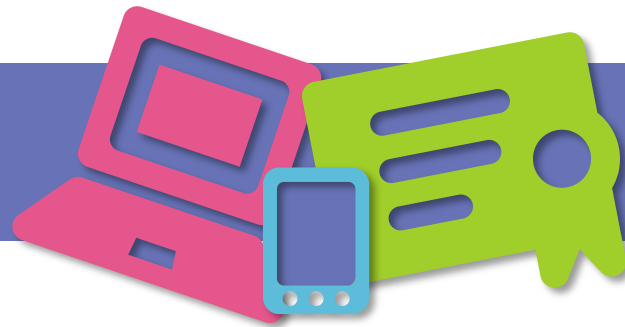


# SECURITY 2014

22. ročník konference o bezpečnosti v ICT



## **Bezpečnost tlustých klientů**

Oldřich Válka

AEC, spol. s r.o.



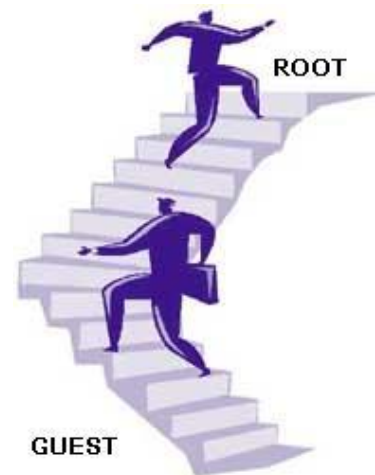
# Agenda

- Proč řešit bezpečnost tlustých klientů.
- Kde se s nimi můžeme setkat.
- Základní detekce aplikace.
- Nejčastější typy zranitelností.
- Ukázky kompromitace.



# Proč řešit bezpečnost TK

- Uživatelé mají velmi často plnou kontrolu nad aplikací.
- Útok na libovolné komponenty.
- Vystavená data, administrátorské skryté funkce.
- Povýšení práv nad aplikací.
- Povýšení práv OS.





# Kde se s TK můžeme setkat?

- Firemní Internetové bankovníctví.
- Účetnictví a ekonomické systémy.
- Administrativa (docházka, mzdy atd.)
- Dohledové systémy, monitoring.
- Aplikace na míru.
- Krabicový SW.
- ...



# Základní detekce aplikace

## UNMANAGED CODE APPLICATIONS

- C a C++ ("unmanaged" nebo také "native" language).
- Kompilace do strojového kódu.
- Zahrnuje exportovatelné funkce.

## PRO

- Rychlost aplikace.
- Nelze snadno dekompilovat do původního zdrojového kódu.

## PROTI

- Není snadná přenositelnost.
- Dekompilace a rekompilace je složitější, ale stále možná.
- API hooking.

## MANAGED CODE APPLICATIONS

- Frameworks .net, Java, ...
- Kompilováno do bytecode.

### PRO

- Nezávislost na architektuře.
- Rychlost programování.

### PROTI

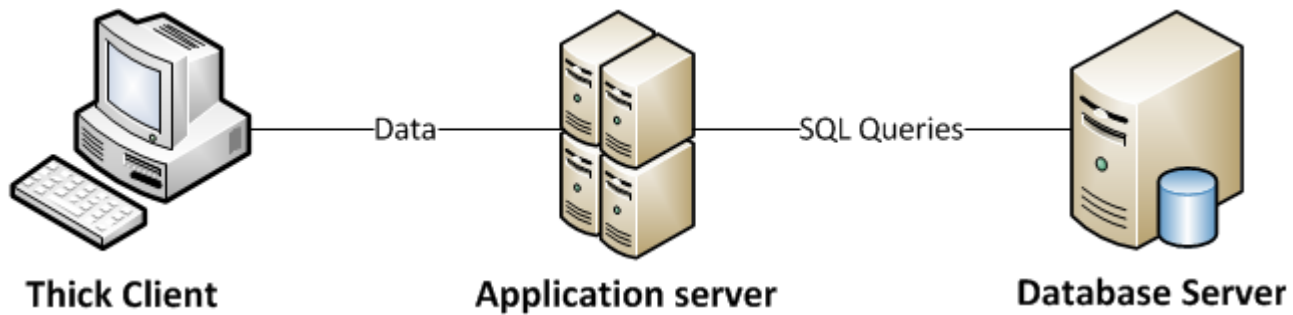
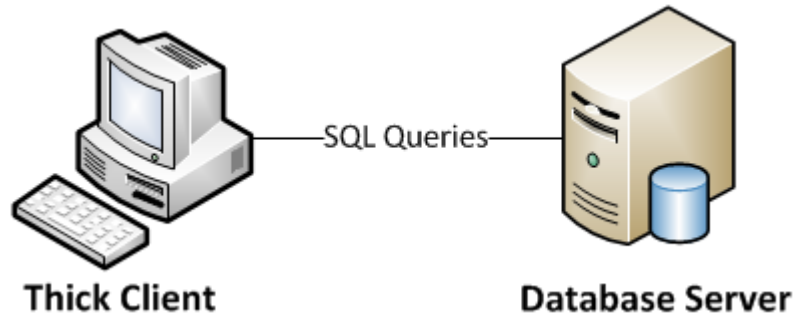
- Pomalejší z důvodů (JIT) Just in Time compilation.
- Lze snadno dekompilovat do různých programovacích jazyků.
- API hooking.



# Nejčastější zranitelnosti

- 2-tier architecture model.
- Injecting, SQL Injecting.
- Impersonation.
- Authentication Bypass.
- Unencrypted Communication.
- Information Disclosure from Memory.
- HardCoded Passwords.
- Information Disclosure form Configuration.
- etc.

# 2 versus 3-tier Architecture

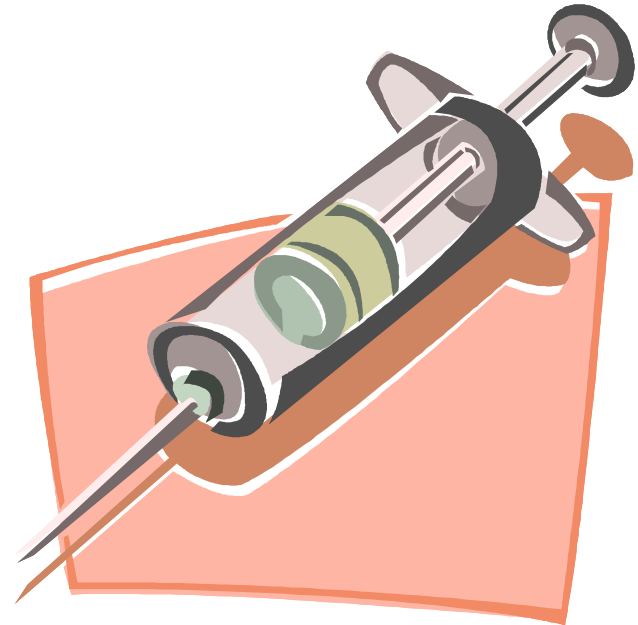






# Injecting, SQL Injecting.

- GUI injekce.
- API injekce.
- TCP injekce.
- Socket injekce.
- Binary injekce.
- Konfigurační soubory.
- Dočasné soubory.

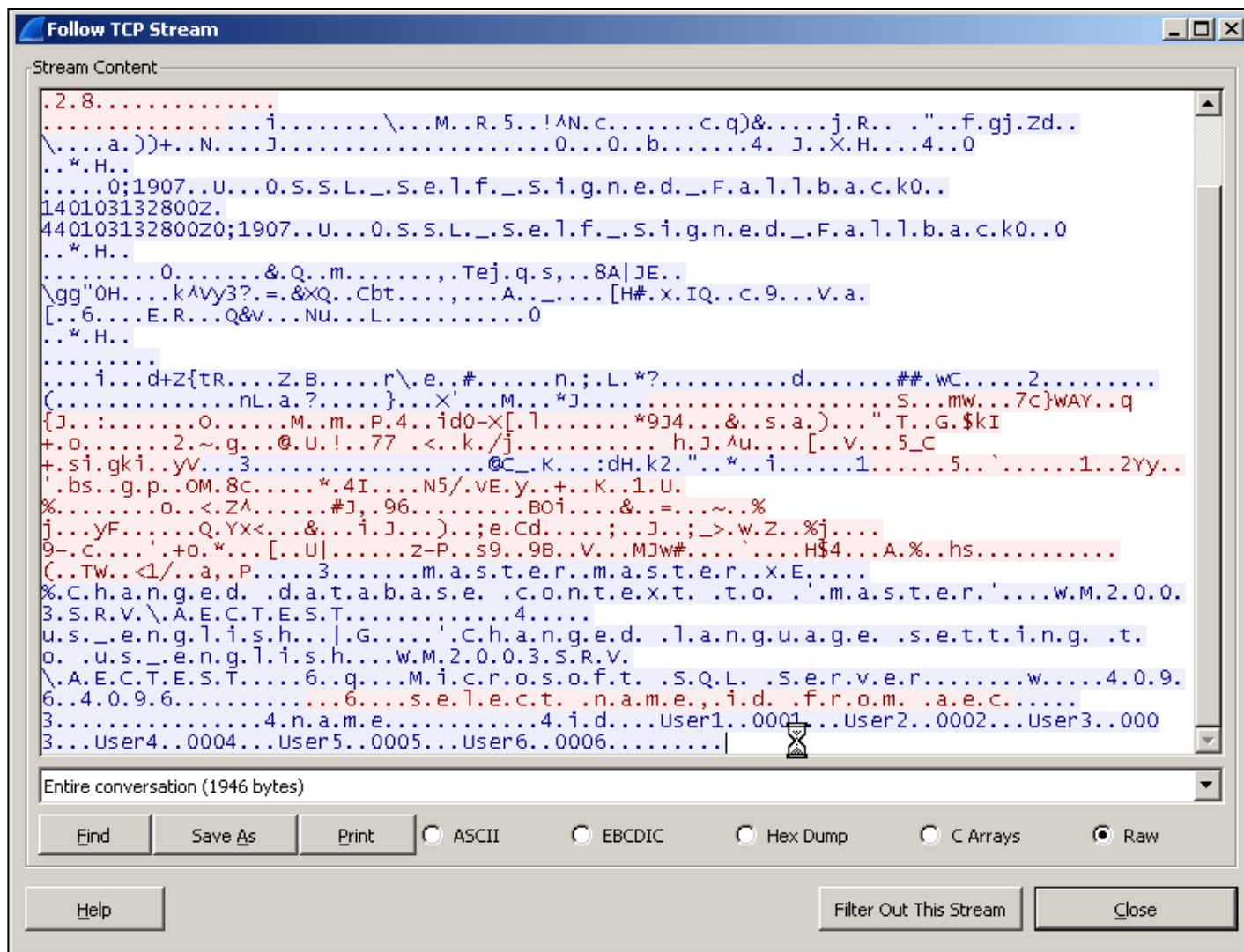


# Impersonation, Auth. Bypass

- SSO.
- Přihlašovací jméno.
- ID.
- Systémová nastavení.
- Lokální uživatel.

```
9zvva#)(+>.1.0.7.3..0.  
9zvva#)(+>.62998....5SCA$IBS...5  
9zvva#)(+>.2.0.....OPEN CURSOR 1-244675831 AS SELECT SCAU.%UCLS, SCAU.%UFN, SCAU.BRCD,  
SCAU.TSCR, SCAU.TSDR, SCAU.TPM, SCAU0.MAXEFD, SCAU0.MAXFT, SCAU0.OVRFT, SCAU0.OVR,  
CUVAR.EFD, CUVAR.EFDFTFLG FROM SCAU, SCAU0, CUVAR WHERE UID = :D1 AND SCAU0.UCLS = SCAU.%  
UCLS./ROWS=30/USING=(D1='7705097')..;0.  
9zvva#)(+>.2.0.7.3...!.0.....01500..1.....1-244675831..`T..... SCAU.%UCLS..`T.(.  
(..FN..`N.....BRCD..`N.  
.....TSCR..`N.  
.....DR..`L.....PM..`N.....0.MAXEFD..`N.....FT..`N.....OVRFT..`L.....`
```

# UnEncrypted Communication





# Information Disclosure - Memory

- Hesla.
- Privátní klíče.
- Připojovací řetězce.
- ...

Address	Hex dump	ASCII
004069DA	50 00 57 00 44 00 3D 00 40 00 79 00 56 00 65 00	P.W.D.=M.y.U.e.
004069EA	72 00 79 00 53 00 74 00 72 00 6F 00 6E 00 67 00	r.y.S.t.r.o.n.g.
004069FA	50 00 61 00 73 00 73 00 77 00 6F 00 72 00 64 00	P.a.s.s.w.o.r.d.
00406A0A	31 00 32 00 33 00 34 00 2A 00 2D 00 3B 00 01 03	1.2.3.4.*.-.;@#
00406A1A	09 00 00 05 00 00 0A 00 00 1D 43 00 6F 00 6C 00	...#...#C.o.l.
00406A2A	75 00 6D 00 6E 00 73 00 2F 00 52 00 6F 00 77 00	u.m.n.s./R.o.w.
00406A3A	73 00 3A 00 20 00 00 03 2F 00 00 49 73 00 65 00	s.:./..Is.e.
00406A4A	6C 00 65 00 63 00 74 00 20 00 6E 00 61 00 6D 00	l.e.c.t..n.a.m.
00406A5A	65 00 2C 00 69 00 64 00 20 00 66 00 72 00 6F 00	e.,i.d..f.r.o.
00406A6A	6D 00 20 00 61 00 65 00 63 00 20 00 77 00 68 00	m..a.e.c..w.h.
00406A7A	65 00 72 00 65 00 20 00 6E 00 61 00 6D 00 65 00	e.r.e..n.a.m.e.
00406A8A	3D 00 27 00 01 03 27 00 01 1B 46 00 69 00 6C 00	=.'@'.0+F.i.l.'

# HardCoded Passwords

- EXE soubory.
- DLL soubory.

The screenshot shows the HxD hex editor interface. The title bar reads 'HxD - [C:\TOOLS\ThickClientApp16.exe]'. The menu bar includes 'File', 'Edit', 'Search', 'View', 'Analysis', 'Extras', and 'Windows'. The toolbar shows a search icon, a folder icon, a save icon, a refresh icon, and a hex editor icon. The status bar shows 'ThickClientApp16.exe'. The main window displays a hex dump of the file's contents. The columns are labeled 'Offset (h)' and range from 00 to 0F. The data is displayed in hexadecimal and ASCII. The ASCII column shows a string of characters: 'R.=.{.S.Q.L. .S. e.r.v.e.r.}).;. . S.E.R.V.E.R.=.W. M.2.0.0.3.S.R.V. \.A.E.C.T.E.S.T. ;.U.I.D.=.A.E.C. U.s.e.r.;.P.W.D. =.M.y.V.e.r.y.S. t.r.o.n.g.P.a.s. s.w.o.r.d.1.2.3. 4.\*.-.;.....'. The characters 'P.W.D.' are highlighted in a blue box.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00005970	52	00	3D	00	7B	00	53	00	51	00	4C	00	20	00	53	00	R.=.{.S.Q.L. .S.
00005980	65	00	72	00	76	00	65	00	72	00	7D	00	3B	00	20	00	e.r.v.e.r.}).;. .
00005990	53	00	45	00	52	00	56	00	45	00	52	00	3D	00	57	00	S.E.R.V.E.R.=.W.
000059A0	4D	00	32	00	30	00	30	00	33	00	53	00	52	00	56	00	M.2.0.0.3.S.R.V.
000059B0	5C	00	41	00	45	00	43	00	54	00	45	00	53	00	54	00	\.A.E.C.T.E.S.T.
000059C0	3B	00	55	00	49	00	44	00	3D	00	41	00	45	00	43	00	;.U.I.D.=.A.E.C.
000059D0	55	00	73	00	65	00	72	00	3B	00	50	00	57	00	44	00	U.s.e.r.;.P.W.D.
000059E0	3D	00	4D	00	79	00	56	00	65	00	72	00	79	00	53	00	=.M.y.V.e.r.y.S.
000059F0	74	00	72	00	6F	00	6E	00	67	00	50	00	61	00	73	00	t.r.o.n.g.P.a.s.
00005A00	73	00	77	00	6F	00	72	00	64	00	31	00	32	00	33	00	s.w.o.r.d.1.2.3.
00005A10	34	00	2A	00	2D	00	3B	00	01	03	09	00	00	05	0D	00	4.*.-.;.....



# Information Disclosure – Conf.

- Registry.
- INI soubory.
- Konfigurační soubory.
- Binární soubory.
- Dočasné soubory.
- Parametry příkazové řádky.



```
HKEY_LOCAL_MACHINE\Software\Application  
Password REG_SZ PrivateAccessPass38920((*@#
```



# DEMO

- Informace o aplikaci, kompilátoru, programovacím jazyku.
- Vyhledání hesla v paměti.
- GUI odemčení oken (.NET).
- Injekce do datového toku.
- Modifikace rozhraní a SQL injekce.



# SECURITY 2014

22. ročník konference o bezpečnosti v ICT

## Děkujeme za pozornost.

Oldřich Válka

AEC, spol. s r.o.

[oldrich.valka@aec.cz](mailto:oldrich.valka@aec.cz)

