VicOne

2022 年
汽車網路資安報告

VicOne Report

前言

過去一年，全世界各地的能源生產都發生了快速的變動，而汽車產業也跟上了這波變革。能源危機迫使許多政府重新檢討其可再生能源政策，電動車 (EV) 也趁勢崛起。不僅如此，一般大眾接觸到的汽車相關新聞也變多，越來越多人開始意識到該產業當前面臨的趨勢和問題。然而，改變是一把雙面刃，當人們邁開大步勇於改變時，很自然地會犯下一些錯誤，而在科技領域，改變總是伴隨著一些漏洞和缺失。

汽車資安問題排行榜

我們研究了 2021 年初至 2022 年 6 月為止有關汽車產業的新聞報導，結果發現了一些有趣的現象，同時也點出了目前真實世界的一些威脅。無鑰匙系統的問題在 2021 年的所有討論當中占了 26.1%，在 2022 年我們觀察的那幾個月中占 24%。無鑰匙系統的問題是人們直覺想到的第一個汽車資安破口，因為這項技術能讓歹徒在不插入實體鑰匙的情況下解鎖車門或發動引擎。

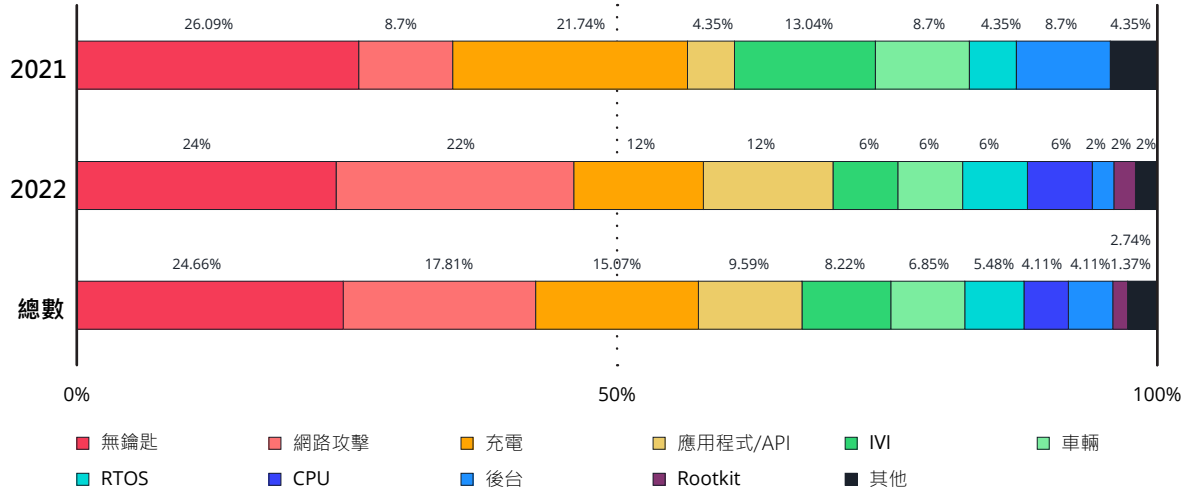

圖 1：汽車相關新聞報導所涵蓋的資安議題。

一般來說，無鑰匙遠端解鎖系統使用的是無線射頻 (RF) 訊號，但也可使用數位晶片卡或行動應用程式透過 RFID (無線射頻識別系統)、藍牙、NFC (近場通訊) 以及 UWB (超寬頻) 來運作。有時候，這些技術也可以彼此互相搭配使用。

車用資訊娛樂系統 (IVI) 是另一個新聞報導經常討論的議題。IVI 是使用者與車輛溝通的另一種管道，使用者可透過 USB、藍牙、Wi-Fi、SD 卡、DVD、觸控螢幕、GPS 或者手機連線來與該系統互動。最近，使用者甚至可經由網際網路連線從遠端遙控車輛，這會增加車用內部網路遭人從遠端駭入的風險。此外，IVI 還會經由 CAN 匯流排或乙太網路與其他車用電子控制單元 (ECU) 連接，等於為駭客提供一個可用來橫向移動的閘道口。基本上，IVI 提供了不少讓汽車更便利、更友善的功能，但卻也讓駭客有更多方式入侵車輛。駭客可修改 IVI 韌體，讓攻擊常駐於車內，並讓駭客將惡意封包注入車用內部網路連線。有些 IVI 系統還含有重大漏洞，例如，某導

航系統就存在著 Y2K22 臭蟲，會將時鐘重設回到 2002 年 1 月 1 日。還有另一個臭蟲是當系統遇到無副檔名的影像檔時會無法處理，導致系統重新開機或當機。最近，我們在「Pwn2Own 2022」駭客競賽中看到研究人員示範了一個遠端程式碼執行 (RCE) 漏洞，透過發送 CAN 訊息來開啟目標車輛的頭燈和雨刷，並且打開後車廂[1]。

除了車用系統之外，自從充電站與充電樁成為可能的攻擊目標之後，充電的問題也受到大量討論。充電站與充電樁就如同物聯網 (IoT) 裝置一樣，他們具備了軟體作業系統、除錯專用連接埠，並採用 CAN 通訊協定以及 PLC (電力線通訊) 協定。使用者可透過行動應用程式或是 API、RFID、藍牙、Wi-Fi、4G 來與充電站或充電樁互動。此外，也可透過網頁來互動，所以這些充電站也會連接到一個雲端後台伺服器。

去年，CVE 即收錄了一些充電站相關的重大漏洞。有些研究人員發現，使用者可利用網頁內寫死的登入憑證來存取充電站、修改組態設定，或者設定從遠端修改韌體。駭客還可發動一些網頁攻擊，如跨網站腳本 (XSS) 攻擊以及跨站請求偽造 (XSRF/CSRF)、伺服器端請求偽造 (SSRF) 以及暴力登入攻擊，進而與使用者互動並獲得存取權限或機敏資訊。有些設備存在著程式碼注入漏洞，可能讓駭客執行程式碼及下載新的韌體。這些漏洞還可能讓駭客經由 Wi-Fi 網路監控並修改系統，進而發動中間人 (MitM) 攻擊，攔截金鑰 (Token) 或 API、發動訊號干擾讓充電站無法運作，甚至可以免費充電。例如，2022 年有研究人員在研究充電樁[2] 時發現了一個存在於「隨插即充」(Plug-and-Charge) 功能中的漏洞，並利用這個漏洞來免費充電。

2022 年 2 月發生了一件值得注意的事件。一家知名車廠[3] 在其某家供應商遭到網路攻擊之後暫停營業了兩天。從此之後，我們便看到有更多供應商遭網路攻擊的事件。駭客通常是先竊取資料之後，再威脅企業如果不支付贖金就將機敏資料公布。

近年來，許多製造商都開始從事數位轉型，但大多數廠商卻很少考慮到網路資安的問題，因此讓供應鏈[4] 暴露於越來越高的資安風險中。規模較小的企業及供應商是比較容易得手的目標，因此容易引來駭客。這樣的威脅也同樣會危及汽車產業，因為只要供應鏈攻擊能造成營運中斷，那麼整個企業都將受到影響。

通用漏洞與暴露在外的攻擊管道

我們蒐集了 2021 年至 2022 年 6 月與汽車相關的通用漏洞及弱點 (Common Vulnerabilities and Exposures，簡稱 CVE)，同時也彙整了通用弱點列表 (Common Weakness Enumeration，簡稱 CWE) 的相關資料。CWE 是一個經由社群力量蒐集的軟體與硬體弱點清單。下表列出我們找到的 10 大弱點：

通用弱點列表 (CWE)	2021	2022	總數
複製緩衝區時未檢查輸入大小 (典型的緩衝區溢位)	30	3	33
重複釋放	3	3	6
未確實檢查輸入資料	14	0	14
網頁產生過程未確實中和 (neutralize) 輸入資料 (跨網站腳本)	15	3	18
整數溢位或繞回	15	3	18
NULL 指標位址解析	17	1	18
讀取超出邊界	29	3	32
寫入超出邊界	30	7	37
可觸發的斷言程式 (Reachable Assertion)	22	0	22
使用已釋放記憶體	22	9	31

表 1：十大 CWE 弱點 (2021 年 1 月至 2022 年 6 月)。

這些弱點可能造成的問題包括：資料損毀、系統或程式當機、阻斷服務 (DoS) 以及程式碼執行。它們如果發生在車輛當中，有可能會影響車輛的運作及安全。OEM 製造商及供應商應特別留意這些漏洞及弱點。我們將資料彙整成下圖並列出汽車及車用資安產業應該關注的議題，其中前三大議題分別是：系統單晶片 (SoC)、系統核心 (kernel)、即時作業系統 (RTOS)。

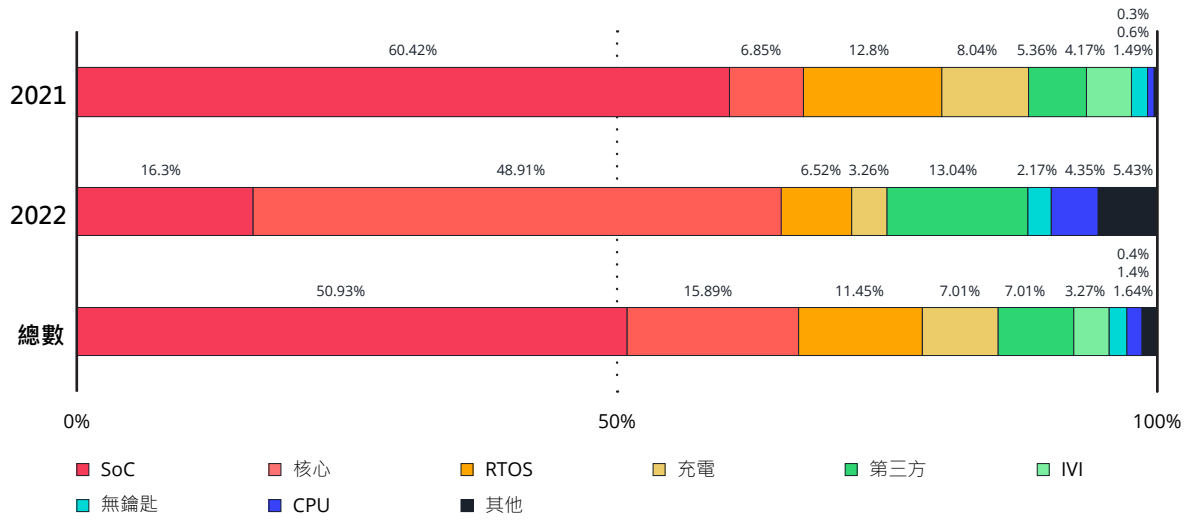

圖 2：CVE 排行榜漏洞對應的資安議題分布狀況。

SoC 問題

系統單晶片 (SoC) 是一種結合了多種不同運算模組的單一處理器，如：CPU 與繪圖晶片。車用連網 SoC 可支援 Wi-Fi、藍牙、2G/3G/ LTE/4G/5G，提供 C-V2X 車聯網通訊和 Dual Sim Dual Active (DSDA) 雙卡雙通功能。此外，也支援各種車用情境所需的定位功能，例如：無線電話、相機、顯示器、語音、音樂、耳機、喇叭、定位等等。不僅如此，一套採用 SoC 的可擴充電腦架構還可用來開發進階駕駛輔助與自動駕駛技術。其相關的晶片組也可能含有資安漏洞，造成硬體核心、音訊、多媒體、資料、數據機、甚至加密相關的問題。此外，還可能被用來避開安全機制與認證。

一般來說，硬體漏洞不容易修補，而且生命週期比其他漏洞更長。有時候，漏洞是電路的設計所造成，例如：預測執行處理器漏洞，而這些漏洞將永遠存在於 ECU 當中。其最好的解決方法就是修補軟體和作業系統來避開可能造成問題的情況發生。其他的硬體漏洞，或許可透過升級韌體來解決。以往，若要升級韌體，沒有將車輛召回維修中心幾乎是不可能辦到。但現在，OTA 更新技術已經越來越成熟，意味著車廠已經可以更完美、有效地解決問題。

核心與 RTOS 問題

核心問題是排行榜上第二名的漏洞，不過，核心跟 RTOS 的問題數量越來越多。而同時牽涉到兩者的漏洞，很明顯地是深植於軟體開發的問題。使用專屬軟體並不意味著就一定安全，封閉原始碼軟體仍會遇到開放原始碼軟體所遭遇的問題。毫無疑問地，今日的汽車產業正試圖利用開放原始碼軟體來快速打造一套紮實的軟體系統，並提供各式各樣的應用程式。但這樣一來，汽車也會承襲傳統軟體現有的資安問題。而這些問題的解決方法也並非涇渭分明。

ECU 是一個用來控制車輛引擎、雨刷、煞車及其他電子功能的裝置，其狀態深深左右著車輛的安全。一台車裡面可能包含多個 ECU，這些單元是由一些微控制器 (MCU、SoC、核心單元) 所組成，內含一個或多個 CPU、記憶體、輸入/輸出 (I/O)、類比/數位 (A/D) 轉換器，以及通訊連接 (如 CAN 匯流排或乙太網路)，還有嵌入式軟體。嵌入式軟體還包含一套專為硬體子系統所撰寫的作業系統 (絕大多數都是某種 RTOS 再加上一些裝置驅動程式)。

RTOS 是一種對資料及事件處理時間要求極為嚴格、不能有任何緩衝延遲的作業系統。RTOS 可分成幾種不同類型，但基本上都含有一個「硬式即時」(hard real-time) 作業系統，也稱為「安全攸關系統」(safety-critical system)，它可確保工作在指定時間內完成，並準確做出回應。許多 OEM 廠商和供應商都使用基於 Linux 核心的軟體解決方案，例如：汽車級 Linux (AGL) 或客製化系統，甚至是上游採用 Linux 長期支援 (LTS) 核心的 Android 系統。根據我們蒐集到的資料，駭客可能利用核心當中的一些漏洞在 MCU 上提升權限並注入或執行程式碼。

打造一個反應靈敏且安全的軟體系統至關重要，汽車產業應該考慮導入原始程式碼稽核與漏洞管理系統，並搭配一套軟體物料清單 (SBOM) 來進一步強化。想要徹底消除一套系統中的所有漏洞是不可能的任務，不過卻可以藉由一些努力來盡可能降低風險。

針對汽車產業的重大網路攻擊

根據我們對 2022 年的觀察以及汽車產業重大網路資安事件的分析，我們蒐集了 52 起重大事件來示範網路攻擊對該產業的影響層面。這些事件涵蓋了供應鏈的多個層面 (從供應商到經銷商)，證明它們幾乎會影響生產的每一個階段，而且每個月幾乎都有多起事件發生，毫無例外。

那麼這些事件主要有哪些類型？排行榜第一名和第二名分別是：勒索病毒與資料外洩。這兩種事件都會對受害企業或工廠造成重大影響，其中影響最嚴重的環節是供應商。供應商遭到攻擊，意味著在事件發生期間，工廠的生產必須被迫暫停或中斷。而且通常需要很長時間才能復原，因為絕大多數供應商都沒有所謂的應變計劃可應付這類攻擊和威脅。也正因如此，他們需要比傳統 IT 企業更長的復原時間。

以下各節將進一步詳細說明。

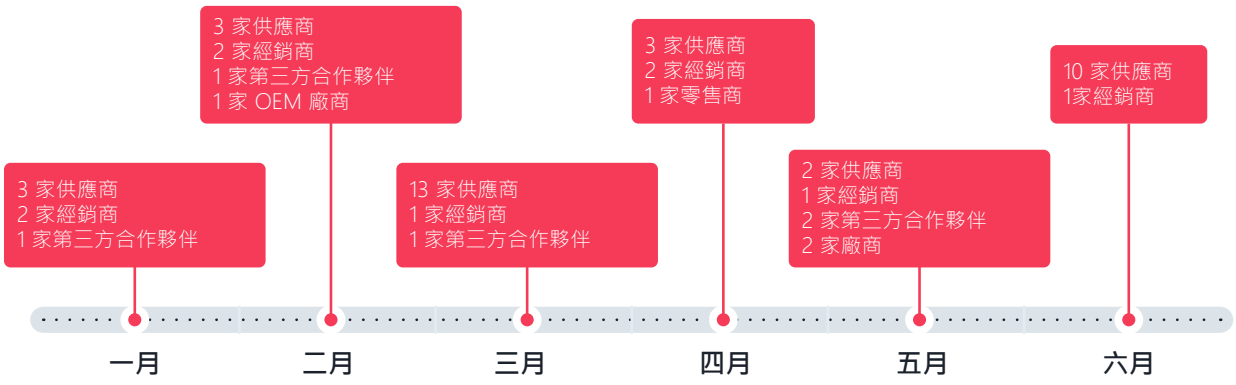

圖 3：針對汽車供應鏈的網路攻擊事件時間軸 (6 個月期間)。

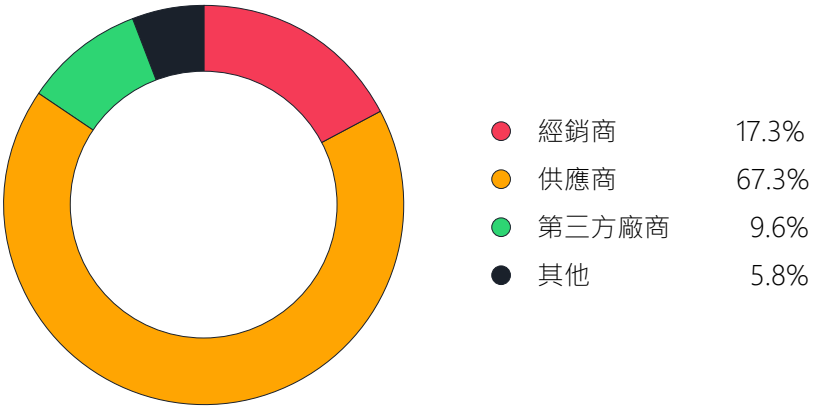

圖 4：受影響的供應鏈角色分布百分比。

勒索病毒

勒索病毒是一種會讓使用者無法正常使用其系統的惡意程式，它會將系統的畫面鎖住，或將使用者的檔案加密，然後向使用者索取贖金。勒索病毒已經是每個產業都面臨的重大資安議題。勒索病毒集團不只會攻擊銀行或支付系統，還會攻擊各種規模的企業和部門。

根據我們 2022 年第一季蒐集到的公開來源情報 (OSINT) 顯示勒索病毒正快速成長。若將這些勒索病毒資料與 2021 年前三個月相比，就會發現受害機構數量大約增加了 30%。這些受害機構遍布每一個產業，而且不限於大型企業，即使是小型企業也無法倖免。

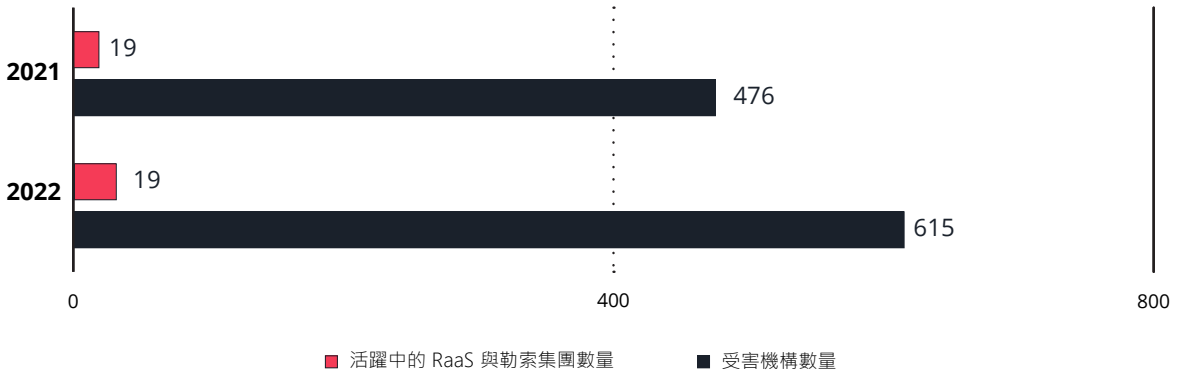

圖 5：勒索病毒集團與受害機構數量比較 (2021 年第 1 季與 2022 年第 1 季)。

近幾年來，汽車產業也不例外地開始數位轉型。複雜的超大型汽車製造廠需要大量的 IT 設備來維持營運的順暢。任何類型的事件都會影響營運並造成財物損失。我們從 2022 年 1 月至 6 月的資料當中觀察到 43 起汽車產業相關的受害案例。

影響汽車產業最嚴重的勒索病毒家族是 Conti，其次是 LockBit 和 Hive。這些勒索病毒家族在 IT 產業早已惡名昭彰，而且它們專門利用已知的技巧和方法來入侵汽車產業的系統。儘管沒有用到任何神秘配方或全新技巧，它們還是成功攻陷了這些企業，而且沒惹上麻煩。

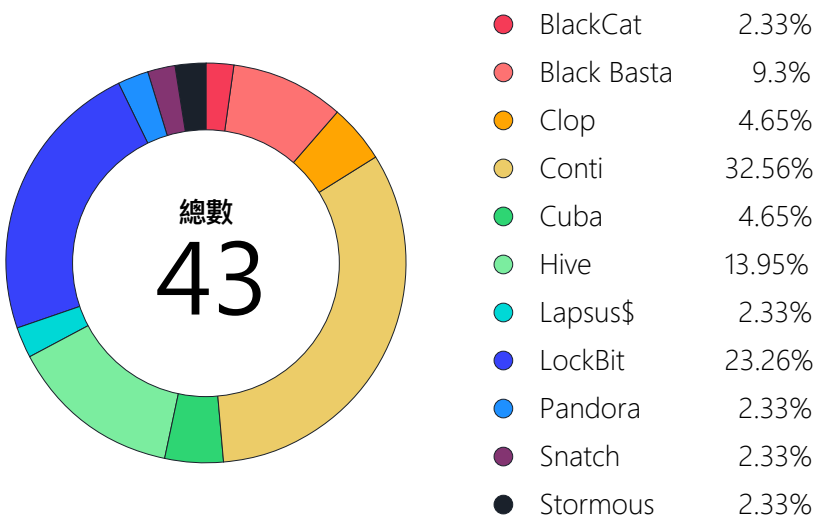

圖 6：影響汽車產業最深的勒索病毒家族排行榜。

典型的勒索病毒攻擊是從某個漏洞或某種資安破口開始。駭客集團發動攻擊的其中一種方式就是利用系統或網路的漏洞來滲透到廠商的內部網路。另一種手法是經由非法的方式取得存取權限，例如今年發生在 Nvidia[5] 的攻擊案例。如同大多數攻擊一樣，駭客一旦進入系統內部，接下來就會將資料加密，然後向受害者勒索一筆贖金以解開被鎖住的系統。現在，大部分現代化勒索病毒集團的作法不是直接將受害者名單與竊取到的資料類型公開，就是威脅要公開這些資料來製造壓力、逼迫受害者支付贖金。

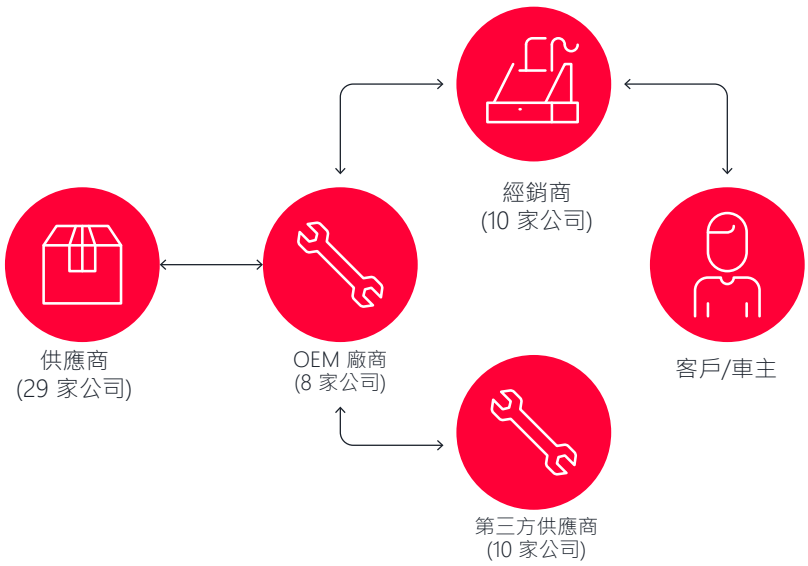

圖 7：汽車供應鏈網路攻擊目標分布情況，以及受害的企業數量。

資料外洩

所謂的「資料外洩」是指資訊在擁有者不知情或未經授權的情況下從系統被偷走的事件。視資料的類型以及被偷的對象而定，資料外洩有可能造成一些危害客戶生命安全或企業商譽的嚴重後果，不論其產業別為何。

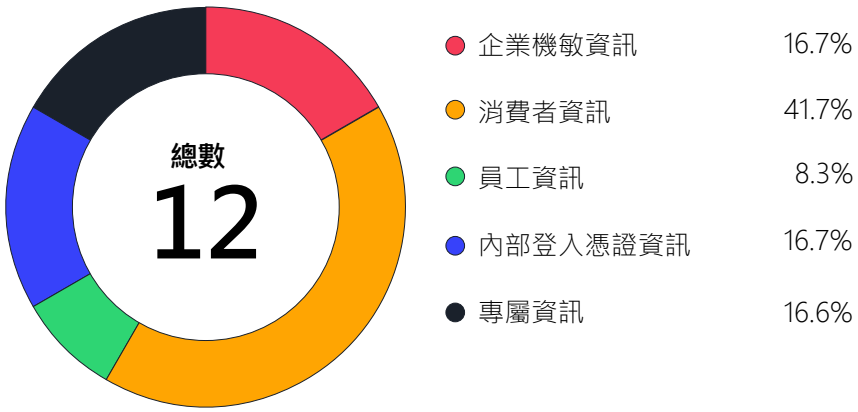

圖 8：汽車產業資料外洩事件可能遭外流的資訊類型
(2021 年 1 月至 2022 年 6 月)。

我們的研究檢視了汽車供應鏈內有關資料外洩案例的公開報告，從中整理出每個案例被偷的資料類型。如圖 8 所示，消費者資訊與企業機敏資訊是過去兩年當中通報數量最多的外洩資料類型。這些資料一旦落入不法之徒手中，有可能引來更複雜的攻擊。

失竊的消費者資訊或任何個人資訊，可能導致消費者成為詐騙的直接目標。在憑證填充 (credential stuffing)、電話詐騙以及魚叉式網路釣魚攻擊當中，犯罪集團會利用偷來的資料以及個人詳細資訊攻擊特定的個人或族群。

機敏資訊與專屬資訊一旦失竊，企業將直接受到衝擊。這類資料的外洩可能不會立即產生後果，但一旦駭客集團仔細研究過資料之後，他們很可能會發動意想不到的攻擊。

專屬資訊就像原始程式碼或基礎設施架構圖一樣，可能讓駭客更快找到企業的弱點或漏洞。由於車輛需靠程式碼來運作，而且基本上就是一種連網裝置，因此漏洞攻擊可能衍生的損失將難以估計。

至於失竊的基礎設施架構圖就如同一張藏寶圖一樣，能讓駭客看到整套系統的所有路徑，以及市售車所使用的原始程式碼。

日期	企業	資料
2022年1月11日	某汽車品牌的資料記錄應用程式[6]	消費者資訊，內部登入憑證資訊
2022年1月25日	汽車經銷商[7]	消費者資訊
2022年2月1日	汽車經銷商[8]	消費者資訊
2022年2月10日	汽車經銷商[9]	消費者資訊、員工資訊
2022年2月23日	軟體公司[10]	內部登入憑證、專屬資訊
2022年3月4日	鐵氧體 (Ferrite) 製造商[11]	員工資訊、企業機敏資訊
2022年3月9日	汽車經銷商[12]	員工資訊
2022年5月23日	汽車製造商[13]	消費者資訊
2022年6月1日	無晶圓廠 IC 設計公司[14]	企業機敏資訊、專屬資訊

表 2：資料外洩案例清單 (2021 年 1 月至 2022 年 6 月)。

網路攻擊趨勢

從以上觀察可透露出一些供應鏈攻擊最新的發展趨勢，這些趨勢在短期的未來可能還會繼續延續下去，這一點值得汽車產業特別留意。

- **攻擊將更具針對性。**勒索病毒與資料外洩並非什麼新式威脅，以往駭客可能利用垃圾郵件或偷渡式下載來散播勒索病毒，希望能散播得越廣越好。但近年來，他們已經改採目標式攻擊的手法、技巧與程序 (TTP) 來提升其運作的效率和利潤。相較於一般個人使用者，企業機構不僅更付得起贖金，也更願意支付贖金來避免營運中斷。

- **營運中斷不是唯一的問題。**傳統上，駭客是利用勒索病毒讓使用者或企業無法使用裝置或資料來賺錢。即使是擁有良好資料備份習慣的企業，在資料復原之前的營運停擺期間同樣也會造成重大損失。但這還不是最糟的狀況，從近期的勒索病毒攻擊事件當中可以看到，駭客會威脅受害者如果不支付贖金，就要將偷到的資料外流。這對受害者來說是個相當可怕的情況，因為其涉及的智慧財產對許多企業來說可能相當重要。有時候，那些被外洩的資料甚至不是受害企業本身、而是他們客戶的資料。因此，勒索病毒攻擊或資料外洩事件不但會中斷企業的營運，還可能損害企業的商譽。

- **受到影響的不單只有受害者本身。**如同我們在某些事件當中看到，勒索病毒攻擊或資料外洩事件影響的不單只有受害者本身而已，還有上游的客戶和下游的供應商。前面提到，駭客已經開始採用目標式攻擊的手法、技巧與程序。除此之外，他們還可能搜刮一些資訊或登入憑證來攻擊與受害企業有生意往來的其他公司。我們在許多案例中看到一些製造商基於預防性因素而暫時停止生產，直到其供應商解決勒索病毒或資料外洩事件為止。

已知且日益嚴重的高風險領域

電動車充電站

有關電動車充電站及其相關技術與充電標準資安問題的更多背景資訊，請參閱「附錄」一節。

充電站與電池管理系統很容易成為駭客的目標，一般來說，電動車大多採用鋰離子聚合物 (LiPo) 電池，因此需要完善的智慧控制機制來讓它運作順暢。相較於傳統車輛，電動車配備更多的感測器，還有車輛與充電站之間的通訊協定，因而導致許多資安上的問題。以下是我們發現的三大受攻擊面：

1. **電動車與充電站之間的 CAN 匯流排通訊協定**

   電動車與充電站之間的通訊經常採用 CAN 匯流排通訊協定，而且資料的傳輸是透過純文字方式。這讓駭客有機會挾持連線發動中間人 (MitM) 攻擊，此外，還可傳送惡意程式碼給電動車或充電站。

2. **電動車充電站專用應用程式/雲端服務**

   電動車充電站通常會連上雲端來執行交易和扣款程序。有些電動車甚至有專屬的應用程式來提供更便利的使用體驗。但就網路資安角度來看，這是一個傳統的受攻擊面，駭客可取得權限從行動裝置或入侵雲端伺服器來蒐集使用者資訊。

3. **無線電通訊**

   電動車充電系統經常會用到一些無線電通訊、RFID、藍牙，以及客製化無線電訊號。這些有可能成為一種遠端受攻擊面，讓駭客存取電動車內部元件。例如，駭客可從遠端開啟充電埠或傳送惡意程式碼給電動車或充電站來取得控制權。

雲端 API

連網汽車是汽車產業一股持續演變的風潮，這類車輛的典型網路架如圖 9 所示。目前市場上銷售的大多數新車都內建嵌入式 SIM 卡 (eSIM)，只不過有些車輛並未啟用。內建的 eSIM 是用於傳輸監測資料、與雲端後台伺服器通訊、提供 Wi-Fi 無線熱點、取得即時交通資訊等等的功能。雲端後台伺服器應用程式的範例包括：可從遠端啟動、停止、上鎖、解鎖車輛的智慧應用程式，以及可自動傳送當前路況到雲端 (然後再傳送至其他已訂閱相同服務的車輛) 的應用程式，這些都是廠商可能提供的雲端服務範例。

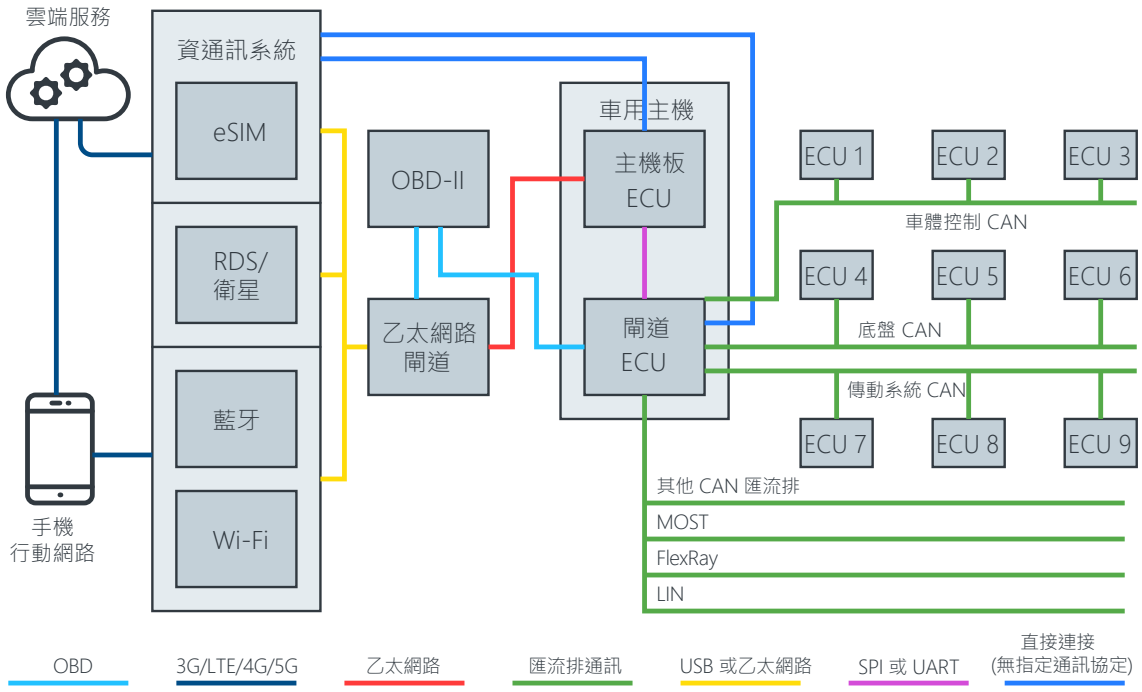

圖 9：現代連網汽車通用網路架構假想示意圖[15]。

雲端 API 是在這整體網路架構當中負責提供各種功能的主要角色。開發人員可利用其資料和功能來達成不同目的。它有點像是一個簡單的 OBD-II GPS 追蹤器，可讓使用者追蹤或發送簡單指令給指定車輛。不過，API 提供的還不止這樣，今日的雲端 API 已經與車輛本身密切整合，能為使用者提供許多進階的功能。

Tesla API 就是一個絕佳範例，其所有操控完全仰賴一個存取金鑰 (access token)，您只要拿到這把金鑰，車子就等於歸您所有。2022 年初，一名十幾歲的駭客在一項實驗當中從遠端遙控了 25 台以上的 Tesla 電動車[16]，暴露出 API 金鑰對於汽車安全有多重要，也讓人們看到萬一 API 金鑰遺失或失竊可能會發生什麼狀況。這起事件點出了幾個我們絕對不能忽視的資安基本原則。例如，金鑰的管理必須遵循最低授權原則，也就是說，單一 API 金鑰不應該用來存取所有的功能。這樣一來，即使遭到外流，也還能控制損害。此外，完整的存取記錄檔也非常重要，此記錄檔對於解決未經授權的不當存取以及在事情發生之前預先警告使用者至關重要。

傳統 IT 產業在 API 安全方面已有一些最佳實務原則可以遵循，該領域已經相當成熟，且相關的工具也很完備。既有的技巧和指導原則其實可以善加利用。開放網頁應用程式安全計畫 (Open Web Application Security Project，簡稱 OWASP) 每年都會提供一份 10 大排行榜來提醒開發人員留意一些最嚴重的資安問題，此外，MITRE 的 CWE 也提供了一份軟體與硬體通用弱點清單，剩下的問題就是要在工作上培養一種資安意識。

無鑰匙遠端解鎖 (RKE)

從 2021 年 1 月至 2022 年 6 月，有關無鑰匙遠端解鎖系統的老問題一再被提及。儘管這項議題在過去幾年一直不乏相關的討論，但卻由於造車成本的考量、消費者習慣以及市場的變化而尚未獲得有效解決。一些實際案例包括：NBC News 在 2022 年 6 月報導的車輛失竊事件[17]，以及連續兩年都被爆出的 Honda 遙控鑰匙問題 (CVE-2021-46145、CVE-2022-27254 和 CVE-2022-37305)。

過去，無線電裝置對一般社會大眾來說都是高門檻又神祕的領域，今日，隨著軟體定義無線電的普及與容易入手的價格，無線電領域已變得相對親民。例如，2022 年推出的 Flipper Zero 就是一個價格大約 165 美元的軟體定義無線電裝置。它採用類似 Arduino 的可客製化整合式驅動電子 (Integrated Drive Electronics，簡稱 IDE) 介面，進一步降低了軟體定義無線電的程式撰寫難度。正如一名 Twitter 用戶「inf0sec1」發文表示[18]，Flipper Zero 可以輕易對福特 (Ford) 汽車發動回放 (replay) 攻擊。針對這類回放攻擊，製造商只需更換其使用的解決方案就能避開，例如，使用滾碼 (rolling code) 機制，但基於成本與使用體驗的考量，過去很少有廠商給予適當的關注。例如，Honda 已經在新車款裡面使用了滾碼機制，但有些駭客還是找到方法來避開這項安全機制[19]。

汽車產業遙控鑰匙的演進[20] 有點類似工業物聯網 (IIoT) 通訊協定的演進。工業無線射頻 (Industrial RF) 遙控器基本上就是一種外觀上有許多功能按鈕的強固型遙控器，汽車的 RKE 遙控鑰匙也是如此。RF 遙控器採用的是封包無線電通訊協定，其原理是將位元串流經由調變 (modulation) 方式轉換成無線電波。其日益強化的裝置連線能力 (如 Anybus 和 CAN 匯流排) 也引起了駭客的興趣。

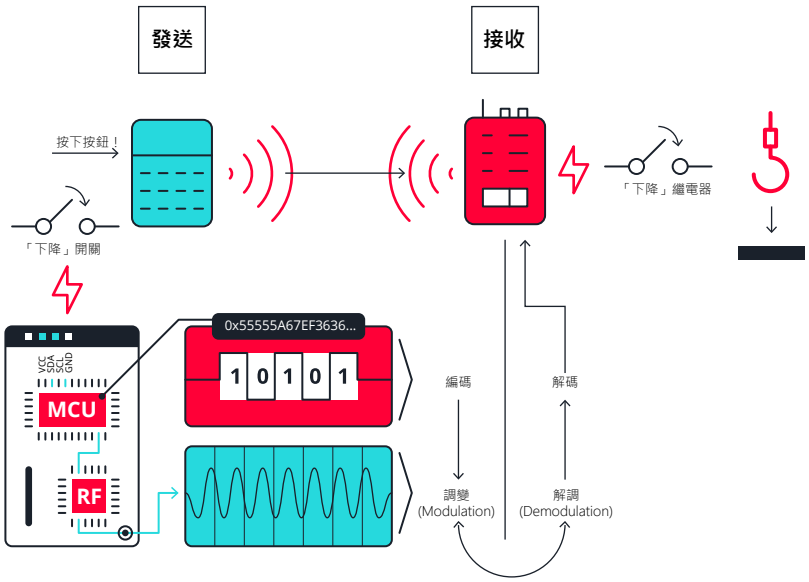

圖 10：發送器、接收器與受控制設備之間的關係示意圖。

由於無線電波在一定範圍之內任何人都能接收，因此，這項技術必須內建適當的安全機制與措施來防止濫用。

漏洞	說明	攻擊類型	修補更新開發	修補更新部署
無滾碼機制	每個封包都獨立完整，不含需要解譯的動態機密。任何被攔截到的封包未來都永遠有效。	1, 3	非常容易	修補難度：目前已有數百萬個單元流通在外，這些元件不容易修補。
加密強度不足或完全缺乏	發送器與接收器之間傳輸的資料並未加密，或者編碼強度太弱容易被猜測。	1, 2, 3, 4	容易	修補難度：除了前面提到的修補更新問題之外，純韌體式方案或許也不足以解決問題，因為硬體可能不支援加密。
缺乏軟體保護	發送器與接收器上用來上傳韌體的軟體沒有防止程式碼被篡改的機制。	5	非常容易	修補難度：容易，廠商只需在軟體中加入適當的存取控管即可。

表 3：我們研究發現的一些漏洞。

趨勢科技在一篇先前的研究報告中發現了一些常見的遠端遙控系統漏洞。我們發現車用 RKE 系統也存在著和工業營運技術 (OT) 一樣的漏洞。

正如趨勢科技先前發現，車輛的遙控器基本是在工業、科學及醫療 (ISM) 頻段上運作，但更常見的是介於 315 到 915 MHz：

> *「...其中最常見的是 915 MHz。雖然實際的頻段隨國家而有所不同，但 ISM 頻段是國際上保留給工業、科學和醫療用途的頻段，而非用於通訊。最近，市場上開始出現使用 2.4 GHz 頻段的工業無線遙控器，主要是為了解決 315、433、868 和 915 MHz 頻段過於擁擠的問題[21]」。*

在 ISM 頻段當中，我們有許多常見的調變方法可以選擇，例如：頻率偏移調變 (FSK)、相位偏移調變 (PSK)、最小偏移調變 (MSK) 等等。在汽車遙控器領域，FSK 是最常用的方法，因為絕大部分的汽車遙控器都不需要太強的傳輸能力。簡單、易用、低成本、穩定是採用這項技術的決定性因素。

在常見的網際網路通訊協定中 (如 802.11 家族乙太網路)，我們不會在實體層 (也就是調變層) 直接傳輸我們所需的資料。大多數汽車遙控器採用的傳輸方法相對簡單且暴力，直接利用 FSK 調變將特定的位元序列發送到 ISM 頻段。

這樣的設計對於家用電器或許沒問題，但如果用在車門上肯定會出狀況，因為我們不可能讓同一車款的每一輛車都共用同一個遙控器。因此，就需要有一組密碼來區分不同的車輛，以避無鑰匙共用的問題。在早期，這個密碼相對較短，大多是 6 位數字 (甚至在鑰匙移除之後只有 4 位數字)，這樣一來，我們只需將遙控器上的 6 位數字與車輛控制器的數字設成一樣，就能讓車輛接受來自遙控器的開/關訊號。

這樣的設計跟行李箱的密碼鎖是一樣的，事實上，駭客只要有有充裕的時間就能破解這個密碼，所以這種設計在今日相對少見。大部分 RKE 遙控鑰匙的設計 (固定密碼) 都內含快閃記憶體 (不論是內建在晶片當中或外加) 來儲存一組相對較長的固定密碼以供比對。

不過，這樣的設計很明顯地容易遭到回放攻擊，如圖 11 所示。

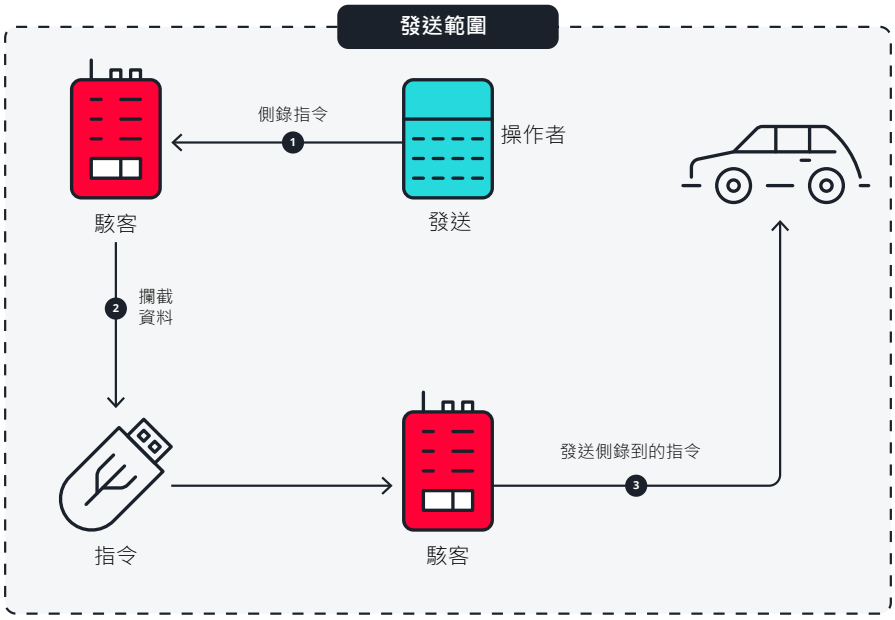

圖 11：汽車遨控器回放攻擊示意圖。

在這個情境中，駭客會暗中側錄使用者遙控器的訊號，然後直接發送到車輛來執行相同的功能。如前面提到，Flipper Zero 是一個入門級的軟體定義無線電裝置，可用來解鎖舊款的 Ford 汽車。

之前 GitHub 上的一個研究專案[22] 即發現有很大比例的 Honda 汽車都使用簡單的 FSK 調變，甚至其固定密碼的設計還存在著一個漏洞讓問題更加嚴重。在一份有關 Honda 和 Acura 汽車回放攻擊的研究報告：「Unorignal-rice-patty」[23] 當中，作者指出有許多 Honda 汽車的 RKE 訊號都使用固定密碼設計，但其車門解鎖的訊號只是將上鎖訊號的位元對調而已。這意味著針對採用這種設計的 Honda 汽車，回放攻擊的難度直接減半，因為駭客不需苦苦等候車主按下解鎖按鈕就能得到解鎖的訊號。

正如前面提到，防範回放攻擊非常有效的一種方法叫做滾碼機制。

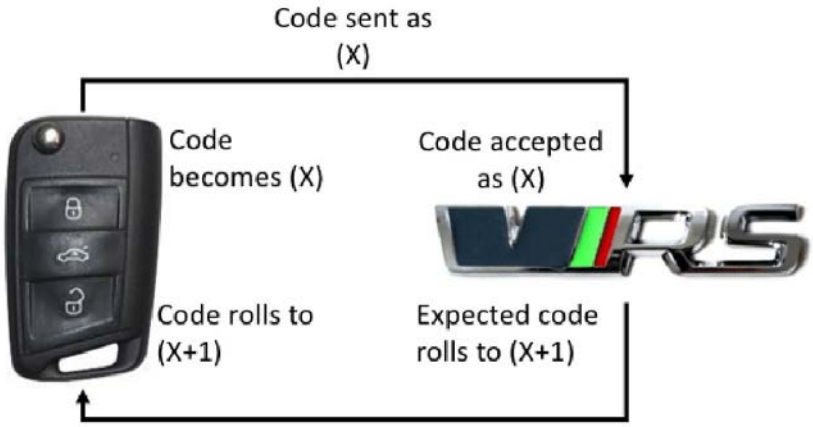

圖 12：滾碼機制示意圖[24]。

圖片來源：Colin Urquhart 等人/Researchgate.net。

上圖示範滾碼機制的核心概念，那就是密碼用完一次就丟。每當指令被車輛接受之後，鑰匙和車輛就會丟棄這次使用的密碼，這樣的設計對於反制回放攻擊非常有效。然而在現實世界裡，滾碼機制的應用卻有一些限制，例如，它需要一份密碼表。

解決的方法，首先要在配對階段產生一份密碼表並寫入遙控鑰匙的記憶體內。其次，要設計一套可動態產生偽隨機亂數 (PRNG) 的專屬加密演算法。目前歐洲車普遍採用的 HCS301 家族微晶片，就是使用這樣的設計。

最知名的攻擊案例就是 Keeloq 專屬硬體加密技術的問題，這是由 Samy Kamkar 在 2015 年的「Defcon23」大會上提出[25]。Keeloq 演算法的設計並未包含時間參數，這意味著，如果車主在遙控器超出感應範圍或受到干擾時按壓或誤觸遙控器按鈕，那麼駭客就能錄到下次指令的訊號。此外，大部分採用 Keeloq 的裝置，其密碼都不長。早期的 32 位元設計只需兩個禮拜就能輕易破解，不過後期的產品已經增加到 66 位元。但是，隨著半導體技術的快速發展，這也只是暫時的解決方法。

滾碼的設計還有另一項問題，那就是使用者體驗。從前面的滾碼機制示意圖就知道，其核心概念是將用過的密碼丟棄。換句話說，假使遙控鑰匙已經將某個密碼丟棄，但車輛卻不知情的話，下次使用遙控鑰匙時，兩邊的密碼就會不符，結果車主可能以為遙控鑰匙壞了。為了解決使用者體驗的問題，Honda 加入了一個類似滑動窗 (sliding window) 的設計。

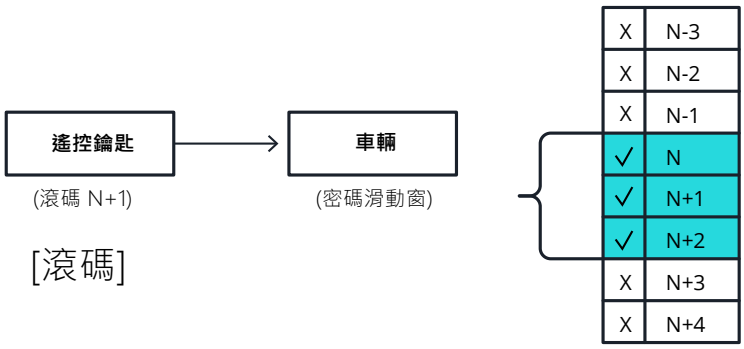

圖 13：滑動窗設計示意圖[26]。

Star V 實驗室研究人員發現，Honda 2012 年車款已經過重新設計，允許一定範圍內的密碼可以被重複使用，以方便兩邊重新同步。不過，這樣的設計卻反而破壞了滾碼機制本身的安全性，讓回放攻擊的問題又再回歸：

> *「藉由回放之前側錄的 Honda Civic 車款上鎖/解鎖指令，就能將其內部計數器重新同步。一旦計數器同步，之前計數器週期內用過的指令就能再次回放。[27]」*

Tesla 的鑰匙採用了一種新的方法，放棄原本傳統的 RKE 設計，改用藍牙低功耗 (BLE) 技術以及一個資料層/應用程式層認證與加密的設計來生產遙控鑰匙。隨著 BLE 裝置的成本下降，越來越多的車廠也開始跟進，在高階車款當中採用這類設計。藉由將配對與密碼驗證的工作轉移到資料層，我們就能使用各種 IT 領域開發的加密與認證解決方案。

不過，這樣的設計卻一再因為成本的問題而遭受打擊，以至於在 2022 年 5 月，一名 NCC Group 的資深安全顧問 Sultan Qasim Khan 在該公司的部落格上發表了一篇研究[28] 間接影射了這項問題。 此外，由於 Tesla BLE 遙控鑰匙的訊號存在著一定的延遲彈性，因此可能會遭遇所謂的「中繼攻擊」(relay attack)，而且 2022 年式 Model 3 車款已經成功被攻擊了。

2021 年，Lennert Wouters 在 Tesla Model X 的鑰匙上發現了一系列漏洞[29]，包括一個沒有安全機制的 OTA 功能以及一個有瑕疵的配對協定。這協定讓他能夠製造一連串的攻擊，將惡意韌體刷到遙控鑰匙的晶片上，然後觸發更換金鑰的程序，讓駭客直接 (無須接觸) 產生大量金鑰到目標車輛。

我們 (VicOne) 的研究團隊將這些 RKE 相關的問題整理之後繪製成以下心智圖：

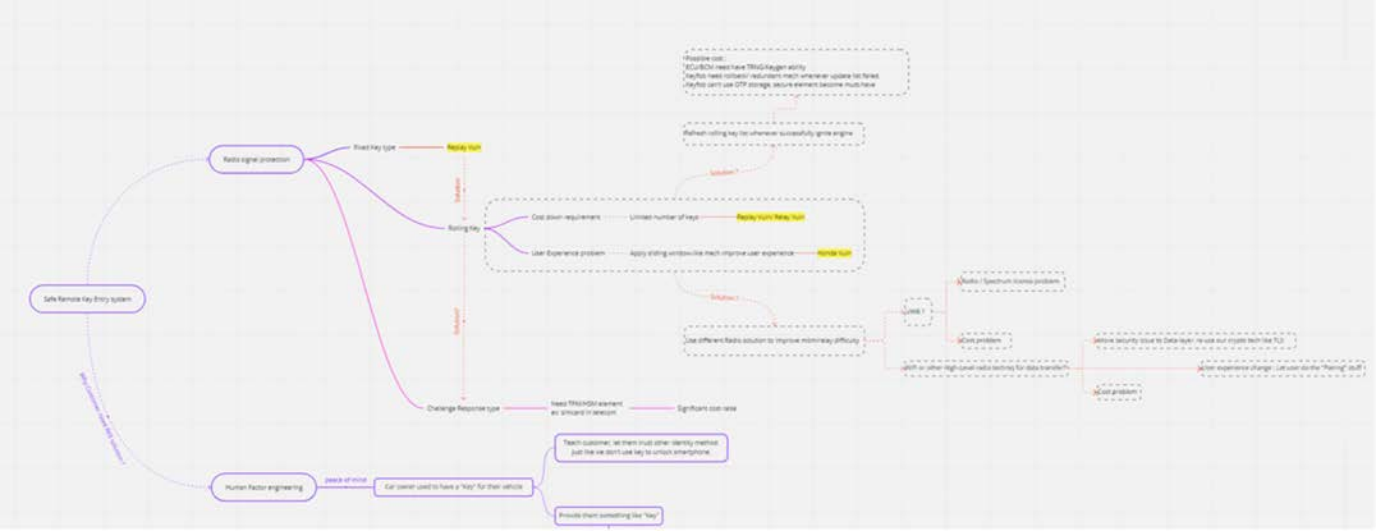

圖 14：連網汽車 RKE 系統相關問題的心智圖。

RKE 的漏洞是一連串成本與體驗之間的妥協。這並非靠時間就能改變的問題，但還是有一些可以反制的必要策略：

- 採用滾碼機制，並盡量避免過度節省成本。
- 將門鎖與引擎啟動功能分開，以避免出現只要能夠打開車就能將車開走的問題。
    - 例如，今日許多車輛都配備了所謂的「晶片鎖」，這類晶片鎖通常透過遙控鑰匙上的 RFID 標籤來提升安全，借助 RFID 訊號本身可以遠距離發送的特性。
- 記住「容易上鎖、不易解鎖」的原則。
    - 在人因工程方面，車主很少需要從遠距離解鎖車門。對車主來說，不論是到車內拿一些東西或是要使用車輛，他們都必須近距離打開車門。因此，遠距解鎖車門的功能是否真的必要？例如，使用具備精準定位能力的 UWB 訊號來發送解鎖訊號的議題就蠻值得討論，因為這麼做可以防止遠距離攻擊。

在可預見的未來，我們相信這些 RKE 攻擊將越來越常見。隨著軟體定義無線電 (SDR) 裝置越來越便宜，以及供應鏈變得更加全球化，汽車製造商應嚴肅看待遙控鑰匙的設計，並拋棄老舊的防禦思維。例如，在導入日益受到車主青睞的無鑰匙系統時，可結合多種無線通訊系統來提高駭客攻擊的難度。

最終，竊車賊也許會覺得乾脆直接打破車窗進入車內還更有效率。例如，在北美地區被戲稱為「Kia Challenge」的青少年竊車事件[30] 就是最佳證明，他們先打破車窗，然後再透過簡單的 USB 介面就能將車開走。因此，如果考量到成本的話，我們建議汽車製造商應該花多些心力在引擎啟動防盜機制上。

資安建議及預測

在前面的內容當中，我們點出了高風險的受攻擊面，以及汽車產業整體所面臨的資安威脅。其中許多威脅都是資安產業目前所熟知的，因此汽車產業應該好好利用其他產業所累積的經驗和知識，然後再針對其特殊需求打造一套量身訂做的方案。正如先前所討論，善用現有的技術和遵循一些已證明有效的資安技巧是值得的。

以下提供汽車產業決策者應該知道的一些資安建議：

雖然目前有各式各樣的開放原始碼軟體可用來快速開發車用軟體，但這些軟體通常不具備資安功能。每年都持續舉辦的「Tesla Pwn2Own」[31] 駭客競賽也證明了軟體開發生命週期 (SDLC) 的重要性，因為事實證明軟體的弱點很可能在多年後被用來攻擊使用者。真正的進步是在快速開發的同時還要維持相對的安全性，所以我們必須增加資安上的投資。

- OTA 更新是現代化汽車設計當中不可或缺的一環，這不僅是為了透過線上更新來強化車輛功能，同時也是為了在發現問題時能不須將車輛召回原廠就能修正問題。既可提升安全性，又能節省日後的成本。

- 車輛的維護非常重要。為了提升便利性，現代化汽車都配備了大量的電子裝置，而且可說是一台強大的行動電腦。就這點來看，資安要求的提升是必要的，而同樣必要的還有即時回報車輛的狀況。這有助於發掘潛在的問題並預防未來發生問題，此外，車輛安全營運中心 (VSOC) 也變成了一種必要的存在。

駭客的演進速度也跟上了產業發展速度，因此我們預料汽車從業人員應該注意以下幾點：

- 短期之內，勒索病毒將繼續危害汽車供應鏈，並將其攻擊目標延伸至雲端及車內元件。

- 汽車產業將會有更多元件受到開放原始碼漏洞所影響。開放原始碼軟體在汽車產業相當普遍，而且大量應用在晶片、硬體、韌體、作業系統及應用程式當中。一個最佳的案例就是 Log4j 漏洞，該漏洞讓 Tesla 電動車及充電站都陷入了危險。

- 無線電訊號攻擊 (回放、中繼、干擾、中間人攻擊) 未來將會增加。
- 惡意程式將被植入車用資訊娛樂系統 (IVI) 或遠距通訊控制單元 (TCU) 當中。
- 採用 AI 技術的感測裝置，例如先進駕駛輔助系統 (ADAS)，將受到生成對抗網路 (Generative Adversarial Network，簡稱 GAN) 更大的影響。自從 GAN 在 2014 年問世以來，許多研究都指出這項技術可被用來提升 ADAS 的安全性。在功能安全方面，GAN 可應用於影像對影像轉譯來提升解析度，並且改善環境光源、強化物件偵測能力。在資訊安全方面，GAN 已被建議用來偵測偽造資訊。反之，其設計也可能被用來協助駭客躲避異常偵測機制。
- 未來將出現晶片層級的漏洞與攻擊。晶片層級的設計並非絕無安全漏洞，過去，駭客就曾利用這類漏洞來避開上層的安全機制 (例如作業系統或應用程式層級的安全機制)。
- OTA 將成為攻擊目標。OTA 是現代化汽車之所以能更新到最新軟體或是能訂閱軟體更新的一項關鍵。駭客可利用這項機制來入侵更新流程，或者在軟體升級當中植入惡意程式碼。
- 駭客可避開汽車製造商在車上安裝的數位鎖。駭客能利用數位鎖的漏洞來解鎖或避開製造商的付費機制。

附錄

電動車充電

根據國際能源署 (International Energy Agency，簡稱 IEA) 的「2022 年全球電動車展望」(Global EV Outlook 2022)[32] 報告，從 2018 年至 2021 年全球電動車總量成長了三倍，而公共充電站數量也同樣線性成長， 這還不包括家用充電設備與各家車廠設置的私有充電站。

國際電工委員會 (International Electrotechnical Commission，簡稱 IEC) 在其 62196 號報告中[33] 列出了當今主流的充電樁種類。

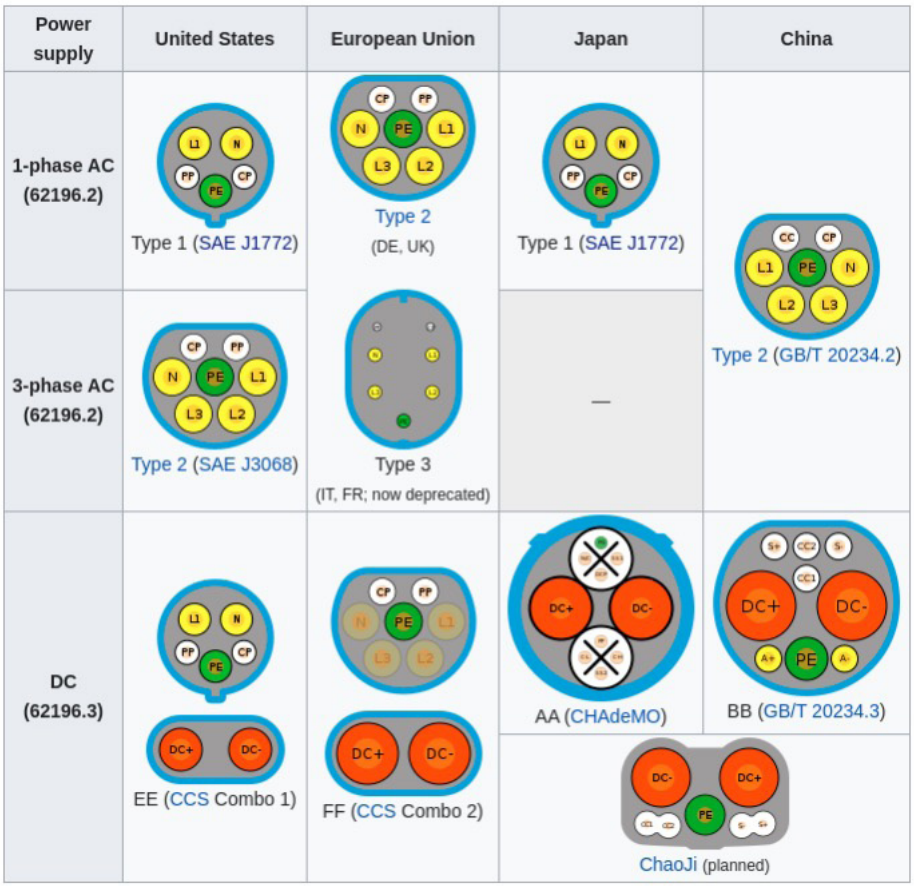

圖 15：IEC 62196 報告[34] 所列的主流充電樁種類。

圖片來源：International Electrotechnical Commission/IEC 網路商店。

基於不同的設計目標與安全規範，基本上我們可將充電樁的規格分成幾類。

AC/DC

幾乎每種電池都是直流電 (DC) 裝置，這意味著我們只能使用 DC 充電器幫電池充電。目前家庭用電基本上是採用交流電 (AC)，因此大多數的汽車製造商的電動車都會內建充電器以方便車主在家充電，這就是為何電動車充電站大多採用交流電。

基於大小、散熱、能源效率等各種因素 (當然還有成本)，車上內建的充電器瓦數通常相對較低。以北美所採用的 SAE J1772 類型為例，交流電充電最高只能達到 19.2 KW (千瓦)，這還不計算能源轉換的損失。

如果直接連接至電池管理系統或使用 Ucharging 充電站透過 DC 模式來充電，通常可獲得比 AC 充電更高的瓦數。例如，繼承自 J1772 規格的 CCS1 充電規格在 DC 模式下甚至可提供高達 100 KW 的電力。

CAN 匯流排或 PLC 充電樁的設計必須要能滿足不同車型甚至不同車廠的需求。因此，無論使用何種充電系統，其規格和設定都是由車輛主動發起，充電樁只是在其規格內被動提供電力給車輛。早期的 J1772 充電樁不一定會透過數位資料傳輸介面來與車輛溝通，但會使用一套 PWM 訊號來與車輛溝通。這套通訊協定規範在 IEC61851 標準當中，而這套通訊方式也保留了一個狀態給 CAN 匯流排或 PLC 協定使用：通常，當工作循環 (duty cycle) 下降至 5% 以下就會觸發狀態切換，讓電動車充電設備 (EVSE) 和電動車 (EV) 都知道該切換至 CAN 匯流排或 PLC 來進行後續通訊。

電動車充電相關的資安問題

這一節，我們將討論有關充電站與電動車充電技術相關的資安現況。汽車製造商與車主目前所面臨的挑戰之一就是「類比」電力的問題。例如，DC 快充採用的是高電壓、高電流的充電方式。這使得 DC 快充在許多方面都變得相當危險，而 ODM 廠商與車廠也都知道這點。所以，不僅 CAN 匯流排本身就具備軟體互鎖 (interlock) 的機制，而且還具備了一項永久性容錯設計。

此外，趨勢科技也曾經剖析「可程式化儀器標準指令/虛擬儀器軟體架構」(Standard Commands for Programmable Instruments/Virtual Instrument Software Architecture，簡稱 SCPI/VISA) 通訊協定的安全設計及弱點[35]，此一通訊協定普遍應用於測試儀器。SCPI 的安全問題跟快充協定所面臨的問題相似，例如，舊的資料匯流排並無安全設計，所以新的標準必須解決一些像使用 TLS 協定的安全問題，但這仍在制定當中。

這些問題絕對是網路資安風險，而且如果攻擊得逞的話，很可能影響用戶安全。目前，ODM 廠商已經實作了一些容錯機制來防止火災或緊急狀況發生。但是，製造商及用戶不能單靠這些措施。一些容錯設計 (如阻抗監控、超高速保險絲或近身感測器) 都是用戶安全的最後一道防線，因此不應被視為解決網路資安問題的第一手段。

分析充電協定、設計與新式標準

針對 Tesla 充電樁的 Tencent X-in-the-Middle 攻擊

在「Black Hat 2021」駭客大會上，Tencent 的資安團隊發表了一份有關 Tesla「隨插即充」充電樁的研究[36]。他們所研究的充電樁屬於一種基於 CAN 匯流排技術的 DC 充電樁，該團隊指出 Tesla 使用了部分的 GB/T 類型協定再加上他們自己的專屬協定。

其中間人攻擊背後的主要概念是利用 Tesla 用來與充電樁溝通的 CAN 匯流排訊息。CAN 匯流排在汽車領域應用廣泛，屬於一種廣播式網路架構，但卻無認證或稽核機制，因此 CAN 匯流排當然可能遭到中間人攻擊。

該攻擊也可稱為一種假冒應用程式或 CAN 匯流排訊息以獲得免費充電的範例。Tesla 充電樁是透過應用程式或雲端再配合 CAN 匯流排車輛識別碼 (VIN) 來識別使用者。駭客可以在應用程式與充電樁之間、或是電動車與充電樁之間冒用別人的 VIN，就能免費幫車子充電。

CHAdeMO 的獨特設計

CHAdeMO[37] (2021 年出現的一種專門幫使用電池的電動車快速充電的系統) 是唯一在規格中將「車聯網」(V2X) 與「車輛到電網」(V2G) 納入考量的充電協定。CHAdeMO 2.0 甚至還延伸至 V2G 部分來涵蓋由車輛反向輸出電力的情況。TEPCO (亦稱為 Toden) 設計了這項技術並且在開發 CHAdeMO 規格時也考慮到未來的情境。例如，他們還估算了當電動車全面取代燃油車之後，將對都市或國家的電網帶來多大的衝擊和效益。

此外，該公司還分析了在東京電網的限制下使用快充所帶來的衝擊。其計畫包括將電動車充電視為電網設計的一環，而且 CHAdeMO 2.0 還提供了一個選項讓電動車反向為電網提供 500KVA 的電力。不過這項計畫 (以及將電動車納入都市的電網中) 存在著關鍵基礎設施方面的問題及資安疑慮。

如果您還記得，大多數的充電樁都是被動接受電動車的指令，CHAdeMo 也是採同樣的設計。電動車上的充電控制單元會負責協調充電的程序，甚至在連上電網之後當成電力輸出。

在先前的研究中，我們看到大多數 CAN 匯流排流量都採用純文字傳送，因此要發動中間人攻擊並不困難。Tencent 的 X-in-the-middle 攻擊就是利用隨插即充的收費程序漏洞來獲得免費充電。然而當電動車變成了電網的一環時，我們就不能輕忽這些資安疑慮。

IEC 15118 與隨插即充系統

在本文作者所在的地方 (台灣台北)，大部分的快速充電站目前都是由車廠自行設置。例如，Tesla 的車主會到 Tesla 的充電站，Toyota 的車主會到 Toyota 展示廳或使用自己的充電設備。不過，高速公路休息站和其他地點已開始出現一些隨插即充的充電站。未來，當電動車越來越普及時，隨插即充充電站應該會成為充電樁的主流。

目前，不同的充電樁都有自己的資料鏈、規格，甚至是收費方式。這顯然不利於隨插即充的發展，所以才會出現 IEC 15118 標準[38]。

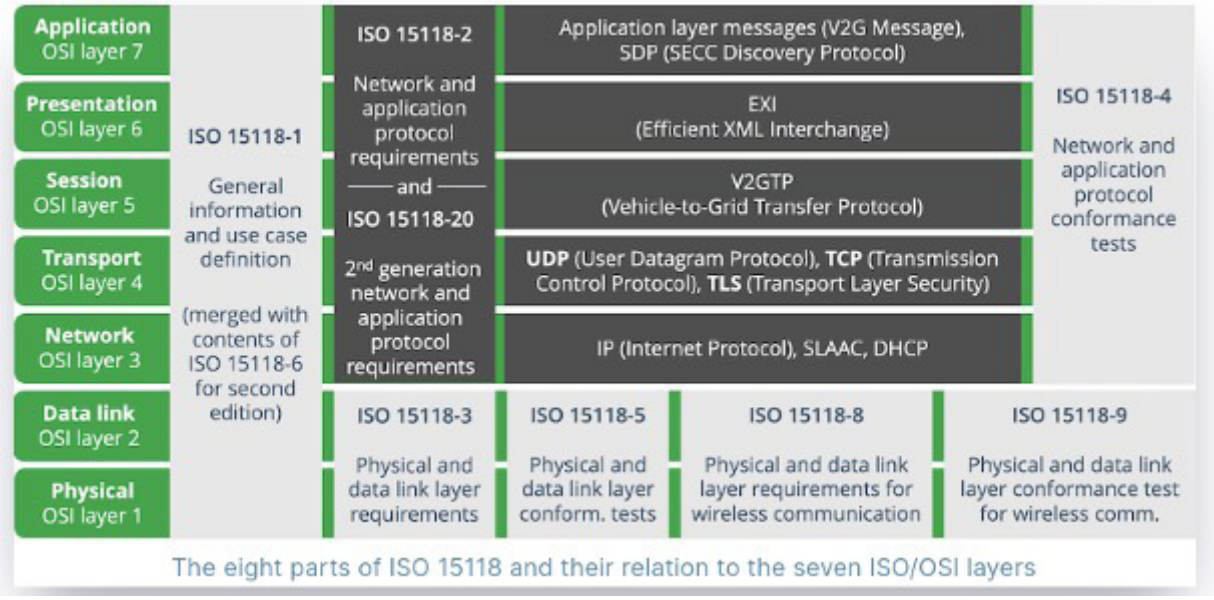

圖 16：IEC 15118 標準[39]。

圖片來源：Marc Mültin/Switch-EV.com。

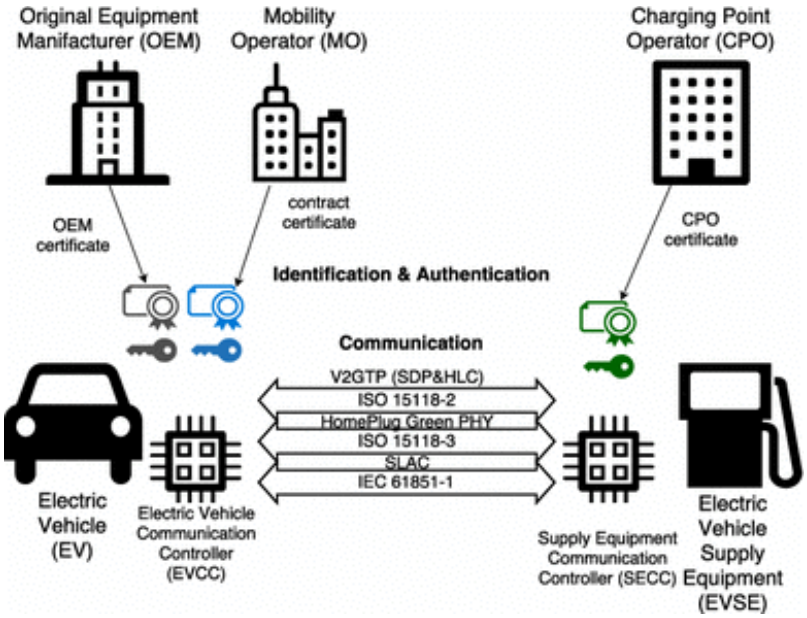

圖 17：ISO 15118 系統架構示意圖[40]。

圖片來源：Kaibin Bao 等人/Researchgate.net。

如果 IEC 15118 未來成為充電站的一項共通標準，我們從上圖就能看到，充電站與電動車之間的通訊將導入多項現代化網路功能，例如使用 OSI 的 7 層網路模型、TLS 及 HTTP/2。藉由導入 Open Systems Interconnection (OSI) 的多層網路模型，充電槍使用何種通訊方式就變得不重要。導入 OSI 模型之後，就有可能使用相同的通訊協定堆疊來達成「通用隨插即充」(Universal Plug-and-Charge) 的理想，不管充電槍使用何種通訊方式，例如 CAN 匯流排或 PLC。

不過，目前的 IEC 15118 當中已經被發現一些潛在的問題，例如金鑰交換的流程是否足夠安全，或者近身感應動作缺乏逾時的設計，因而可能導致阻斷服務 (DOS) 攻擊。

高風險受攻擊面的問題

隨插即充的風險

作者相信，隨插即充是電動車產業未來發展非常重要的一環，而廣設技術成熟的隨插即充充電站，將是消除電動車車主續航力焦慮的一項重要關鍵。儘管 IEC 15118 目前仍未上路，但作者發現台灣當地已經有某些快速充電樁產品[41] 具備隨插即充功能。

我們可看到台灣的充電樁已經支援多種通訊方式，如：RFID、乙太網路、3G/4G、Wi-Fi 以及 OCPP (開放充電點協定)。這顯然對一些隨插即充功能 (如收費和操作人員管理) 相當有利。不過，相較於車廠目前自己建置的快速充電樁，這類充電樁產品對駭客來說更具吸引力。

電動車的充電埠可能遭到駭客的無線電訊號回放攻擊

Tesla 的充電埠由於並未使用安全的無線電通訊協定，因此駭客可能經由簡單的無線電訊號側錄/回放攻擊而將它打開。根據 RTL-SDR 所通報的一個案例[42]，我們看到充電埠協定並無任何滾碼機制的設計，而且同樣的資料還能觸發不同台 Tesla 的充電埠，就如同一把萬能鑰匙一樣。

參考資料

1 Dustin Childs. (May 18, 2022). *Zero Day Initiative.* "Pwn2Own Vancouver 2022 - The Results." Accessed on Nov. 14, 2022, at https://www.zerodayinitiative.com/blog/2022/5/18/pwn2own-vancouver-2022-the-results.

2 Wu HuiYu and Li YuXiang. (May 7, 2021). *Blackhat Asia 2021.* "X-in-the-Middle : Attacking Fast Charging Piles and Electric Vehicles." Accessed on Nov. 14, 2022, at https://i.blackhat.com/asia-21/Thursday-Handouts/as-21-Wu-X-In-The-Middle-Attacking-Fast-Charging-Piles-And-Electric-Vehicles.pdf.

3 Reuters. (March 1, 2022). *Reuters.* "Toyota suspends domestic factory operations after suspected cyber attack." Accessed on Nov. 14, 2022, at https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/.

4 David Fiser. (March 3, 2021). *Trend Micro.* "Identifying Weak Parts of a Supply Chain." Accessed on Nov. 14, 2022, at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/identifying-weak-parts-of-a-supply-chain.

5 Dan Goodin. (March 30, 2022). *Ars Technica.* "Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA." Accessed on Nov. 14, 2022, at https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/.

6 David Colombo. (Jan. 25, 2022). *Medium.* "How I got access to 25+ Tesla's around the world. By accident. And curiosity." Accessed on Nov. 14, 2022, at https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028.

7 Office of the Maine Attorney General. (n.d.). *Office of the Maine Attorney General.* "Data Breach Notifications." Accessed on Nov. 14, 2022, at https://apps.web.maine.gov/online/aeviewer/ME/40/ec8e5dc7-e259-4847-8a94-23b789691b54.shtml.

8 Coya Vallejo Hägi. (Jan. 13, 2022). *Digitec.ch.* "Cyber attack on car dealer Emil Frey." Accessed on Nov. 14, 2022, at https://www.digitec.ch/en/page/cyber-attack-on-car-dealer-emil-frey-22420.

9 Office of the Maine Attorney General. (n.d.). *Office of the Maine Attorney General.* "Data Breach Notifications." Accessed on Nov. 14, 2022, at https://apps.web.maine.gov/online/aeviewer/ME/40/62ea1496-1f06-4120-aa97-fe1952bd418b.shtml.

10 Ionut Ilascu. (March 1, 2022). *Bleeping Computer.* "NVIDIA confirms data was stolen in recent cyberattack." Accessed on Nov. 14, 2022, at https://www.bleepingcomputer.com/news/security/nvidia-confirms-data-was-stolen-in-recent-cyberattack/.

11 Mullen Coughlin LLC. (March 4, 2022). *New Hampshire Department of Justice.* "Notice of Data Event." Accessed on Nov. 14, 2022, at https://www.doj.nh.gov/consumer/security-breaches/documents/fair-rite-products-20220304.pdf.

12 Hayes Connor Solicitors. (n.d.). *Hayes Connor Solicitors.* "LHS Auto UK contact current and former employees to report data breach." Accessed on Nov. 14, 2022, at https://www.hayesconnor.co.uk/group-actions/lsh-uk-contact-current-and-former-employees-to-report-data-breach/.

13 Bill Toulas. (May 23,2022). *Bleeping Computer.* "General Motors credential stuffing attack exposes car owners info." Accessed on Nov. 14, 2022, at https://www.bleepingcomputer.com/news/security/general-motors-credential-stuffing-attack-exposes-car-owners-info/.

14 Red Packet Security. (June 13, 2022). *Red Packet Security.* "Cuba Ransomware Victim: Etron." Accessed on Nov. 14, 2022, at https://www.redpacketsecurity.com/cuba-ransomware-victim-etron/.

15 Numaan Huq, Craig Gibson, and Rainer Vosseler. (Aug. 18, 2020). *Trend Micro.* "The Cybersecurity Blind Spots of Connected Cars." Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

16 Matthew Humphries. (Jan 13, 2022). *PCMag.* "Teenage Hacker Gains Remote Control of 25 Teslas in 13 Countries." Accessed on Nov. 14, 2022, at https://www.pcmag.com/news/teenage-hacker-gains-remote-control-of-25-teslas-in-13-countries.

17 NBC News. (June 16, 2022). *YouTube.* "Thieves Turning To Cutting Edge Technology To Steal Cars." Accessed on Nov. 14, 2022, at https://www.youtube.com/watch?v=rx5mjOEixMY.

18 inf0sec1. (July 10, 2022) *Twitter.* "Playing around with #FlipperZero..." Accessed on Nov. 14, 2022, at https://twitter.com/inf0sec1/status/1545804925522829313?t=4-n6SQ3H8OhD_WFXwiLZMg&s=19.

19 Rolling Pwn. (n.d.). *GitHub.* "Rolling Pwn Attack." Accessed on Nov. 14, 2022, at https://rollingpwn.github.io/rolling-pwn/.

20 Jonathan Andersson et al. (Jan. 15, 2019). *Trend Micro.* "A Security Analysis of Radio Remote Controllers for Industrial Applications." Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf

21 Jonathan Andersson et al. (Jan. 15, 2019). *Trend Micro.* "A Security Analysis of Radio Remote Controllers for Industrial Applications." Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf.

22 Hacking Into Your Heart. (July 17, 2022). *GitHub.* "Replay-based Attack on Honda and Acura Vehicles." Accessed on Nov. 14, 2022, at https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty.

23 Hacking Into Your Heart. (July 17, 2022). *GitHub.* "Replay-based Attack on Honda and Acura Vehicles." Accessed on Nov. 14, 2022, at https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty.

24 Colin Urquhart et al. (Oct. 2019). *Research Gate.* "Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach." Accessed on Nov. 14, 2022, at https://www.researchgate.net/figure/Rolling-Code-Overview_fig2_336715499.

25 Samy Kamkar. (2015). *DefCon 2015.* "Drive It Like You Hacked It." Accessed on Nov. 14, 2022, at https://samy.pl/defcon2015/.

26 Starvlab. (n.d.). *Starvlab.* "Honda-Civic Keyfob system affected by counter resynchronization attack." Accessed on Nov. 14, 2022, at http://starvlab.qianxin.com/?p=409.

27 Starvlab. (n.d.). *Starvlab.* "Honda-Civic Keyfob system affected by counter resynchronization attack." Accessed on Nov. 14, 2022, at http://starvlab.qianxin.com/?p=409.

28 Sultan Khan. (May 15, 2022). *NCC Group.* "Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks." Accessed on Nov. 14, 2022, at https://research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

29 Lennert Wouters, Benedikt Gierlichs, and Bart Preneel. (Aug. 11, 2021). *Ruhr-Universität Bochum.* "My other car is your car: compromising the Tesla Model X keyless entry system." Accessed on Nov. 14, 2022, at https://tches.iacr.org/index.php/TCHES/article/view/9063.

30 Brad Anderson. (Aug. 2, 2022). *Carscoops.* "When Is This Going To Stop? TikTok's Latest 'Kia Challenge' Encourages Users To Steal Cars." Accessed on Nov. 14, 2022, at https://www.carscoops.com/2022/08/social-medias-kia-challenge-has-led-to-a-spike-in-car-thefts/.

31 Kieran Press-Reynolds. (May 20, 2022). *Insider.* "The world's top hackers are competing to break into a Tesla. The winner gets $600,000 and keeps the car." Accessed on Nov. 14, 2022, at https://www.insider.com/pwn2own-hacking-tesla-contest-cybersecurity-tesla-2022-5.

32 International Energy Agency. (May 2022). *IEA.* "Global EV Outlook 2022." Accessed on Nov. 14, 2022, at https://www.iea.org/reports/global-ev-outlook-2022.

33 International Electrotechnical Commission. (Feb. 18, 2016). *IEC Webstore.* "Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories." Accessed on Nov. 14, 2022, at https://webstore.iec.ch/publication/24204.

34 International Electrotechnical Commission. (Feb. 18, 2016). *IEC Webstore.* "Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories." Accessed on Nov. 14, 2022, at https://webstore.iec.ch/publication/24204.

35 Philippe Lin et al. (Jan. 28, 2020). *Trend Micro.* "Security Dive: Devices Supporting SCPI, VIS Protocols." Accessed on Nov. 14, 2022, at https://www.trendmicro.com/en_us/research/20/a/security-analysis-of-devices-that-support-scpi-and-visa-protocols.html. .

36 Wu HuiYu and Li YuXiang. (May 7, 2021). *Blackhat Asia 2021.* "X-in-the-Middle: Attacking Fast Charging Piles and Electric Vehicles." Accessed on Nov. 14, 2022, at https://i.blackhat.com/asia-21/Thursday-Handouts/as-21-Wu-X-In-The-Middle-Attacking-Fast-Charging-Piles-And-Electric-Vehicles.pdf.

37 CHAdeMO. (n.d.). *CHAdeMO.* "About Us." Accessed on Nov. 14, 2022, at https://www.chademo.com/about-us.

38 Marc Mültin. (Oct. 11, 2021). *Switch EV.* "What is ISO 15118?" Accessed on Nov. 14, 2022, at https://www.switch-ev.com/knowledgebase/what-is-iso-15118.

39 Marc Mültin. (Oct. 11, 2021). *Switch EV*. "What is ISO 15118?" Accessed on Nov. 14, 2022, at https://www.switch-ev.com/knowledgebase/what-is-iso-15118.

40 Kaibin Bao et al. (Feb. 2018). *Research Gate.* "A threat analysis of the vehicle to grid charging port protocol ISO 15118." Accessed on Nov. 14, 2022, at https://www.researchgate.net/figure/System-overview-of-the-ISO-15118-protocol_fig1_319431250.

41 E-value. (n.d.). *Fortune.* "DC Charging Pile." Accessed on Nov. 14, 2022, at https://www.fortune.com.tw/tw/attached/product/evi/tw/DC%E7%9B%B4%E6%B5%81%E5%85%85%E9%9B%BB%E6%A8%81.pdf

42 RTL-SDR. (April 5, 2022). *RTL-SDR.* "Tesla Charging Ports Opened With HackRF Replay Attack." Accessed on Nov. 14, 2022, at https://www.rtl-sdr.com/tesla-charging-ports-opened-with-hackrf-replay-attack/

VicOne

A Subsidiary of Trend Micro

Learn more about VicOne by visiting **www.vicone.com** or scanning this QR code