The Token is Dead. Long Live the Token!

文章來源: SafeNet 提供 | 翻譯整理: 叡揚資訊 資訊安全事業處

摘要

當傳出 RSA 演算法被破解消息時，私底下有非常多的討論關於這整件事情所造成的影響。雖然最近也有許多類似的破解，但這也更加強調了沒有網路是無法侵入的。

最初大家所困惑的是，到底這造成什麼樣的損失以及當下是否有加密。當 Lockheed Martin 宣佈其近期的破解是利用早前 RSA 的漏洞，之後整個遊戲規則被永遠地改變了。現在整個事件所造成的似乎只是產品召回。任何曾經經歷過產品召回的製造商都會同情 RSA，因為這是一個代價高昂和耗時的過程，當然造成最大不便的是他們的客戶。估計 RSA 花了多達 9 個月的時間利用公司所有的資源完成這次的召回。

整件事所令人驚訝的是，RSA 似乎已設好哪些客戶是有資格獲得 Token 替換-那些比較「大的客戶」且有「大量集中的使用者」或那些以「消費者為中心」的用戶是有資格獲此次的自動召回或更換。此規則有點含糊並交待不清他們對於絕大多數沒有達到標準的客戶要如何處理。

然而當我們急於去更換 Token 之前，平心而論（即便是與其他提供同功能的 Token 供應商），我們必須基於作為提供基本服務給我們的企業，善盡其責確定做這樣的決定是否正確-無論您是否與其他廠商一樣直接更換 Token。其實對於我們這些負責企業系統架構也許會被問到在做這樣決定時是否有做任何評估。

所以，這審查過程該看起來該如何進行？

1. 審查自從上一次決定採用的認證策略，到目前是否有新的技術可以採用，決定是否該採用新的技術如 SaaS 或如果是行動裝置改用 iPAD？
2. 審查市面上的供應商所提供的解決方案，是否有較低風險的模型或架構，相對於依賴安全供應商，也許我們可以考慮自己擁有加密種子和密鑰。

另外對於目前使用較舊的硬體形式 Token，評估是否換較小的 Token 或以軟體解決方案取代，通常都需要發生一個重大事件，我們才會去檢討或主動去檢閱上次所制定的安全策略是否要改進。而這次所發生的即是此類事

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

件。自從 5 年前買 RSA Token 後，世界上已發生許多的改變：

雲端應用的成長

- SaaS 市場 2010 年增長到估計$150 億美元(IDC 2010)
- Salesforce.com 在 2010 收入達到$14 億美元(Salesforce 2010)
- 虛擬主機每日建置 90,000 台 (The Economist December 2010)

IT 消費化

- 相較於 PC 出貨量，智慧手機出貨量明顯出色（IDC，2011 年 1 月）
- iPAD 在前 14 月達到 2500 萬台的銷售量 (蘋果，2011 年)
- 2 億的 iOS 設備出貨量 (蘋果，2011 年 6 月)
- 1 億的 Android 設備啟動（谷歌 IO，2011 年 5 月)

虛擬化

- 168 億美元的虛擬伺服器硬體市場（IDC 2010 年）
- 每季 8.6 億美元的虛擬化軟體市場（IDC 2010 年）

行動員工

- 在 2010 年有 10 億員工以「遠端」方式存取公司系統，等於三分之一的世界勞動力（ IDC 2010 年）

社交網路

- 2011 年前幾名的 Web 網站：1.Google、 2.Facebook、 3.YouTube、 4.Yahoo、 5.Blogger.com（Alexa.com)
- 2006 年前幾名的網站：1.Google、 2. Wikipedia、 3.HP、 4.Cisco、 5.IBM（bytelevel.com)

正如我們所看到的，時間過去了，世界在變而我們的認證策略呢？我聽到您說『如果沒有壞，就沒必要修』，沒錯，但您猜如何，現在正是時候了！而您是否真的該急著去汰換 Token（如果您是那幸運兒之一）繼續使用下去?，還是您該利用這一個機會告知董事會您已盡職檢討並更新公司的認證策略嗎？

Safenet 建議 RSA 客戶不需急著汰換新的 Token（無論是否從其他的供應商採購)。相反的，該看看自從您上次審查您的驗證策略是否有需求上的改變。

硬體 Token 是否還是可行的解決方案嗎？也許目前在工作場所中大量消費設備已採用，是您決定繼續使用的原因嗎？照統計您知道嗎，使用者會發現他們的行動電話在他們發現錢包或錢包遺失前遺失！

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw

也許採用一次性密碼保護已不符所需，尤其是您已經採用硬碟加密和開機前驗證，您或許可以另外考慮使用憑證類的身份驗證去提供一次性登入到行動裝置和使用者的應用程式。也許您的使用者已使用太多的裝置，改採加密的 USB 磁碟機來整合所有的驗證 Token 能同時提供安全的存儲和身份驗證。您是否應確保您新的驗證策略包含快速成長的軟體作為服務（SaaS）市場，並整合使用者驗證到雲端？

這些都是值得深思的問題，尤其是因為這一事件而受影響的每個使用者。而所有的決策您必須考慮其衍生的成本，並確保能達到最大的利益。如果還是依照舊有方法，而不去做相關的評估，這只是失去大好的機會，而可能會導致您在未來遇到更多的問題。您有權利去提供您的組織更現代、 更方便、 更安全、 更有擴展性的身份驗證解決方案！

SafeNet 不僅提供更佳保證的加密方法為您的業務提供增強式的驗證解決方案，還能夠讓您透過雲端達成 IT 消費化來節省費用，透過 SafeNet 提供您正確的做法，為您的組織，現在和未來的需要。

關於 SafeNet

SafeNet 成立於 1983 年，是全球領先的資訊安全公司。SafeNet 致於保護其客戶寶貴的資產，其中包括身份、交易、通信、資料和軟體授權，在整個資料生命週期。在各地商業企業、政府機構和 100 多個國家的 25000 多個客戶信任 SafeNet 能提供其資訊安全的需要。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw