行政院及所屬各機關出國報告

（出國類別：出席國際會議）

參加「第 14 屆 EAI 通訊網路安全及隱私權國際會議（SecureComm 2018:14th EAI International Conference on Security and Privacy in Communication Networks）」出國報告

服務機關：財政部財政資訊中心

姓名職稱：郭啓容設計師

派赴國家：新加坡

出國期間：107 年 8 月 7 日至 8 月 11 日

報告日期：107 年 10 月 23 日

摘要

「第 14 屆 EAI 通訊網路安全及隱私權國際會議（SecureComm 2018:14th EAI International Conference on Security and Privacy in Communication Networks）」於 2018 年 8 月 8 日至 10 日舉行，本會議係 European Alliance for Innovation(EAI)主辦系列研討會之一，採各國輪辦方式進行，之前舉辦國家計有美國、英國、加拿大、澳洲、法國、義大利、希臘、土耳其、新加坡及中國等國家，本年度會議地點安排於新加坡 ibis Singapore on Bencoolen Hotel。該研討會旨在彙集世界各地之專家學者交流及分享有關資通訊安全領域之經驗，展示與討論資通訊安全技術創新趨勢及其遭遇到之挑戰與解決方案。

本中心藉由參加此研討會了解國際最新資通訊趨勢及相關資訊安全技術，並透過與各國精英學者之交流及實地觀摩，帶回嶄新技術與觀念，並據以強化本中心資通訊安全技術與管理措施及提升本中心資通訊安全研究能量。

本次會議研討之主題包括各項資通訊安全主題，本報告聚焦於網站系統安全、網路技術安全及通訊隱私權等主題，撰寫相關內容以作為本中心資通訊安全業務精進之參考，包括下列 3 篇論文主題內容：

一、基於 HTML 模板恢復的 XSS 過濾器：現有的 XSS 過濾器採用在 HTTP 請求中尋找到攻擊代碼以檢測 XSS，攻擊者有時可以透過精心製作和發送攻擊代碼的機制繞過檢測。本論文提出了一種新的 XSS 過濾器 Xilara 來檢測包括上述這些複雜的 XSS 攻擊，Xilara 的設計可以透過檢查 HTML 文件檔案的結構來檢測 XSS 攻擊。Xilara 不僅可以應用於 Reflected XSS，還可以應用於 Stored XSS，並且可以獨立於應用程式使用。

二、用於增強網際網路網域表現力的超策略（metapolicy）框架：本 metapolicy 框架方案為網域提供了定義和管理與網域相關的安全策略的機制。此機制的所有相關的網域以及強制執行的網域可以由對應網域的 TLS 證書私鑰或 DNSSEC 密鑰簽章的 metapolicy 達成。Metapolicy 發布一系列網域的 DNS TXT 記錄，因此不需要新的基礎設施，本方案可以部署於現存的網路環境。

三、用於保護隱私資料共享的安全及高效多方目錄：本論文解決分散式隱私保護目錄發布的問題；而此發布問題可以模式化為安全的多方計算（簡稱為 MPC）問題。為了提高效率本論文提出一個預先計算框架，並提出具有不同程度的積極性預計算策略。此外，本論文使用通用圖形處理單元上的平行預先計算以提高系統效率並在實際的 MPC 軟體上實作及進行效能評估。

目次

壹、目的

一、參加目的

為了解國際最新資通訊趨勢及相關資訊安全技術，本中心每年皆派員參與各類重要國際會議，透過與各國精英學者之交流及實地觀摩，帶回嶄新技術與觀念，並據以強化本中心資通訊安全技術及管理措施。本次於新加坡舉行「第 14 屆 EAI 通訊網路安全及隱私權國際會議（SecureComm 2018:14th EAI International Conference on Security and Privacy in Communication Networks）」，彙集世界各地專家學者交流及分享有關資通訊安全領域之經驗，展示與討論最新資通訊安全技術創新趨勢及其遭遇之挑戰及解決方案，藉由參加此研討會瞭解其相關趨勢及研究。

由於網際網路與分散式計算技術不斷進步，加速巨量資料與雲端運算技術應用之發展，也造成網路資通訊安全問題。冀藉此次參與該會議，瞭解及資通訊安全技術與趨勢，期能產生對本中心資通訊安全管理及技術具參考價值之創意啟發，據以提升本中心資通訊安全研究能量。

二、會議主題

本次會議研討之主題包括網路安全及隱私權、網路入侵偵測防禦、惡意軟體分析及偵測、網站系統安全、分散式阻斷服務攻擊及防禦、通訊隱私權及匿名、規避及反審查技術、網路取證技術、身分驗證系統、安全路由及定址、普及計算之安全及隱私權、點對點及覆蓋網路之安全及隱私權、新興網路技術之安全及隱私權、雲端及資料中心與軟體定義網路之安全與隔離等 14 項資通訊安全主題，會議分 3 天不同場次同時進行，相關主題綱要內容如下：

表 1　會議主題綱要

序號	主題綱要
1	網路安全及隱私權（Security & Privacy in Wired, Wireless, Mobile, Hybrid, Sensor, Ad Hoc networks）： 採討有線網路、無線網路、行動網路、混合網路、無線感測網路及無線隨意網路的網路安全與隱私權相關議題。
2	網路入侵偵測防禦（Network Intrusion Detection and Prevention, Firewalls, Packet Filters）： 包含網路入侵偵測防禦、防火牆及封包過濾等主要網路防禦技術最新研究及趨勢之探討。
3	惡意軟體分析及偵測（Malware Analysis and Detection including Botnets, Trojans and APTs）： 惡意軟體包括電腦病毒、電腦蠕蟲、邏輯炸彈、特洛依木馬、後門軟體及勒索軟體等，不僅會影響電腦系統運作，更可能竊取或破壞電腦檔案資料，如何有效防範惡意軟體攻擊是重要資訊安全課題之一；本議題包含惡意軟體分析偵測、僵屍網路、特洛依木馬及 APT 攻擊網站系統安全之探討。
4	網站系統安全（Web and Systems Security）： 網站應用系統提供網際網路服務應用便利性，但設計不佳的網頁程式及網站平台漏洞往往造成嚴重資訊安全問題，本議題探討確保網站系統安全之最新研究及趨勢。
5	分散式阻斷服務攻擊及防禦（Distributed Denial of Service Attacks and Defenses）： DDoS（分散式阻斷服務攻擊）是利用分散於不同地方的多部資訊設備（多數為跨國之殭屍網路）來進行多對一的攻擊，透過發送難以追查且大量的封包，癱瘓目標資訊設備，使之無法提供服務；本議題探討 DDoS 攻擊及防禦之相關最新研究。
6	通訊隱私權及匿名（Communication Privacy and Anonymity）： 網際網路日益增長的資料存儲及大數據分析能力，對於大眾的隱私權及匿名性構成越來越大的威脅，如何保護網際網路隱私權及匿名性是當今資訊安全重要課題。
7	規避及反審查技術（Circumvention and Anti-Censorship Technologies）： 網際網路規避及反審查為用於繞過網際網路審查之技術，本議題探討網際網路規避及反審查相關技術及研究。
8	網路取證技術（Network and Internet Forensics Techniques）： 網路取證是分析網路攻擊關鍵步驟，完整的網路取證，有助於識別及分析網路攻擊事件，本議題探討網路取證相關技術及研究。
9	身分驗證系統（Authentication Systems: Public Key Infrastructures, Key

	Management, Credential Management）： 探討公鑰基礎建設、金鑰管理及憑證管理等身分驗證技術相關研究議題。
10	安全路由、定址及網路管理（Secure Routing, Naming/Addressing, Network Management）： 探討避免網路定址、路由被惡意干擾破壞之安全路由、安全定址及安全網路管理等議題。
11	普及計算之安全及隱私權（Security & Privacy in Pervasive and Ubiquitous Computing, e.g., RFIDs）： 在普及計算的模式下，人們能在任何時間、任何地點以任任何方式進行資訊擷取與處理，因此衍生更為嚴重的網路安全及隱私權問題。
12	點對點及覆蓋網路之安全及隱私權（Security & Privacy in Peer-to-Peer and Overlay Networks）： 點對點網路為用戶端直接互相連線之技術，而覆蓋網路為建立於其他網路上的延伸應用網路之技術，本主題探討網路取證點對點及覆蓋網路相關安全及隱私權議題。
13	新興網路技術之安全及隱私權（Security & Privacy for Emerging Technologies: VoIP, Internet-of-Things, Social Networks）： 探討網際協議通話技術（VoIP）、物聯網（IoT）及社交網路等新興網路技術的安全及隱私權議題。
14	雲端、資料中心及軟體定義網路之安全與隔離（Security & Isolation in Cloud, Data Center and Software-Defined Network）： 由於網際網路和分散式計算技術不斷進步，加速雲端運算與資料中心技術之發展；另一新型網路架構為軟體定義網路，乃利用 OpenFlow 協定將路由器的控制平面從資料平面分離，改以軟體方式實作，此新型網路架構可以在不更動硬體架構下，以中央控制程式重新規劃網路。本主題探討雲端、資料中心及軟體定義網路的安全與隔離議題。

貳、過程

一、會議簡介

本次會議為「第 14 屆 EAI 通訊網路安全及隱私權國際會議（SecureComm 2018:14th EAI International Conference on Security and Privacy in Communication Networks）」，係 European Alliance for Innovation(EAI)主辦系列研討會之一，採各國輪辦方式進行，之前舉辦國家計有美國、英國、加拿大、澳洲、法國、義大利、希臘、土耳其、新加坡及中國等國家。

本次會議旨在彙集世界各地之專家學者交流及分享有關資通訊安全領域之經驗，展示與討論資通訊安全技術創新趨勢及其遭遇之挑戰與解決方案。與會者包括研究人員、從業人員以及教育工作者，討論最新創新技術、趨勢、關注議題、面臨的實際挑戰及解決方案等，會議以簡報方式進行。

二、會議時間及地點

本次會議於 107 年 8 月 8 日至 10 日假新加坡 ibis Singapore on Bencoolen Hotel 1 樓 Jasmine 及 Hibiscus 會議廳舉行。

圖 1 及圖 2 新加坡 ibis Singapore on Bencoolen Hotel 外觀及 1 樓 Jasmine 會議廳

表 2　會議行程表：完整議程詳如附錄，並簡要說明如下。

日期	行程
107 年 8 月 7 日	啟程（臺北→新加坡）
107 年 8 月 8 日至 8 月 10 日	SecureComm 2018:報到、出席會議
107 年 8 月 11 日	回程（新加坡→臺北）

由於會議涵蓋主題相當廣，每位講者僅約有 20 分鐘口頭簡報時間，共計報告 61 篇論文（議程詳附錄），無法就每場簡報內容一一摘述，謹就主要關注論文主題「Xilara: An XSS Filter Based on HTML Template Restoratio」（Xilara：基於 HTML 模板恢復的 XSS 過濾器）、「A Metapolicy Framework for Enhancing Domain Expressiveness on the Internet」（用於增強網際網路網域表現力的超策略框架）及「Secure and Efficient Multi-Party Directory Publication for Privacy-Preserving Data Sharing」（用於保護資料共享的安全及高效多方目錄發布）3 篇內容詳述於後續章節。

三、論文主題 1：Xilara：基於 HTML 模板恢復的 XSS 過濾器（Xilara: An XSS Filter Based on HTML Template Restoratio）

（一）引言

跨站腳本（XSS）是對 Web 應用程式最可怕的攻擊之一，攻擊者為了各種目的濫用 XSS，例如存取使用者敏感資料、控制瀏覽器或透過呈現虛假資訊欺騙使用者。保護使用者免受 XSS 的影響非常重要，但仍然有許多易受攻擊的應用程式，因為這些應用程式仍然存在許多漏洞。

已有多種針對 XSS 的保護和緩解技術，本論文專注於 XSS 過濾器，它透過監控網路來檢測 XSS 客戶端與服務器之間的通信，且可獨立於 Web 應用程式運作。一些網路瀏覽器有內置的 XSS 過濾器，而一些 Web 應用防火牆提供 XSS 過濾功能。但是，由於現有的 XSS 過濾器採用在 HTTP 請求中尋找到攻擊代碼以檢測 XSS，攻擊者有時可以透過精心製作及發送攻擊代碼的機制繞過檢測。例如攻擊是使用

base64 編碼之攻擊代碼，並利用已存儲在伺服器中被攻擊代碼污染 HTML 檔案的 XSS 代碼。

本論文提出了一種新的 XSS 過濾器 Xilara 來檢測包括上述這些複雜的 XSS 攻擊，Xilara 的設計可以透過檢查 HTML 文件檔案的結構來檢測 XSS 攻擊。Xilala 先在無害的 HTTP 回應中收集 HTML 文件檔案，並透過從收集 HTML 文件檔案中提取資料的方法以恢復 HTML 模板。然後，Xilara 確認 HTTP 回應中的 HTML 文件檔案的結構是否可從還原的模板生成以檢測 XSS 攻擊，如果 HTTP 回應的文件檔案結構與模板不匹配，則判定此 HTTP 回應為有害。Xilara 不僅可應用於 Reflected XSS，還可以應用於 Stored XSS，並且可獨立於應用程式使用。

（二）相關技術

2.1 Web 應用程式防火牆中的 XSS 篩選器

一些 Web 應用程式防火牆（WAF）具有使用正規表達式的 XSS 篩選器，例如 Javed 和 Schwenk 中的黑名單；因為它可以獨立於 Web 應用程式運作，使用者可以輕鬆安裝這些 XSS 過濾器。當 HTTP 請求符合正規表達式就會被視為攻擊；OWASP ModSecurity 核心規則集是其中一個眾所周知的過濾器。

當這些方法可在 HTTP 回應中檢測到攻擊代碼時，這些方法是有效的；但是當攻擊者使用複雜轉換程式隱藏攻擊代碼時，這些方法是無效的。例如 Kettle 報導攻擊者可繞過應用程式使用某些 WAF 與 Web 瀏覽器內建 XSS 過濾器時的技術；另一個例子，Web 應用程式將不可信任的十六進制資料轉換成 UTF8 編碼字符串並顯示，上述的 XSS 過濾器無法檢測對此 Web 應用程式的攻擊；而本論文提出的方法可以檢測到這樣的攻擊。

2.2 安裝於應用程式中 XSS 保護機制

另一種方法是修改應用程式代碼，因為必需手動更新應用程式代碼而且僅適用於特定應用程式語言，所以這種方法是相對困難的。但是此方法用於應用程式代碼

中，因此可以準確檢測和處理不受信任的資料。

一種伺服器 XSS 的基本保護方法是跳脫（escape）不受信任的資料中的 HTML 特殊字符，但因為清理所有不受信任的資料在某些情況下變得非常困難。

此外，還有一些使用在 Web 應用程式伺服器中構建政策（policy）以驗證 HTTP 回應的方法，該政策用於防止 Web 瀏覽器加載應用程式管理員不想要的代碼。但是由於這些方法需要對每個應用程式進行組態設定，且必需重寫代碼，這對伺服器管理員來說是一個很大的負擔。

2.3 Web 瀏覽器內置 XSS 過濾器

一些 Web 瀏覽器內置防止 XSS 攻擊機制，例如 IE 8 使用 XSS 過濾器和 Google Chrome 使用 XSS Auditor，這些過濾器檢測及防止 HTTP 請求中的攻擊代碼；這些防止 XSS 攻擊機制與 WAF 中的 XSS 過濾器具有相同的問題。

（三）本論文的方法

本論文提出了一個新的 XSS 過濾器，Xilara（基於 HTML 模板恢復的 XSS 過濾器），從 HTTP 回應中恢復 HTML 模板並使用它們檢測 XSS。

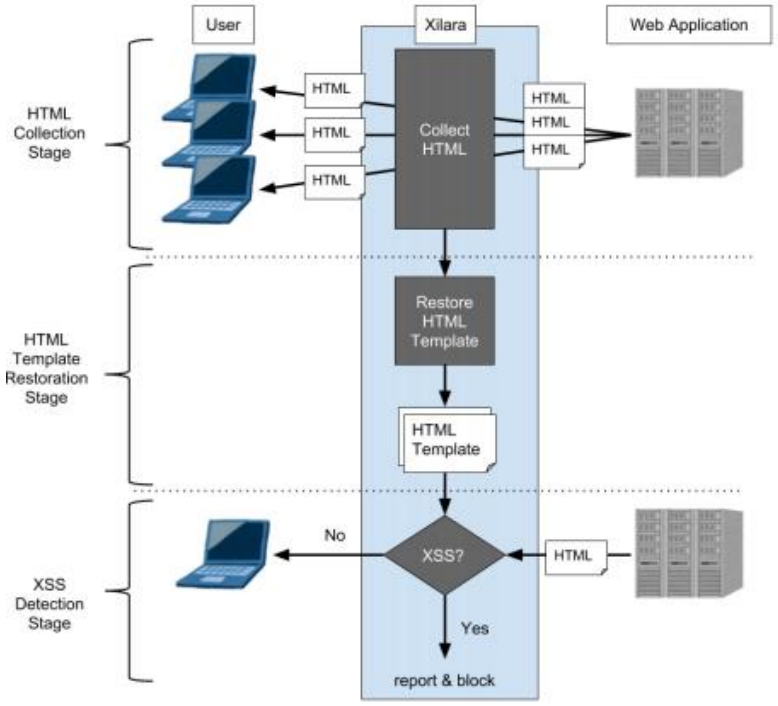


圖 3 Xilara 的概述

圖 3 顯示了 Xilara 的概述，Xilara 運作包括以下三個階段：（1）HTML 收集階段—Xilara 從 Web 伺服器收集 HTTP 回應持續一段時間；（2）HTML 模板恢復階段—Xilara 嘗試從 HTTP 回應恢復 Web 應用程式使用的 HTML 模板；（3）XSS 檢測階段—Xilara 使用恢復的 HTML 模板來檢測 HTTP 回應是否含有 XSS 攻擊。

3.1 HTML 模板

本論文將 HTML 模板定義為由以下節點組成的值組：

Tag－此節點表示具有 HTML 元素列表的 HTML 元素及成對的屬性名稱及其值。

Loop－此節點表示至少連續出現一個 HTML 模板。

Optional－此節點表示有時會出現一個模板有時候不會出現。

Ignore－此節點表示無法還原 HTML 模板的元素。

3.2 HTML 收集階段

在第一階段，Xilara 充當 HTTP 代理並收集 HTML 檔案。此階段需確保收集的 HTML 檔案是一個沒有任何 XSS 攻擊的 HTML 檔案，因此應用程式是在沒有攻擊者的環境中工作。

3.3 HTML 模板恢復階段

在此階段，Xilara 從 HTML 檔案中恢復在前一階段收集的 HTML 模板，Xilara 應用現有 ExAlg 和 RoadRunner 等演算法。這些演算法輸出的 HTML 模板節點模會對應 Tag 節點、Loop 節點、Optional 節點等。因此，我們可以由這些演算法輸出的 HTML 模板轉換成 Xilara 可處理的 HTML 模板。Xilara 會根據每個屬性的值是否是 javascript 開頭以產生 HTML 模板。

3.4 XSS 檢測階段

在此階段，應用程式是在外部攻擊者可以造訪應用程式的真實環境中運作。Xilara 擔任反向 HTTP 代理並監視客戶端和服務器之間的通信，Xilara 透過檢查應用程式伺服器向使用者發送的 HTML 文件檔案是否是前一階段恢復的 HTML 模板的

實例以檢測 XSS。

（四）評估

4.1 具有特定漏洞的深度評估

為了評估 Xilara 的處理速度和 XSS 檢測能力，本論文用一個 Web 應用程式和兩個 WordPress 插入物件進行實驗評估；目標應用程式如表 3 所示。本論文使用的 MacBook Pro 2016 配備 2.9 GHz Intel Core i5 CPU 和 8GB 記憶執行實驗評估。

表 3 用於實驗的應用程式和漏洞

Application	Version	CVE or vuln info
Webmin	1.678	CVE-2014-0339
Count Per Day	3.5.4	https://wpvulndb.com/vulnerabilities/8587
AffiliateWP	2.0.9	https://wpvulndb.com/vulnerabilities/8835

表 4 列出上述受攻擊頁面的平均回應時間（計算十次）以及 Xilara 解析 HTML 檔案和檢查 XSS 攻擊所用的平均時間；實驗結果顯示 Xilara 的處理時間適中或低。

表 4 Xilara 的執行表現

Application	Response time	Xilara overhead
Webmin	423.46ms	14.16ms
Count Per Day	109.72ms	27.5ms
AffiliateWP	186.84ms	21.4ms

4.2 使用易受攻擊的網站資料集進行大規模評估

接下來，本論文使用更多 Web 應用程式進行實驗來研究 Xilara 與另一個 XSS 過濾器之間的行為差異。本論文用 OpenBugBounty 作為評估資料集，OpenBugBounty 列出包含 XSS 漏洞和針對頁面的攻擊代碼。

表 5 列出 Xilara 和 ModSecurity 與 OWASP ModSecurity CRS 之間 XSS 檢測率和 XSS 誤檢測之比較。

表 5 針對攻擊 URI 的 XSS 檢測率

	Xilara	ModSecurity with CRS
All attacks (3,417 attacks)	94.5%	99.6%
Attacks using some encodings (9 attacks)	88.9%	0%

表 5 中的第 1 行呈現針對 3417 個攻擊 URI 的 XSS 及 ModSecurity 檢測率：Xilara 檢測到 3,230 個 XSS 攻擊（94.5%）；Xilara 不能檢測 121 個 HTML 文件檔案中的 XSS 攻擊（它無法恢復 HTML 模板）；Xilara 無法檢測 66 個 HTML 文件檔案中的 XSS 攻擊（雖然它可以恢復 HTML 模板）。ModSecurity 可以檢測到 99.6%的攻擊，因為它使用識別攻擊模式（pattern）技術。

表 5 中的第 2 行呈現針對 9 個編碼攻擊 URI 的 XSS 及 ModSecurity 檢測率：ModSecurity 無法檢測到所有用 base64 或十六進制編碼的 9 種攻擊。Xilara 檢測到其中 8 起攻擊，而 Xilara 未能恢復其中 1 次攻擊的 HTML 模板。

（五）結論

本論文提出一個新的 XSS 過濾器，解決攻擊者可以繞過現有 XSS 過濾器檢查 HTTP 請求中的攻擊代碼的問題。本論文主要想法是 HTTP 回應中的有害 HTML 文件檔案具有不同的結構，而許多 Web 應用程式生成 HTTP 回應中的 HTML 文件檔案具有非常相似的結構、相同的計畫。Xilala 先在無害的 HTTP 回應中收集 HTML 文件檔案，然後，Xilara 確認 HTTP 回應中的 HTML 文件檔案的結構是否可以從還原的模板生成以檢測 XSS 攻擊，如果 HTTP 回應的文件檔案結構與模板不匹配，則判定此 HTTP 回應為有害。本論文將 Xilara 實作為客戶端與客戶端之間的 HTTP 反向代理服務器，且 Xilara 可與現有的 XSS 過濾器共存。

本論文進行實驗以評估 Xilara 的性能，先從 OpenBugBounty 收集了 XSS 攻擊資料集並確認了 Xilara 檢測到 94.5%的 XSS 攻擊，但誤判了無攻擊的 HTTP 回應中的 20.6%為 XSS 攻擊。Xilara 還可識別 XSS 編碼攻擊，而現有的 XSS 過濾器無法檢測到這些攻擊。此外，實驗結果顯示 Xilara 的處理時間為適中或低。因此，整體而言，Xilala 是一種有效可以檢測 XSS 攻擊的技術。

四、論文主題 2：用於增強網際網路網域表現力的超策略框架（A Metapolicy Framework for Enhancing Domain Expressiveness on the Internet）

（一）引言

網域名稱是識別電腦、網路、服務和網上的其他資源的標準方式。網域安全策略提供網域所有者可以透過它指定的規則藉由網域名稱以限制使用者存取電腦、服務或資源一種方法。

目前，大多數網域安全策略都是單獨指定並使用 DNS 基礎設施發布（例如 SPF、DKIM 及 DMARC）或在網域 Web 伺服器上指定並通過專用的 HTTP 標頭與策略代理進行通信（例如 HSTS 及 HPKP）。

在某些情況下安全策略是無法自動強制執行且需使用者環境配合，而造成安全策略失效，這種情況的例子是接受或拒絕與網域的安全連接時提交過期證書。但是大多數安全策略都是由軟體供應商與網際網路社區進行標準化及管理，且網域名稱不能影響這些程序，只能遵循這些用於規範其安全策略之標準。

現有的安全策略機制是不完備，基於下列原因未來的網際網路需要更高水平的網域名稱表達能力：

1. 使用者不熟悉在策略代理人要求時做出安全決策。先前研究，觀察到許多使用者甚至沒有注意到瀏覽器安全指示（如掛鎖圖標），或者他們忽略瀏覽器顯示給他們的警告而仍然進行點擊動作。
2. 由於可擴展性原因，軟體供應商與網際網路社區僅導入全局及通用策略，而不關注特定網域政策。但是全局策略可能不適合網域所有不同的資源、服務及商業模式。一個具體的例子是非安全關鍵網站（如新聞或資訊網站）主要向訪問者顯示只讀內容，並在廣告上獲利。在這種情況下，網站可能希望放寬其安全策略並顯示訪問者的內容（與廣告），即使某些安全屬性未得到滿足（例如網站的證書已過期）。另一方面，電子銀行網站可能需要更嚴格的安全策略，必須在證書錯誤的情況下產生錯誤，並且不允許其用戶

與網站連線。當前的政策規範幾乎不考慮特定領域的要求。

3. 軟體供應商實施政策的結果是不同的軟體可能會不一致地強制執行這些策略，尤其是當政策規範留下一些選擇給開發人員的情況。例如如果瀏覽器不統一實施策略，它可能導致使用可以從一個瀏覽器切換到另一個瀏覽器，以克服產生的政策錯誤。因此任何新的安全框架政策規範可以由相對性的網域指定與減少管理軟體供應商、使用者代理甚至用戶的參與得到一些益處。

4. 降級攻擊，如剝離政策標題；政策標題可以由中間人（MITM）對手操縱，或者在客戶端透過修改後的方式達成（如惡意瀏覽器擴展）。這樣的標題剝離可能會導致降級攻擊，攻擊者可以向客戶端假裝聯繫的網域不會部署給定的策略。第三方擴展，例如 Google Chrome 的修改標頭功能可用於修改或剝離 HTTP 標頭，使應用程式層更容易破壞本身的安全策略。

5. 已有一組安全策略是透過網域表達；因此，如果網域可以輕鬆表達和管理更多安全策略，網際網路安全則可能會有更多的受益。

為了更好地表達網域級安全策略，本論文建議使用 metapolicy 框架（超策略框架），網域可以通過它來指定和管理綜合他們的安全政策。此框架利用 DNS 基礎結構用於發布和存取 metapolicy，以及 TLS 或 DNSSEC 信任基礎結構提供必要的安全層。

（二）需求與挑戰

在當前的網際網路，沒有由網域所有者可以全面而安全的框架可以輕鬆定義、管理、存儲及發布安全策略。本論文定義了一組這樣的安全策略要求框架應遵循以增強網際網路上的網域名稱表達能力。這些包括：

1. 易於管理：新的策略規範框架或協議必須使網域很容易指定、管理和發佈各種安全性政策以具有足夠的安全保障威脅。

2. 安全性：協議必須提供策略之安全性，例如策略代理可以驗證其真確性。

3. 可部署性：協議必須易於部署、管理及使用。此外，應使用現有政策傳播與保護政策之基礎設施，以大幅度降低營運及部署成本。

4. 可恢復性：協議不應該以不可恢復的狀態結束。在策略配置錯誤的情況下，它必須提供合適的恢復機制。

5. 適應性：協議必須可以適應當前部署機制而無需進行重大修改。

6. 可用性：策略應具高度可用性及公開存取性。

（三）高層次概述

為了滿足上述要求，本論文提出一個全面而安全的 metapolicy 網域安全策略規範與管理框架。該框架允許網域指定、管理所有現有的網域級安全策略作為 metapolicy。Metapolicies 在 DNS 中發布時，使用現有的 TLS 或 DNSSEC PKI 基礎設施進行保護。

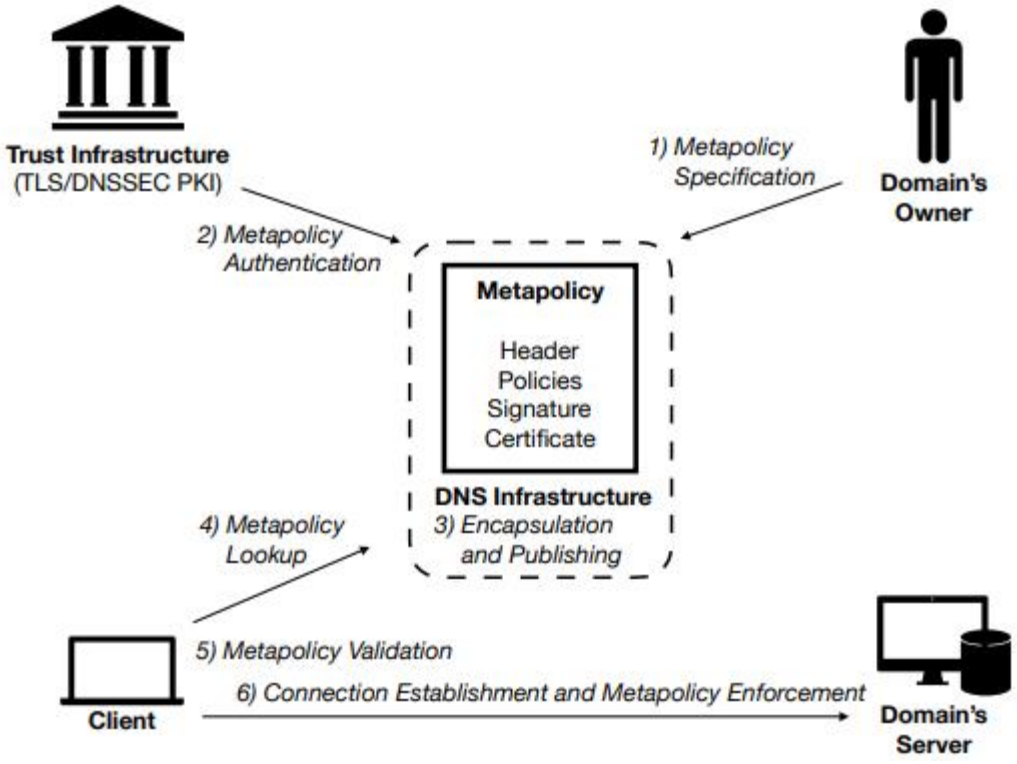


圖 4 Metapolicy 框架的高層次概述

圖 4 為 metapolicy 框架的高層次抽象概述，相關順序工作流程描述如下：

1. Metapolicy 規範：網域級策略是由網域所有者使用 metapolicy 框架的策略規範格式所定義描述（下一節說明 metapolicy 格式的內容）。

2. Metapolicy 身分驗證： metapolicy 使用網域的 X.509 TLS 證書私鑰或 DNSSEC 密鑰簽章。因為 TLS 證書（或 DNSSEC 密鑰簽章）可以被驗證，所以 metapolicy 綁定網域也可以驗證。

3. 封裝與發布：已簽章的 metapolicy 被發布在 DNS 中。為此，必須將 metapolicy 編碼為資源記錄；在 DNS 中發布 metapolicy 會增加基礎架構成本及延遲。

4. Metapolicy 查詢：當使用者拜訪網域時策略代理隨時可以查詢策略（例如當 DNS 解析網域名稱時）。

5. Metapolicy 驗證：使用網域的 TLS 證書公鑰或 DNSSEC 公鑰驗證 metapolicy 的簽章；metapolicy 的所有資訊都必需被驗證。

6. ※連接建立和 metapolicy 執行：一旦完成驗證 metapolicy 的內容，個別安全策略會被提取並在拜訪網域的服務及資源期間會由策略代理強制執行其規範。

（四）框架的內容

上述的框架，所有網域安全策略都包含在其中單一的 metapolicy。每個 metapolicy 包括：

－標題：此部分包含有關 metapolicy 的 metadata。

－策略：此部分包含網域各種所有者指定的安全性策略的實際內容。

－簽章：此部分包含使用網域的 TLS 證書密鑰或 DNSSEC 密鑰產生的簽章。

－證書：此部分包含網域的 TLS 證書鏈。當 metapolicy 是使用 DNSSEC 密鑰簽章，則此段是空的；網域的 DNSSEC 密鑰可以透過 DNSKEY 記錄獲得。

Metapolicy 的生命週期：

(1)創建：網域透過所指定安全策略來產生其 metapolicy，然後使用與其 X.509 TLS 證書或其相關的私鑰 DNSSEC 私鑰對 metapolicy 進行數位簽章。最後，已簽章的 metapolicy 被發布在 DNS 成為一系列的 TXT 記錄。

(2)查詢和實施 metapolicy：每當策略代理收到一個連接到網域的請求，它獲取來自該網域（如果沒有緩存）的 DNS TXT 記錄的 metapolicy；如果網域 metapolicy 已被策略代理緩存是，只有第一個 DNS TXT 記錄會被下載；而 metapolicy 內容的完整性及真實性由電子簽章得到了保證

(3)更新和恢復：至少有一個 metapolicy 的 section 需要更新時，則進行 metapolicy 更新。

（五）相關分析

5.1 安全分析

本論文假設與 DNS 的第一個連接沒有受到攻擊，因為如果是這種情況，那麼中間攻擊者就可以查看所有後續通訊內容而客戶永遠不會達成 metapolicy。我們也假設用戶的系統和策略代理是可信的，系統無惡意軟體。

基於上述假設，metapolicy 框架可能於下列情況會受到損害：（1）策略代理或用戶在策略失敗時做出錯誤的決定，或者（2）當用於簽署元策略的密鑰被洩露或使用 PKI 時受到了損害。

對於第一種情況，因為所有資訊都存在於 metapolicy 中且由網域所有者指定；策略代理或用戶不參與在政策失敗期間做出決策。因此，用戶的不當決策或從向後兼容的規定而引發攻擊將不會發生。因為策略代理可以緩存 metapolicy 記錄，透過使用 metapolicy 框架，降級攻擊的可能性也降低了。

攻擊者能破壞網域的私鑰或能獲得私鑰代表可以產生網域的惡意證書以建立惡意的 metapolicy。在這種情況下，網域所有者可以啟動恢復機制，撤銷惡意公鑰並建立新的 metapolicy。

因此本論文提出的 metapolicy 框架是安全的。

5.2 可部署性

由於本論文提出的 metapolicy 框架使用 TLS 或 DNSSEC 密鑰簽署 metapolicy，因持所有支援 TLS 或 DNSSEC 的網域都可以部署此框架。為了要了解有多少域可以部署本論的框架，本論文對 Alexa 排名前 100 萬的網域列表的 120K 頂級網站的資料集進行了實驗分析並使用 tls-scan 庫獲取這些統計結果。實驗結果顯示大約 77.8%網站支援 TLS，2.6%的網站支援 DNSSEC，因此目前大部分網站都可以使用 metapolicy 框架。另外，目前約 76.3%網域至少設置了 1 個安全策略；32.67%網域至少設置了 2 個安全策略。

5.3 額外負擔

(1)Metapolicy 大小：TLS 證書鏈的大小是影響 metapolicy 總體大小的主要因本本論文使用 openssl 工具，進行在 Alexa 13k 頂級網站的實驗，發現網域的 TLS 證書鏈平均大小大約是 4.75KB。因此，使用 TLS 證書保護的 metapolicy 將含有平均 4.75 KB 大小的證書鏈。

(2)延遲：另一個額外負擔是獲取 metapolicy 所需的額外時間。為計算此額外負擔，本論文執行了發送 DNS 查詢的實驗計算獲取單個 DNS TXT 記錄所需的時間。在網路下載速度為 13 Mbps 的系統上，拜訪的平均時間約為 20 ms，在相同的設備中獲得額外的 10 條記錄，即使是最糟糕的情況順序，也會增加約 200ms 延遲（對於平行查詢的記錄，應該只有大約 20ms）。因此，本論提出的 metapolicy 框架增加的時間延遲是可接受的

(3)計算的額外負擔：為確定證書驗證的計算額外負擔（發生於客戶端的簽名驗證），本論文使用了 OpenSSL 程式庫和在上述的實驗中獲得的證書鏈，發現平均需要 4ms 用於證書鍊和簽名驗證過程。

（六）結論

本論文提出了一個增強網際網路網域表現力的 metapolicy 框架，本方案為網域提供了定義和管理與網域相關的安全策略的機制。此機制的所有相關的網域以及強制執行的網域可以由對應網域的 TLS 證書私鑰或 DNSSEC 密鑰簽章的 metapolicy 達成。Metapolicy 發布一系列網域的 DNS TXT 記錄，因此不需要新的基礎設施，本方案可以部署於現存的環境。

本框架使得網域擁有者可以輕鬆地自行管理策略，因為此機制指定了故障轉移機制必須遵循 metapolicy，軟體與用戶都無法決定政策失敗作法，因此可以減少因用戶或其用戶代理錯誤的決定而導致降級攻擊的可能性。它還提供了一種簡單的管理方式及策略規範（例如 HTTPS 相關的安全策略，包括 HSTS、HPKP 或電子郵件相關的安全策略，包括 SPF、發件人 ID、DMARC，DKIM 或其他安全政策，包括 DANE 或 CAA）。相信未來透過本論文的 metapolicy 框架，網域可以表達更多的安全策略。

五、論文主題 3：用於保護隱私資料共享的安全及高效多方目錄發布（Secure and Efficient Multi-Party Directory Publication for Privacy-Preserving Data Sharing）

（一）引言

在巨量資料時代，個人資料以數位形式產生、蒐集和利用，為社會帶來前所未有的便利。資料的生產和利用在不同的網路端點，通過 Internet 共享特定於人的資料成為廣泛在各種領域中的流行的應用範例，應用範圍從電子醫療保健、社交網路、物聯網及惡意軟體檢測等。

公共目錄服務是關鍵的資料共享組件：資料利用者在資料共享中工作流，查詢目錄服務以尋查感興趣的資料；目錄服務維護私有生產者位置資訊，並連接資料利用者和生產者。例如在電子醫療的 HIE（醫療資訊交換）是一個新興的資料共享平台，其中名為 locator service 的目錄服務幫助醫生（資料利用者）找到患者的電子病歷（EMR）（資料生產者）。資料位置資訊（"患者去過的醫院"）可能會洩露隱私敏

感的事實；例如知道某位名人去過勒戒中心，便可以推斷他/她可能有毒品問題。

構建目錄的一種簡單方法是任何資料生成者直接發布其相關人員列表(例如去過醫院的患者列表)；而這種方法於網路公開了私有位置資訊，此項隱私資料的暴露洩露了"可識別資訊"並且違反個人資料保護法。

本論文解決上述分散式隱私保護目錄發布（distributed, privacy-preserving directory publication）的問題－例如保護 HIE 的資料位置資訊（"患者去過的醫院"）；而此發布問題可以模式化為安全的多方計算（Multi-Party Computation 簡稱為 MPC）問題。目錄發布的簡單作法是將"整個"發布邏輯轉入 MPC 協議中，但會導致高度額外計算負擔並且是無效率；傳統的補救措施是識別計算的"私有"部分並僅將該部分轉換至 MPC，但這種方法對本論文的問題仍是非常沒有效率。

為了提高效率，本論文提出一個預先計算框架，可以最小化私有計算並對公共資料進行積極的（aggressive）預先計算；本論文提出具有不同程度的積極性預計算策略，可以幫助優化適應具有不同私有資料大小的情況。此外，本論文使用通用圖形處理單元（GPGPU）上的平行預先計算以提高系統效率並在實際的 MPC 軟體上實作及進行效能評估。

（二）研究之系統定義

2.1 系統模式

目標系統涉及三個角色：資料生產者，資料利用者和資料利用者主機的目錄服務。每個資料生產者都擁有一張個人記錄表而每筆記錄都以所有者的身份識別當作鍵值（key），資料利用者希望在所有生產者網站上找到這些記錄，該目錄服務幫助資料利用者"發現"相關資料生產者產生的記錄。

本論文主要使用 ε -隱私概念： ε -隱私的主要作法是限制干擾或假的發布生產者名單中的誤報率為 ε 百分比；將難以區分其真實性的假生產者混入真生產者中－例如目錄服務發布**"真"**資料位置資訊（"患者**去過**的醫院"）時混入 ε 百分比難以區

分的"**假**"資料位置資訊（"患者**未去過**的醫院"）。相似性是根據外部特質及共同認知來衡量的，例如在 HIE 中，醫院（生產者）之間的相似性可以由醫院專業及地理位置來定義。

ε -隱私可以由 top-K 演算法（圖 5）來達成：具體而言，給出一個真的生產者列表，top-K 演算法找到最接近真的 K 個假生產者，$K = \varepsilon \times |T|$ （$|T|$為真的生產者數量）。

```
1  TopK(true_producers T, all_producers S){
2    R = T;
3    while (less than K iterations){
4      //find NN in S to T
5      for (any j in S){
6        for (any i in T){
7          min_dist_j = min(dist(T[i],S[j]),min_dist_j);
8          min_j = j;
9        }
10       min_dist = min(min_dist,d);
11     }
12     R.add(S[min_j]);
13     S.remove(S[min_j]);
14   }
15   return R;
16 }
```

圖 5 達成 ε -隱私之 top-K 演算法

2.2 威脅模式及安全目標

本論文的目標是不信任的資料生產者間隱私保護目錄分散式發布；本論文的問題定義為"資料生產者自主運行並且不信任外部任何人（包括其他資料生產者）。

在此威脅模式中，攻擊者可以竊聽所有正在交換的資訊；資料生產者的威脅者可能是個網路竊聽者或其他資料生產者。

2.3 多方計算（Multi-Party Computation）

本論文使用現有的多方計算（MPC）協議，每個輸入都是私有的提供方（party），MPC 的協議確保不會洩漏任何有關的資訊，但 MPC 的高度額外計算負擔，使得 MPC 應用於真實的分佈式應用程式有其困難度。

（三）預先計算的安全目錄發布

3.1 MPC-based 發布方式（原來方式）

隱私保護目錄發布是 MPC 問題，等同於將圖 5 的 top-K 演算法應用於 MPC，此方式以 M_0 表示；以向量（例如醫院的專業）及相似性（每個生產者生產者之間可以通過漢明距離來表示 dist（））。這種 MPC 方法效率不彰，特別是在大量的個人紀錄共享情況，主要是因為昂貴的加解密運算（例如資料移轉遺忘要求）。

3.2 全部預先計算方式（本論文提出的方式）

為了減少 MPC 的使用，本論文提出全部預先計算。鑑於圖 5 的 top-K （T，S）演算法，其中只有輸入 T（真正的生產者）是私有的，我們預先計算 top-K （T，S）演算法公共輸入 S 和私有輸入 T 的所有可能值。預先計算產生所有不同 T 值的搜尋表，然後使用 T 的實際值搜尋此表。全部預先計算等於是計算 top-K（2^S，S），2^S 包含私有輸入 T 所有可能值（詳參二項式定理），此方式以 M_1 表示。

3.3 選擇式預先計算方式（本論文提出的方式）

本論文深入研究 top-K（）和有選擇地預先計算 top-K（）中的某些計算密集型部分。選擇性技術認為 top-K（）由不同粒度的距離計算組成：（1）選擇性預計算 M_2 考慮到預先計算 T 和 S-T 之間的距離 T 的所有可能值。（2）預先計算所有成對資料生產者

之間的距離，此方式以 M_3 表示。

（1） 選擇性預計算 M_2

預計算考慮了真生產者 T 的所有可能值，它預先計算 T^*和 S -T*之間的比較距離，產生了後續 MPC 的距離表。在 MPC 中，圖 5 的 top-K （T，S）演算法第 6 行到第 9 行，它被替換為搜尋預先計算距離表（使用 ms-PIR 協議實作搜尋距離表） 。

（2） 選擇性預計算 M_3

預先計算成對距離矩陣：對於任何資料生產者 s_1 和 $s_2 \in S$，預先計算它們的距離並將其存儲在一個表中。在 MPC 中，圖 5 的 top-K （T，S）演算法第 7 行的

dist（T [i]，S [j]）被替換為搜尋預先計算成對距離矩陣（使用 ms-PIR 協議實作搜尋成對距離矩陣）。

表 5 預先計算-MPC 架構下，修改過的 top-K （T，S）演算法

	Pre-compute	MPC+msPIR
M_0	-	$topK(T,S)$
M_1	$D_1 = topK(2^S,S)$	$Lookup_{msPIR}(D_1,T)$
M_2	$D_2 = dist(2^S,S)$	$topK2_{MPC}(T,S)$ invoking $Lookup_{msPIR}(D_2,T)$
M_3	$D_3 = dist(S,S)$	$topK3_{MPC}(T,S)$ invoking $Lookup_{msPIR}(D_3,T[i],S[j])$

3.4 平行預先計算方式（本論文提出的方式）

在本論文透過資料平行計算任務來實現平行預先計算，其中每個任務具有不同的輸入 value 在專用線程中運行，不同的線程同時運行而沒有同步；本論文在多核 CPU 和通用 GPU（GPGPU）兩者上實作平行預先計算框架。

本論文使用 pthread 程式庫實作多核 CPU 平行預先計算，在一個線程中打包多個可能的輸入值，並且線程數是兩倍的硬體超線程數；使用 CUDA 程式庫實作 GPGPU 平行預先計算，底層的 NVidia-Tesla GPU 具有全局內存 5 GB，線程在 65,635 個塊的一個網格中運行，每個塊包含 1024 個 GPU 線程，此結構允許將線程數量調整至 2^{27}，可以輕鬆處理超過 27 個資料生產者網路。

（四）案例研究：醫療保健資料定位及查詢

本論文之案例研究為公共定位服務應用於醫療保健資訊交換網路（HIE）。 HIE 是一個健康資料共享網路；共享的資料是患者電子病歷（EMR），資料生產者是醫院，每次患者就診皆會在 EMR 產生新的資料項目，資料利用者是臨床醫生。典型的應用場景是在臨床就診期間有效共享患者的 EMR，醫生診斷患者需要查看相關在遠程醫院生產和儲存的患者的 EMR。

（五）評估

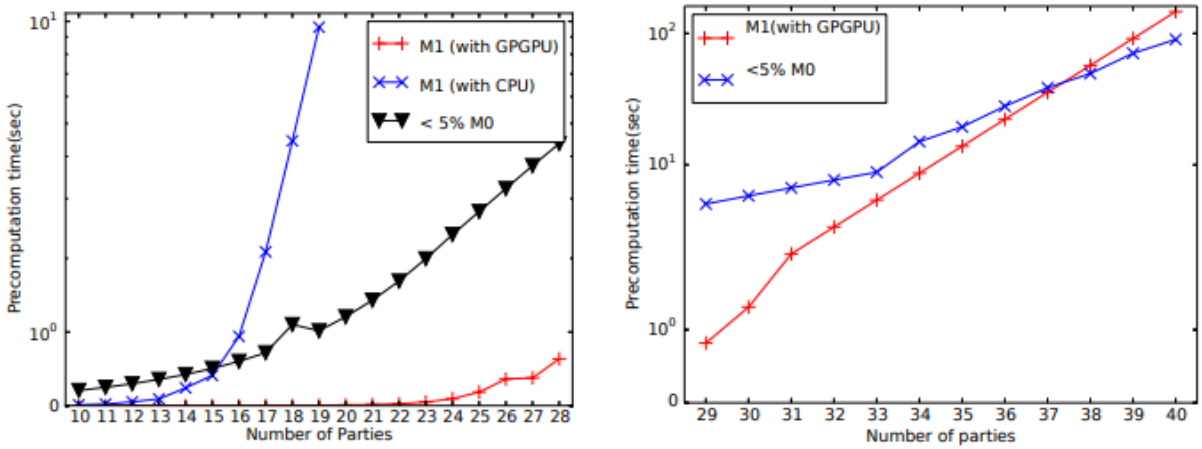
5.1 評估採用之資料集

（1） USNEWS 資料集：本論文使用 USNEWS 資料集模擬醫院概況。

（2） Open-NY 醫療保健資料集（'Sparcs"）：本論文使用 Sparcs 的 Open-NY 醫療保健資料集模擬病患資料概況。

5.2 目錄發布執行效率

（1）平行預先計算評估結果：本論文在多核 CPU 和 GPGPU 上實作平行預先計算，執行結果如圖 6 所示，其中還包括執行 M_0 的 5%執行時間（沒有任何預先計算）一個基線。



（a） With ≦ 28 parties　　（b） With > 28 parties

圖 6 多核 CPU 和 GPGPU 上平行預先計算執行結果

（2） ※MPC 的執行評估結果：本論文使用 GMW 及 PIR 軟體（皆為 open-source）實作 MPC 的目錄發布，執行結果如圖 7 所示；很明顯地，本論文提出的 M_1 方式比原方式 M_0 在 parties=39 的情況下快了 13 倍（執行效率 $M_1>M_2>M_3>M_0$）。

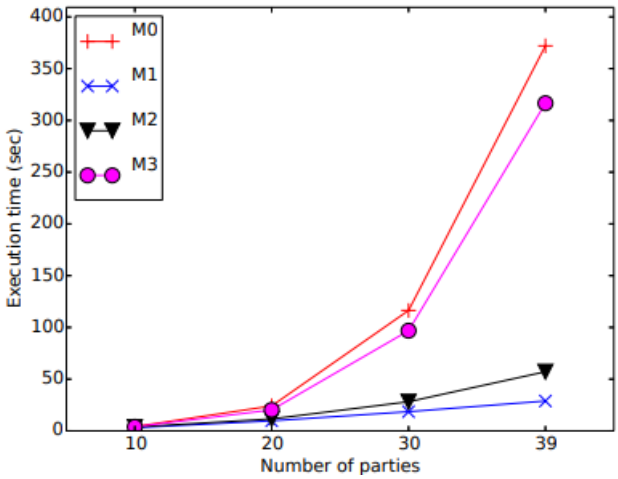


圖 7 多核 CPU 和 GPGPU 上平行預先計算執行結果

（六）結論

本論文提出了一個專為保護隱私量身制定的資料共享發布 MPC 預先計算框架。藉由最小化私有資料計算與以平行方式預先計算公共資料使得此預先計算框架得以改善 MPC 之執行效率；另外，本論文也提出 2 個選擇式預先計算方式。本論文證明了所提出的預先計算方式適用於真實的醫療保健方案，並藉由真實資料集和開源 MPC 軟體的實作，證明本論文所提出的預先計算方式確實能改善 MPC 之執行效率。

參、心得與建議

本中心每年皆派員參與各類重要國際會議，冀望藉由參加國際性之研討會，與世界各地之專家學者互動，汲取國際最新資通訊趨勢及相關資訊安全技術，並據以強化本中心資通訊安全技術及管理措施。本次參加由 European Alliance for Innovation(EAI) 主辦「第 14 屆 EAI 通訊網路安全及隱私權國際會議」(SecureComm 2018)，本會議彙集世界各地專家學者交流及分享有關資通訊安全領域之經驗，展示與討論最新資通訊安全技術創新趨勢及其遭遇之挑戰及解決方案。與會講者均將其最新研究成果公開，而且各有其獨到成果與見解；與會人員來自世界各地，如：美國、澳洲、德國、新加坡、日本、印度、臺灣及中國等，參與本次會議，對於各國資通訊安全領域之研究發展，有概括的瞭解。

謹以聚焦於本會議之網站系統安全、網路技術安全及通訊隱私權等主題，提出下列 3 點心得與建議供本中心及其他機關參考：

一、有效防範 XSS 攻擊之建議

XSS 攻擊是對 Web 應用程式最可怕的攻擊之一，此種攻擊手法一直列名於 OWASP Top 10，根據 XSS 攻擊預期的結果可以將 XSS 分為三種：（1）Reflected XSS：指網站會反應所輸入的 JavaScript，因此，當駭客在受害網站植入駭客的惡意 JavaScript，當被害人點擊該受害網站 URL 時，就會執行該 JavaScript。（2）Stored XSS：指讓 JavaScript 可儲存在網站資料庫中，最常見的例子就是網站留言板或是訊息。由於留言版可留的訊息格式不拘，因此，駭客就可把程式碼放在留言板中，等待下一個瀏覽該留言板的受害者。（3）DOM-Based XSS－是利用文件檔案對象模型（Document Object Model，DOM)的一種用戶端漏洞攻擊。常見的 DOM 攻擊的有

document.url、document.cookie、window.location.search、history.replaceState 等。

有效防範 XSS 攻擊方法：

（一）同時採用輸入過濾與輸出編碼

XSS 攻擊根本防護之道就是輸入過濾與輸出編碼；同時採用此兩層防禦，即使駭客發現其中一種方式的缺陷，另一種方式仍能在很大程度上阻止駭客攻擊。

（二）網頁應用程式安全檢測

為提高網頁應用程式之安全強度，應在開發階段先進行「源碼安全檢測」，待開發完成後再進行「黑箱安全檢測」。

（三）Web 瀏覽器內置 XSS 過濾器

例如 IE 8 使用 XSS 過濾器及 Google Chrome 使用 XSS Auditor。

（四）Web 應用程式防火牆中的 XSS 篩選器

主要的功能是防範注入網頁木馬、XSS 以及 CSRF 等常見漏洞的攻擊。

上述個別方法無法確保可防範所有的 XSS 攻擊，建議同時採用上述防範方式，再加上本次研討會提出之新的 XSS 過濾器 Xilara 來檢測複雜的 XSS 攻擊（例如攻擊是使用 base64 編碼之攻擊代碼），Xilara 可以透過檢查 HTML 文件檔案的結構來檢測 XSS 攻擊，而且 Xilara 可以與現有的 XSS 過濾器共存；同時採用上述方式就可提供有效的多層次 XSS 攻擊防禦。

二、網域安全策略之應用

國際間相關組織為了防治濫發電子垃圾郵件，在國際間的電子郵件交換協定上，制訂了 SPF、DKIM 以及 DMARC 等規範。收信服務器如 Gmail、Yahoo、Hotmail 等，在收郵件時會去檢查這些規範有無被加入，如果沒有，電子郵件很可能被判定成垃圾信件。

SPF 用來規範在選定的電子郵件發送服務器位址，可用來發送寄件人的網域郵

件，此機制可避免垃圾信濫發業者，偽裝網域發送假冒郵件。DKIM 是一種數位簽章，採用公鑰與私鑰加密驗證法進行。在發送電子郵件時由發信伺服器對郵件以私鑰進行簽章，而在電子郵件接收伺服器上會透過 DNS 到發信者的網域查詢 DKIM 紀錄，擷取上面記載的公鑰資料以驗證這封郵件的數位簽章，如果數位簽章無誤，則代表電子郵件確實為原始發信伺服器所發出。DMARC 是用來輔助 SPF 與 DKIM 的不足，用來讓發信端網域通知收件端郵件服務器，當遇到 SPF 與 DKIM 的設定檢查不過時，進行的處理方式（通過/隔離/拒絕）。

DNSSEC 的 Domain Name System Security Extensions，它主要是在現有 DNS 的基礎上，加入數位簽章的機制，用來驗證 DNS 伺服器解析結果的真實性，避免 DNS 快取中毒（DNS cache poisoning）攻擊的發生。DNS 解析網址是有階層性的，因此想要完整部署 DNSSEC，就必須從最高等級的 root，一直到下層的所有 DNS 伺服器，及個人端電腦都必須提供支援。上述安全策略可有效加強網路安全性，也漸漸全面普及應用，政府機關也應積極評估導入上述安全策略。

在某些情況下安全策略是無法自動強制執行且需使用者環境配合，而造成安全策略失效。本研討會提出一個全面而安全的 metapolicy 網域安全策略規範與管理框架之方案。本方案允許網域指定、管理所有現有的網域級安全策略作為 metapolicy，所有相關的網域以及強制執行的網域可由對應網域的 TLS 證書私鑰或 DNSSEC 密鑰簽章的 metapolicy 達成。Metapolicy 發布一系列網域的 DNS TXT 記錄，因此不需要新的基礎設施，本方案可以部署於現存的環境，代表其具有技術可行及方便性之價值。但一項安全策略的推行成功與否，除了技術可行性、方便性及成本因素外，仍需取決於是否有足夠的誘因迫使網路大眾接受此 metapolicy 框架方案，畢竟此方案仍是實驗室之產物，尚未接受市場考驗。

三、安全 MPC、預先計算或處理及平行運算技術之應用

（一）安全 MPC（Multi-Party Computation）技術之應用

當前政府如火如荼推動電子化政府及開放資料，但也會造成相對的資安問題，尤其是如何有效保護民眾個人資料；此外，歐盟為提升個人資料保護規範，並建立歐盟境內一體適用的規則，於 2016 年通過「一般資料保護規則」（General Data Protection Regulation, GDPR），如何保護個人隱私權已是刻不容緩的議題。

資料使用者在資料共享中工作流查詢目錄服務以尋查有感興趣的資料；目錄服務維護私有生產者位置資訊，並連接資料利用者與生產者，但由於目錄服務不當透露資料位置資訊（例如於電子醫療的 HIE 資料共享平台透露"患者去過的醫院"）可能會洩露隱私敏感資料，而安全 MPC 可有效解決此一問題；此一安全 MPC 技術值得政府機關於推動電子化政府及開放資料時加以參考應用，以有效保護民眾個人資料。

（二）預先計算或處理技術之應用

預先計算或處理技術應用範圍非常廣泛，從最常見的二元搜尋（預先將資料排序）到巨量資料分析，皆可加快後續的資料搜尋及計算分析等作業。本中心建置許多巨量資料分析平台，如果有大量資料運算分析時間過久情況，則建議可分析其資料運算的瓶頸，而將此瓶頸進行預先計算或處理，則可大幅提升後續資料運算分析的速度。

另外，本中心「強化商品流程溯源追蹤與跨域稽查整合計畫」委外服務案於分析相關商品流程溯源追蹤時，會建構一般圖（general graph）並利用工具以視覺化方式呈現；但圖論（graph theory）的一般圖在解決特殊問題（大都為 NP hard 的問題），無有效的演算法，只能限制圖規模的大小，以求在可容忍時間內找出問題解。如果分析其演算法瓶頸，而將此瓶頸進行預先計算或將原圖預先轉換成特殊圖（可能有好的有效率演算法），而不用侷限於圖規模的大小。

（三）平行運算技術之應用

另一種普遍採用提高演算法效率的方法就是平行化，但此法受限於平行運算之間的相依性，若平行運算之間是完全獨立則平行效果是最佳的，反之，有些演算法可能無法被平行化。受惠於多核 CPU 及 GPU 普及，平行運算已可普遍實作於單一電腦，因此，若採用高多核 CPU 及高效 GPU 再加上合適的平行運算演算法，一台普通的個人電腦於執行大量資料運算分析時，其運算速度甚至比頂尖工作站或伺服器更快；一款由美國 The MathWorks 公司出品的商業數學軟體 MATLAB，其平行運算工具箱增加支援 GPU 運算以大幅加快計算速度就是一個實例。

肆、附錄

一、會議攜回資料

（一）參加名牌

（二）大會手冊

二、會議議程

August, 08

Main Conference Day 1

8:00 Morning Coffee with Refreshments

8:00 - 18:00 Registration

8:30 - 9:00 Opening session

9:00 - 10:00 Keynote speech(Venue: Jasmine Room)

Title: A User Centric Approach to Secure Mobile Systems and Applications
Robert Deng (Singapore Management University)

10:00 - 10:30 *Coffee-break*

10:30 – 12:00 Session 1 IoT Security (Venue: Jasmine Room)

Session Chair: Aziz Mohaisen

A Secure Remote Monitoring Framework Supporting Efficient Fine-grained Access Control and Data Processing in IoT

Chen, Yaxing (Xi'an Jiaotong University); Sun, Wenhai (Virginia Tech); Zhang, Ning (Virginia Tech); Zheng, Qinghua (Xi'an Jiaotong University); Lou, Wenjing (Virginia Tech); Hou, Y.Thomas (Virginia Tech)

Securing the Smart Home via a Two-Mode Security Framework

Sisodia, Devkishen (University of Oregon); Mergendahl, Samuel (University of Oregon); Li, Jun (University of Oregon); Cam, Hasan (United States Army Research Lab)

Out of Kilter: Holistic Exploitation of Denial of Service in Internet of Things(short)

Setikere Sreedhara Murthy, Suhas Kala Bhairav (Singapore University of Technology and Design); Sachidananda, Vinay (Singapore University of Technology and Design); Elovici, Yuval (Singapore University of Technology and Design)

Augmented chain of ownership : Configuring IoT devices with the help of the blockchain(short)

Drame-Maigne, Sophie (Gemalto SA & Telecom SudParis, Universitat Paris-Saclay); Laurent, Maryline (SAMOVAR, Telecom SudParis, CNRS, Universitat Paris-Saclay); Castillo, Laurent (Gemalto SA); Ganem, Herve (Consultant)

12:00 - 13:30 *Lunch*

13:30 - 15:00 Session 2 User and Data Privacy (Venue: Jasmine Room)

Session Chair: Yingjiu Li

Secure and Efficient Multi-Party Directory Publication for Privacy-Preserving Data Sharing

Areekijseree, Katchaguy (Syracuse University); Tang, Yuzhe; Chen, Ju (Syracuse University); Wang, Shuang (UCSD); Iyengar, Arun (IBM Research); Palanisamy, Balaji (University of Pittsburg)

A Formal Logic Framework for the Automation of the Right to be Forgotten

Tiwari, Abhishek (University of Potsdam); Bendun, Fabian (Saarland University); Hammer, Christian (University of Potsdam)

Privacy-Preserving Biometric-Based Remote User Authentication with Leakage Resilience

Tian, Yangguang (SMU); Li, Yingjiu (SMU); Chen, Rongmao (National University of Defense Technology); Li, Nan (University of Newcastle); Liu, Ximeng (SMU); Chang, Bing (SMU); Yu, Xingjie (SMU)

Differentially Private High-Dimensional Data Publication via Markov Network(short)

Wei, Fengqiong (Nanjing University of Posts and Telecommunications); Zhang, Wei (Nanjing University of Posts and Telecommunications); Chen, Yunfang (Nanjing University of Posts and Telecommunications); Zhao, Jingwen (Nanjing University of Posts and Telecommunications)

15:00 - 15:30 *Coffee-break*

15:30 - 17:00 Session 3 Mobile Security I (Venue: Jasmine Room)

Session Chair: Sachin Shetty

Automated Identification of Sensitive Data via Flexible User Requirements

Yang, Ziqi (National University of Singapore); Liang, Zhenkai (National University of Singapore)

Understanding Android Obfuscation Techniques: A Large-Scale Investigation in the Wild

Dong, Shuaike (The Chinese University of Hong Kong); Li, Menghao (Institute of Information Engineering, Chinese Academy of Sciences); Diao, Wenrui (Jinan University); Liu, Xiangyu (Alibaba Inc.); Liu, Jian (Institute of Information Engineering, Chinese Academy of Sciences); Li, Zhou (ACM Member); Xu, Fenghao (The Chinese University of Hong Kong); Chen, Kai (Institute of Information Engineering, Chinese Academy of Sciences); Wang, Xiaofeng (Indiana University Bloomington); Zhang, Kehuan (The Chinese University of Hong Kong)

Transparent Low-Latency Network Anonymisation for Mobile Devices(short)

Koepsell, Stefan (TU Dresden); Byrenheid, Martin (TU Dresden); Naumenko, Alexander (TU Dresden); Strufe, Thorsten (TU Dresden)

Inferring UI States of Mobile Applications through Power Side Channel Exploitation(short)

Guo, Yao (Peking University); Ma, Junming (Peking University); Wu, Wenjun (Peking University); Chen, Xiangqun (Peking University)

August, 09

Main Conference Day 2

8:00 Morning Coffee with Refreshments

8:00 - 18:00 Registration

8:30 - 9:30 Keynote speech (Venue: Jasmine Room)

Title: Uncovering Server Side Vulnerabilities via Mobile App Analysis

Zhiqiang Lin, Ohio State University

9:35 - 10:45 Panel session(Venue: Jasmine Room)

Chair: Min Suk Kang

Title:Blockchain and its Emerging Applications

Panelists:Prateek Saxena (National University of Singapore), Stanley Yong (CTO, IBM), Aziz Mohaisen (University of Central Florida), Wenjing Lou (Virginia Tech).

10:45 - 11:05 *Coffee-break*

11:05 - 12:3 0Session 4 Wireless Security (Venue: Jasmine Room)

Session Chair: Wenjing Lou

An Adaptive Primary User Emulation Attack Detection Mechanism for Cognitive Radio Networks

Dong, Qi (Binghamton University); Chen, Yu (Binghamton University); Li, Xiaohua (Binghamton University); Zeng, Kai (George Mason University); Zimmermann, Roger (National University of Singapore)

VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs

Van der Heijden, RensWouter (Ulm University); Lukaseder, Thomas (Ulm University); Kargl, Frank (Ulm University)

Birds of a Feather Flock Together: Fuzzy Extractor and Gait-Based Robust Group Secret Key Generation for Smart Wearables

Javali, Chitra (National University of Singapore); Revadigar, Girish (Singapore University of Technology and Design)

Unchained Identities: Putting a Price on Sybil Nodes in Mobile Ad hoc Networks(Short)

Bochem, Arne (University of Goettingen); Leiding, Benjamin (University of Goettingen); Hogrefe, Dieter (University of Goettingen).

11:05 - 12:30 Session 5 Software Security (Venue: Hibiscus Room)

Session Chair: Sencun Zhu

Understanding the Hidden Cost of Software Vulnerabilities: Measurements and Predictions

Anwar, Afsah (University of Central Florida); Khormali, Aminollah (University of Central Florida); Nyang, DaeHun (Inha University); Mohaisen, Aziz (University of Central Florida)

Privacy-Enhanced Fraud Detection with Bloom filters

Arp, Daniel (Technische Universitat Braunschweig); Quiring, Erwin (Technische Universitat Braunschweig); Krueger, Tammo (Zalando Payments GmbH); Dragiev, Stanimir (Zalando Payments GmbH); Rieck, Konrad (Technische Universitat Braunschweig)

FriSM: Malicious Exploit Kit Detection via Feature-based String-Similarity Matching(short)

Kim, Sungjin (Korea Institute of Science Technology); Kang, Brent ByungHoon (Korea Institute of Science Technology)

A Machine Learning Framework for Studying Domain Generation Algorithm (DGA)-Based Malware(short)

Chin, Tommy (Rochester Institute of Technology); Xiong, Kaiqi (University of South Florida); Hu, Chengbin (University of South Florida); Li, Yi (University of South Florida)

12:30 - 14:00 *Lunch*

14:00 - 15:30 Session 6 Cloud Security I (Venue: Jasmine Room)

Session Chair: Kaiqi Xiong

Se-Lambda: Securing Privacy-Sensitive Serverless Applications Using SGX Enclave

Qiang, Weizhong (Huazhong University of Science and Technology); Dong, Zezhao (Huazhong University of Science and Technology); Jin, Hai (Huazhong University of Science and Technology)

CAVAS: Neutralizing Application and Container Security Vulnerabilities in the Cloud Native EraTorkura,KennedyAondona (Hasso Plattner Institute, University of Potsdam, Germany); Sukmana, MuhammadI.H (Hasso Plattner Institute, University of Potsdam, Germany); Cheng, Feng (Hasso Plattner Institute, University of Potsdam, Germany); Meinel, Christoph (Hasso Plattner Institute, University of Potsdam, Germany)

Shuffler: Mitigate Cross-VM Side-channel Attacks via Hypervisor Scheduling

Liu, Li (George Mason University); Wang, An (George Mason University); Zang, Wanyu (TAMU at San Antonio); Yu, Meng (University of Texas at San Antonio); Xiao, Mengbai (George Mason University); Chen, Songqing (George Mason University)

Building Your Private Cloud Storage on Public Cloud Service Using Embedded GPUs(short)

Cheng, Wangzhao; Zheng, Fangyu (Institute of Information Engineering, CAS, China); Pan, Wuqiong (Institute of Information Engineering, CAS, China); Lin, Jingqiang (Institute of Information Engineering, CAS, China); Li, Huorong (Institute of Information Engineering, CAS, China); Li, Bingyu (Institute of Information Engineering, CAS, China)

14:00 - 15:30 Session 7 Mobile Security II (Venue: Hibiscus Room)

Session Chair: Chitra Javali

PoliteCamera: Respecting Strangers' Privacy in Mobile Photographing

Li, Ang (University of Arkansas); Du, Wei (Michigan State University); Li, Qinghua (University of Arkansas)

Lexical Mining of Malicious URLs for Classifying Android malware(short)

Wang, Shanshan (University of Jinan); Yan, Qiben (University of Nebraska-Lincoln); Chen, Zhenxiang (University of Jinan); Wang, Lin (University of Jinan); Spolaor, Riccardo (University of Padova); Yang, Bo (University of Jinan); Conti, Mauro (University of Padova)

GranDroid: Graph-based Detection of Malicious Network Behaviors in Android Applications(short)

Li, Zhiqiang (University of Nebraska-Lincoln); Sun, Jun (University of Nebraska-Lincoln); Yan, Qiben (University of Nebraska-Lincoln); Srisa-an, Witawas (University of Nebraska-Lincoln); Bachala, Shakthi (University of Nebraska-Lincoln)

FGFDect: A Fine-Grained Features Classification Model for Android Malware Detection(short)

Li, Jianan (Institute of Information Engineering, Chinese Academy of Sciences); Liu, Chao (Institute of Information Engineering, Chinese Academy of Sciences); Yu, Min (Institute of Information Engineering, Chinese Academy of Sciences); Luo, Bo (University of Kansas); Li, Song (Institute of Information Engineering, Chinese Academy of Sciences); Chen, Kai (Institute of Information Engineering, Chinese Academy of Sciences); Huang, Weiqing (Institute of Information Engineering, Chinese Academy of Sciences); Lv, Bin (Institute of Information Engineering, Chinese Academy of Sciences)

15:30 - 16:00 *Coffee-break*

16:00 - 17:30 Session 8 Social Network and Enterprise Security (Venue: Jasmine Room)

Session Chair: Raheem Beyah

A Mobile Botnet That Meets Up at Twitter

Dong, Yulong (California State University, Sacramento); Dai, Jun (California State University, Sacramento); Sun, Xiaoyan (California State University, Sacramento)

Detecting Suspicious Members in An Online Emotional Support Service

Li, Yu (Wright State University); Kim, Dae Wook (Eastern Kentucky University); Zhang, Junjie (Wright State University); Doran, Derek (Wright State University)

Towards a Reliable and Accountable Cyber Supply Chain in Energy Delivery System Using Blockchain

Liang, Xueping (Institute of Information Engineering, Chinese Academy of Sciences); Shetty, Sachin (Old Dominion University); Tosh, Deepak (Norfolk State University); Ji, Yafei (Institute of Information Engineering, Chinese Academy of Sciences); (Institute of Information Engineering, Chinese Academy of Sciences)

Social Bot Detection Using Tweets Similarity

Wang, Yahan (Beijing University of Posts and Telecommunications); Wu, Chunhua (Beijing University of Posts and Telecommunications); Zheng, Kangfeng (Beijing University of Posts and Telecommunications); Wang, Xiujuan (Beijing University of Technology)

16:00 - 17:30 Session 9 Network Security I (Venue: Hibiscus Room)

Session Chair: Min Suk Kang

A Multi-Protocol Authentication Shibboleth Framework and Implementation for Identity Federation

Li, Menyi (Tsinghua University); Chi, Chi-Hung (Data61/CSIRO); Ding, Chen (Ryerson University); Wong, Raymond (University of New South Wales); She, Zhong (IntelShare Initiative)

SDN-Assisted Network-Based Mitigation of Slow DDoS Attacks

Lukaseder, Thomas (Ulm University); Maile, Lisa (Ulm University); Erb, Benjamin (Ulm University); Kargl, Frank (Ulm University)

A Holistic Approach Towards Peer-to-Peer Security and why Proof of Work Won't Do(short)

Prunster, Bernd (Secure Information Technology Center, Austria (A-SIT), Graz, Austria); Ziegler, Dominik (Know-Center GmbH, Graz, Austria); Kollmann, Christian (A-SIT Plus GmbH, Vienna, Austria); Suzic, Bojan (Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria)

A Robust Intrusion Detection Network using Thresholdless Trust Management System with Incentive Design(short)

Rezapour, Amir (National Chiao Tung University); Tzeng, Wen-Guey (National Chiao Tung University)

18:30 - 21:00 Banquet (Venue: Taste Restaurant in Hotel Ibis)

August, 10

Main Conference Day 3

8:00 Morning Coffee with Refreshments

8:00 - 12:00 Registration

8:30 – 10:00 Session 10 Applied Cryptography (Venue: Jasmine Room)

Session Chair: Girish Revadigar

Neural Network based Min-entropy Estimation for Random Number Generators

Yang, Jing (Institute of Information Engineering, Chinese Academy of Sciences); Zhu, Shuangyi (Institute of Information Engineering, Chinese Academy of Sciences); Chen, Tianyu (Institute of Information Engineering, Chinese Academy of Sciences); Ma, Yuan (Institute of Information Engineering, Chinese Academy of Sciences); Lv, Na (Institute of Information Engineering, Chinese Academy of Sciences); Lin, Jingqiang (Institute of Information Engineering, Chinese Academy of Sciences)

Improved Quantum Key Distribution Networks Based on Blom-scheme

Song, Ya-Qi (Institute of Information Engineering, Chinese Academy of Sciences); Yang, Li (Institute of Information Engineering, Chinese Academy of Sciences)

Implementation of High Throughput XTS-SM4 Module for Data Storage Devices

Zheng, Liang (Institute of Information Engineering, CAS); Li, Changting (Institute of Information Engineering, CAS); Liu, Zongbin (Institute of Information Engineering, CAS); Zhang, Lingchen (Institute of Information Engineering, CAS); Ma, Cunqing (Institute of Information Engineering, CAS)

Detecting and Defending against Certificate Attacks with Origin-Bound CAPTCHAs

Yegneswaran, Vinod (SRI International); Ahmad, Adil (Purdue University); Ahmad, Faizan (LUMS); Lei, Wei (Apple); Fareed, Zaffar (LUMS)

8:30 – 10:00 Session 11 Network Security II (Venue: Hibiscus Room)

Session Chair: Daisuke Kotani

A Metapolicy Framework for Enhancing Domain Expressiveness on the Internet

Varshney, Gaurav (SUTD); Szalachowski, Pawel (SUTD)

Adaptive Deterrence of DNS Cache Poisoning

Chau, Sze Yiu (Purdue University); Chowdhury, Omar (The University of Iowa); Gonsalves, Victor (Purdue University); Ge, Huangyi (Purdue University); Yang, Weining (Google Inc.); Fahmy, Sonia (Purdue University)

; Li, Ninghui (Purdue University)

Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout

Saghaian N. E., SayedM (The Pennsylvania State University); La Porta, Tom (The Pennsylvania State University); Jaeger, Trent (The Pennsylvania State University); Celik, Z.Berkay (The Pennsylvania State University); McDaniel, Patrick (The Pennsylvania State University)

On the Feasibility of Fine-Grained TLS Security Configurations in Web Browsers Based on the Requested Domain Name(Short)

Alashwali, EmanSalem (University of Oxford); Rasmussen, Kasper (University of Oxford)

10:00 - 10:30 *Coffee-break*

10:30 – 11:50 Session 12 **Cloud Security II** (Venue: Jasmine Room)

Session Chair: Zhiqiang Lin

Secure and Efficient Outsourcing of Large-Scale Overdetermined Systems of Linear Equations

Pan, Shiran (Institute of Information Engineering, Chinese Academy of Sciences); Zhu, Wen-Tao (Data Assurance and Communication Security Research Center, Chinese Academy of Sciences); Wang, Qiongxiao (Institute of Information Engineering, Chinese Academy of Sciences); Chang, Bing (Singapore Management University)

Privacy-Preserving Multiparty Learning For Logistic Regression

Du, Wei (Michigan State University); Li, Ang (University of Arkansas); Li, Qinghua (University of Arkansas)

Privacy-Preserving Outsourcing of Large-Scale Nonlinear Programming to the Cloud(short)

Li, Ang (University of Arkansas); Du, Wei (Michigan State University); Li, Qinghua (University of Arkansas)

A Verifiable and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data with Accuracy Improvement(short)

Zhang, Qi (National University of Defense Technology, China); Fu, Shaojing (National University of Defense Technology, China); Jia, Nan (National University of Defense Technology, China); Xu, Ming (National University of Defense Technology, China)

10:30 – 11:40 Session 13 **Web Security** (Venue: Hibiscus Room)

Session Chair: Berkay Celik

FrameHanger: Evaluating and Classifying Iframe Injection at Large Scale

Tian, ke (Virginia Tech); Li, Zhou (RSA Laboratories); Bowers,KevinD. (RSA Laboratories); Yao, Danfeng (Virginia Tech)

Xilara: An XSS Filter Based on HTML Template Restoration

Yamazaki, Keitaro (Kyoto University); Kotani, Daisuke (Kyoto University); Okabe, Yasuo (Kyoto University)

Local Storage on Steroids: Abusing Web Browsers for Hidden Content Storage and Distribution

Parra Rodriguez, Juan David (University of Passau); Posegga, Joachim (University of Passau)