MO447 – Análise Forense de Documentos Digitais – Fichamento do Seminário

Voice over IP Forensics

por Jill Slay e Matthew Simon

21 de Outubro de 2011

Autor: Anderson Soares Ferreira — RA 974530

1 Visão global

Neste trabalho, os autores apresentam as implicações forenses do uso de tecnologias de comunicações de voz sobre IP. O documento apresenta uma comparação entre os sistemas de telefonia convencionais e os sistemas baseados na comutação de pacotes IP. Os autores também discutem as questões legais do uso da tecnologia e descrevem um método para coleta de evidências baseados na análise da memória RAM.

2 Resumo

O trabalho dá continuidade ao detalhamento de questões relacionadas às implicações forenses do uso de tecnologias de comunicação VoIP, inicialmente tratados em [5].

Os autores apresentam uma técnica de coleta de evidencias a partir de computadores com aplicativos VoIP (*softphones*). Para isso foram utilizadas técnicas abordadas por [3], que têm por objetivo a coleta e análise de informações a partir da memória RAM dos equipamentos enquanto estes ainda estão ligados.

A técnica proposta destinam-se a cenários "pós evento", ou seja, o equipamento utilizado para realizar comunicação VoIP não foi desligado depois de finalizada a ligação e baseia-se em características dos protocolos SIP e RTP para identificação de informações. Como ambos são protocolos de aplicação estes devem ser tratados pela própria aplicação o que obrigatoriamente demanda a reserva de espaços de memória para seu processamento. Como SIP é um protocolo que representa suas mensagens (*request/response*) em forma textual, torna-se relativamente simples sua identificação na memória. Já o protocolo RTP utilizado para o transporte de mídia, possui campos específicos para contornar as limitações de seu protocolo de transporte (UDP), permitindo que estes, uma vez encontrados, possam ser ordenados de forma a reconstruir a conversação.

O primeiro passo a ser realizado é a criação de uma imagem da memória RAM do computador. Segundo os autores, esta etapa pode ser realizada ou através de um hardware dedicado previamente instalado no computador, situação que inviabiliza seu uso numa análise real ou através de uma aplicação voltada para leitura das páginas de memória do sistema. Após a geração da imagem, dá-se inicio ao processo de busca de informações dos pacotes SIP e RTP. Em um ambiente de testes a partir de imagens de computadores com

os sistemas operacionais Windows XP e MacOS X, foi possível identificar e ordenar os pacotes RTP e em alguns casos até mesmo foi possível ouvir o áudio da proveniente da ligação.

3 Contribuições

A principal contribuição do trabalho é a apresentação de uma técnica capaz de coletar alguma informação originada de um fluxo contínuo de dados após este fluxo ter sido finalizado.

Outra relevante contribuição deste artigo diz respeito a discussão sobre a atual situação da análise forense de comunicação VoIP e a necessidade de desenvolvimento de novas técnicas para a área, visto que tal tecnologia se mostra cada vez mais presente e já existe uma forte preocupação quanto a seu uso em ações criminais.

4 Defeitos/Desvantagens

Apesar da base teórica do artigo parecer correta e bem descrita, a apresentação da técnica, bem como os resultados não foram apresentados com o nível de detalhes que seria necessário.

De forma geral os principais problemas encontrados no artigo foram:

1. Não foram abordados aspectos quanto a relação do tempo entre o início da análise e o volume de informações identificadas.
2. Não há informações sobre a interferência de outras aplicações na obtenção de evidencias.
3. Não foram especificados quantas, nem quais aplicações foram testadas.
4. Questões relacionadas a tempo de busca e ferramentas utilizadas não foram descritas.
5. Apesar do ambiente utilizado nos testes possuir um servidor VoIP, os testes foram focados nos clientes não havendo nenhuma referência sobre testes utilizando o servidor.
6. Embora o texto cite a existência de mecanismos em ambientes Linux que facilitam a coleta de imagens de memória, esta plataforma não foi utilizada nos testes.

5 Trabalhos correlatos

5.1 Digital Forensics in VoIP networks – Jérôme François et al. [2]

Relação com o artigo avaliado: Neste trabalho, os autores apresentam um método de identificação da aplicação ou dispositivo utilizado em uma comunicação VoIP a partir da mensagens de sinalização SIP.

Descrição: Os autores um método de identificação (*fingerprint*) de aplicações e dispositivos VoIP a partir da análise de árvores estruturais das mensagens de sinalização SIP. O método se baseia na ideia de que apesar de utilizar o mesmo protocolo, diferentes aplicações constroem mensagens com diferentes parâmetros e até mesmo com mensagens que não correspondem à especificação do protocolo.

A partir de cada mensagem coletada, uma representação em árvore estrutural é gerada e então é feita uma atribuição de tipo de dispositivo. Para isso, é utilizado um conjunto de aprendizagem formado por N amostras, formadas pelo tipo do dispositivo e a sua respectiva árvore estrutural. A classificação utiliza SVM com a utilização de *kernels* baseados na distância entre duas árvores.

Os testes do método proposto foram realizados a partir de um conjunto de dados com 6 tipos de dispositivos SIP diferentes, o número de mensagens utilizadas durante a fase de treinamento variou de 10% a 90% do total de mensagens, como resultado, 98% dos dispositivos foram corretamente classificados e todos os dispositivos foram identificados com precisão de 95%.

Conforme demonstrado pelos autores, a técnica baseada em árvores estruturais apresentou resultado satisfatório mesmo se comparado a outras técnicas como análise de árvores sintática [1], que embora apresente um melhor resultado, também consome mais tempo durante a análise de conjuntos de dados muito grandes.

5.2 Speaker Recognition from Encrypted VoIP Communications – L.A. Khan et al. [4]

Relação com o artigo avaliado: O artigo apresenta uma técnica para identificação de locutores a partir de fluxos SRTP criptografados.

Descrição: O artigo apresenta uma técnica para identificação e verificação de locutores a partir de seguimentos de fluxo SRTP criptografados. Para isto, a técnica se baseia no fato de que apenas a carga (*payload*) de pacotes SRTP é criptografado e também que o tamanho de uma carga criptografada é o mesmo de uma carga não criptografada em um pacote SRTP.

A partir desta características, os autores conduziram uma série de experimentos que demonstram a relação entre as frequências vocais e o *bit rate* resultante utilizando a codificação VBR (*variable bit rate*) em uma mesma qualidade de codificação. Devido ao fato da codificação VBR utilizar *bitrates* de tamanhos variáveis de acordo com a frequência, é possível então relacionar os tamanhos das cargas em pacotes RTP e as frequências do som, e então por relação com cargas criptografadas dos pacotes SRTP.

A técnica propões formas de identificação e verificação do locutor, a primeira diz respeito a identificação positiva de um locutor dado que existe um conjunto registro de áudio de suspeitos e uma amostra criptografada que será comparada.

Já a verificação diz respeito a um conjunto de amostras que deve ser comparada a um determinado locutor. Para a identificação, os autores utilizaram diversos modelos, entre eles *Hidden Markov Model*(HMM), *Gaussian Mixture Model* (GMM) e também *Ensemble of Nested Dichotomies* (END), o qual mostrou o melhor resultado na identificação. A verificação foi tratada como um problema de classificação de duas classes e foram testados dois métodos diferentes, a verificação através de classificação, onde foram utilizadas três técnicas de classificação: Adaboost.M1, DMNB e redes Bayesiana; a verificação através de regressão também utilizou três técnicas: regressão linear, SVM com SMO e SVM com kernel RBF, sendo a última a técnica que apresentou melhores resultados.

Os resultados mostraram que apesar da precisão obtida na identificação e verificação de dados criptografados ser muito inferior a precisão de dados não criptografados, a técnica demonstrou que a precisão é muito superior a escolha aleatória.

Um aspecto importante a ser observado é que apesar da técnica descrita se basear em codificação do tipo VBR, a maior parte dos codificadores existentes utilizam bitrate constante, o que limita a aplicação do método. trabalho é que apesar da técnica

6 Extensões

Como a técnica apresentada baseia-se na busca de padrões de pacotes SIP e RTP em arquivos de imagem da memória, uma extensão para o trabalho seria a busca a partir do arquivo ou partição de troca de memória virtual (*SWAP*). Esta abordagem seria útil na localização de informações que foram movidos da memória

principal devido a necessidade de mais recursos de um aplicativo em execução ou ainda pelo fato de que as páginas armazenadas em disco terem baixa utilização.

7 Notas

1. Relevância: 7.5
2. Originalidade: 7.5
3. Qualidade científica: 7.0
4. Apresentação: 8.0
5. Nota final: 7.5

Referências

[1] J. François, H. Abdelnur, R. State, and O. Festor. Advanced fingerprinting for inventory management. Rapport de recherche RR-7044, INRIA, 2009.

[2] J. François, R. State, T. Engel, and O. Festor. Digital forensics in voip networks. In *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, pages 1 –6, dec. 2010.

[3] K.J. Jones, R. Bejtlich, and C.W. Rose. *Real Digital Forensics*. Addison-Wesley, 2005.

[4] L.A. Khan, M.S. Baig, and A.M. Youssef. Speaker recognition from encrypted voip communications. *Digital Investigation*, 7(1-2):65–73, 2010.

[5] M. Simon and J. Slay. Voice over ip: forensic computing implications. In *Proceedings of the 4th Australian Digital Forensics*, volume 1, pages 1–6. School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2006.