Středoškolská technika 2015

Setkání a prezentace prací středoškolských studentů na ČVUT

Encryption Protection System

Jaroslav Vondrák

Vyšší odborná a Střední škola Varnsdorf
Mariánská 1100, Varnsdorf

OBSAH

Úvod

Už od samotného začátku, kdy se objevil první počítač na světě, byl problém s bezpečností dat. Díky této problematice, které čelí celý dnešní virtuální svět, jsem se zaměřil na šifrovanou komunikaci a samotné šifrování dat.
Proto vznil projekt Encryption Protection System (EPS).

Tento projekt se skládá ze tří částí:

1. Data System Encryption (DSE)
2. Back Up System Encryption (BuSE)
3. Operation System Encryption (OSE)

Data System Encryption

Tento program se zabývá zašifrováním dat. Uživatel si může libovolně zvolit co má být zašifrováno. Také přes tento program lze provozovat šifrovanou komunikaci.

Back Up System Encryption

Program, díky němuž si můžete zálohovat data na svůj server šifrovaně.

Operation System Encryption

Operační systém, díky kterému můžete zašifrovat rovnou celý hard-disk.

Cíl projektu

Cílem tohoto projektu je udělat takový program, který bude na 100 % spolehlivý, ale také uživatelsky přívětivý, aby uživatel ani nepoznal, že se v jeho počítači dějí složité výpočetní úkony. To je ovšem problém, pokud uživatel bude chtít zašifrovat obrovské množství dat (především celý HDD). Proto je hlavním cílem projektu co nejvíce optimalizovat algoritmus, aby zašifroval data v co nejkratším čase.

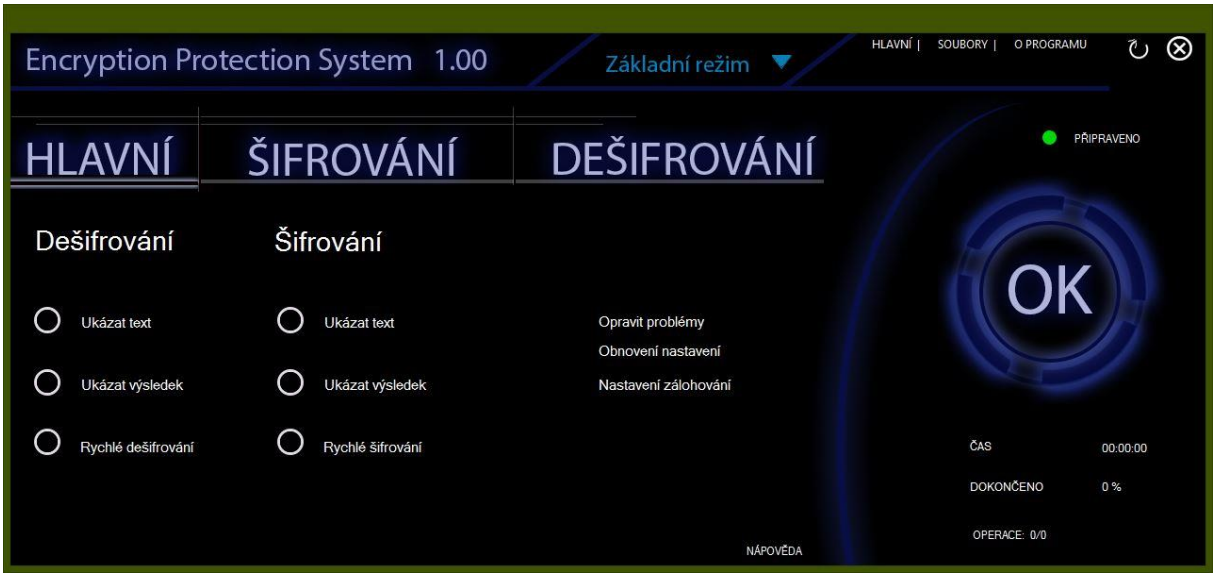
Algoritmus je zatím navržený tak, že výsledný efekt šifrování zabírá mnohem více paměti. Z tohoto důvodu bylo potřeba vymyslet algoritmus, který provede jistou kompresi zašifrovaných dat. Proto vedle tohoto projektu vznil také Compression Protection System (CPS). Tento kompresní systém je částí každého programu (DSE, BuSE) a samotného systému (OSE). Výsledek této komprimace by mě být ten, že samotná šifrovaná data budou zabírat méně paměti.

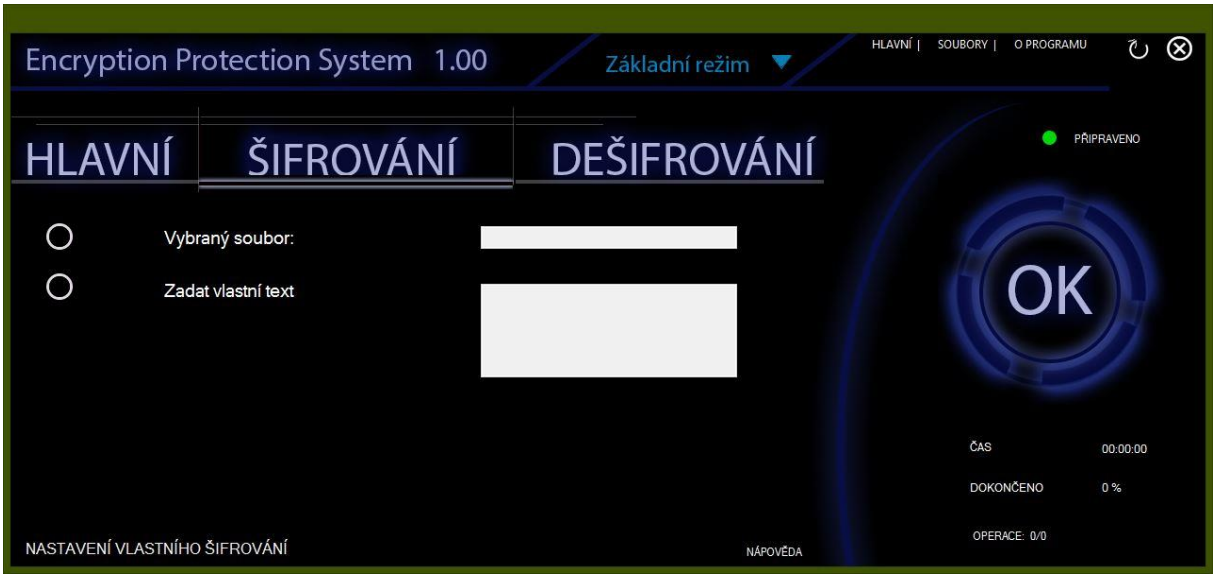
Encryption Protection System

Data System Encryption – DSE

Primárně určený k šifrování dat pod platformou Windows a Linux. Uživatel si sám zvolí, co chce zašifrovat (složky, soubory, obrázky....). Ještě před tím je potřeba, aby uživatel zadal své heslo. Díky tomuto heslu se vytvoří unikátní kód, díky kterému se zašifrují data. K dešifrování je samozřejmě potřeba zadat stejné heslo, poté se vykoná opačný proces, tedy vytvoří se kód (stejný jako při šifrování) a díky tomuto kódu se data dešifrují. Stejný princip funguje i u BuSe a OSE.
Sekundární využití tohoto programu je šifrovaná komunikace. Pokud je tento program nainstalován na dvou nebo více počítačích, je možnost provést šifrovanou komunikaci po počítačové síti. Princip je více méně stejný jako v předešlém případě, ale s tím rozdílem, že heslo musí znát všichni uživatelé, kteří provozují komunikaci.
Tato komunikace bude fungovat na bázi klient-server. Je tedy potřeba, aby jeden z uživatelů vytvořil server, poté se na tento server ostatní uživatele přípojí. Šifrování se bude provádět na počítači klienta, server jej poté odešle všem uživatelům, kteří jsou na něj připojeni. Dešifrování se bude opět provádět na straně klienta.

Grafické uživatelské rozhraní programu





Back Up System Encryption – BuSE

BuSE je zálohovací program, který funguje na principu klient-server. Na počítač, na který chceme zálohovat data založíme server. Klienti se poté budou na tento server připojovat a bude se provádět záloha. Veškeré zálohování přes síť je šifrované. Na server se data ukládají šifrovaným způsobem. Poté se můžou dešifrovat buď serverem, který tuto funkci obsahuje nebo samotným DSE.
Princip šifrování je opět stejný, jako v předchozím případě.

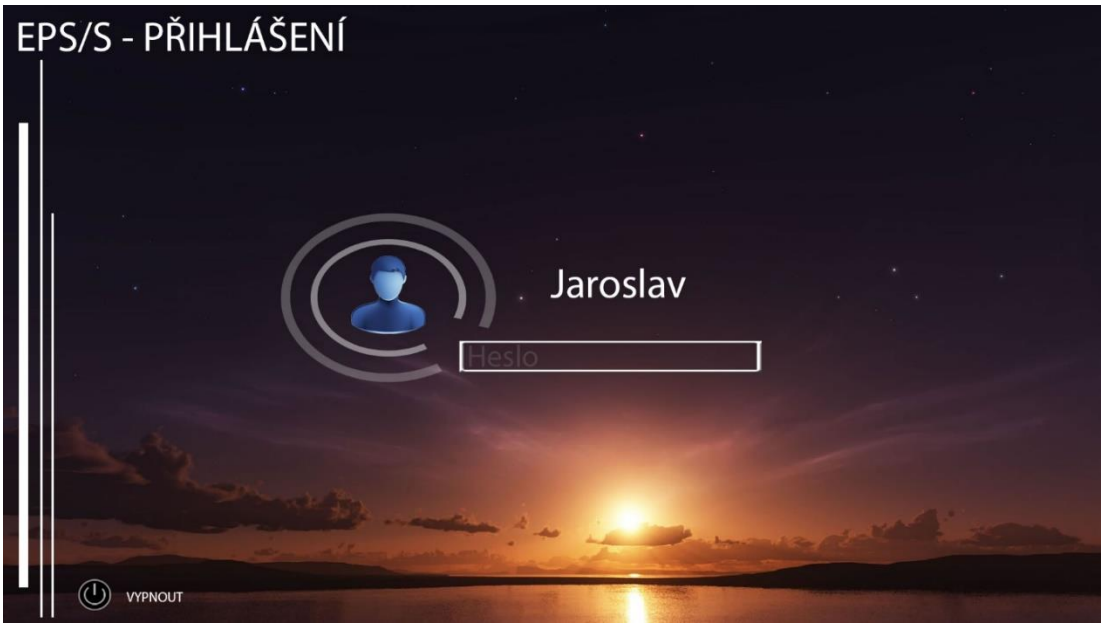
Grafické uživatelské rozhraní programu

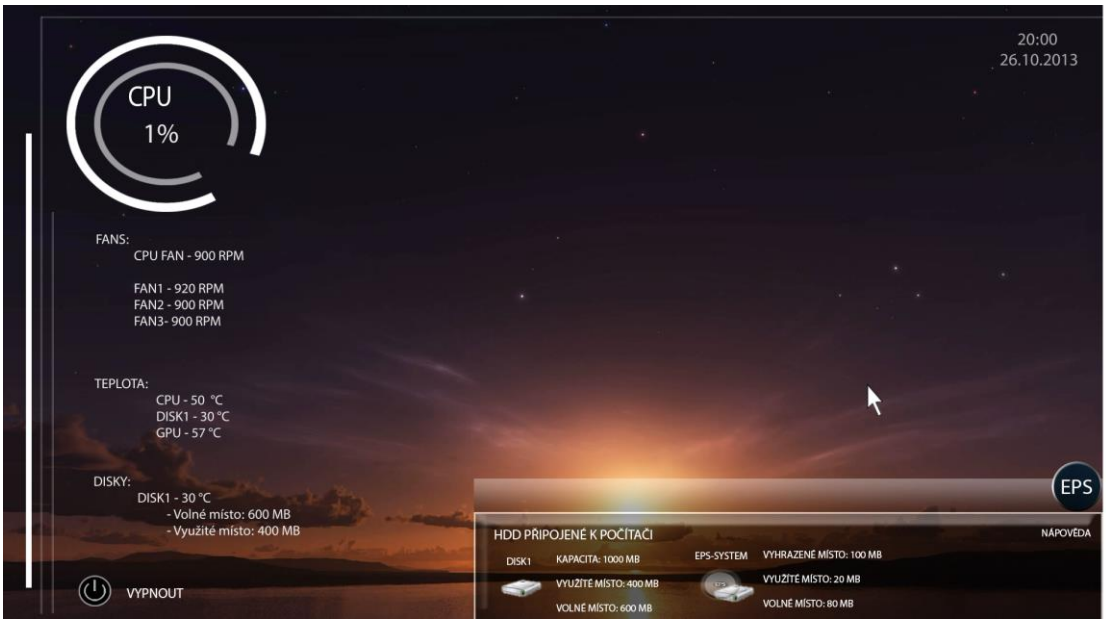

EPS-BUc
Encryption Protection System - BUc
IP-SERVER:
192.168.2.96
PORT:
2000
Spojení navázáno
Připraveno
Zálohovat
Navázat spojení
Vlastní název složky
Zapisovat historii
Připojit po spuštění
Odpojit
Čas:
00:00:00
Dokončeno:
0%
Operace:
0/0
Nastavení
Command line:
//command
PŘIPOJUJI...
IP: 192.168.2.96
PORT: 2000
PŘIPOJENÍ NA SERVER BYLO ÚSPĚŠNÉ!

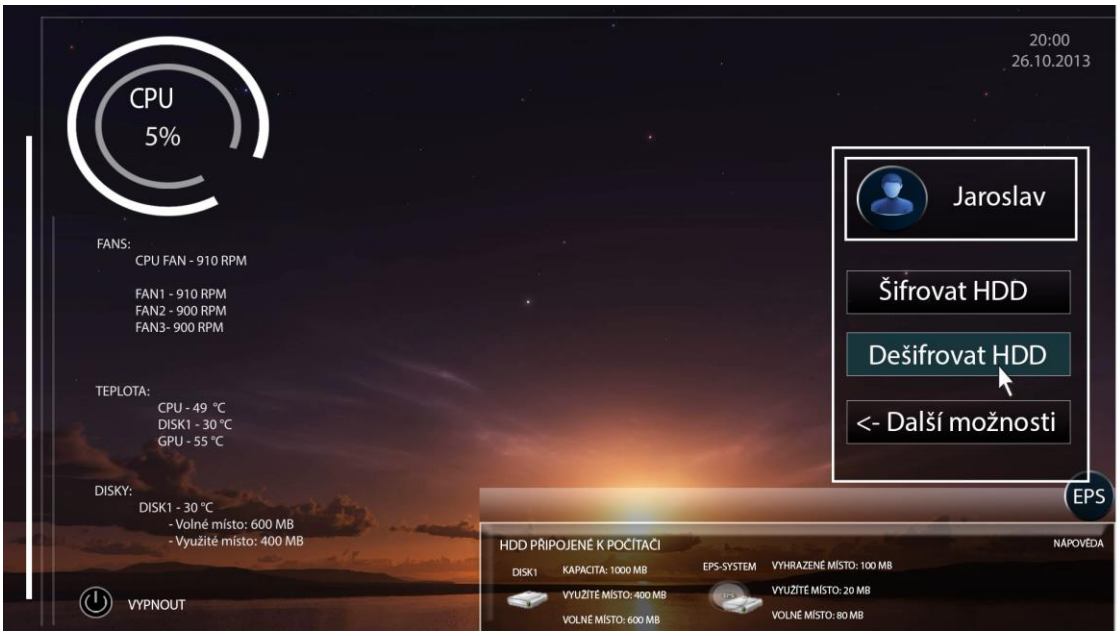
Operation System Encryption - OSE

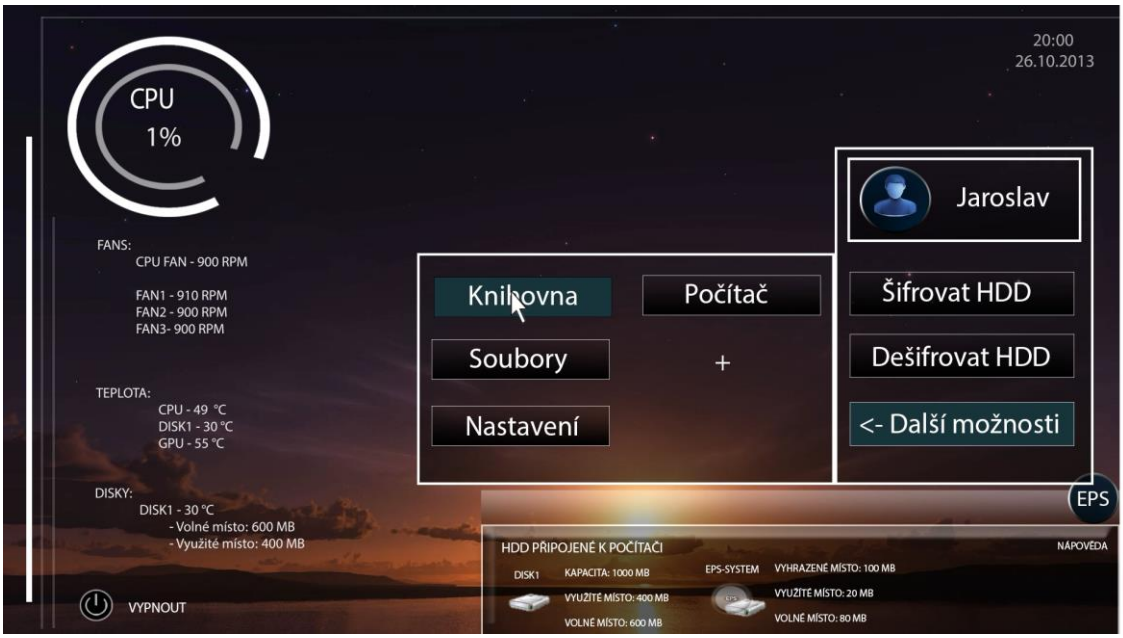
Šifrovací operační systém. Tento systém by měl být mobilní, což znamená, že uživatel zapojí do počítače (např. USB flash disk) a může systém okamžitě spustit. Tento systém by se měl spustit vždy po vypnutí primárního OS (např. Windows). Pokud se tento OS vypne, naběhne OSE.
Systém umožňuje zašifrovat celý HDD (pokud je systém nainstalován přímo na HDD, je tento disk rozdělen na oddíly. Oddíl, na kterém je OSE se šifrovat nebude). Po naběhnutí systému máme k dispozici relativně všechny možnosti normálního OS.
Uživatel si zvolí, jaký oddíl HDD chce zašifrovat. Princip šifrování je stejný jako v předešlých případech. Výhodou tohoto systému by měla být hlavně malá náročnost na paměť a tak je možno využít celý potenciál daného počítače naplno, což by u primárního OS nebylo možné.

Grafické uživatelské rozhraní systému




20:00
26.10.2013
CPU
1%
FANS:
CPU FAN - 900 RPM
FAN1 - 920 RPM
FAN2 - 900 RPM
FAN3- 900 RPM
TEPLOTA:
CPU - 50 °C
DISK1 - 30 °C
GPU - 57 °C
DISKY:
DISK1 - 30 °C
- Volné místo: 600 MB
- Využité místo: 400 MB
VYPNOUT
EPS
HDD PŘIPOJENÉ K POČÍTAČI
NÁPOVĚDA
DISK1
KAPACITA: 1000 MB
VYUŽITÉ MÍSTO: 400 MB
VOLNÉ MÍSTO: 600 MB
EPS-SYSTEM
VYHRAZENÉ MÍSTO: 100 MB
VYUŽITÉ MÍSTO: 20 MB
VOLNÉ MÍSTO: 80 MB


20:00
26.10.2013
CPU
5%
FANS:
CPU FAN - 910 RPM
FAN1 - 910 RPM
FAN2 - 900 RPM
FAN3- 900 RPM
TEPLOTA:
CPU - 49 °C
DISK1 - 30 °C
GPU - 55 °C
DISKY:
DISK1 - 30 °C
- Volné místo: 600 MB
- Využité místo: 400 MB
VYPNOUT
Jaroslav
Šifrovat HDD
Dešifrovat HDD
<- Další možnosti
EPS
HDD PŘIPOJENÉ K POČÍTAČI
NÁPOVĚDA
DISK1
KAPACITA: 1000 MB
VYUŽITÉ MÍSTO: 400 MB
VOLNÉ MÍSTO: 600 MB
EPS-SYSTEM
VYHRAZENÉ MÍSTO: 100 MB
VYUŽITÉ MÍSTO: 20 MB
VOLNÉ MÍSTO: 80 MB


20:00
26.10.2013
CPU
1%
FANS:
CPU FAN - 900 RPM
FAN1 - 910 RPM
FAN2 - 900 RPM
FAN3- 900 RPM
TEPLOTA:
CPU - 49 °C
DISK1 - 30 °C
GPU - 55 °C
DISKY:
DISK1 - 30 °C
- Volné místo: 600 MB
- Využité místo: 400 MB
VYPNOUT
Knihovna
Počítač
Soubory
+
Nastavení
Jaroslav
Šifrovat HDD
Dešifrovat HDD
<- Další možnosti
EPS
HDD PŘIPOJENÉ K POČÍTAČI
NÁPOVĚDA
DISK1
KAPACITA: 1000 MB
VYUŽITÉ MÍSTO: 400 MB
VOLNÉ MÍSTO: 600 MB
EPS-SYSTEM
VYHRAZENÉ MÍSTO: 100 MB
VYUŽITÉ MÍSTO: 20 MB
VOLNÉ MÍSTO: 80 MB

Závěr

Každý chce mít svá data v bezpečí a pokud se zajistí rychlost a spolehlivost, mohl by se EPS využívat i v rozšířenějších prostředí. OSE by mohl mít využití hlavně ve firmách, které chtějí své informace zachovat v bezpečí. Pro běžné uživatele je přívětivější DSE, který šifruje jen potřebná data.
Pro firmy se určitě ještě hodí BuSE. Díky tomuto programu mohou svá data zálohovat po síti šifrovaně a nemusí se tak bát, že jejich data budou zneužita...