Keys under doormats

R07944058 網媒碩一 陳鵬宇

1. Summary

這篇論文在探討，是不是該讓政府能夠透過公權力的方式去取得通訊間的資料，這可能有很多目的，例如：為了未來在辦案時能夠更容易掌握證據及一些關鍵資訊，但相對的，多開啓了一道通道，讓訊息有了新的管道能夠被取得，同時也增加了風險性。論文中提到了幾個日常生活中可能遇到的例子：舉凡在智慧型手機與人透過通訊軟體進行對談，收發電子郵件系統在 90 天後將對談刪除等，最後也提到了一些國與國之間的議題，以及相關法律的定訂措施。

2. Strength(s)

當我們提供政府、立法機關擁有最高權限去取得資訊，打開了這層通道後，會有很大的漏洞疑慮，這意味著有心人事只要對這層通道協定做攻擊，就能夠馬上取得大家的所有資訊。因此論文提到了一個重要的概念叫前安全性（forward security），這是一個密碼學中重要的通訊協定，解密的金鑰會在被使用過後，馬上被刪除。代表即便我們的主金鑰被洩漏，也不會導致過去的對談馬上暴露。若能有效的運用前安全性，可以「一定程度」保障當打開新的渠道後，舊資訊的安全。

3. Weakness(es)

很顯而易見的，提供額外的通信訪問權，會使得目前已經佈署好的技術面臨 U-turn 的現象，我們反而必需花更多的心力去確保互聯網的安全性，顧此失彼。

此外，新增額外協定也會提升整體架構複雜度，而資安研究者也同意了「複雜度即是資安的敵人。」每一個新功能，都可能連鎖反應導致其它的漏洞。我們也不能排除有內鬼，當政府機關有不肖人士時，這就像將安全的大門敞開，是極度危險的。我們不能要求每個人道德標準都在一定水平，但假設「最低道德標準」，從法律層面去規範卻是有機會的。

4. Reflection

還記得 2016 年時，蘋果公司與 FBI 的訴訟案，當時 FBI 要求 Apple 必須協助幫忙駭入兩名恐怖份子所使用的 iPhone 來協助辦案。這讓我想到政府部門在面對「資安 vs 辦案」這件事時總會說：「如果你想要擁有安全，那就必須交出一部分隱私作為交換。」論文中也有提到：「正是因為電腦工程師擁有豐富的安全性與系統經驗，我們認為若執法部門用特殊的方式存取系統，將會帶來巨大風險。」

設置後門以便讓某些人存取系統的風險，包括必須將原本就已經很複雜的系統變得更加複雜難解，也不能保證其安全性，況且企業不可能專為聯邦調查局打造特殊的存取機制。再加上若是有這樣的後門存在，意味著駭客也能利用漏洞來駭入系統。

老師上課時有說要確保資安的三大要求，其中有一項是「保密性」，若今天我們希望將解密的鑰匙交付給「信任的第三方機構」，那等於我們引清兵（Eve）入關，只是這個 Eve 不見得會將你資料拿去亂搞罷了！（但他還是可以選擇這麼做）

想要實現這樣的架構，還同時必需考慮國與國之間資訊不對等的問題，美國的企業總不會希望中國為了破案，就輕易的使用第三方的金鑰去解鎖訊息。如果這個鑰匙是 long-term 的，既然能夠透過這鑰匙去解鎖某段訊息，那同理也可以將之用在其它方面，而道德不管用時，就有賴法律出來說話，但不同國家是很難共同制定法律的。

總括來看，不論從現實面，可能遇到的人有劣根性；或是從實作面，可能太過於複雜，要打照這樣一個系統都還是充滿挑戰。