Autentizace operátorů
pomocí otisku prstu v průmyslových aplikacích

Tento článek si bere za cíl ukázat praktické možnosti využití biometrických metod pro autentizaci jednotlivce, zejména metody založené na snímání otisků prstů. Pomocí snímání otisků prstů lze totiž značně zjednodušit prokazování identity jednotlivce například v průmyslových aplikacích. Jak již bylo naznačeno, tentokrát nepůjde o problematiku řízení přístupu v rámci inteligentních budov či zabezpečených areálů, kde se snímače otisků prstů úspěšně rozšiřují již několik let. Půjde o využití při autentizaci operátorů v oblasti řízení technologických procesů, shrnutí přínosů, které do této oblasti biometrické metody přinášejí, a v neposlední řadě také popis praktického využití tohoto řešení ve výrobním závodě farmaceutické společnosti Boots v Nottinghamu (Velká Británie).

Otisky prstů jako lék na zapomnětlivost

Zní to možná absurdně, ale je to pravda. Zkuste přijít do velínu, ze kterého se operátorsky řídí nějaká technologie a zkuste přítomným operátorům navrhnout, že mohou opravdu zapomenout ta složitá a dlouhá hesla, která je navíc administrátor systému nutí z bezpečnostních důvodů změnit každý měsíc…

Ano, bezpečnosti a zabezpečení se dnes věnuje patřičná pozornost. Právě kvůli ní je třeba důsledně dodržovat řízení přístupu k aplikaci, která může ovlivňovat procesy v řízené technologii a tak kvalitu výstupu.

Dalším aspektem dneška, na který se klade velký důraz, je archivace všech důležitých technologických událostí a parametrů výroby. Chcete-li, archivace úplné výrobní historie. Dnes mnohde nestačí vynutit si přihlášení operátora při jeho příchodu před obrazovku s vizualizační a řídicí aplikací (dále jen „operátorská aplikace“), ale je třeba, aby operátor prokázal svou identitu při každém významném zásahu do technologie. Například při změně poměru směsi, při zastavení nebo spouštění výrobní linky apod.

A právě kvůli bezpečnosti a požadavkům na archivaci původce změn ve výrobní technologii je nutné, aby v rámci operátorské aplikace bylo možné prokazovat identitu operátora, tj. provádět autentizaci. Od vynálezu klávesnice je klasickou metodou autentizace vložení uživatelského jména a hesla. Ano, jde o klasickou a zároveň léty prověřenou metodu, rozhodně však ne o metodu člověku přirozenou. Alternativou jsou biometrické metody prokázání identity, zejména dnes nejpoužívanější prokazování identity pomocí otisků prstů.

Pokud místo psaného hesla uložíme „průkaz“ identity v rámci lidského těla, zcela eliminujeme nutnost si heslo pamatovat, a tím také šanci jej ztrácet. Pak už jen stačí

Obr.1 Čtečka otisků prstů

položit prst na okénko čtečky otisků prstů a systém rychle pozná, kdo jsme zač. To by se operátorům mohlo líbit…

Čtečky otisků prstů

Na současném trhu je bohatá nabídka různých typů čteček otisků prstů. Čtečky pro kancelářské použití mohou mít podobu malých samostatných jednotek připojitelných přes rozhraní USB nebo PC Card nebo mohou být zabudovány přímo do klávesnice. Naproti tomu čtečky určené pro průmysl či identifikaci při vstupu do budov jsou téměř výhradně samostatné jednotky s robustnějším designem.

Nejčastěji používaným snímačem je dosud optický snímač (scanner) nebo různé druhy kapacitních snímačů. Spíše teoreticky se lze setkat se snímačem fungujícím na principu teplotním, ultrazvukovém či radiofrekvenčním.

Některé čtečky mají zabudován algoritmus identifikace (porovnávání 1:N) v rámci svého firmware, jiné podporují jen ověřování identity (porovnávání 1:1) a některé čtečky dokáží jen přenést sejmutý otisk do připojeného počítače a zpracování nechávají na něm.

Přínosy

Do oblasti aplikací SCADA přináší autentizace pomocí otisku prstu následující přínosy:

- **Věrohodnost.** Přínosem zejména pro technologické provozy, kde se klade důraz na zaznamenání všech technologicky významných akcí provedených operátorem. Přesně lze určit kdo, kdy a jakou akci provedl, a to s jistotou, že nedochází k záměně identity poskytnutím či vyzrazením hesla.
- **Vyšší stupeň bezpečnosti.** Přínos spočívá v zabezpečeném přístupu k operátorské aplikaci, protože je provozována s dostatečně silnými hesly (ve formě otisků prstů), která není nutné nikam zapisovat pro případ zapomenutí. Současně se eliminuje nebezpečí vyzrazení hesla.
- **Zrychlení procedury autentizace.** Zrychluje se autentizace proti klasickému způsobu přihlášení uživatelským jménem a heslem. Pro sejmutí otisku prstu a jeho porovnání s uloženou šablonou je potřeba času kratšího než jedna sekunda!
- **Možnost identifikace.** Kromě autentizace (porovnání 1 : 1) se otevírá možnost identifikace (1 : N), což je dáno jedinečností otisku prstu každého jedince.
- **Nízké nároky na umístění autentizačního zařízení.** V řadě případů je složité umístit přímo do provozu počítač s klávesnicí pro přihlášení uživatele. Řešením je použití pouze čtecího zařízení připojeného na jednoduchý terminál.
- **Snížení požadavků na technickou podporu.** Hesla (otisky prstů) jsou jedinečná a nelze je ztratit. Proto lze zcela eliminovat požadavky na technickou podporu související s vyzrazenými nebo zapomenutými hesly.

Při implementaci metod založených na snímání otisků prstů je však současně třeba zvážit určitá omezení. Ta spočívají v nezbytné ochraně uložených elektronických otisků prstů, potřebě zabránit použití duplikátů, řešit případné snížení spolehlivosti v důsledku znečištěných rukou nebo snímačů. Při implementaci identifikace se omezením může stát i rychlost, avšak v systému obsahujícím 100 uživatelů lze dosáhnout času potřebného pro identifikaci okolo 1 sekundy, což je možné považovat za vyhovující. Čas potřebný na identifikaci samozřejmě roste s rostoucím počtem uživatelů v systému.

Možnosti využití

Rozeberme dvě hlavní možnosti využití, které ověřování identity pomocí otisků prstů přináší do oblasti aplikací SCADA.

- Archivace identity původce důležitých změn ve výrobě.
  Toto řešení má význam pro technologické provozy, kde se klade důraz na zaznamenání všech technologicky významných akcí provedených operátorem. To znamená kdo, kdy a jakou akci provedl.
- Zabezpečení přístupu k operátorské aplikaci.
  Identifikace či ověření identity operátora a v případě úspěchu přidělení příslušných uživatelských práv k řízení technologie.

Identifikace operátorů pomocí otisků prstů v Boots plc

V následující části je popsán způsob nasazení řešení identifikace operátorů ve výrobním závodě farmaceutické společnosti Boots plc v Nottinghamu (Velká Británie). Boots je nadnárodní společnost zabývající se prodejem farmaceutického zboží s maloobchodní sítí v mnoha státech světa. Kromě toho část své produkce sama vyrábí. Jeden z výrobních závodů je právě v Nottinghamu.

Požadavky

V rámci instalace nové výrobní linky bylo třeba řešit také způsob vizualizace a operátorského řízení celé technologie (operativní a výrobní úroveň řízení). Pomineme-li požadavky související přímo s řízenou technologií, pak hlavní požadavky managementu nebyly z dnešního pohledu nijak mimořádné:

- Vyhovění požadavkům na certifikaci podle směrnice FDA CFR 21 Part 11
- Možnost dokladovat úplnou výrobní historii každého produktu
- Zabezpečení s různými úrovněmi přístupu při minimální časové provizi ověřování identity a maximální jednoduchosti použití
- Vysoký stupeň spolehlivosti a dostupnosti systému (nepřetržitý provoz)
- Minimalizace nákladů na správu systému
- Minimalizace nákladů na hardware, software a implementaci

Způsob implementace

Systémovým integrátorem byla společnost Invensys APV (Crawley, Velká Británie) ve spolupráci s firmami Pantek (Stockport, Velká Británie) a AppTima (Ostrava, ČR).

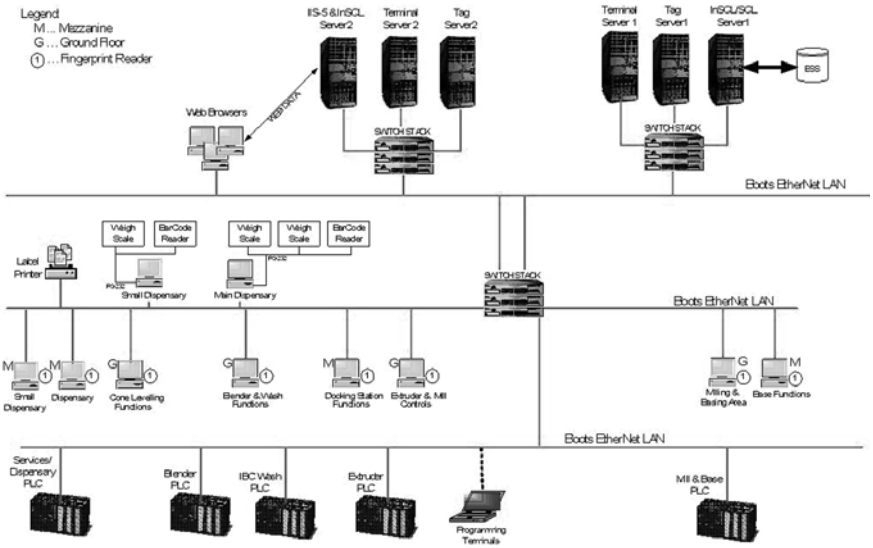
Jako základní stavební kámen systému byla navržena dvojice redundantních tag serverů, které prostřednictvím I/O Serverů sbírají veškerá data od programovatelných automatů (PLC). Tato data jsou poskytována všem klientským aplikacím v systému, určeným pro vizualizaci a operátorské řízení.

Kromě tag serverů byla do systému začleněna dvojice redundantních databázových serverů pro ukládání veškerých výrobních dat v reálném čase. Pro tuto funkci je použit produkt Wonderware IndustrialSQL Server. Archivovaná data jsou pro účely tvorby sestav a analýz dále poskytována klientským aplikacím na počítačích připojených do podnikové sítě Boots.

Minimalizace nákladů na správu systému bylo dosaženo pomocí maximální centralizace správy celého systému. Z tohoto důvodu bylo rozhodnuto provozovat všechny klientské aplikace určené pro vizualizaci a operátorské řízení v prostředí terminálových služeb. Všechny aplikace tak fyzicky běží v relacích na dvojici redundantních terminálových serverů, jen vlastní interakce s operátorem probíhá na operátorských stanicích. Použity jsou produkty Windows 2000 Advanced Server, ACP Thin Manager a Wonderware InTouch 7.11 for Terminal Services. Operátorská aplikace využívá pro účely řízení přístupu k ní uživatelské účty definované ve Windows Active Directory, což rovněž přispívá k jednoduché centrální správě systému.

Operátorské stanice jsou realizovány jako hardwarově tenký klient na bezdiskových počítačích třídy Biscuit PC (Advantech). Pro interakci s uživatelem je na každé stanici použita dotyková obrazovka (touch screen) a čtečka otisků prstů pro autentizaci operátorů. Stanice není vybavena klávesnicí, v případě nutnosti se alfanumerické znaky vkládají pomocí virtuální klávesnice zobrazené na dotykové obrazovce.

Spolupráce operátorské aplikace s čtečkami otisků je realizována pomocí software



Obr.2 Schéma architektury řídicího systému výrobní technologie v Boots PLC (Nottingham)

AppTima Advanced Security Solution. Čtečky jsou připojeny k sériovým portům operátorských stanic. Aby s nimi mohl software Advanced Security Solution komunikovat, jsou tyto porty virtuálně mapovány na terminálovém serveru, kde tento software běží spolu se všemi operátorskými aplikacemi.

AppTima Advanced Security Solution

Problematika autentizace operátorů je v Boots řešena pomocí software AppTima Advanced Security Solution. Jedná se o sadu řešení určenou pro integraci bezpečnostní politiky založené na snímání otisků prstů do prostředí operátorských aplikací SCADA.

Cílem tohoto řešení je:
- Rozšířit možnosti klasické autentizace prováděné pomocí uživatelského jména a hesla.
- Využít přínosů autentizace pomocí otisků prstů v oblasti aplikací SCADA.
- Přizpůsobit proces autentizace konkrétním podmínkám a požadavkům uživatele.

V případě nasazení v Boots zajišťuje tento software následující úlohy:
- Zprostředkování interakce mezi operátorskou aplikací InTouch a čtečkou otisků prstů.
- Zabezpečené ukládání elektronických obrazů otisků na terminálový server.
- Synchronizace elektronických obrazů otisků mezi primárním a záložním terminálovým serverem.
- Logování všech akcí souvisejících s ověřováním identity včetně výsledků akcí.
- Realizace bezpečnostní politiky využívající uživatelské účty a skupiny z Active Directory.
- Zavádění nových uživatelů a jejich otisků do systému.
- Správa databáze elektronických obrazů otisků prstů.

Společnost AppTima je aktivní v prosazování nových způsobů autentizace a identifikace jedince do oblasti průmyslového využití. Dokladem je podpora jejího Advanced Security Solution nejen pro různé typy SCADA systémů (např. Wonderware InTouch, Citect aj.), ale také podpora čteček různých výrobců (Bioscrypt, Identix). Samozřejmostí je flexibilita v implementaci speciálních požadavků, například podpora prostředí terminálových služeb jako v případě Boots.

Závěr

Oživování celé technologie by mělo být v Boots ukončeno v průběhu listopadu 2003, takže na oprávněné hodnocení přínosů nového systému budeme muset ještě počkat. Již dnes je však zřejmé, že navržená koncepce způsobu ověřování identity operátorů bude znamenat vysoký stupeň zabezpečení při minimální zátěži operátorů, kterou by při použití klasických metod ověřování představovala nutnost neustále si pamatovat a pomocí klávesnice vkládat složitá hesla.

Je vysoce pravděpodobné, že i přes svá určitá omezení se budou biometrické metody stále více prosazovat i v oblasti průmyslových aplikací a systémů a to zejména díky značnému zjednodušení prokazování identity jednotlivce.

Ing. Petr Klen, Ph.D.
AppTima s.r.o.