Computação Autonômica Aplicada à Criminalística Computacional

José Helano Matos Nogueira[1], Joaquim Celestino Júnior[2]

[1]Criminalística – Setor Técnico-Científico – Departamento de Polícia Federal e Faculdade Farias Brito (FFB)
Fortaleza – CE – Brasil

[2]Laboratório de Redes e Segurança da Informação (LARCES)
Universidade Estadual do Ceará (UECE)
Fortaleza – CE – Brasil

helano@apcf.org.br, celestino@larces.uece.br

1. Introdução

É comum ver na mídia jornalística que as policiais têm apreendido grande quantidade de equipamentos computacionais de criminosos envolvidos nos mais diversos tipos de delitos digitais (fraudes eletrônicas, furto de informações sensíveis como senha de bancos e de cartões de crédito, crimes contra o sistema financeiro, pedofilia, venda de drogas via Internet, terrorismo cibernético, etc.). É de se ressaltar que todo esse material deverá ser investigado e gerenciado com rigor científico visando apresentar o vestígio computacional de uma maneira legalmente aceitável como prova em juízo. Esse é o objetivo da Criminalística Computacional, também chamada de Forense Computacional, ou ainda Perícia Criminal Computacional. Ademais, o notável crescimento do número de investigações e exames periciais realizados na área da Criminalística Computacional, bem como a integração de uma variedade de diferentes tecnologias, têm transformado a atividade de gerenciamento em uma tarefa bastante complexa. Neste cenário de crescente complexidade, torna-se necessário delegar a maior quantidade possível das tarefas de gerenciamento para as próprias máquinas. Este trabalho cria um novo paradigma de gerenciamento para Criminalística Computacional a partir dos aspectos abordados pela computação autonômica [Horn 2001]. O objetivo deste novo paradigma é diminuir a complexidade das tarefas para peritos, investigadores e administradores, aumentando a produtividade, a confiabilidade dos exames e diminuindo a redundância de tarefas.

2. Modelo Autonômico

A inspiração para o uso do termo "computação autonômica" vem do sistema nervoso autonômico humano, o qual é capaz de manter as funções vitais sem qualquer iniciativa, participação ou esforço consciente do ser humano. É neste sentido que o autogerenciamento torna-se a essência da computação autonômica e o aprendizado a característica fundamental que separa os sistemas autônomos ou automáticos de sistemas autonômicos. Desta forma, a idéia é liberar o ser humano dos detalhes de operação e manutenção, provendo aos usuários máquinas capazes de trabalhar com alto

desempenho 7 dias por semana, 24 horas por dia [Kephart and Chess 2003]. Para ser considerada uma abordagem autonômica é preciso que execute quatro propriedades (serviços) básicas: autoconfiguração, auto-otimização, autoproteção e autocura [Parashar 2007].

Antes de iniciar qualquer elaboração de uma arquitetura autonômica é necessário compreender e desmistificar o escopo de atuação da Criminalística Computacional. Portanto, primeiramente, criamos uma ontologia para realizar o mapeamento do mundo real em um ambiente computacional. Foi utilizado como parâmetro para montagem dessa ontologia o cenário real de atuação do Serviço de Perícias em Informática que faz parte da Criminalística da Polícia Federal brasileira. A seguir, foram utilizadas as ferramentas para criação de ontologias: Chimaera, Ontolingua e Protégé [Nogueira 2007], sendo esta última a que demonstrou ser a mais adequada para o tipo de domínio ao qual nos propomos tratar. Em um segundo momento, criamos nosso modelo autonômico de autogerenciamento. Neste modelo propomos uma arquitetura dividida em cinco níveis de gerenciamento: gerência de recursos (nível 1), gerência da base de conhecimento e aprendizado (nível 2), gerência de elementos autonômicos (nível 3), coordenação autonômica (nível 4) e a interface autonômica integrada (nível 5). Neste modelo optamos pelo uso de agentes inteligentes móveis [Nogueira 2006] para se obter as propriedades autonômicas, pois os sistemas multiagentes possuem características prementes, naturais e desejáveis tais como: autonomia, orientação a objetivos, adaptabilidade, pró-atividade, flexibilidade, comunicação, mobilidade, adaptação dinâmica, operação em ambientes heterogêneos e "inteligência".

3. Conclusão

Este trabalho apresenta uma nova abordagem de gerenciamento para Criminalística Computacional usando os elementos e propriedades da computação autonômica. Primeiramente, criamos uma ontologia para representação do conhecimento em um cenário real de investigações em crimes por computador do Serviço de Perícias em Informática da Criminalística da Polícia Federal do Brasil. Como passo seguinte, criamos um novo modelo autonômico de autogerenciamento aplicado às investigações em crimes por computador. Neste novo paradigma a idéia foi criar elementos capazes de gerenciar a si próprios com pouca ou nenhuma intervenção do perito ou investigador.

Referências

Horn P. (2001), "Autonomic Computing: IBM´s Perspective on the State of Information Technology", http://www-03.ibm.com/autonomic/library.html. Last access in 7th June 2008.

Kephart J. O. and Chess D. M. (2003), "The Vision of Autonomic Computing", IEEE Computer, January, 2003, pp.41–50.

Nogueira J. H. M. (2007), "Ontology for Complex Mission Scenarios in Forensic Computing", In proceedings of the 2nd International Conference of Forensic Computer Science, Guarujá: Brazil, 2007

Nogueira J. H. M. (2006), "Mobile Intelligent Agents to Fight Cyber Intrusions", International Journal of Forensic Computer Science, Brasília: Brazil, 2006.

Parashar, M. and Hariri S. (2007), "Autonomic Computing: Concepts, Infrastructure, and Applications", CRC Press, USA.