APPLICATION FOR SCANNING USERS ACTIVITIES

Aleš Skopal
Master Degree Programme (1), FIT BUT
E-mail: xskopa13@stud.fit.vutbr.cz

Supervised by: Petr Matoušek
E-mail: matousp@fit.vutbr.cz

ABSTRACT

This project deals with suggestion of system for monitoring the users` activities. It should run on the .NET Framework 2.0 platform. A part of whole project is the architecture design, develop right models and specification of functions and demands on this system. Next step is an system implementation and presentation of the outputs and results. Last but not least, this project talks about the question of ethic within the context of users monitoring.

1. ÚVOD

Na úvod si nastíníme obecnou problematiku monitorování uživatelských aktivit. Jelikož v dnešní době zřejmě neexistuje společnost, která by nevyužívala výpočetní techniku a počítačové sítě, tak vyvstává mnoho problémů, jak si v takové společnosti udržet přehled o využití softwaru a pracovním nasazení zaměstnanců. Právě přehled o tom, zda software, který je instalován na stanicích v počítačové síti, je produktivně využíván, je pro firemní IT manažery klíčový. Tyto informace pak usnadňují rozhodování při nákupu licencí na software a vytváří rovněž lepší přehled o chodu příslušné firmy.

Vyvíjený systém, který by měl zmíněnou problematiku řešit zasahuje do mnoha oblastí informačních technologií. Pro úspěšnost projektu je nutné aby část systému byla dvou vláknová, data byla přenášena po síti, posléze ukládána do databáze (MS SQL Server) a nakonec byla vhodně prezentována. Jelikož byla použita platforma .NET Framework 2.0, byly využity následující technologie: .NET Windows Services, .NET Threading, ADO.NET, ASP.NET, WinForms a knihovny Win32 API. Vše ve spolupráci s programovacím jazykem C#, popř. JavaScript.

Zaměříme se tedy na důležité části projektu, od jeho architektury, přes etickou stránku věci, až po samotný výstup a znázornění získaných výsledků. Prodiskutujeme i možná zkreslení, ke kterým může při použitém přístupu docházet.

2. ROZBOR PROBLEMATIKY

Každý uživatel počítače spouští aplikace a je v nich nějakým způsobem aktivní. Touto aktivitou jsou myšleny stisky kláves a pohyby myší. Systém sleduje, které aplikace byly spuštěny, jak dlouho běžely na popředí a jak dlouho v nich byl uživatel aktivní, resp. neak-

tivní. Toto je základem veškerého monitorování jeho aktivit. Získaná data musí být inteligentním způsobem zpracována a prezentována. U každé aplikace, která disponuje uživatelským rozhraním, se sleduje nadpis jejího okna, její název, proces, kterým byla spuštěna, výrobce této aplikace, uživatele, který aplikaci spustil, počítač, na kterém běžela a mnoho dalšího.

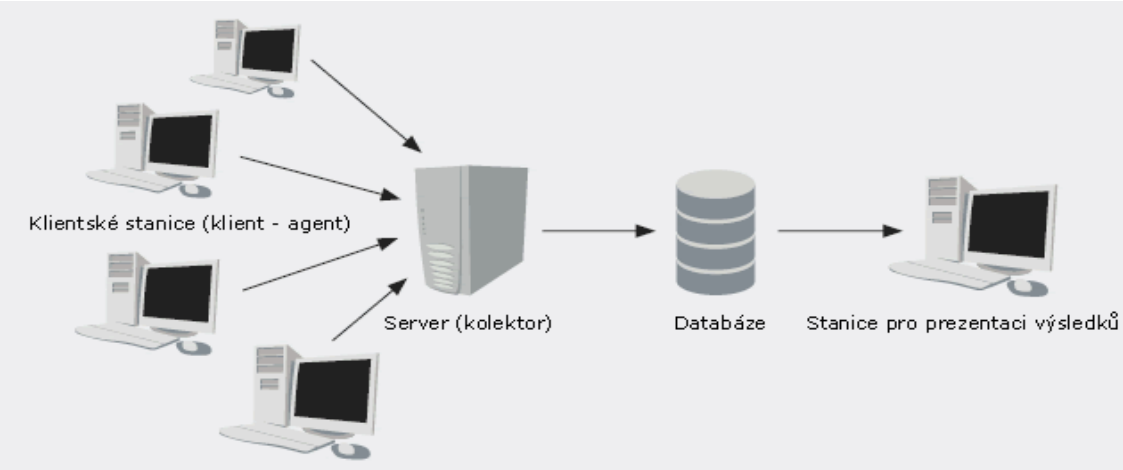
Důležitým faktorem je, aby celý systém nijak neomezoval uživatele, který na příslušné stanici pracuje. Z toho důvodu některé části systému (tzv. monitorovací agent a kolektor) běží jako služba a pracovník o nějakém monitorování nemá ani tušení. Tyto části však mohou být spuštěny i jako běžné aplikace s GUI (Graphical User Interface).

2.1. ARCHITEKTURA A FUNKCE SYSTÉMU

Celý systém je založen na architektuře klient-server a lze jej rozdělit na čtyři části:

1. **Monitorovací agent (klient)** - jedná se o dvou vláknovou aplikaci. První vlákno provádí monitoring a zápis získaných dat do souboru. Druhé vlákno, které nazýváme též komunikační, sleduje, na předem dohodnutém portu, žádost o přenos dat. Ve chvíli, kdy tuto žádost zjistí, tak soubor přenese na kolektor. K souboru s daty, používají obě vlákna výlučný přístup, aby nedošlo k problémům s nekonzistencí dat.
2. **Kolektor (server)** – jeho úkolem je, v předem dohodnutém intervalu, zažádat o data, která, pokud jsou dostupná, zpracuje a uloží do databáze. V případě neúspěšného přenosu je schopen žádost opakovat tak dlouho, dokud nejsou data bez problému přenesena a zpracována.
3. **Portál pro prezentaci výsledků** – jde o portálové řešení zobrazení získaných dat. Přistupuje do databáze, ze které získává data a inteligentním způsobem je interpretuje. Obsahuje řadu filtrů, vyhledávacích formulářů a prostředků, pomocí kterých se s výslednými informacemi velmi dobře pracuje. Portál současně slouží i pro správu databáze ve smyslu správy osob, počítačů a mazání záznamů.
4. **Ostatní aplikace** - součástí projektu jsou i aplikace pro instalaci agenta a kolektoru, a pro tvorbu samotné databáze s prvotní rolí správce systému. Těmito pomocnými aplikacemi se nebudeme dále zabývat.

Na obrázku č.1 můžeme vidět architekturu vyvíjeného systému.



Obrázek 1: Architektura systému

2.2. ETIKA A SLEDOVÁNÍ AKTIVIT UŽIVATELŮ

Posouzení etického hlediska sledování aktivit uživatelů značně přesahuje rámec tohoto textu. Přesto bychom se měli zmínit o základních požadavcích na systém v kontextu etiky. Systém sleduje pouze nadpisy oken aplikací a nikoliv jejich obsah. Kdyby tomu tak nebylo, mohl by se systém dokonce dostat do rozporu se zákonem např. u aplikací jako jsou poštovní klienti. Podobný problém nastává u sledování skutečné aktivity, tj. stisku kláves a pohybu myši. Nemělo by se jednat o sledování stisku konkrétních kláves (tzv. „key loggers“), protože bychom tím velmi zasahovali do soukromí pracovníka a proto systém sleduje pouze časový údaj o tom, kdy byl uživatel podobným způsobem aktivní.

2.3. PREZENTACE VÝSLEDKŮ

Jelikož získaných dat je velké množství, důležitou úlohu hraje i jejich vhodná interpretace. Tuto zajišťuje intranetový informační systém za pomocí technologie ASP.NET, který umožňuje zpracovávat data a získávat z nich cenné informace. Na obrázku č. 2 můžeme vidět jednu z tabulek, která zobrazuje informace o spouštěných aplikacích. Mnoho funkcí portálu je postaveno na agregačních SQL dotazech, jejichž výstupem jsou informace, které mají velkou vypovídací hodnotu.

Nadpis	Aktivní od	Aktivní do	Doba neaktivity pracovníka (min.)	Název aplikace	Výrobce aplikace
Total Commander 7.01 - NOT REGISTERED	22.2.2008 14:32:05	22.2.2008 14:32:11	0,067	Total Commander	C. Ghisler & Co.
13% ze souboru - Stahování	22.2.2008 14:32:11	22.2.2008 14:32:15	0	Firefox	Mozilla Corporation
Total Commander 7.01 - NOT REGISTERED	22.2.2008 14:32:15	22.2.2008 14:32:17	0	Total Commander	C. Ghisler & Co.

Obrázek 2: Tabulka prezentující část výsledků

2.4. ZKRESLENÍ VYSLEDOVANÝCH INFORMACÍ

Pokud monitorovaný pracovník spustí aplikaci a zmenší velikost jejího okna, může kupř. číst text obsažený v okně pod ní a přesto bude za aktivní považována zmíněná aplikace se zmenšeným oknem. Tento fakt může nepříjemně zkreslit získané informace. Je samozřejmé, že tento postup by pracovník provedl, pokud by si nepřál, abychom zjistili, že takovou aplikaci používal. Dobu běhu takové aplikace však můžeme zjistit alespoň podle doby běhu jí příslušejícího procesu. Celkovým řešením této problematiky by mohlo být dodatečné sledování velikosti a pozice aktivního okna.

3. ZÁVĚR

Systém byl zatím otestován v síti s třemi stanicemi a byl plně funkční. Byl schopen poskytovat informace, ze kterých bylo jasně vidět, co přesně uživatel počítače dělal. V budoucnu by měla být větší část systému (agent a kolektor) nasazena v praxi, čímž budou otestovány velice důležité vlastnosti systému, kterými jsou funkčnost, použitelnost, spolehlivost a škálovatelnost. Především je důležité, že se nejedná pouze o modelovou úlohu, ale o produkt, který skutečně ověří až koncový uživatel.

V současné době je systém zakomponován do softwarového balíku s podobnými programy a jako takový zvyšuje svoji konkurence schopnost vedle již existujících systémů pro monitorování uživatelských aktivit.