4G/5G 多媒體系統之資安弱點檢測與威脅防護

文／翁健棋

第四代行動通訊（4G）自技術萌芽之初，發展至今已逾數十載，憑藉著更快的網速與更大的網路頻寬，許多過去在 3G 時代所面臨的技術障礙被一一克服，伴隨 4G 系統的出現，人們的生活也由「固定式」轉為「行動式」，獲得更大程度的便利性。科技發展日新月異，轉眼無線通訊領域也將進入「高速度、低延遲、多連結」的 5G 時代，面對嶄新技術架構一併帶來的未知資安挑戰，本院資訊工程學系李奇育副教授與其團隊，開發出一款適用 4G/5G 多媒體系統之資安弱點檢測模組，用以應對技術更新所產生的資安威脅。

從技術層面切入討論，已支援現有 4G 語音服務 VoLTE 和 VoWiFi 的 IP 多媒體子系統（IMS，IP Multimedia Subsystem）將在未來支援 5G 語音服務 VoNR （Voice over New Radio）和影像服務 ViNR （Video over New Radio），可見 IMS 系統是未來 5G 通訊生態系統提供服務的必要元件。換言之，該系統若存在資安弱點，將對 5G 通訊造成嚴重資安威脅。李奇育副教授與團隊成員利用所開發之檢測模組，檢測出三個存在於 IMS 系統中的重大資安漏洞;同時使用七個廠牌的手機，在台灣和美國共四個電信商網路中進行實驗，証實此三個資安漏洞將造成用戶承受包括：秘密通話拒絕服務攻擊（Denial of Service）、社交工程攻擊之幽靈通話與來電號碼偽裝攻擊等風險。

特別是前述第一項攻擊威脅一旦出現，將造成用戶在未收到警示，毫無防備的情況下，無法撥打或接收任何來電，對於使用者資安影響可見一斑。開發團隊也於檢測過程中發現，此三個資安漏洞主要分別發生於 IMS 系統的通話狀態機、通話管理和號碼驗證，攻擊者可以藉由 VoWiFi 的資安漏洞截取 VoWiFi 應用程式和 IMS 系統之間的會話連線，偽造對話啟動協定 SIP 封包，對 IMS 系統的三個資安漏洞進行攻擊。為了檢視此資安威脅可能帶來的最大損害，開發團隊設計了具自動調適的拒絕服務攻擊，實驗顯示，此攻擊對受害用戶的有效攻擊時間竟可達 99%，再次凸顯此漏洞急需解決應對之法，否則將產生極大的資安疑慮。

運用 AI 技術，開發團隊還發現現有 4G/5G 電信網路的另一個資安漏洞——通話資訊洩漏，它可被利用來對目標用戶的電話進行遠端偵測。也就是在用戶毫不知情的情況下，攻擊者僅需知道用戶的電話號碼，便可判斷其是否可為攻擊目標。為了應對上述潛在威脅，李奇育副教授與開發團隊除了將檢測結果回報給 GSMA 行動網路協會，同時提出系列解決方案，包含應用層資料來源認證、延遲通話資源綁定技術和通話管理限制分離；並使用開源軟體 OpenIMSCore 證明，該解決方案在不影響系統效能前提下之實踐可行性。一併搭配應用 AI 發展出的「來電號碼偽裝攻擊之防護檢測技術」，檢測來電通話是否為號碼偽裝攻擊，為 4G/5G 技術下新生之資安危脅提供對應參考解方。

隨著 5G 時代來臨，相關技術不僅在全球經濟發展中扮演關鍵角色，其於各行業、領域的應用範圍和規模也將逐步擴大，高速穩定的通訊技術一旦普及，潛在的資安威脅將讓人難以忽視。李奇育副教授與團隊成員所研發之資安弱點檢測與威脅防護技術，將有助於行動通訊技術標準（如 3GPP 和 GSMA）、國內外電信商、設備商和手機製造商，檢測和修補存在於多媒體服務應用程式和系統的資安風險。如此卓越貢獻，也將造福全球行動通訊技術相關產業，期待此項技術未來於運作系統中的實際應用！

4G/5G Multimedia Application Security Vulnerability Detection and Threat Protection

The fourth-generation mobile communication (4G) has been developed for more than decades since the mobile communication technology debuted. With faster network speed and larger bandwidth, many technical obstacles of 3G mobile network have been overcome. Moreover, the emergence of 4G has changed people's lives from "fixed" to "mobile" so that people have gained a higher degree of convenience. With the rapid development of technology in modern life, the wireless communication network is driving towards the 5G era, promising "high speed, low latency and massive connections". Facing the unknown challenges in information security associated with the new technical framework, Associate Professor Chi-Yu Li of the Department of Computer Science and his team have developed an information security vulnerability detection module for 4G/5G multimedia systems to defend against information security threats introduced by technology revolution.

From a technical perspective, the IP Multimedia Subsystem (IMS, IP Multimedia Subsystem), which supports the existing 4G voice services VoLTE and VoWiFi, will support 5G voice service VoNR (Voice over New Radio) and video service ViNR (Video over New Radio) in the future. The IMS system is definitely a key component for the future 5G communication ecosystem. In other words, if some information security weaknesses exist in the IMS system, it will pose a serious threat to 5G communications. Professor Li and his team used the developed detection module to identify three major information security vulnerabilities in the IMS system. In the experiment, they simultaneously used seven brands of mobile phones in four telecom networks both in Taiwan and in the United States. Finally, they have confirmed that these three security vulnerabilities can put a user's plan in jeopardy, such as secret call denial of service attacks (Denial of Service), social engineering attacks (ghost calls), and caller number spoofing attacks.

In particular, once the first attack threat mentioned above occurs, users are unable to make or receive any calls without warnings and precautions, thereby greatly affecting user experience with information security. During the detection process, the team also discovered that these three information security vulnerabilities are mostly found in the call state machine, call management and number verification in the IMS system. Through the security vulnerabilities of VoWiFi, attackers can intercept the connection session between the VoWiFi application and the IMS system, as well as create fake Session Initiation Protocol (SIP) packets, thereby attacking the three security vulnerabilities of the IMS system. In order to examine the maximal potential damage caused by the information security threat, the team designed a self-adaptive denial-of-service (DOS) attack. Their experiments show that the effective attack time of this attack on victims can reach 99%, which once again highlights that this vulnerability needs to be solved in no time, otherwise it will cause critical security concerns.

Meanwhile, the team uses AI technology to find another information security loophole in the existing 4G/5G telecommunications network: call information leakage, which can be used to remotely identify the target user's phone. In other words, an attacker can target the victim by the phone number without the knowledge or consent of the user. In order to deal with the above potential threat, Professor Li and his team not only reported the results to The Global System for Mobile Communications Association (GSMA), but also proposed a series of solutions, including application layer data source authentication, delayed call resource binding, and call control isolation. In addition, the team used the open-source software OpenIMSCore to demonstrate the practical feasibility of the solution while maintaining system performance. Combining with "Caller Number Masquerade Attack Protection Detection Technology", which checks if the incoming request is a request forgery attack by AI technology, this package provides a corresponding solution for the emerging information security threat under 4G/5G technology.

With the advent of the 5G era, related technologies not only play a key role in the development of the global economy, but also gradually expand the application scope and scale to diverse industries and fields. However, once the stable high-speed communication technology becomes popular, the following potential threat to information security would be too severe to ignore. The information security vulnerability detection and threat protection technology developed by Associate Professor Li and his team will assist mobile communication standards organizations(3GPP and GSMA), domestic and foreign telecom carriers, equipment manufacturers, as well as mobile phone manufacturers to identify and reduce application-level and system-related security risks of multimedia services. Such an outstanding contribution will also benefit the global mobile communication industry. We look forward to the practical applications of this technology in the system in the future.