CS Software
Consulting and Services GmbH

Two Easy (?) Pieces

Berichte aus dem Consulting Alltag

GTUG Stuttgart
27./28. September 2022

Two Easy (?) Pieces
Eine Warnung

- Vortrag wird (zumindest in Teilen) sehr technisch
- Vorsicht, falls jemand gegen C allergisch ist
- Folien können Spuren von Quellcode enthalten

Two Easy (?) Pieces
Fall 2: Security bei Debuggen im Pathway

- Pathway System läuft unter ABC.SUPER
- Entwickler haben Userids ABC.USER1 usw.
- Entwickler möchten ihre Programme debuggen
- Wenn PATHMON die Prozesse startet, laufen diese unter ABC.SUPER
- Versuch des Entwicklers, Server zu debuggen, scheitert mit Security Violation
- ABC.SUPER Passwort soll nicht allen Entwicklern bekannt sein

Two Easy (?) Pieces
Fall 2: PROGID?

- Bisherige Praxis: Entwickler setzen PROGID für ihre Executables
- Geht mit FUP, aber auch mit SQLCI
- Ergebnis: Programme laufen unter dem User, der sie erstellt hat…
- … und die Entwickler können debuggen
- Aber: Setzung geht z.B. beim Kopieren verloren...
- … und ist ein zusätzlicher Schritt im Bauvorgang
- Remote Compile und Deploy und dann wieder auf die Plattform
- Progid kann z.B. auch bei Audits negativ auffallen
- Funktioniert, ist aber hässlich

Two Easy (?) Pieces
Fall 2: Was geht…

- Kann das Programm nicht selbst entscheiden, unter welchem User es läuft?
- Guardian stellt (u.a.) dafür eine Funktion zur Verfügung:

```
short USER_AUTHENTICATE_ ( char *inputtext
,short inputtext-len
,[ short options ]
,[ __int32_t *dialog-id ]
,[ short *status ]
,[ short *status-flags ]
,[ char *displaytext ]
,[ short displaytext-maxlen ]
,[ short *displaytext-len ]
,[ short cmon-timeout ]
,[ char *termname ]
,[ short termname-len ]
,[ char *volsubvol ]
,[ short volsubvol-maxlen ]
,[ short *volsubvol-len ]
,[ char *initdir ]
,[ short initdir-maxlen ]
,[ short *initdir-len ]
,[ char *initprog ]
,[ short initprog-maxlen ]
,[ short *initprog-len ]
,[ short *initprog-type ]
,[ __int32_t *last-logon-time ]
,[ __int32_t *time-password-expires ]
,[ char *ipaddress ]
,[ short ipaddress-len ] );
```

Two Easy (?) Pieces
Fall 2: Guardian kann viel

- USER_AUTHENTICATE_ kann viele Dinge:
  - Überprüfen des Passworts
  - Ändern der effektiven Userid des Prozesses
- Benutzung nicht völlig simpel (viele Parameter)
- … aber es gibt schlimmere Funktionen
- Benutzung hier: Anmelden unter anderem User
- … d.h. ABC.HUBER statt ABC.SUPER

Two Easy (?) Pieces
Fall 2: Die Idee

- Prozess wird im Pathway von ABC.SUPER gestartet…
- … und meldet sich dann selbst als ABC.HUBER an
- Damit kann ABC.HUBER den Prozess debuggen

Two Easy (?) Pieces
Fall 2: Fragen

1. Woher weiß das Programm, dass es sich als ABC.HUBER anmelden soll?

2. Braucht man für die Anmeldung nicht das Passwort von ABC.HUBER?

3. Was, wenn man das Debuggen schon beim Programmstart übernehmen will?

Two Easy (?) Pieces

Fall 2: Wem gehört das Programm?

Woher weiß das Programm, dass es sich als ABC.HUBER anmelden soll?

1. PROCESS_GETINFO_ liefert den Filenamen des Executables des aktuellen Prozesses

2. FILE_GETINFOLISTBYNAME_ liefert den Owner des Executables (numerisch, z.B. 32,10)

3. USER_GETINFO_ liefert zu 32,10 den Usernamen ABC.HUBER (Gruppe 32 = ABC, User 10 = HUBER)

USER_AUTHENTICATE_ braucht Format „ABC.HUBER“

Two Easy (?) Pieces
Fall 2: Braucht man das Passwort?

- Im Prinzip braucht USER_AUTHENTICATE_ zum Anmelden das Passwort…
- … aber es gibt die Option „blind logon“
- Wurde Programm unter ABC.SUPER gestartet, ist die Anmeldung zu ABC.<irgendwer> ohne Passwort möglich
- Voraussetzung hier erfüllt, da PATHMON von ABC.SUPER gestartet

Two Easy (?) Pieces
Fall 2: „Ummelden“ vor main

- Man kann Code ausführen, bevor die „main“ Funktion („Hauptprogramm“) ausgeführt wird
- Wird z.B. von DLLs beim Laden genutzt
- Globale C++ Objekte mit Konstruktoren brauchen das auch
- Dokumentiert in DLL Manual
- Funktion mit Namen __INIT__() wird vor main() aufgerufen
- Genauer gibt es eine ganze Liste solcher Funktionen (siehe Manual)

Two Easy (?) Pieces
Fall 2: Rezept

- Man schreibe eine Funktion namens __INIT__, die…
  - … den Owner des Executables herausfindet
  - … und sich dann als dieser User anmeldet.
- Funktion muss nur zu allen betroffenen Programmen gebunden werden
- Keine Änderungen am Sourcecode erforderlich
- Funktion wird automatisch von der Laufzeitumgebung aufgerufen

Two Easy (?) Pieces
Fall 2: Funktioniert!

- Rezept umgesetzt und getestet: Funktioniert!
- Sourcecode (95 Zeilen) an Kunden geliefert
- Problem gelöst!
- Aufwand: Ein entspannter Nachmittag

Two Easy (?) Pieces

Fragen?