區塊鏈技術與應用

Blockchain Techniques and Applications

CYBERSEC 2025

臺灣資安大會

心得報告

班　級：　資工碩一

學　號：　113598043

姓　名：　張育丞

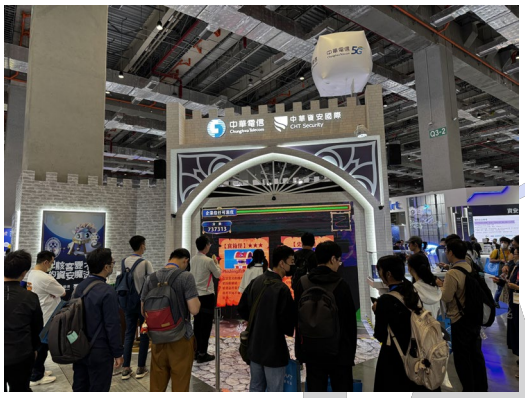
April 17, 2025

一、 心得內容

這次有幸參加到「CYBERSEC 2025 臺灣資安大會」其實挺開心的，雖然整體來說就是個從住家到南港可謂舟車勞頓。過去參觀的展覽數不勝數，但大多數屬於 AI、IoT 或 Sensors 領域，頂多大到 Computex 那種商業性極強的，因此這也是我對於資安領域實際參觀展會的經驗，展會除了有商業行銷，也有不少教育或研究推廣，相較於過去看到都是一些設備，顯得俐落許多。過去因為讀網路工程相關科系，因此同學和學長姐們都從事著資安和網工相關，對此在現場不免俗看到許多熟識，對於一個資安圈外人加上畢業後沒再連絡他人的我來說，真的是個不錯的相見歡，看著大家成長並且推廣自家產品，內心感到開心與榮幸當他們的同學甚至學弟。

由於傍晚剛好有事，因此選擇較早議程，由 Anatomist Security 團隊的 Co-Founder 王建元分享「Breaking Down Web3 Attack Surfaces: A Dive into Consensus, VMs, Smart Contracts and Toolchains」，在議程中，除了分析 Consensus Layer 和 Execution Layer 的問題，接著透過 Sway 在 X 平台上面發表的事件進行說明漏洞，也看到漏洞留著一直不修，到系統即將發行時才改期，進行修漏洞，其實滿有趣的，但是滿多系統為了顏面也不會坦承漏洞啦！在 Consensus 的 Part 他說到多數決以及檢查前兩區塊的狀態進行驗證的事情，還有關於分岔（Fork）的部分，例如當接不到區塊會產生的跳躍（Skip）等待恢復後補上，對於偽造會需要六個區塊，在創始塊出塊後，當第一塊沒有成功在鏈上，而 Skip 接著會產生第二塊，然後第二塊也沒有成功在鏈上，也 Skip，以此類推到第三塊也 Skip 時，在第四塊出塊後，返回來補上 Fack 的三塊，就有機會達到偽造，因為他只檢查當前的前兩塊出塊的資訊，其實這理論滿有意思的，可惜時間到了不然會想知道後續解決與發展的更多細節。

二、 活動花絮



三、 議程簡報

https://drive.google.com/file/d/1ah_exznHWYrGPqSlPX6XeR-poZip8LNj/view?usp=drive_link