AEC
DATA SECURITY COMPANY

informační bulletin

(Připravuje AEC Data Security Company – jakékoliv připomínky, náměty či dotazy posílejte na e-mailové adresy tomas.pribyl@aec.cz nebo petr.nadenicek@aec.cz)

Počítačové viry, antivirové technologie, elektronický podpis, šifrování dat – prostě ochrana datových informací vůbec.

Dnes přinášíme:

- **AEC na veletrhu Infosecurity v Londýně**
- **Novinky mezi počítačovými viry: Fizzer**
- **Novinky mezi počítačovými viry: Coronex**
- **Časové razítko není úřední šiml**

Na přelomu dubna a května 2003 se firma AEC zúčastnila veletrhu Infosecurity v Londýně.

AEC
DATA SECURITY COMPANY

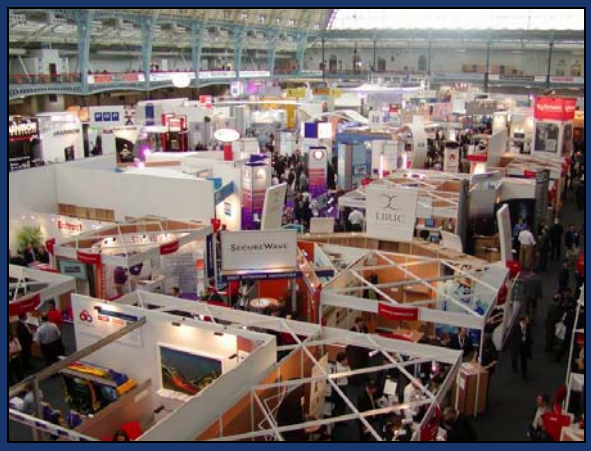
AEC na veletrhu Infosecurity v Londýně

Ve dnech 29. dubna až 1. května 2003 se v londýnském veletržním paláci Olympia konal další ročník výstavy věnované počítačové bezpečnosti Infosecurity. Mezi zúčastněnými firmami nechyběla ani AEC.

Na stánku 184 jsme oplatili pohostinství partnerské firmě Eutron z Itálie, která nám nabídla možnost využít svůj stánek v průběhu hannoverského CeBITu. Dlužno říci, že tato symbióza AEC jakožto výrobce bezpečnostního software a Eutronu jakožto výrobce bezpečnostního hardware (v daném případě tokenů) přináší plody pro všechny zúčastněné. Hardware vhodně doplňuje software a naopak – nejvíce ovšem získává zákazník, který v konečném důsledku dostává ověřené komplexní bezpečnostní řešení.

Cílem účasti na veletrhu bylo především získat zahraniční partnery pro rozšíření naší distribuční sítě. Zdali se to podařilo, ukáže až čas. Že by veletrh byl tedy neúspěšný či úspěšný jen částečně? Ale kdeže. Navázali jsme slibnou spolupráci hned s několika partnery, ale dlouholeté zkušenosti nás naučily, abychom neříkali hop, dokud jsme nepřeskočili. Nechceme to zakřiknout, ale vše nasvědčuje tomu, že nás v případě expanze na zahraniční trhy čeká opravdu pořádné „hop“.

Upřímně můžeme říci, že i po tříleté odmlce na jejímž počátku byl prodej vlastního software IronWare zahraničnímu zájemci a na konci vývoj nových vlastních řešení, jsme byli překvapeni, že AEC má v Londýně stále dobrý zvuk. Pamatovali si nás bývalí partneři, pamatovali si nás novináři, návštěvníci se pamatovali jména bývalých i současných zaměstnanců firmy… Dobré jméno je každopádně velkým příslibem do budoucna. Příslibem, na kterém se dá mnohé vybudovat.



AEC
DATA SECURITY COMPANY

Novinky mezi počítačovými viry: Fizzer

Fizzer je poměrné komplexní červ, který se objevil v prvních květnových dnech. Kromě e-mailu do svého repertoáru přibral i šíření pomocí výměnné sítě KaZaa. Do světa se vydal s další „těžkou výzbrojí“. Obsahuje totiž také zadní vrátka (backdoor) na bázi IRC, nástroje pro podnikání DoS (Denial of Service) útoků, trojského koně kradoucího hesla (externí DLL keylogger) a další „drobnosti“.

Dokáže ukončovat běžící procesy antivirových programů. Šíří se jako příloha e-mailu s příponou EXE, PIF, SCR nebo COM. Jméno souboru, předmět a text zprávy je náhodně zvolen. E-mailové adresy sbírá z Windows Address Book a adresáře Outlooku infikovaného počítače.

Kickin je dalším současným červem, který se nespokojuje se šířením pouze pomocí e-mailu. Dokáže se „protáhnout“ také přes IRC a P2P výměnné sítě Kazaa, Edonkey, Bearshare a Morpheus.

Pokud jej uživatel spustí, červ se uloží pod názvem CYBERWOLF.EXE do adresáře Windows se systémovým atributem „skrytý“. Do stejného adresáře kopíruje ještě řadu dalších souborů. Stejně jako většina jeho „kolegů“ i on manipuluje se systémovými registry, čímž si zajišťuje svoje spuštění současně se systémem.

Adresy pro další šíření e-mailem vyhledává v souborech aplikací Yahoo Messenger, MSN Messenger, .NET Messenger, ICQ a ve Windows Address Book. Umí je také čerpat z HTML a EML souborů uložených na disku infikovaného počítače. Kickin disponuje seznamem SMTP serverů, na které se snaží napojit v případě, že se mu nepodaří využít uživatelův. Jeho e-maily mají náhodně poskládaný obsah. Různé je i jméno přiloženého souboru. Šíření přes výměnné sítě provádí tak, že vyhledává sdílené adresáře a kopíruje se do nich pod lákavými názvy souborů.

Novinky mezi počítačovými viry: Coronex

E-mailový červ Coronex je údajně prvním, který ke zmatení uživatele zneužívá široce medializované téma epidemie „biologického viru“ SARS.

Červ sám o sobě představuje aplikaci Windows vytvořenou v Assembleru. Pokud je uživatelem spuštěn, nakopíruje se do adresáře Windows jako „corona.exe“ a v systémových registrech pro sebe vytvoří příslušný klíč, který zajistí jeho spuštění při každém startu systému.

Instalační procedura červa však obsahuje chybu, která může v některých případech způsobit jeho neschopnost se v systému „usadit“. I v tomto případě se však může dále šířit. Za tím účelem sbírá e-mailové adresy z Windows Address Book. Potom se každou hodinu napojuje na SMTP server „ns.execulink.com“, přes který se rozesílá dále.

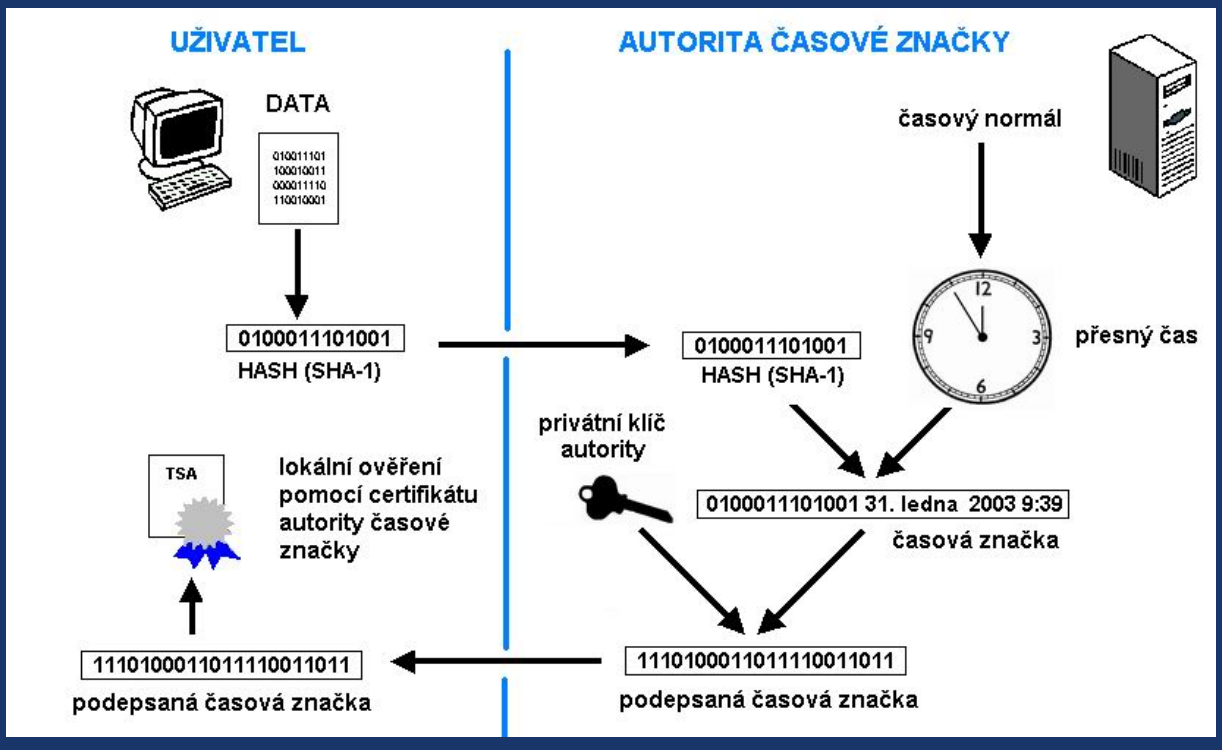
AEC
DATA SECURITY COMPANY

Časové razítko není úřední šiml!

Pokud se hlouběji ponoříme do problematiky digitálního podpisu, určitě dříve či později narazíme na problém důvěryhodného určení (pokud možno) přesného časového okamžiku, kdy byl podpis vytvořen. Jedná se o jedno ze zranitelných míst jinak robustní technologie. Jenomže i zde existuje určité řešení. Jedná se o tzv. časové razítko (nebo časovou značku). Časové razítko jednoznačně potvrzuje, že jím označená data existovala v dané podobě nejpozději těsně před uvedeným časovým okamžikem.

V praxi by případné zneužití podpisu bez důvěryhodné časové značky mohlo vypadat tak, že podvodník v čase T1 např. uzavře smlouvu, kterou digitálně podepíše. Následně v čase T2 (>T1) nahlásí „ztrátu“ svého soukromého podpisového klíče a označí jej za zdiskreditovaný. Logicky tedy požádá svého poskytovatele certifikačních služeb o zneplatnění digitálního certifikátu náležejícího ke „ztracenému“ soukromému klíči. V čase T3 (>T2>T1) pak může podvodník prohlašovat svůj digitální podpis vytvořený v čase T1 za neplatný, resp. vytvořený třetí osobou pomocí „ztraceného“ soukromého klíče a zříci se z toho vyplývajících právních závazků.

O vydávání časových razítek se stará autorita časové značky, která funguje velice podobně jako „klasická“ certifikační autorita. Princip celého procesu je poměrně jednoduchý. Začíná tím, že speciální software (klient) zjistí HASH určených dat (viz. závěr prvního dílu našeho seriálu), který doplní dalšími údaji do celkové normalizované podoby žádosti o vydání časové značky. Žádost je následně přes internet odeslána autoritě časové značky. Tam její zpracování probíhá tak, že autorita k dodanému HASHi přidá přesný časový údaj, který se získává např. z přesných „atomových“ hodin, GPS nebo DCF přijímače. Celý „balíček“ je následně digitálně podepsán privátním klíčem autority časové značky. Tímto krokem je zajištěna důvěryhodnost vloženého časového údaje. V poslední fázi je časové razítko doručeno žadateli.



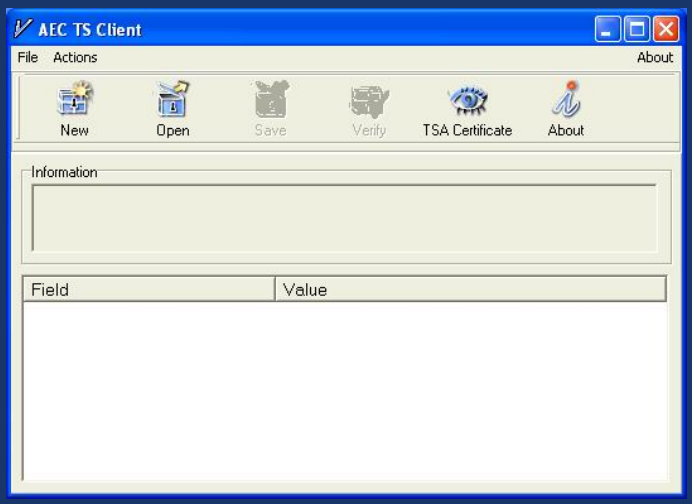
AEC
DATA SECURITY COMPANY

Ověření platnosti časového razítka je v podstatě ověřením jeho digitálního podpisu a celistvosti označeného souboru. Program, který ověření provádí, zjistí HASH souboru a porovnává jej s HASHem dešifrovaného z časového razítka pomocí certifikátu autority časové značky. Pokud se oba HASHe shodují, je časové razítko neporušené a uvedený časový údaj je platný. Rovněž máme jistotu, že se obsah souboru nezměnil. Pokud by se tak stalo, lišil by se také HASH souboru a časové razítko by pozbylo platnost.

Časové razítko můžeme stejně dobře aplikovat na digitální podpis nebo na jakýkoliv soubor. Potřebujeme k tomu jen vhodný klientský software na straně jedné a serverovou aplikaci (autoritu) na straně druhé, která bude časová razítka vydávat. V české republice prozatím není podobných řešení mnoho – prvním a pravděpodobně zatím jediným je AEC TrustPort TimeStamp Authority (TSA), která již funguje v rámci vzpomínané certifikační autority.

TSA představuje volitelný modul pro „On-line CA“ server. Stejně jako v případě certifikační autority může na jednom „On-line CA“ serveru běžet několik podepisovacích strojů TSA s vlastním izolovaným PKI úložištěm. TSA může běžet v tzv. „corporate“ instalaci společně s certifikační autoritou nebo v tzv. „stand-alone“ módu – pouze autorita časové značky bez certifikační autority.

Stěžejní součástí TSA je TimeServer, který je zdrojem přesného času a zjišťuje jeho případné odchylky od času systémového. TSA, kterou již AEC provozuje, získává přesný čas z GPS (Global Positioning System - ze satelitů přijímá mimo jiné i časové věty). Další možností je signál DCF šířený z vysílače DCF77 v Mainflingenu na dlouhých vlnách s kmitočtem 77,5 kHz. Pokud provozovateli nevyhovuje ani jeden z těchto způsobů, může přesný čas pro TimeServer získávat jiným způsobem.



K praktickému využití autority časové značky slouží program AEC TS Client, který si může kdokoliv zdarma stáhnout z webu certifikační autority (www.trustport.cz). Klient umožňuje označit časovým razítkem jakýkoliv soubor. Komunikace klienta s autoritou je realizováno pomocí protokolu HTTP (http://time.trustport.cz:8000/). Mezi klientem a „On-line CA“ je zařazena speciální HTTP brána (Gateway), která filtruje a formálně kontroluje žádosti o časová razítka. Zajišťuje, aby se ke zpracování v „On-line CA“ dostávaly pouze „správné“ žádosti a nedocházelo ke zbytečnému zatěžování podepisovacího stroje.

Autoritu časové značky najdete na webových stránkách certifikační autority AEC TrustPort CA (www.trustport.cz) v záložce označené „TSA“. Najdete zde politiku autority časové značky i AEC TS Clienta ke stažení. Vydávání časových razítek je zcela ZDARMA.

AEC
DATA SECURITY COMPANY