Validação remota de aplicações de informática forense com recurso a *dongle*s por USB/IP

Albano Afonso
Instituto Politécnico de Leiria
Portugal

Mário Antunes
Instituto Politécnico de Leiria
Center for Research in Advaced Computing Systems (CRACS), DCC/FC, Universidade do Porto
Portugal

Filipe Mota Pinto
Instituto Politécnico de Leiria
Centro Algoritmi, Universidade do Minho
Portugal

***Resumo* — O uso de *dongles* USB para alojamento de licenças de utilização é uma técnica muito usada por várias aplicações de software. Na área da informática forense há duas aplicações comerciais de renome internacional muito utilizadas: o Encase Forensic© da Guidance Software e o Forensic ToolKit (FTK)© da AccessData Group. A validação das licenças destas aplicações por meio de *dongles* levanta vários problemas às equipas de investigação em informática forense, designadamente o perigo de furto e perda, com o consequente acesso não autorizado às respetivas aplicações, bem como a inviabilização da otimização dos recursos, tanto humanos como tecnológicos, já que cada examinador terá de ter um *dongle*, que deverá ser transportado e utilizado por si. Neste artigo apresenta-se uma arquitetura distribuída para a gestão de *dongles*, recorrendo ao uso do protocolo USB/IP. A abordagem utilizada permite o acesso remoto e distribuído aos *dongles* USB com as licenças das aplicações de informática forense, recorrendo a uma rede TCP/IP. A solução apresentada foi desenvolvida em colaboração com a Secção de Investigação da Criminalidade informática e Tecnológica (SICIT) da Polícia Judiciária Portuguesa (PJ), tendo sido realizados testes de aceitção.**

Keywords— USB, dongle, USB/IP, Acesso Remoto a Licenças

I. INTRODUÇÃO

A informática forense é um ramo da ciência forense e uma área da investigação criminal relacionada com as provas digitais encontradas em suportes de armazenamento digital [*1*]. De forma a auxiliar os examinadores de informática forense e os peritos a otimizar a recolha da prova digital, há duas aplicações comerciais, lideres de mercado a nível internacional de informática forense [2], que são muito utilizadas por estes profissionais: Forensic Toolkit (FTK)© [3] e o Encase© [4]. Para validar a licença do utilizador e conceder-lhe o respectivo acesso, estas aplicações recorrem ao uso de um *dongle* [5]. Um *dongle* é um dispositivo de hardware com uma interface USB, utilizado na deteção da licença de utilização de um software. O maior desafio dos examinadores que utilizam estas aplicações consiste na necessidade de terem que ligar fisicamente o *dongle* no computador onde está instalada a aplicação, tendo para isso de o transportar fisicamente de computador para computador. Desta forma, o risco de perda ou furto do *dongle* aumenta, bem como a possibilidade do seu uso não autorizado.

Neste artigo apresenta-se uma solução distribuída, assente numa rede TCP/IP, que pretende mitigar o problema apresentado e com o qual os examinadores de informática forense se deparam constantemente. O objectivo principal consiste em agilizar o acesso remoto aos *dongle*s onde estão as licenças das aplicações de informática forense, através da rede local TCP/IP.

O trabalho apresentado consiste na replicação das portas USB existentes nas máquinas, a partir de um servidor TCP/IP pertencentes à rede local privada e isolada do exterior [6]. Desta forma, os clientes acedem remotamente aos *dongle*s USB ligados fisicamente no servidor, como se os mesmos estivessem ligados localmente à interface USB. Os *dongles* são partilhados e acedidos remotamente pela rede local, através dos pedidos efetuados pelos clientes, através do protocolo USB/IP. O desenvolvimento efetuado no servidor USB/IP foi realizado recorrendo a componentes de software *opensource* [7]. Foi igualmente desenvolvida uma interface gráfica para o cliente USB/IP.

II. CONCEITOS FUNDAMENTAIS

A limitação física de acesso às portas USB pode ser ultrapassada através do uso de uma solução de USB sobre TCP/IP, através do protocolo USB/IP. A aplicação servidor, em execução na máquina que disponibiliza o acesso físico às portas físicas USB, é acedida remotamente por uma aplicação cliente, através de uma máquina onde não existe o recurso físico a essas portas USB.

A possibilidade de aceder remotamente a uma porta USB através da rede TCP/IP foi inicialmente proposta por Hirofuchi, *et al.* [7]. Em 2007, Kwon et al. [8], implementaram uma nova versão do USB/IP em que estenderam a possibilidade do cliente ser compatível com o sistema operativo Microsoft Windows. Posteriormente, em 2009 procedeu-se ao desenvolvimento de um cliente baseado na linha de comandos para o Windows. Em 2011, com o suporte da ReactOS [9], foi publicada uma versão melhorada desse cliente Microsoft Windows, em que os *drivers* USB/IP necessários para a aplicação são assinados digitalmente e tornam-se compatíveis com sistemas operativos Windows de 32 bits e 64 bits [9].

Atualmente, a versão do USB/IP que está disponível para ser instalada por um instalador de software do Linux (p.e. `apt-get`), encontra-se obsoleta e é incompatível com as versões do *kernel* superior à 2.6.

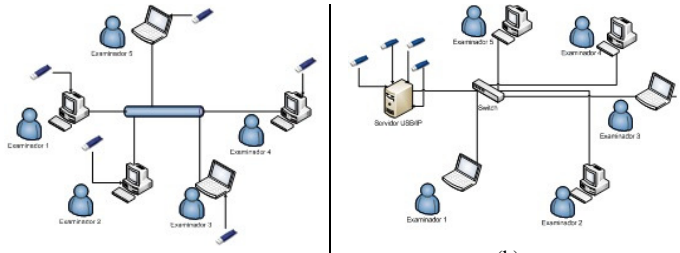
O protocolo aplicacional USB/IP utiliza uma arquitetura do tipo cliente/servidor. Desta forma, o servidor exporta os dispositivos USB, colocando-os a disposição dos clientes que

procedem a importação dos mesmos. Além disso, o *driver* do dispositivo USB exportado é executado na máquina cliente.

III. ARQUITETURA

Nesta seção, é apresentada a arquitetura do sistema desenvolvido para validação remota de licenças guardadas em *dongles*, assente numa solução distribuída com acesso remoto por USB/IP. O caso de estudo usado neste trabalho utilizou o acesso remoto às aplicações de informática forense em uso na Secção SICIT da PJ.

A Figura 1 ilustra a situação atual (a) e a solução proposta (b). Actualmente as aplicações encontram-se instaladas em cada um dos computadores dos examinadores, sendo o seu acesso validado através de um *dongle* que se encontra ligado fisicamente em cada máquina.



(a) (b)

Figura 1. Cenário Atual (a) e a solução desenvolvida (b)

O cenário desenvolvido, ilustrado em (b), consiste na implementação de uma solução distribuída em que o servidor USB/IP é uma máquina Linux que aloja fisicamente no seu barramento USB, todos os *dongles* USB disponíveis e necessários a cada aplicação de informática forense.

A aplicação USB/IP do servidor encontra-se instalada e está à escuta de pedidos TCP no porto 3240. As máquinas onde estão a ser executadas as aplicações de informática forense são os clientes USB/IP e usam o sistema operativo Microsoft Windows com os *drivers* USB/IP devidamente instalados. Nestas máquinas encontra-se também instalada a aplicação cliente USB/IP que vai interagir com o servidor USB/IP e será responsável pelos pedidos de acesso aos dispositivos USB ligados fisicamente no servidor e partilhados através da rede TCP/IP.

Cada máquina cliente virtualiza um acesso remoto através da rede local TCP/IP ao dispositivo USB, como se de uma porta USB de acesso local se tratasse. Com o objetivo de validar a licença de utilização antes de iniciar uma das aplicações de informática forense, o examinador recorre à aplicação cliente USB/IP e obtém o acesso ao *dongle* remoto que se encontra ligado fisicamente no servidor. Neste novo cenário de utilização dos *dongles*, o número de licenças é exatamente igual ao utilizado no cenário actual, respeitando assim as condições de licenciamento.

IV. DESENVOLVIMENTO

O desenvolvimento efectuado baseou-se no projeto *open source* USB/IP [7], que inicialmente foi concebido para um ambiente homogéneo Linux, para a versão 2.6 do *kernel*. Durante o desenvolvimento constatou-se que nesta versão do USB/IP, sempre que um cliente terminasse a ligação virtual ao dispositivo USB, este automaticamente era removido no servidor. Ou seja, o servidor removia automaticamente esse dispositivo da lista dos dispositivos exportados, sendo por isso obrigatório proceder-se novamente à partilha do mesmo no servidor USB/IP.

Esta situação verificava-se tanto no cliente Linux como no cliente Microsoft Windows, tornando assim a utilização desta versão pouco viável. No entanto, a versão compatível com o *kernel* 3.0 tenta mitigar estes problemas, conforme descrito em [9]. Nesta versão foi também incrementada a funcionalidade que permite no servidor parar a partilha de um determinado dispositivo. Constatámos no entanto que não existe compatibilidade com versões do *kernel* anteriores à 3.0, atendendo a que são utilizados módulos diferentes do kernel. Além disso, esta versão não se encontra disponível no repositório de software do Linux.

Desta forma, a única alternativa consistiu em obter o código fonte do USB/IP presente no *kernel* 3.2.28, disponível em `\linux3.2.28\drivers\staging\usbip\userspace`, e proceder à compilação e instalação manual a partir do código fonte, respeitando todas as dependências necessárias.

Após a compilação desta nova versão verificou-se que a aplicação servidor de USB/IP ficou devidamente instalada e que o problema anteriormente existente ficou resolvido. No entanto, estas alterações ao código do servidor tornou-se incompatível com o cliente para Microsoft Windows baseado na linha de comandos.

Assim, foi necessário obter o código fonte do cliente Windows e compilá-lo. Também com o recurso ao Windows Driver Kit 7 e a partir dos ficheiros do código fonte, foram gerados os ficheiros binários `.sys` para 32 e 64 bits, compatíveis com o Windows 7, Windows Server 2008 e Windows 8. A partir deste momento constatou-se a compatibilidade entre o servidor na sua versão mais recente e o novo cliente para o Windows baseado na linha de comandos. A Figura ilustra aplicação gráfica desenvolvida para o cliente USB/IP.

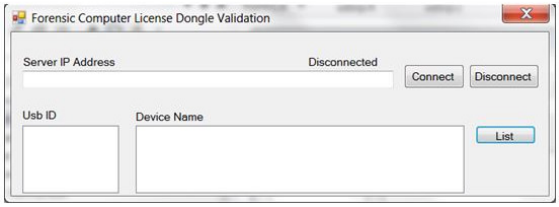


Figura 2. Aplicação gráfica de interação com o utilizador

V. TESTES REALIZADOS

Esta secção resume os principais testes realizados com *dongles* USB. Foram realizados testes recorrendo aos *dongle* USB, ligados fisicamente no servidor através de um *hub* USB. Para cada *dongle* foi realizado um teste entre o servidor e o cliente em que este último acedeu remotamente ao *dongle* USB como se de um *dongle* USB local se tratasse, possibilitando assim a validação remota da licença de utilização das aplicações de informática forense, Encase© e FTK© utilizadas pelos examinadores. Os *dongles* utilizados

nos testes são um CodeMeter que suporta a licença da aplicação de informática forense FTK© e dois Aladdin HASP HL que suportam a licença da aplicação de informática forense Encase©.

Neste teste a máquina servidor USB/IP tem o sistema operativo Ubuntu 12 LTS e o cliente tem o sistema operativo Microsoft Windows 7 (64bits). Na máquina cliente USB/IP estão instaladas as aplicações Encase© e CodeMeter Control Center©, sendo esta última responsável pela gestão das licenças utilizadas na aplicação FTK©. Também neste teste as máquinas encontram-se ligadas a um *switch* na mesma rede local, conforme ilustrado na Figura 2.

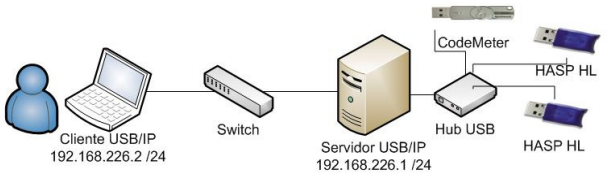
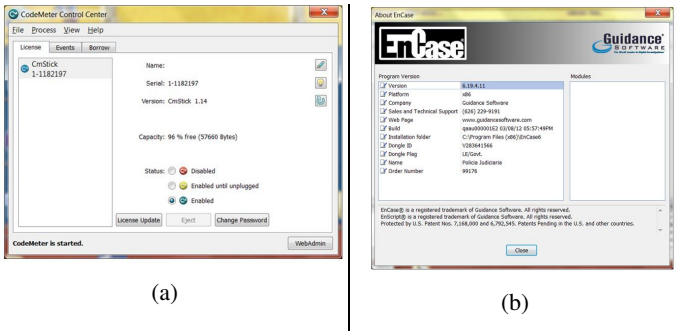


Figura 2. Cenário de teste com os *dongles* USB

Neste teste, o cliente através da aplicação gráfica USB/IP, estabeleceu com sucesso uma ligação TCP ao servidor USB/IP, e obteve a lista dos *dongles* exportados pelo servidor através da rede local.

Após a ligação virtual estabelecida entre o cliente e os *dongles* remotos CodeMeter e Aladdin HASP HL, as aplicações de informática forense do FTK© (Figura 11-a) e do Encase© (Figura 11-b) realizaram a validação remota da licença de utilização.



(a) (b)

Figura 3. (a) A aplicação CodeMeter detetou o *dongle* remoto e (b) Informações sobre a licença encontrada no *dongle* remoto

O processo decorreu de forma transparente para o utilizador final, não tendo havido necessidade do examinador ligar fisicamente um dongle USB na máquina onde a aplicação forense está instalada.

VI. CONCLUSÕES

Neste artigo foi abordada a validação remota das aplicações de informática forense e o desenvolvimento realizado na adaptação do protocolo USB/IP existente em *open source*. Do lado do servidor conseguiu-se colocar em funcionamento uma versão estável da aplicação, compatível com o *kernel* 3.2 do Linux. Por outro lado, no que diz respeito ao cliente USB/IP, foi possível realizar os desenvolvimentos necessários para o colocar em funcionamento no sistema operativo Windows 7, na versão de 64 bits, mantendo-se disponível um cliente Linux nativo no kernel 3.2, através de comandos executados na shell.

Foram realizados vários testes com a aplicação desenvolvida, no laboratório da PJ em Lisboa, quer com discos externos USB, quer com *dongles* USB usados para o acesso remoto ao licenciamento das aplicações de informática forense, EnCase© e FTK©, que constituiam o objectivo principal deste trabalho. Embora os testes tenham sido realizados com duas aplicações muito específicas, cuja licença se encontra alojada em *dongles*, o mesmo procedimento poderá ser igualmente bem sucedido com outras aplicações que utilizem o mesmo processo de validação de licenças. Por exemplo, a aplicação de desenho assistido por computador AutoCAD©, as aplicações de gestão e contabilidade PHC© e algumas aplicações utilizadas na saúde, na área da radiologia.

BIBLIOGRAFIA

[1] Eoghan Casey, *Handbook of Digital Forensics and Investigation*.: Academic Press, 2010.

[2] 2013 SC Awards US Finalists: Round Three; "SC Magazine", "http://www.scmagazine.com//2013-sc-awards-us-finalists-round-three/article/270295/"; Consultado em Setembro 2013.

[3] "AccessData Group Software FTK", ", http://www.accessdata.com/products/digital forensics/ftk", Consultado em Setembro 2013.

[4] "Guidance Software Encase",, "http://www.guidancesoftware.com/encase-forensic", Consultado em Setembro 2013.

[6] Piazzalunga, U., Salvaneschi, P., Balducci, F., Jacomuzzi, P., & Moroncelli, C. (2007). "Security strength measurement for dongle-protected software"; Security & Privacy, IEEE, 5(6), pp. 32-40.

[5] "Wibu-Systems", "http://www.wibu.com/hardware-copy-protection.html", Consultado em Setembro 2013.

[6] Albano Afonso; "USBport Through TCP/IP - Replicação de portas USB," Relatório de Projeto de Mestrado, Novembro de 2012.

[7] Takahiro Hirofuchi, Eiji Kawai, Kazutoshi Fujikawa, and Hideki Sunahara, "USB/IP a Peripheral Bus Extension for Device Sharing over IP Network," in *FREENIX Track: USENIX Annual Technical Conference*, 2005, pp.47-60.

[8] Han Wook Cho, and Yong Ho Song Wonhong Kwon, "Design and Implementation of Peripheral Sharing Mechanism on Pervasive Computing with Heterogeneous Environment," 5th IFIP WG 10.2 International Workshop Seoul 2007, pp. 537-546.

[9] "USB/IP Project", " http://usbip.sourceforge.net/", Consultado em Setembro 2013.