國立中山大學資訊工程學系
(07)5252-000 轉 4301, 4302, 4303
804 高雄市鼓山區蓮海路 70 號

每週演講心得分享 08

Weekly Seminar Memoir 08

鄭欣明 教授

Prof. Shin-Ming Cheng

108 年 04 月 26 日(星期五)14:10~15:40
Apr. 26, 2019 (Fri.) 14:10~15:40
電資大樓 EC1009 室
EC 1009, Building of EE & CS

發布日期： 108 年 04 月 27 日

演講資訊

講題 TOPIC

5G 開源網路技術之應用：大規模的偽造基地台攻擊

Application of 5G Open Source Technology: A Large-scale Rouge Base Station Attack

主講人 SPEAKER

鄭欣明 教授/國立台灣科技大學資訊工程系

Prof. Shin-Ming Cheng / Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology

摘要 ABSTRACT

搭配近年來普遍的 5G 網路的開源網路軟體與便宜的軟體無線電平台，學者能實作出簡易的 5G 環境，並且驗證所設計的相關機制。本演講從資安的角度出發，以設計一個大規模惡意基地台攻擊，以說明 5G 開源網路的優勢與可行性。

With the aid of popular 5G open source software and cheap software defined radio, researcher could implement a simplified 5G environment and verify the corresponding mechanism. This speech starts from the perspective of security, and designs a large-scale rouge base station attack to describe the advantages and feasibility of 5G open source technology.

心得分享

戴立恩

碩士班一年級，無線通訊與行動計算實驗室

本次演講主要講述如何在未來 5G 環境中使用偽造基地台攻擊，讓使用者無法連線到電信公司基地台。在 LTE 中，現今的 4G 與未來即將出現的 5G，其兩者主要差別並不只於通訊技術上的差異，而是虛擬化的技術； 5G 將內部元件以軟體虛擬化後，可以節省許多外在成本，但相對的，Coding 難度便會提升很多，想於現有 4G 環境中使用偽造基地台是可行的，但是由於 AKA (Authentication Defined Radio)的出現，使得困難度提升，當使用者要連線到基地台，必須建立一個通道，然後進一步驗證身分，因此，我們可以利用這個通訊連結中的漏洞，於 AKA 之前實現攻擊。

攻擊行為是如何進行的？首先聽取附近基地台的基地台資訊，複製整個基地台，接著修改 TAC，此時手機發現區域變更便會去確認偽基地台，偽基地台可以有兩種方式來達到目的：第一個為發送 Reject message 給手機端，必須回到手機註冊前的狀態，此時手機便會向偽基地台傳送使用者端的資訊；第二個方法是令某個 TAC 認定所有基地台都不能連線，以達到使用者無法連上網路。目前要實現這個攻擊非常容易，因為成本低，甚至未來 5G 虛擬化後，我們也不需要透過外部硬體設備，只需要透過網路就能達成攻擊，使得被攻擊的對象無法上網，相信這種情形不久的將來即將發生，我們則可以先預想防備方案，例如：透過加入 Public Key 方式增加安全性...等等，以提升未來 5G 在使用上的安全。

白育誠

碩士班二年級，無線通訊與行動計算實驗室

系上今天演講邀請到臺灣科技大學鄭欣明教授，講者為我們介紹關於5G 的演進與資安問題。5G 是透過虛擬化的管理程式技術，使得網路傳輸的效率大幅提升，在基地台與使用者的資安問題上，講者提到透過 SDR 搭配 GNU 訊號，以及利用偽基地台(Rogue Base Station)進行惡意攻擊，使得用戶無法正確連上基地台，這種攻擊方法的成本非常低，但需要 telecom 的專業知識與系統分級的程式技術；攻擊步驟為：一、先取得周圍合法基地台資訊；二、修改 TAC ；三、回覆 TAU 否決；四、UE 執行 Attach procedure，此種攻擊使得用戶無法正確聯繫基地台，或造成使用者資料洩漏。

Rogue Base Station 所需電力及主機空間並不需要太大，而且攜帶容易，使得攻擊的機動性很高，缺點則是攻擊範圍小，但是將基地台進行虛擬化及動態規劃網路，則能解決攻

擊範圍小的缺陷，這項攻擊技術可應用於軍事攻堅，以取得敵方資訊及破壞其通訊能力。使用 Container Virtualization 的優點為 lightweight，並降低其架設成本，利用虛擬化技術能夠使攻擊方式很彈性，在未來 5G 網路中將可應用此 Rouge Base Station Attack 技術造成資安問題，不僅架設成本低、攜帶性高，可虛擬化的技術，未來將大大影響資料及通訊安全問題。

單　位：國立中山大學資訊工程學系
聯絡人：吳秀珍行政助理，分機 4301
　　黃莉萍行政助理，分機 4303
總　機：(07)5252000