研討會（臺北場）
  - 零信任企業資安實務研討會（臺南沙崙）

培訓課程

- 針對學術/實務的培訓課程
  - 惡意程式攻防實務課程
  - 社交工程實務課程
  - CTF實戰入門與比賽經驗分享工作坊
  - Binary Exploit 漏洞應用入門
- 針對產業的培訓課程
  - 日月光人才培育計畫暨人才鑑定

資安競賽與活動

- AIS3 EOF 決賽第4名及潛力獎
- DEVCORE 全國資訊安全獎學金
- HITCON CTF 2023 決賽第7名
- 神盾杯資安競賽 第4名
- 第54屆全國技能競賽南區分區技能競賽-青年組英雄榜網路安全分區第2名

國際鏈結
International Linkages

建立連結

- 日本兵庫縣立大學
- 日本明治大學
- 日本「國立研究開發法人情報通訊研究機構（NICT）」
- 印度理工學院（IIT）
- 新加坡科技設計大學
- 立陶宛 Vilnius University
- 捷克 Czech Technical University
- 韓國慶北大學
- 韓國延世大學
- 阿曼德國科技大學

延攬國際人才

- 專任助理教授 2 位
- 訪問/客座學者 1 位(申請中）
- 博士後研究員 2 位

雙邊交流會議

- 臺灣、韓國與澳洲交流會議
- 臺灣、日本雙邊交流會議
- 臺灣、印度雙邊交流會議
- 邀請Earle C. Williams傑出學者/IEEE Fellow國外學者演講

移地研究

- 日本「國立研究開發法人情報通訊研究機構（NICT）」
- 日本明治大學
- 日本兵庫縣立大學
- 新加坡科技研究局A*STAR
- 德國奧爾登堡大學

產業落地
Industry Localization

國家資通安全研究院 National Institute of Cyber Security
雲端安全組態檢測與驗證技術

NARLabs 國家實驗研究院 科技政策研究與資訊中心
NARLabs 國家實驗研究院 國家高速網路與計算中心
沙崙資安科研發展與人培基地推動計畫

財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY
半導體產業人才創能加值計畫-
推動客製化企業主題多元模式暨辦理數位人才鑑定考試

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER
聯邦式機器學習技術指引暨驗測方法論與概念性驗證研究

TWNIC 財團法人台灣網路資訊中心 TAIWAN NETWORK INFORMATION CENTER
委託辦理企業推廣及資安防護研討會(高雄、台南)

中華資安國際 CHT Security
「112年臺南市ISAC區域聯防服務」研究計畫專案

跨雲安全原生之虛實情境感知零信任架構

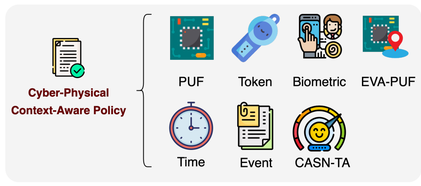
- 跨雲/雲無關
- 虛實情境感知因子
- 多因子認證機制
- 多授權中心存取控制機制
- 功能性加密、安全運算
- 具隱私保護之聯邦式學習
- 安全多方聚合運算
- 自適應性下毒緩解機制
- 威脅評估機制
- 基於圖之異常偵測
- 自適應性堆疊集成演算法

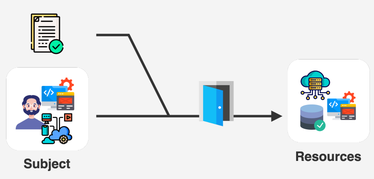
User-Device Identities

I Cyber-Physical Context Awareness-Based Identity Authentication Mechanism (CPCAB-IA)

The 1st Year

CPCAB-IA—Integrating User-Device Identities Through PUF





PUFs

多因子認證機制

Attribute-Based Encryption

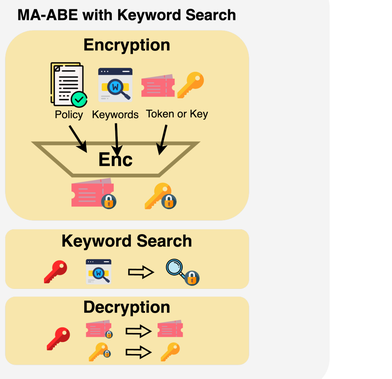
Multi-Authority

Keyword Search

II Multi-Authority Access Control Mechanism for Cloud Agnostic (CA-MAAC)

The 1st Year

CA-MAAC with Keyword Search



Federated Learning

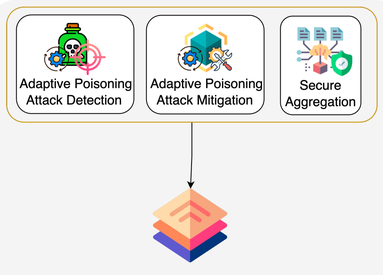
Poisoning Attack Detection

Poisoning Attack Mitigation Mechanisms

III Privacy Preserving Federated Learning with Secure Multi-Party Aggregation and Self-Adaptive Poisoning Attack Mitigation (PAM-PPFL)

The 1st Year

Development of Self-Adaptive Poisoning Attack Detection and Mitigation Mechanisms for Federated Learning



Privacy Preserving Federated Learning with Secure Multi-Party Aggregation and Self-Adaptive Poisoning Attack Mitigation (PAM-PPFL)

Threat Reproduction

Ensemble Algorithm

Graph-Based Anomaly Detection

IV Cloud-Agnostic Security Native Threat Assessment Scheme with Graph-based Adaptive Stacking Ensemble Algorithm (CASN-TA)

The 1st Year

Development of a Cloud-Agnostic Security Testing Framework: Environment Reconstruction and Threat Reproduction