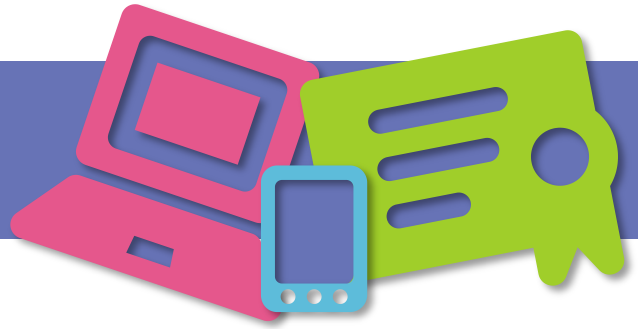
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Bezpečnost tlustých klientů

Oldřich Válka

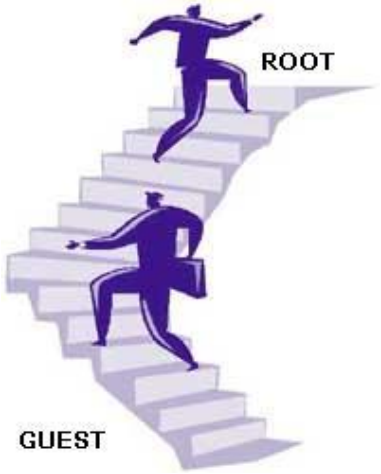
AEC, spol. s r.o.

Agenda

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

Proč řešit bezpečnost TK

- Uživatele 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 bankovnictví.
- 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.

Základní detekce aplikace

MANAGED CODE APPLICATIONS

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

PRO

- Nezávislost na architektuře.
- Rychlost programování.

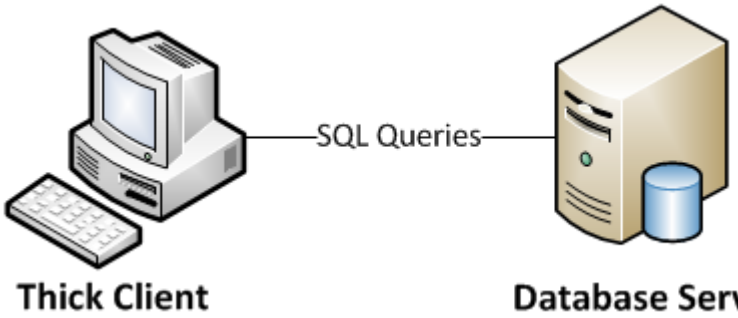
PROTI

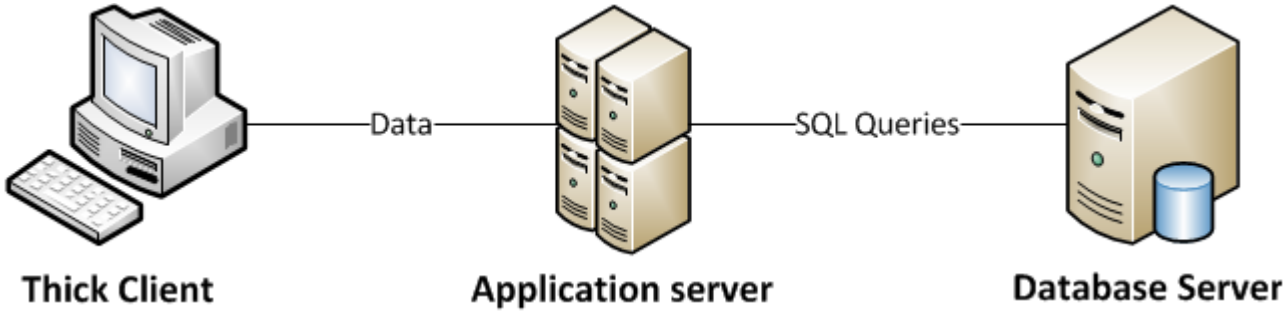
- Pomalejší z důvodů (JIT) Just in Time compilation.
- Lze snadno dekompilovat do různých programovacích jazyků.
- API hooking.

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.

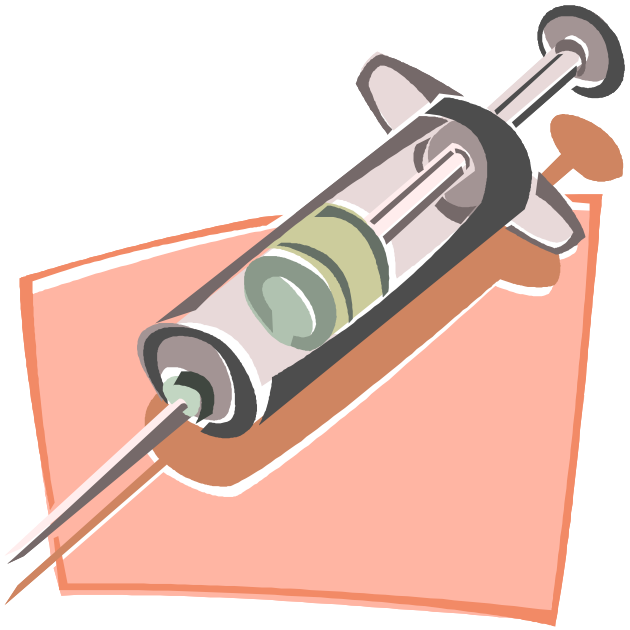
2 versus 3-tier Architecture





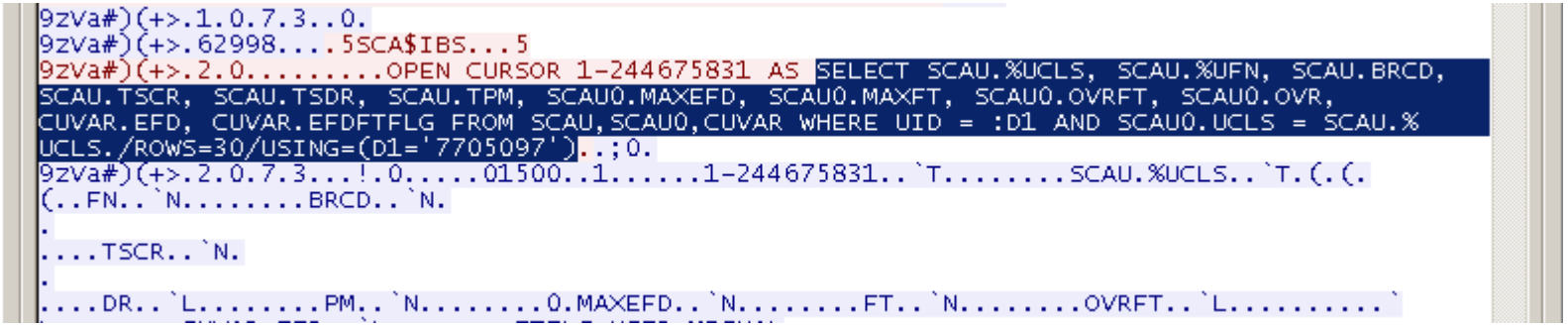
Injecting, SQL Injecting.

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

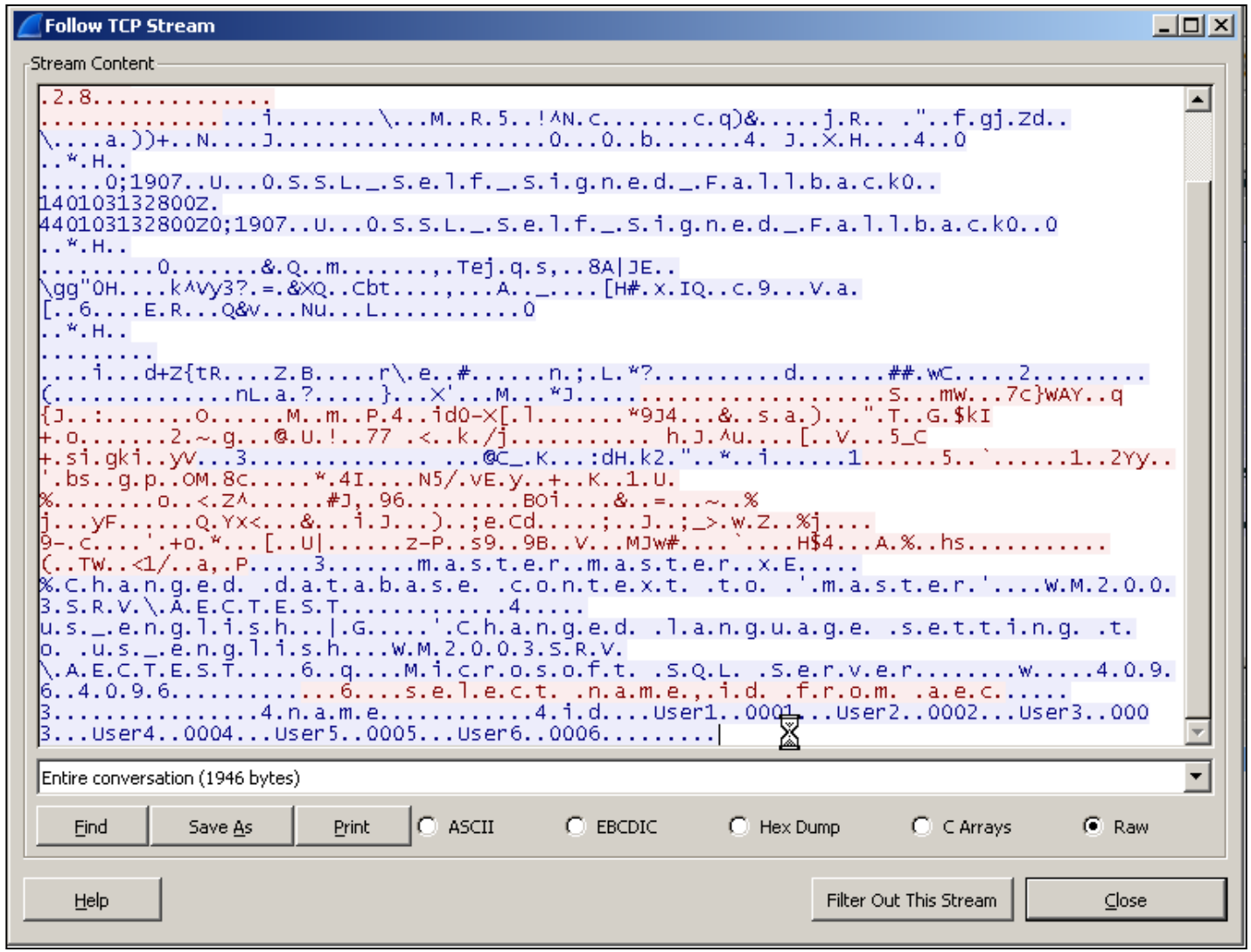


Impersonation, Auth. Bypass

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

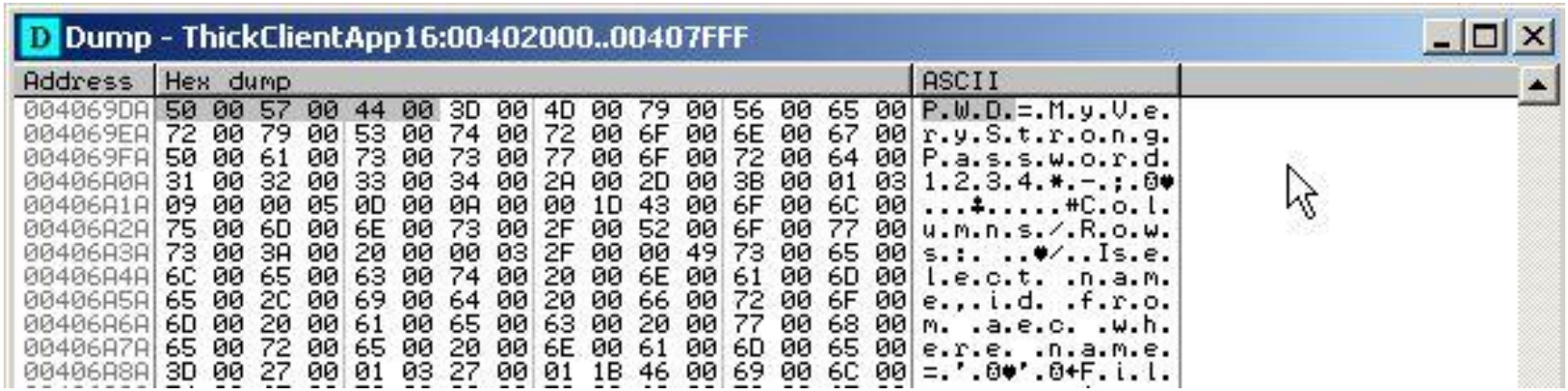


UnEncrypted Communication



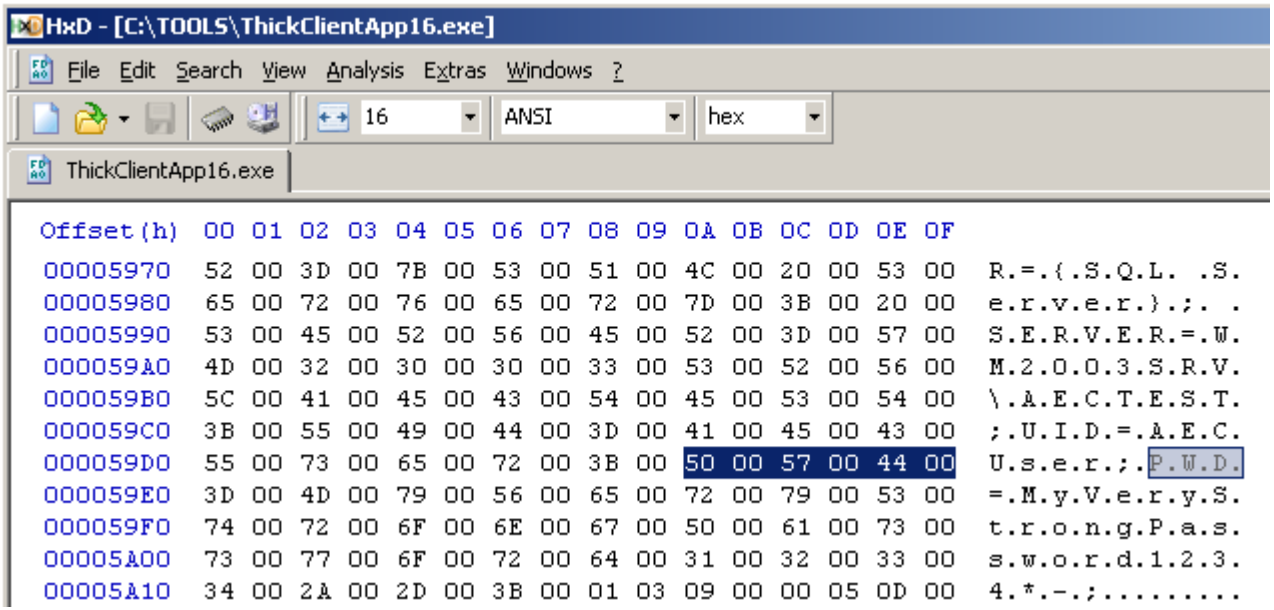
Information Disclosure - Memory

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



HardCoded Passwords

- EXE soubory.
- DLL soubory.



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