談 SQL Server 安全管理大搜集

胡百敬
(http://byronhu.spaces.live.com)
精誠公司 恆逸資訊

2009/9/1 新聞

台灣大跨年當機 工程師搞鬼

【聯合報/記者何祥裕／台北縣報導】 2009.09.01 08:32 am

去年跨年夜，造成台灣大哥大行動電話用戶大當機，檢調查出是台灣諾基亞西門子公司前工程師陳懷先，涉嫌以女友名義登入台灣大資料庫並刪除資料造成大當機，檢方昨天將陳依妨害電腦使用罪嫌起訴。

台灣大當機造成北北基、桃園、新竹縣市、宜蘭及花蓮縣等地區數萬用戶受害，無法撥打行動電話，簡訊、語音信箱等也無法使用，損失約一千五百萬元。檢察官偵訊陳懷先時，陳否認是遭開除而挾怨報復，僅說會這麼做是因為「好玩」。

台灣大原本以為跨年夜系統故障是因為大量話務導致當機，經過內部清查才發現是被人刻意刪除資料庫資料造成，經向調查局北機組檢舉與追查，才查出是台灣大維護商台灣諾基亞西門子公司前工程師陳懷先（廿九歲）所為。

檢調查出，陳懷先前年四月到去年三月底，任職西門子公司維修工程師，負責台灣大哥大的SRRi主機（門號可攜認證系統）及TA主機（客戶話務計費系統）維護，除了熟知兩主機的操作與相關指令外，還知悉登入的帳號密碼。

去年三月底，陳懷先遭公司解雇心生不滿，刻意挑選話務量最大的跨年夜，拿女友申辦的台灣大手機連線到台灣大兩大主機。

去年十二月卅一日晚間八時至十時，陳三度登入主機，將主機內的可攜號碼資料與連線登入紀錄全數刪除，並重新啟動系統，卻因資料全部刪光，導致無法重新開機，停擺時間從當晚十一時廿五分直到隔天凌晨四時許才恢復。

深度防禦

- 利用多層次防禦:
  - 增加攻擊者事蹟敗露的風險
  - 減少攻擊者成功的可能性

大綱

- 認證
- 加解密
- Audit
- 原則管理
- SQL Injection

認證

SQL 認證	WINDOWS 認證
帳號/密碼	Encrypted Token (Kerberos) Challenge-Response (NTLM)
傳遞加密後的密碼	密碼未在網路上傳遞
若通訊間未加密，可能招到 replay 攻擊	不會招到 replay 攻擊 (Kerberos)
沒有交互認證	可透過 Kerberos 交互認證
SQL Server 管理登入	Windows 管理登入
DBA 建立登入帳號	Windows/domain admin 建立登入帳號
藉由 Windows 2003+ 要求密碼原則	Windows 要求密碼原則
伺服器間的 Security context 未必一致	伺服器間的 Security context 是一致的

- Windows 認證較 SQL 認證為佳

資料加密

- 為何考慮加解密
  - 為安全加一層
  - 一些行業的律法要求
- SQL Server 2000 需要協力廠商
- SQL Server 2005
  - 內建資料加密功能：對稱鑰匙、非對稱鑰匙、雜湊
  - 支援鑰匙管理
- SQL Server 2008 為加密增加功能
  - Transparent Data Encryption
  - Extensible Key Management

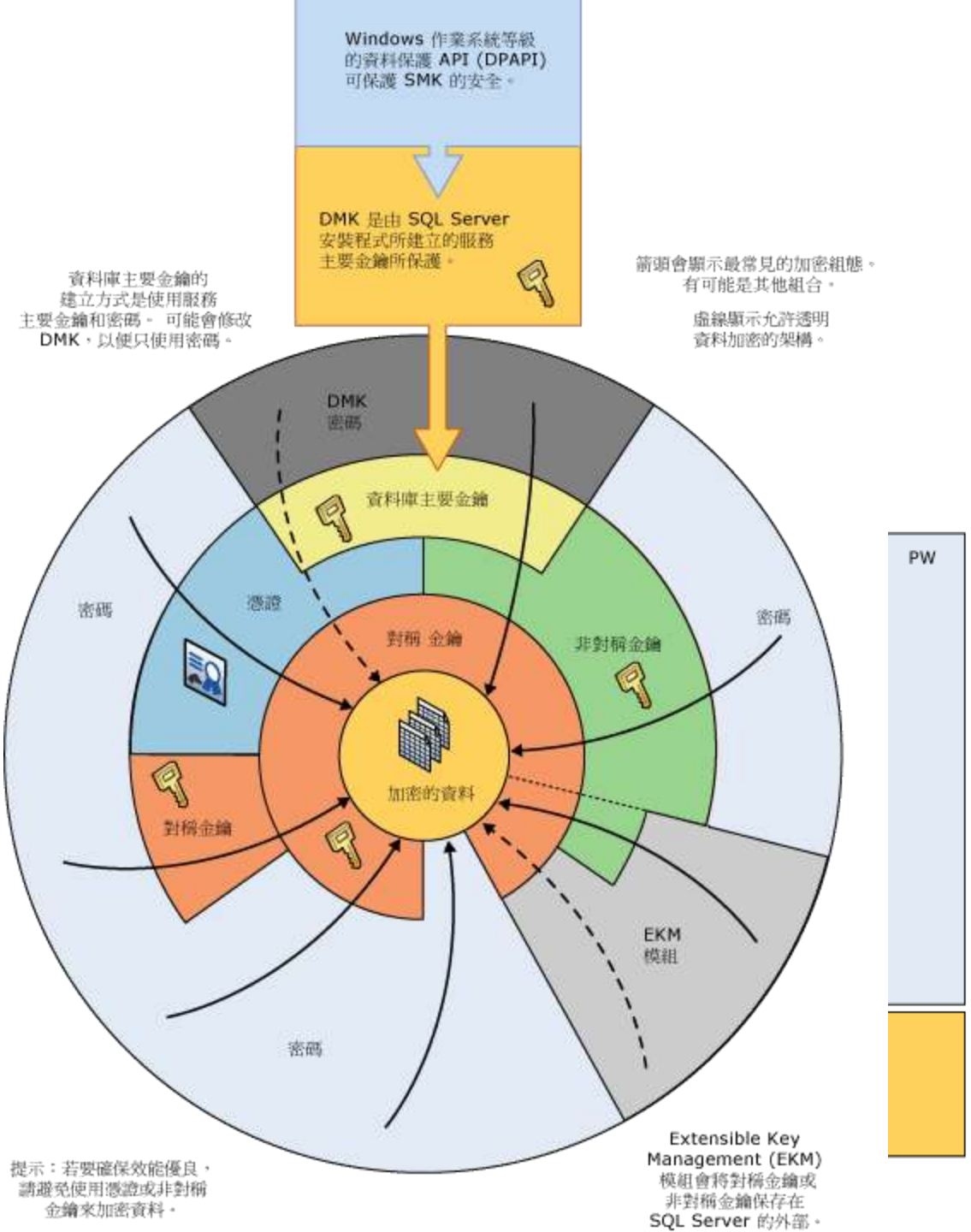
資料加密
Cell-level 加密

- 內建加解密
- 可以 DDL 建立對稱式、非對稱式鑰匙以及憑證
  - 對稱鑰匙與私鑰一定以加密的方式儲存
- 強化鑰匙自身安全
  - 以使用者的密碼為基礎
  - 自動架構在 SQL Server 鑰匙管理的架構中
- 可選擇演算法
  - 包含 DES, TRIPLE_DES, AES(128, 192, 或 256)

資料加密

最佳做法

- 儘量考慮在應用程式層加/解密
- 只對必要的資料加密
- 使用對稱式加密
- 小心規畫
  - 鑰匙管理非常重要
  - 了解既有程式碼所需的改變
  - 考慮鑰匙大小與演算法所需的 CPU 運算力


Windows 作業系統等級
的資料保護 API (DPAPI)
可保護 SMK 的安全。
DMK 是由 SQL Server
安裝程式所建立的服務
主要金鑰所保護。
資料庫主要金鑰的
建立方式是使用服務
主要金鑰和密碼。 可能會修改
DMK，以便只使用密碼。
箭頭會顯示最常見的加密組態。
有可能是其他組合。
虛線顯示允許透明
資料加密的架構。
DMK
密碼
資料庫主要金鑰
密碼
憑證
對稱 金鑰
非對稱金鑰
密碼
加密的資料
對稱金鑰
EKM
模組
密碼
PW
提示：若要確保效能優良，
請避免使用憑證或非對稱
金鑰來加密資料。
Extensible Key
Management (EKM)
模組會將對稱金鑰或
非對稱金鑰保存在
SQL Server 的外部。

資料加密注意事項

- SQL Server 不確認憑證的正確性
  - 過期日
  - CRL(Certificate Revocation List)
  - 不加入 Public Key Infrastructure (PKI)
- 存放加密的資料類型需 Varbinary
- 跨資料庫的共用性
- 備份/還原

端起管理語法範例

```
--Service Master Key
--備份 Service Master Key
BACKUP SERVICE MASTER KEY TO FILE = 'path_to_file'
ENCRYPTION BY PASSWORD = 'password‘

--Database Master Key
--以不同的保護密碼，在建立一份 Database Master Key
ALTER MASTER KEY ADD ENCRYPTION BY PASSWORD =
'SecondDBAP@ssword';

--刪掉另一份 Database Master Key
ALTER MASTER KEY DROP ENCRYPTION BY PASSWORD =
'SecondDBAP@ssword';
```

端點管理語法範例

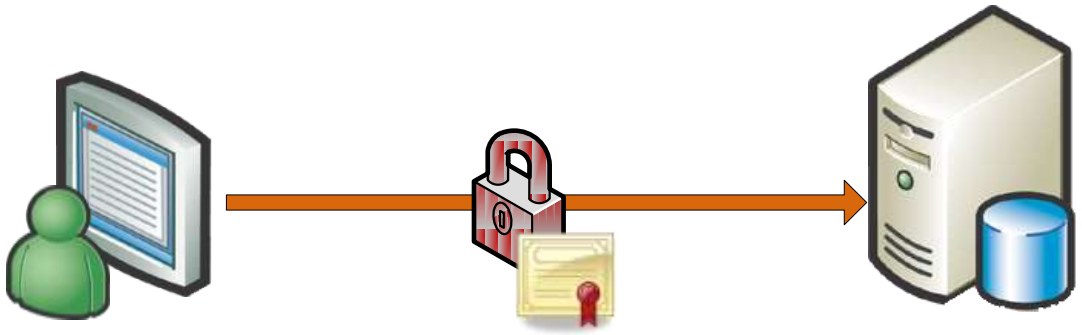
```
--憑證
--備份憑證到硬碟成為檔案
BACKUP CERTIFICATE NorthwindCert
TO FILE = 'C:\MyServerCert'
WITH PRIVATE KEY (FILE = 'C:\MyServerCertKey',
       ENCRYPTION BY PASSWORD = 'password');

--還原先前的憑證
CREATE CERTIFICATE MyServerSert
FROM FILE = 'C:\MyServerCert'
WITH PRIVATE KEY (FILE = 'C:\MyServerCertKey',
       DECRYPTION BY PASSWORD = 'password');
```

鑰匙管理語法範例

```
--對稱鑰匙
-- 透過KEY_SOURCE 和IDENTITY_VALUE 建立對稱鑰匙，所以它可重建
CREATE SYMMETRIC KEY key_demo_recreate WITH ALGORITHM =
TRIPLE_DES,
      KEY_SOURCE = '鑰匙源- 保護這個來源定義的秘密！',
      IDENTITY_VALUE = '鑰匙辨別碼'
      ENCRYPTION BY CERTIFICATE cert_demo
```

Channel 加密

- SQL Server 2000 後完整支援 SSL 加密
  - Clients: MDAC 2.6 or later
  - Force encryption from client or server
- Login 封包加密
  - 不管加密設定為何，都會使用
  - 自 2000 開始支援
  - 自 2005 可以自行產生憑證



Channel 加密

- 安全重於效率時，啟動 channel encryption
- 在伺服器端安裝憑證
- 使用者端啟動”強制通訊協定加密”

透過 SQL Trace/Profiler 監控

- 以可重用的範本為基礎建立追蹤
- 最追蹤進行時，可以監看追蹤結果
- 將追蹤的結果存放在資料表
- 可啟動、暫停、停止追蹤
- 可重新執行追蹤的動作

以 DDL/DML 觸發追蹤

- 當某些變更發生時，執行追蹤
- 建立變更歷程
- 防止登入，架構、資料等變更
- 可以在變更時執行商業邏輯

SQL Server Audit

- 追蹤和記錄系統發生的事件
- 可追蹤伺服器或資料庫等級的變動
- 可透過 Transact-SQL 管理
- 追蹤失敗可以停止執行 SQL Server 服務
- 要稽核 SELECT、UPDATE 等行為在條件式內的資料值部分，需上 Cumulative update package 3 for SQL Server 2008 Service Pack 1

以原則為基礎的管理

- 容易地同時在多部伺服器上檢查有關安全的各項原則
- msdb資料庫中PolicyAdministratorRole資料庫角色的成員對於系統上的原則擁有完整控制權

一般常見的攻擊

可能影響你的常見弱點

- SQL Injection
- Cross-Site Scripting
- Buffer Overflows

SQL Injection

- 讓意圖不軌的使用者透過 SQL 語法控制系統
- 技術門檻低，容易實做，透過網路搜尋可取得大量資料
- 可以從各種地方攻擊資料庫後，再由資料庫影響各種應用系統 (Web, client/server…等)
- **Pattern**：針對無法信任的資料建立動態 SQL 語法！

SQL Injection

March 2006
印度政府

July 2007
Microsoft UK

August 2007
United Nations

January 2008
大量的 SQL injection 攻擊,
10,000+ systems

程式碼哪裡有問題？

```
public void Sample(String NameStr)
{
      String sqlQuery =
      String.Format("SELECT * FROM [Table1]
      WHERE Name = '{0}'", NameStr);

      SqlCommand sqlCmd =
      new SqlCommand(sqlQuery, new
      SqlConnection(connectionString));
      ...
}
```

Pattern: 針對無法信任的資料建立動態 SQL 語法！

NameStr = x'; DROP TABLE Table1;--

SELECT * FROM [Table1] WHERE Name = 'x'; DROP TABLE Table1;--'

防禦資料隱碼 (SQL Injection)

SQL Injection
分析工具

- Microsoft Code Analysis Tool .NET (CAT.NET) v1 CTP

  二進位碼分析工具，分析 Cross-Site Scripting (XSS), SQL Injection 和 XPath Injection
  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=0178e2ef-9da8-445e-9348-c93f24cc9f9d
- Microsoft Source Code Analyzer for SQL injection
  - 對偵測 ASP 原始程式碼的 SQL injection 有幫助
  - July CTP:
    http://www.microsoft.com/downloads/details.aspx?FamilyId=58A7C46E-A599-4FCB-9AB4-A4334146B6BA

參考資料

- SQL Server 2008 White Papers(http://msdn.microsoft.com/en-us/library/dd631807(SQL.10).aspx)
  - Cryptography in SQL Server(http://msdn.microsoft.com/en-us/library/cc837966.aspx)
  - Auditing in SQL Server 2008(http://msdn.microsoft.com/en-us/library/dd392015.aspx)
- http://technet.microsoft.com/en-us/magazine/2008.04.sqlsecurity.aspx?pr=blog
- http://blogs.msdn.com/sqlsecurity/
- http://sharedderrick.blogspot.com/2009/08/sql-server-2008-sql-server-audit-where.html