PROGRAMMING TRACKING ACTIVITY SYSTEM

Karol Jarkovský
Bachelor Degree Programme (4), FIT BUT
E-mail: xjarko00@stud.fit.vutbr.cz

Supervised by: Ladislav Ruttkay
E-mail: iruttkay@fit.vutbr.cz

ABSTRACT

The paper is concerned with the subject of systems designed for monitoring activity of programmers with respect to legal, technical and technological aspects. It ponders on the role and condition of such systems in the present-day legislation and defines boundaries that distinguish the monitoring system from its illegal version. The paper deals with the options for monitoring users' activities within Microsoft Windows systems using technologies included in .NET Framework. The paper further analyses possibilities of information transmission from the monitored station to the processing server by means of standard protocols designed for transmission and identifies potential threats associated.

1. ÚVOD

V dobe kedy svetom otriasa ekonomická kríza a spoločnosti sa snažia šetriť finančné zdroje je jednou z možností ako tento cieľ dosiahnuť zefektívnenie využívania prostriedkov, s ktorými spoločnosť disponuje. Využiteľnosť zdrojov ide ruka v ruke s produktivitou zamestnancov. Efektívnejšie využitie pracovnej doby sa rovná väčšej produktivite, čo má v konečnom dôsledku pozitívny dopad na riadenie a správu firemných prostriedkov.

Potreba získavania informácií o aktivitách, ktoré počas pracovnej doby zamestnanci vyvíjajú je motiváciou pre prácu, ktorej výsledným produktom je implementácia systému na sledovanie aktivity s architektúrou klient- server.

2. SLEDOVANIE AKTIVITY A LEGISATÍVA

Veľmi citlivou témou súčasnosti je ochrana súkromia a osobných údajov. Aplikácie sledovacieho typu sú často považované za niečo čo prekračuje hranicu legálnosti. Tri najpodstatnejšie faktory hovoriace v prospech zavedenia sledovacieho systému do podnikových štruktúr je krádež firemných dát, zatiahnutie škodlivého kódu do siete a v neposlednom rade možnosť kontrolovať dodržiavanie interných podnikových smerníc.

Sledovacie systémy majú dnes oporu aj v súčasne platných zákonoch. Český zákonník práce [1] definuje povinnosti zamestnanca v §73 odst. 1 písmeno b), kde jasne hovorí, že pracovná doba má byť plne využitá na vykonávanie priradenej práce.

3. SLEDOVANIE PROCESOV V OS WINDOWS

Proces počas svojho behu v systéme vykonáva akcie, ktoré mnohokrát vyžadujú spoluprácu so systémom alebo procesom, ktorý beží na rovnakej úrovni. V takýchto prípadoch je potrebné mať k dispozícii mechanizmus, ktorý komunikáciu umožní štandardizovanou cestou. V OS typu Windows poskytuje takéto možnosti skupina funkcií označovaných súhrne ako Win32 API [2].

3.1. WINDOWS API FUNKCIE VOLANÉ Z .NET

Jednoduchosť prístupu k funkcionalite ponúkanej Win32 API nie je zďaleka samozrejmosťou. Komplikácie sú spojené s importovaním nespravovaného kódu (C/C++) Win32 API do tried, ktorých kód je spravovaný jazykom MSIL pre .NET platformu. Ideálnou technikou pre exponovanie funkcií je technika nazývaná Platform Invoke (P/Invoke) [3].

3.2. PLATFORM INVOKE (P/INVOKE)

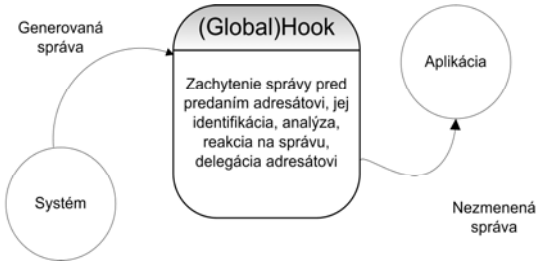
Použitie techniky P/Invoke vyžaduje aby deklarácia funkcie, teda jej hlavička, bola umiestnená okrem pôvodného hlavičkového súboru aj priamo v .NET triede, z ktorej bude volaná. Import exportovateľnej funkcie písanej v nespravovanom kóde sa deje pomocou `DllImport` atribútu.

```
// Import funkcie ShowWindow() z kniznice user32.dll
[DllImport("user32.dll")]
static   extern   IntPtr   ShowWindow([MarshalAs(UnmanagedType.
IntPtr)] hWnd,int nShow);
```

Niektoré funkcie z Win32 API ako parametre, vstupné alebo výstupné, očakávajú typ, ktorý je reprezentovaný na .NET platforme odlišne ako vo Win32 API. V takýchto prípadoch je potrebné explicitne určiť odpovedajúci objekt .NET k typu z Win32 API. Explicitnému predefinovaniu sa hovorí marshalling a v uvedenom príklade je uskutočnené pomocou atribútu `MarshalAs`.

4. ZACHYTÁVANIE SPRÁV V .NET

Pre sledovanie komunikácie jednotlivých aplikácií so systémom je nutné stať sa prostredníkom, cez ktorého bude tok správ prechádzať pred tým, ako dorazí k adresátovi a bude ním spracovaný. Zahákovanie, anglicky „hooking“, je termín v informatike označujúci techniku, ktorá umožňuje nainštalovať rutinu do systému výmeny správ a získať tak prehľad o udalostiach, ktoré v systéme nastávajú. Zahákovanie sa deje pomocou lokálnych (funkcie odchytávajúce správy pre konkrétne vlákno) a globálnych hákov. Graf nižšie popisuje princíp práce s hákmi.



Obrázok 1: Princíp hákovania

5. BEZPEČNOSŤ PRI ZASIELANÍ INFORMÁCIÍ NA SERVER

Na prenos získaných dát sú využívané štandardné webové technológie ako HTTP. Komunikácia medzi aplikáciou a cieľovou webovou službou je založená na výmene správ vo formáte XML. Používanie týchto dvoch štandardov je spojené do jedného protokolu nazývaného Simple Object Access Protocol (SOAP).

Prenos dát zo súkromných sietí cez verejnú sieť internet až k adresátovi, ktorý je opäť súčasťou súkromnej siete, je vystavený nebezpečenstvám, ktoré na neho číhajú v sieťach kde nie je prostredie kontrolovateľné vyššou autoritou. Ide o hrozby spojené s predkladaním falošnej identity, predkladaním škodlivého obsahu a zahlcovaním služby (DoS).

V súčasnosti existujúce štandardy spojené s autentifikáciou a podpisovaním XML dokumentov ako XML-Encryption alebo XML-Signature čiastočne riešia predkladanie falošnej identity na úrovni aplikačnej vrstvy.

Ako obrana proti útokom s predkladaním škodlivého obsahu môže slúžiť používanie vlastnej XML definičnej schémy, ktorá jasne určuje aké hodnoty, maximálne a minimálne, môže ten-ktorý parameter nadobúdať, aká je minimálna, resp. maximálna povolená dĺžka hodnoty atribútu a pod.

Voči DoS útokom je účinnou obranou monitorovanie správ prijímaných službou. Štatistické spracovanie informácií o požadovanej akcii, type a počte parametrov, frekvencii prijímaných správ a pod. umožňuje dynamicky predvídať tento typ útokov.

6. ZÁVER

Úlohou práce bolo ponúknuť ucelený materiál, ktorý popisuje aspekty súvisiace s vývojom systému na sledovanie aktivity programátora. Veľký dôraz bol pri tom kladený na pohľad práva na takéto systémy. Bezpečnosť pri prenose údajov zo sledovanej stanice na cieľovú spracovateľskú centrálu plnila taktiež dôležitú úlohu.

Pre systém odchytávajúci správy pomocou techniky hákovania, využívajúci Win32 API na registráciu prostredníka v komunikácii správami, zasielajúci získane údaje pomocou webových služieb bude pre budúcnosť dôležité, akým smerom sa bude vývoj OS Windows uberať. Sledovanie nových trendov je preto neoddeliteľnou súčasťou pravidelnej revízie systému.

LITERATÚRA

[1] Zákon č. 262/2006 Sb. [on-line], [cit. 2009-03-02],
URL: <http://business.center.cz/business/pravo/zakony/zakonik-prace/>

[2] Windows API [on-line], [cit. 2009-03-02],
URL: <http://msdn.microsoft.com/en-us/library/aa383723(VS.85).aspx>

[3] Platform Invoke Tutorial [on-line], [cit. 2009-01-25],
URL: <http://msdn.microsoft.com/en-us/library/aa288468.aspx>