AreaGuard Notes ver. 1.0

Program AreaGuard Notes slouží k uživatelskému šifrování souborù. Program poskytuje uživateli možnost chránit si svá diskrétní data. Chránìná data jsou na poèítaèi uložena v zašifrované podobì, pøièemž pouze jejich majitel zná tajemství, za pomocí kterého lze k datùm pøistoupit. Takováto data lze zašifrovanì uložit nejen na disku poèítaèe nebo serveru, ale je možné je uložit na pøenosné médium (disketa, CD-ROM, ZIPP …), poslat elektronickou poštou nebo jiným zpùsobem na síti zveøejnit (FTP).

Program AreaGuard Notes dokáže soubory ON-LINE šifrovat a dešifrovat. Program AreaGuard Notes je urèen pro operaèní systém WINDOWS NT ver. 4.0, Service Pack 4 a vyšší. Program se postupnì vyvíjí i do dalších operaèních systémù. Aktuální informace získáte u výrobce programu.

Program AreaGuard Notes používá k ochranì dat standardních šifrovacích algoritmù, které uživatel mùže použít k zašifrování svých diskrétních dat. Uživatel má k dispozici algoritmy 3-DES, IDEA a RC4.

Vlastnosti šifrovaných souborù

Šifrování je dnes považováno za jedinou možnou metodu, jak dokonale ochránit svá diskrétní data. Ovšem není pravdou, že to co je zašifrované je taky bezpeèné. Pøi šifrování je zapotøebí dodržet mnoho zásad a pravidel. Mnohá pravidla za Vás øeší software poskytující možnost šifrovat data, ale úroveò zabezpeèení dat záleží také na samotném uživateli.

Systém AreaGuard® Notes se chová podle všech pravidel, které dnes vyžaduje moderní kryptografie. Soubory zašifrované systémem AreaGuard® Notes mají následující vlastnosti:

1. Soubory jsou na disku (médii) uloženy vždy v zašifrované podobì a pøi použití docházi k ON-LINE šifrování a dešifrování.
1. Hodnota šifrovacího klíèe není nikde v souboru ani systému samotném uložena, ale je vyžadována po majiteli zašifrovaného souboru, který ji musí zadat pøed vlastním šifrováním/dešifrováním.
1. Dva zašifrované soubory se stejným obsahem za použití stejného algoritmu a šifrovacího klíèe jsou zcela rùzné.
1. Pokud se naèítá zašifrovaný soubor ze vzdáleného disku (server, FTP …), pak po síti je pøenášen jako zašifrovaný a k dešifrování nastává na cílové stanici, z které se soubor naèítá.
1. Soubory lze šifrovat a dešifrovat pouze produkty z rodiny AreaGuard®.
1. **Zašifrované soubory nelze bez znalosti šifrovacího klíèe žádným zpùsobem dešifrovat.**

Šifrování souborù se provádí z kontextového menu k souborùm a adresáøùm, ve kterém zvolíte volbu šifruj. K dešifrování soubrù lze použít volbu dešifruj.

Pokud pracujete se zašifrovaným souborem, pak jste vyzváni k vložení hodnoty šifrovacího klíèe. Pokud je již hodnota daného klíèe vložena, pak se dešifrování provádí automaticky.

Pøi práci se šifrovanými soubory se øiïte pravidly pro práci se šifrovacími klíèi a volte vhodný šifrovací algoritmus.

Volba šifrovacího algoritmu

Šifrovací algoritmus je jedním z hlavních pøedpokladù, aby byla diskrétní data dobøe chránìna. V dnešní dobì se k šifrování využívá standardizovaných algoritmù, ke kterým je veøejný popis a zdrojové kódy. Tyto algoritmy jsou neustále vystavovány útokùm ze strany kryptografických specialistù a všechny možné pochybnosti o jejich bezpeènosti jsou ihned masovì zveøejnìny. Všechny algoritmy (3DES, IDEA a RC4), které jsou v systému AreaGuard® použity, jsou v dnešní dobì považovány za **bezpeèné a nerozluštitelné**.

Šifrovací algoritmus používá k šifrování dat šifrovací klíè, který je jedinou neznámou v šifrovacím a dešifrovacím procesu. Pokud není tento šifrovací klíè vyzrazen, pak neexistuje metoda, která by v reálném èase mohla text zašifrovaný systémem AreaGuard® dešifrovat. Pøi práci se šifrovacím klíèem se musíte chovat podle urèitých pravidel.

Popis jednotlivých algoritmù:

3-DES

Je nástupce známého algoritmu DES, který se již dnes považuje díky krátké délce šifrovacího klíèe (pouze 56 bitù) za rozluštitelný v reálném èase. V algoritmu 3-DES se používá 112 bitový klíè. Tento algoritmus nebyl nikdy zpochybnìn a nebyla v nìm nalezena bezpeènostní díra. Z použitých algoritmù je 3-DES algoritmem nejpomalejším, ale poskytuje bezpeènost, které v komerèním svìtì dùvìøuje celý svìt. 3-DES je nejrozšíøenìjším algoritmem pro ochranu informací v USA.

IDEA

Svými vlastnostmi velmi podobný algoritmus algoritmu 3-DES. Délka šifrovacího klíèe je 128 bitù. Není známa metoda, kterou by šlo data dešifrovat v reálném èase. Je podstatnì rychlejší než 3-DES a v Evropì je jeden z nejpoužívanìjších algoritmù.

RC4

Velmi jednoduchý a rychlý algoritmus. Z použitých algoritmù v systému AreaGuard® je nejrychlejší (øádovì 10 krát rychlejší než 3-DES). Algoritmus RC4 používá délku klíèe 128 bitù. V dnešní dobì není znám úspìšný útok na rozluštìní zašifrovaných dat pomocí tohoto algoritmu.

Uživatel si pøi šifrování souboru volí jeden z uvedených algoritmù. Pokud uživatel chce mít data zašifrovány nejdùvìryhodnìjším algoritmem, pøièemž pochopí zpomalení naèítání a ukládání takto zašifrovaných souborù, použije algoritmus **3-DES**. Pokud dá pøednost rychlosti naèítání a ukládání šifrovaných souborù, pak zcela urèitì použije algoritmus **RC4**.

Všechny používané algoritmy systému AreaGuard® jsou vysoce bezpeèné a záleží jen na samotném uživateli, kterému z algoritmù projeví nejvìtší dùvìru.

Práce se šifrovacími klíèi

Šifrovacím klíèem se rozumí tajemství, které zná pouze majitel zašifrovaných dat, bez kterého nelze žádným zpùsobem zašifrovaná data dešifrovat. Šifrovací klíèe se v systému AreaGuard® nikde neukládají, takže bez znalosti šifrovacího klíèe jsou zašifrovaná data nerozluštitelná. Šifrovací klíè je tajemstvím majitele dat, který jej pøi šifrování a dešifrování vkládá z klávesnice.

Po vložení tajemství majite (øetìzce šifrovacího klíèe) se generuje hodnota (hodnota šifrovacího klíèe), která se použije k šifrování a dešifrování dat. Generování této hodnoty zabere v prùmìru 2 sekundy. Tato hodnota se generuje pouze po vložení øetìzce šifrovacího klíèe z klávesnice.

Pøi práci se šifrovacími klíèi se øiïte obecnými doporuèeními.

Pøedpoklad pro dobøe chránìný soubor

Jeden z pøedpokladù, aby byla data opravdu dobøe chránìná, je chování uživatele (majitele) dat pøi šifrování a dešifrování. Øiïte se následujícími pokyny:

1. Nikdy nevkládejte øetìzec šifrovacího klíèe za pøítomnosti cizí osoby.
1. Jako øetìzec šifrovacího klíèe nepoužívejte obecnì známá slova nebo slova, která jsou blízká Vaší osobì. Je velmi pravdìpodobné, že potenciální útoèník nejprve vyzkouší všechna takováto slova.
1. Délku øetìzec volte minimálnì 8 znakù, pøièemž kombinujte èísla, malá a velká písmena, rozné znaky, které lze zadat z klávesnice.
1. Øetìzec si vždy zapamatujte a nikde jinde jej neukládejte. Jen ve Vaší hlavì je v bezpeèí.
1. Pokud je øetìzec prozrazen, zašifrujte všechna data jiným šifrovacím klíèem, protože se nedají považovat za dobøe chránìná.
1. Pøi odchodu od poèítaèe odstraòte všechny šifrovací klíèe z pamìti.
1. Nikdy nesdìlujte øetìzec šifrovacího klíèe prostøednictvím pošty, telefonu, faxu ani e-mailu. Jediným možným pøedáním je osobní sdìlení nebo použití prostøedkù pro bezpeènou výmìnu šifrovacích klíèù.

Pokud zapomenete šifrovací klíè, neexistuje žádná metoda, jak data dešifrovat.

Výrobce systému AreaGuard Notes ver. 1.0

BETA 4.5.2000

SODAT software spol. s r.o.
Sedlákova 33, 602 00 BRNO
Tel./FAX: +420-5-43236177 (8)
e-mail: technická podpora: support@areaguard.cz
informace: info@areaguard.cz

http://www.areaguard.cz

© 2000 SODAT software

Pøidání systému do poèítaèe

Spus□te z instalaèní diskety program SETUP.EXE, který Vás provede celou instalací systému AreaGuard Notes do poèítaèe. Všechny soubory se kopírují pøímo do operaèního systému, protože systém AreaGuard Notes rozšiøuje vlastnosti operaèního systému. Po dokonèení instalace je zapotøebí provést restart poèítaèe. Po novém startu poèítaèe mùžete zaèít pracovat s šifrovacím systémem AreaGuard Notes.

Odstranìní systému z poèítaèe

Spus□te ovládací panel Pøidat nebo Ubrat programy a vyberte položku se systémem AreaGuard Notes. Pak zvolte odinstalování a všechny èásti systému AreaGuard se odstraní z Vašeho poèítaèe. Po odstranìní všech èástí je zapotøebí provést restart poèítaèe.

Pokud by nešlo spustit odinstalování z ovládacího panelu, pak je možné spustit pøímo program \System32\Aguninst.exe.

Základní informace o ovládání systému AreaGuard® Notes

Systém AreaGuard® Notes rozšiøuje možnosti operaèního systému. Standardní nabídky rozšíøí o pøidání nabídek umožòujících práci se šifrovanými soubory.

Operaèní systém je rozšíøen o následující funkce:

1. Kliknutím pravého tlaèítka myši na souboru, adresáøi nebo seznamu souborù a adresáøù se kontextové menu rozšíøí o nabídku AreaGuard šifruj a AreaGuard dešifruj.
1. V oblasti SysTray se pøidá ovládací ikona systému AreaGuard® Notes, která umožòuje mìnit stav šifrování.
1. Pøi práci se zašifrovaným souborem se automaticky zobrazí dialog pro zadání hodnoty šifrovacího klíèe, pokud se šifrovací klíè nenachází v pamìti.

Zašifrování vybraných souborù uživatelem

Døíve než zaènete používat šifrované soubory, musíte si je zašifrovat. Šifrování vyvoláte z Prùzkumníku kliknutím pravého tlaèítka myši na souboru, seznamu souborù, adresáøi nebo seznamu adresáøù a zvolíte volbu AreaGuard šifruj.

Trvalé dešifrování zašifrovaných souborù

Trvalé dešifrování souborù provedete z Prùzkumníku kliknutím pravého tlaèítka myši na souboru, seznamu souborù, adresáøi nebo seznamu adresáøù a zvolením volby AreaGuard dešifruj.

AreaGuard šifrování souborù

Pøed zašifrováním souboru, seznamu souborù nebo adresáøù, musíte zadat údaje, podle kterých se provede požadované zašifrování. Všechny údaje potøebné k provedení šifrování se zadávají v tomto oknì.

Dopuruèené chování a volení šifrovacích klíèù a šifrovacích algoritmù.

Jméno klíèe

Jméno klíèe slouží k oznaèení šifrovacího klíèe, kterým se soubor (soubory) zašifrují. Mùžete zadat zcela nové jméno nebo vybrat jméno ze seznamu jmen, která již byla použita a jejíž šiforvací klíèe jsou již vloženy do pamìti. Seznam vložených jmen mùžete zobrazit kliknutím na šipku u combo boxu, ve kterém se zadává jméno klíèe. Pokud vyberete ze seznamu nebo zadáte z klávesnice jméno, které je již vloženo v pamìti, pak hodnota šifrovacího klíèe nelze zadat. Hodnota šifrovacího klíèe již byla vložena døíve.

Pokud budete chtít použít jméno klíèe, který je již vložený v pamìti, ale chcete vložit jinou hodnotu šifrovacího klíèe, pak je nutné odstranit vložené klíèe z pamìti.

Šifrovací klíè

Zde vložte øetìzec znakù, podle kterého se bude zvolený soubor (seznam souborù) šifrovat. Tato hodnota je Vaším tajemstvím a bez její znalosti nelze soubor dešifrovat. Doporuèujeme volit tento øetìzec podle doporuèených pravidel o heslech.

Ovìøení šifrovacího klíèe

Slouží k ovìøení správnosti vloženého øetìzce se šifrovacím klíèem. Musí být shodný s šifrovacím klíèem.

Šifrovací algoritmus

Zvolte jeden z algoritmù, kterým se pøíslušný soubor zašifruje. K dispozici jsou standardizované algoritmy 3-DES, IDEA a RC4.

SysTray – je oblast v pravém dolním rohu monitoru.

Jméno klíèe je jednoznaèné oznaèení klíèe, které se ukládá k zašifrovaným souborùm a napomáhá uživateli k zadaní hodnoty šifrovacího klíèe. **Jméno klíèe** volte srozumitelné a výstižné pro danou hodnotu šifrovacího klíèe. Doporuèujeme používat stejnou hodnotu šifrovacího klíèe pro dané **jméno klíèe.**

Vložení hodnoty klíèe pro dešifrování

Pokud pracujete se zašifrovaným souborem, pak se tento soubor musí ON-LINE šiforvat pøi zápise a dešifrovat pøi ètení souboru. Každý soubor je zašifrován šiforvacím klíèem, který má svoje jméno a svou hodnotu.

Pokud pøi práci se souborem se šifrovací klíè, kterým je tento soubor šifrován, nenachází v pamìti, pak je nutné jej zadat.

Jméno klíèe

Veøejné jméno klíèe, který napomáhá uživateli identifikovat hodnotu klíèe, kterou musí zadat, aby soubor byl správnì dešifrován.

Šifrovací klíè

Tajemství uživatele, které slouží ke generování šifrovacího klíèe, kterým je daný soubor šifrován.

ON-LINE šifrování a dešifrování souborù

Máte-li zašifrované soubory, pak jsou tyto soubory automaticky pøi práci dešifrovány a šifrovány. Pøi prvním pøístupu k zašifrovaným souborùm je zapotøebí zadat hodnotu šifrovacího klíèe.

Ovládací aplikace v SysTray

V ovládací aplikaci máte možnost:

1. Deaktivovat šifrování – pak šifrované soubory jsou naèítány v zašifrovaném tvaru a mùžete je kopírovat a posílat mailem v zašifrovaném tvaru.
1. Odstranit klíèe z pamìti – odstraní se všechny vložené šifrovací klíèe. Pøi nutnosti šifrovacího klíèe budete vyzvání k novému vložení hodnoty šifrovacího klíèe.

Kopírování šifrovaných souborù

Zašifrované soubory mùžete kopírovat v zašifrovaném tvaru pokud deaktivujete ON-LINE šifrování v Control aplikaci.

Zasílání šifrovaných souborù e-mailem

Šifrované soubory mùžete zašifrovanì poslat mailem, pokud deaktivujete ON-LINE šifrování v Control aplikaci.

Odstranìní šifrovacích klíèù z pamìti

V control aplikaci volnou Odstraò klíèe z pamìti, je zapotøebí provést pøi opuštìní poèítaèe, aby nežádoucí uživatel nemohl použít Vaše šifrovací klíèe a pøistoupit tak k zašifrovaným souborùm.

Jméno klíèe je jednoznaèné oznaèení klíèe, které se ukládá k zašifrovaným souborùm a napomáhá uživateli k zadaní hodnoty šifrovacího klíèe. **Jméno klíèe** volte srozumitelné a výstižné pro danou hodnotu šifrovacího klíèe. Doporuèujeme používat stejnou hodnotu šifrovacího klíèe pro dané **jméno klíèe.**

Šifrovací klíè je tajemství, které zná pouze uživatel. Bez znalosti tohoto tajemství nelze zašifrovaný soubor dešifrovat. Z tohoto tajemství (øetìzce znakù) se generuje hodnota, která vstupuje do šifrovacího algoritmu jako šifrovací klíè.

Šifrovací klíè je tajemství, které zná pouze uživatel. Bez znalosti tohoto tajemství nelze zašifrovaný soubor dešifrovat. Z tohoto tajemství (øetìzce znakù) se generuje hodnota, která vstupuje do šifrovacího algoritmu jako šifrovací klíè.

Ovìøení šifrovacího klíèe slouží k porovnání hodnot šifrovacího klíèe, aby nemohla nastat situace, že se soubor zašifroval jiným klíèem, než uživatel zadal.

3-DES (tripple DES) je algoritmem, který do dnešního dne nebyl rozluštìn a považuje se za kryptografický standard v USA. Délka klíèe je 112 bitù a není znám žádný útok, kterým by žašifrovaný soubor šel rozšifrovat v reálném èase.

IDEA – je šifrovacím algoritmem, který se nejvíce používá v Evropì. Nikdy nebyl standardizován, ale není znám žádný reálný útok, kterým by šlo zašifrovaná data dešifrovat v reálném èase. Délka klíèe je 128 bitù.

RC4 – je velmi rychlý algoritmus, který se dnes používá napøíklad k zabezpeèené komunikaci MS Internet Exploreru. Délka šifrovacího klíèe je 128 bitù. Naní znám reálný útok na zašifrovaná data.

ON-LINE šifrování – pøi naèítání dat ze souboru se automaticky pøevádí z šifrované podoby do nezašifrované podoby, ve které se pøedkládájí uživateli. Pøi ukládání dat do souboru se data automaticky šifrují a uloží se zašifrovaná. To znamená, že diskrétní data jsou v souboru uložena vždy v zašifrované (pro jiné uživatele nepoužitelné) podobì.

Øetìzec šifrovacího klíèe je øetìzec, který uživatel zadává v dialogu pøi šifrování nebo dešifrování souboru. Z tohoto øetìzce je pak generována hodnota šifrovacího klíèe, která se použije ve vybraném šifrovacím algoritmu jako šifrovací klíè. **Øetìzec šifrovacího klíèe** je tajemstvím majitele dat.

Hodnota šifrovacího klíèe je generována z øetìzce šifrovacího klíèe a používá se jako šifrovací klíè šifrovacího algoritmu. Generování této hodnoty zabere v prùmìru 2 sekundy.

Combo Box je pole k editaci (vstupu) øetìzce z klávesnice. Kromì klávesnice lze øetìzec vybrat za seznamu, který se zobrazí po kliknutí levého tlaèítka myši na šipku, která je v pravé èásti tohoto pole.