

簡短訊息服務的保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 介紹.....	3
什麼是簡短訊息服務（SMS）？.....	3
商用趨勢.....	3
II. SMS 的保安.....	5
SMS 的保安基本知識.....	5
SMS 的保安威脅.....	5
SMS 的保安考慮.....	7
III. 結論.....	8

摘要

簡短訊息服務 (SMS) 已成為流動電話用戶最常用的方法，以流動電話或手提設備來發放及接收簡單的純文字訊息。簡短訊息又稱短訊，用戶可用短訊向個別或眾人發放或接收個人訊息、電郵通知、資訊服務、工作分配、股市動向等等。加上不斷演進的個人數碼助理流動設備，除了高效能特性外，還配備了清晰螢幕及方便的文字輸入法，流動電話用戶之間使用 SMS 已愈來愈普及。本文提供 SMS 的基本概覽，並就使用 SMS 的保安問題作出討論。

I. 介紹

什麼是簡短訊息服務 (SMS) ？

SMS 是一個讓人們透過流動電話或與互聯網接駁的電腦，以文字訊息互相溝通的方便途徑。每個訊息可載最多 140 個字節的數據 (1120 個位元)，即等於 160 個英文字母或 70 個中文字。從事電子商貿的人士可發放大量 SMS¹ 給一大組群的客戶，而不用人手操作逐一發放。電話號碼也可使用其它工具透過匯入的文字檔案或流動電話中儲存的聯絡資料收集。

簡短訊息服務中心 (SMSC) 通常由電訊公司擁有及營運，負責 SMS 的通訊路由及傳送。當一個短訊傳送至 SMSC，儲存與轉寄訊息的機制就會啟動，訊息會暫時被儲存下來，然後轉寄至收件人已啟動的電話或接收設備。短訊在傳送到收件者的設備之前，會通過多個 SMSC 或 SMS 通訊閘 (作為兩個或以上、使用不同規約的 SMSC 的橋樑²)，這與電子郵件的通訊原理十分類似。SMSC 指定訊息發放的路線及管理發放進程。如果短訊的收件人沒有啟動電話或接收設備，SMSC 會將短訊暫時儲存，直至「有效期」過後才刪除。

商用趨勢

短訊是一種普及的溝通渠道。一年中的特別日子如元旦日或情人節，短訊的用量也因應增加。根據電訊管理局的統計，2007 年元旦日就有約一千五百萬個短訊，比 2006 年的數量增加 55%³。

短訊現已用作個人和商業通訊的途徑，以下是一些常見的例子：

1. 股票經紀及銀行就股票買賣的狀況向客戶發放警告及通知，信用卡公司就高風險交易向信用卡持有人發放通知，以及通知一些機構的系統管理員有關資訊科技系統出現的嚴重事故等。
2. 銀行或機構透過短訊向客戶發放一次性密碼，用以授權或確認高風險的網上交易。網上交易系統可憑一次性密碼在交易完成之前認證客戶的身份。
3. 透過流動電話，使用者可用雙向互動文字訊息功能 (Two-way interactive text messaging) 交談和聊天。從事電子商貿的人士也可透過加密的短訊向目標客戶

¹ <http://www.sendgroupsms.com/>

² http://www.developershome.com/sms/sms_tutorial.asp?page=smsGateway

³ <http://www.ofta.gov.hk/en/datastat/sms.pdf>

提供方便的途徑回應和提出對產品或服務的要求，如下載電話鈴聲和牆紙（wallpapers）。

在香港，發放大量短訊是由非應邀電子訊息條例（UEMO）所監管⁴。

⁴ <http://www.ofta.gov.hk/en/uem/main.html>

II. SMS 的保安

SMS 的保安基本知識

短訊的技術規格已在 ETSI TS 03.48⁵中列明。技術規格有幾個選項提供安全系數的規格，包括安全系數索引（Security Parameter Index SPI）、加密識別符（Ciphering Key Identifier K_{ic}）及完整值（Integrity Value RC/CC/DS）。冗餘校驗（Redundancy Check RC）、加密算法檢驗和（Cryptographic Checksum CC）或數碼簽署（Digital Signature DS）也可用於核實數據的完整性。

但是，以上的保密及完整性機制只是可供選用的保安措施，而非執行 SMS 系統的強制要求⁶。SMS 也可能受 SMSC 的干擾。如沒有恰當地執行短訊保安的選項，每天在網絡上傳送的短訊只靠傳訊網絡，如 GSM 網絡等的保護。

實際上，短訊在傳送過程中並沒有預設加密的。當短訊通過訊號通道時，會以循環冗餘檢驗（cyclic redundancy check CRC）確保短訊沒有受損。採用傳統加密法的誤差轉寄保護功能（Forward error protection）也包含在內，但短訊中並沒有提供保護機密性及完整性的加密算法（Cryptographic protection on confidentiality and integrity）。

如前所述，如短訊未能成功地傳送給收件人，每個短訊都有一個由 SMSC 提供的暫存有效期。如短訊在有效時間內未能傳遞出去，SMSC 會刪除已存的短訊。短訊刪除後，收件人就無法接收原來的訊息。這種情況通常會在收件人去了沒有短訊覆蓋的地方發生，例如收件人到外地公幹。

SMS 的保安威脅

了解 SMS 保安的基本常識，有助預防一些常見的短訊使用和操作上的保安威脅：

訊息披露

由於在短訊傳送過程中並沒有預設加密，訊息在傳送時有可能被截取及窺視。再者，在 SMSC 成功發放訊息給既定的收件人之前，短訊是以原文的形式儲存起來的。SMSC 中

⁵ http://www.3gpp.org/ftp/Specs/archive/03_series/03.48/

⁶ <http://stinet.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA462720>

能夠取用訊息系統的使用者有可能看到及修改這些訊息。

間諜程式如 FlexiSpy⁷可讓入侵者自動錄取所有進入及發出的短訊，然後將記錄上載至遠端的伺服器，以供日後閱覽及分析。

濫發訊息

當電子商貿人士用短訊作為正當的市場推廣渠道時，很多人會因收到濫發短訊而感到不便。大量短訊的發放功能幾可令任何人也輕易地發放大量短訊。

氾濫／拒絕服務（DoS）的攻擊

氾濫或 DoS 攻擊的方法是重覆向目標流動電話發出訊息，使受害人的流通電話無法接通。有研究指出，短訊規約中的弱點會被用作對流動電話網絡發出 DoS 攻擊。例如在一秒間發出 165 個文字訊息，就足以干擾美國的曼克頓市內所有流動電話⁸。

導致電話當機的短訊（SMS Phone Crashes）

一些有弱點的流動電話，如接收了特定類型的畸形短訊（malformed short message）就會當機。一旦接收了這些畸形訊息，受感染的電話就不能再運作。傳媒的報導也指出，流動電話對這類型的攻擊是難以招架的⁹。

短訊病毒

目前仍然未有任何報告指出有短訊附有病毒，但當流動電話愈來愈多功能和程式時，病毒透過短訊散播的潛在危機就愈來愈大。再者，SIM 應用系統工具的功能容許應用系統取得撥號功能及電話簿的記錄，有可能令短訊成為適合散播自我複製病毒的平台。

短訊仿冒詐騙（SMiShing）

SMiShing¹⁰結合了短訊和仿冒詐騙的特點。它跟使用電郵作互聯網的仿冒詐騙攻擊相似，攻擊者嘗試以偽造的文字訊息愚弄流動電話用戶¹¹。當用戶讀取這些偽造文字訊息時，有可能會連接至短訊中提供的網頁，因而被誘騙下載惡意軟件至流動電話中。

⁷ <http://www.flexispy.com/news-flexispy-blackberry-windows-mobile.htm>

⁸ http://www.schneier.com/blog/archives/2005/10/sms_denialofser_1.html

⁹ http://www.theregister.co.uk/2001/12/06/sms_phone_crash_exploit/

¹⁰ http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci1214281,00.html

¹¹ <http://www.vnunet.com/vnunet/news/2163586/sms-phishing-attack-seen-wild>

SMS 的保安考慮

為免 SMS 受到保安威脅，建議用戶使用下列常見的預防措施：

訊息傳輸

使用互聯網瀏覽器發放短訊時，應要啟動保安裝置以防洩露訊息，例如可以使用保密插口層（SSL）加強傳輸保安。

對一些有需要訊息傳輸保安的應用系統，如流動銀行服務，建議使用傳送人與收件人之間端到端的加密方式。這些交易系統（**transactional systems**）應該已有內置的端到端保安。

至於人們用 SMS 互相通訊時，CryptoSMS¹² 這類產品可協助用戶透過嚴格的加密算法將 SMS 通訊加密，同時也防止短訊受截取的威脅。

儲存保護

如要作出大規模的短訊發放，客戶的流動電話聯絡名單應加以保密，並適當地保護以免外洩。由於聯絡名單被視為個人資料，因此應該根據私隱條例和規例作出恰當的保護。

用戶認證

使用網上短訊服務發放短訊時，必須要以用戶的登入身份和密碼來認證用戶。用戶不應向別人透露登入身份和密碼。如要安全的交易，用戶認證應受 SSL 的保護。

保護發放訊息的個人電腦

如要透過互聯網發放短訊至 SMS 通訊閘時，不建議使用公眾互聯網終端機。如使用桌上設施發放短訊，用來發送訊息的個人電腦不應無人看管。

¹² <http://cryptosms.com/protect.html>

III. 結論

短訊是一種非常普遍的通訊工具，但短訊的保安卻仍未成熟，而且在作業實務上執行也有困難。由於使用短訊來通訊及交換資訊日趨普及，以短訊傳輸敏感資料時就必須更加謹慎。用戶必須知悉短訊有可能被截取，如要以短訊傳送敏感資料，則應考慮使用加密短訊等解決方法。