Implicações forenses do uso de Voz sobre IP

Anderson Soares Ferreira

Série de Seminários

Disciplina de Análise Forense de Documentos Digitais

Prof. Dr. Anderson Rocha
anderson.rocha@ic.unicamp.br
http://www.ic.unicamp.br/~rocha

Organização

Organização

- Introdução
- Motivações
- Conceitos básicos
  - Arquitetura da Telefonia Convencional
  - Arquitetura de Sistemas VoIP
  - Legislação
- Extração de Evidências
- Trabalhos Relacionados
- Conclusões
- Referências

Introdução

Introdução

- A utilização de tecnologias de voz sobre IP está em rápida expansão.
- Sistemas VoIP são atrativas devido a sua flexibilidade, extensibilidade e principalmente custo.
- Existe uma grande preocupação quanto ao uso de VoIP em atividades criminais.

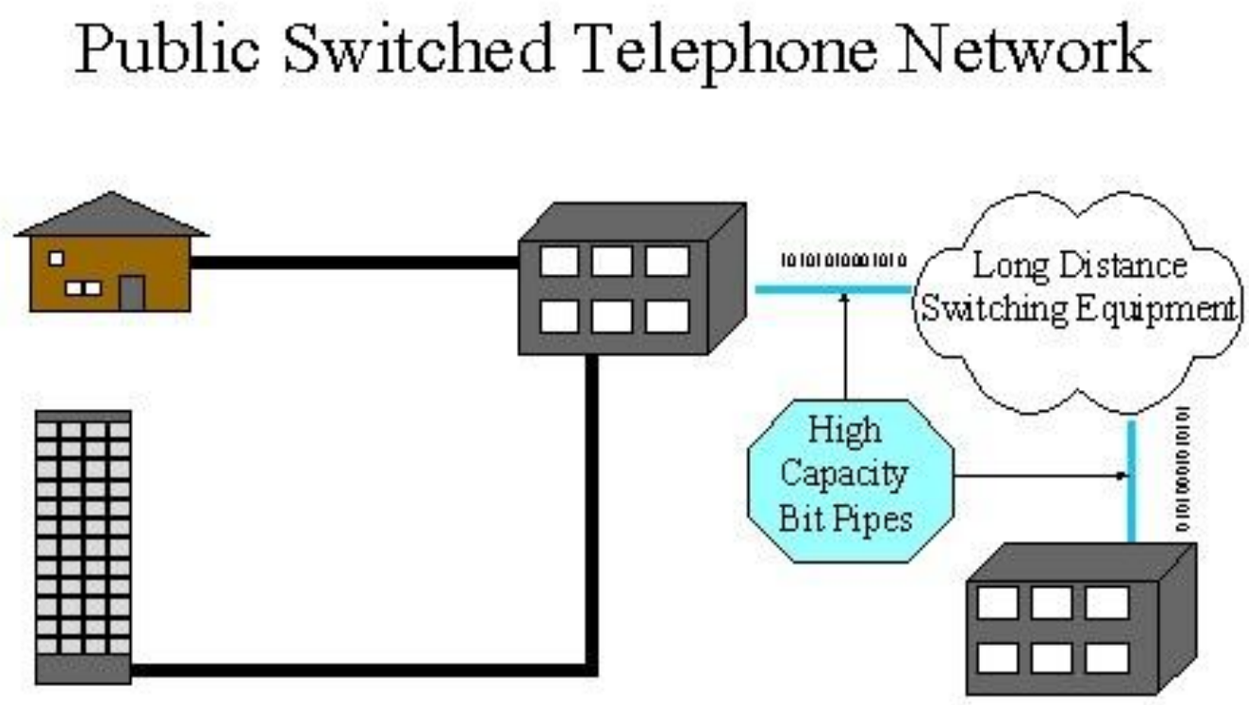
Motivação

- Estima-se que o uso de VoIP chegue a 73% do mercado americano em 2013.
- A legislação sobre telefonia ainda baseia-se em sistemas de comutação de circuitos.
- Há uma grande demanda de técnicas para extração de evidências em sistemas VoIP.

Conceitos Básicos

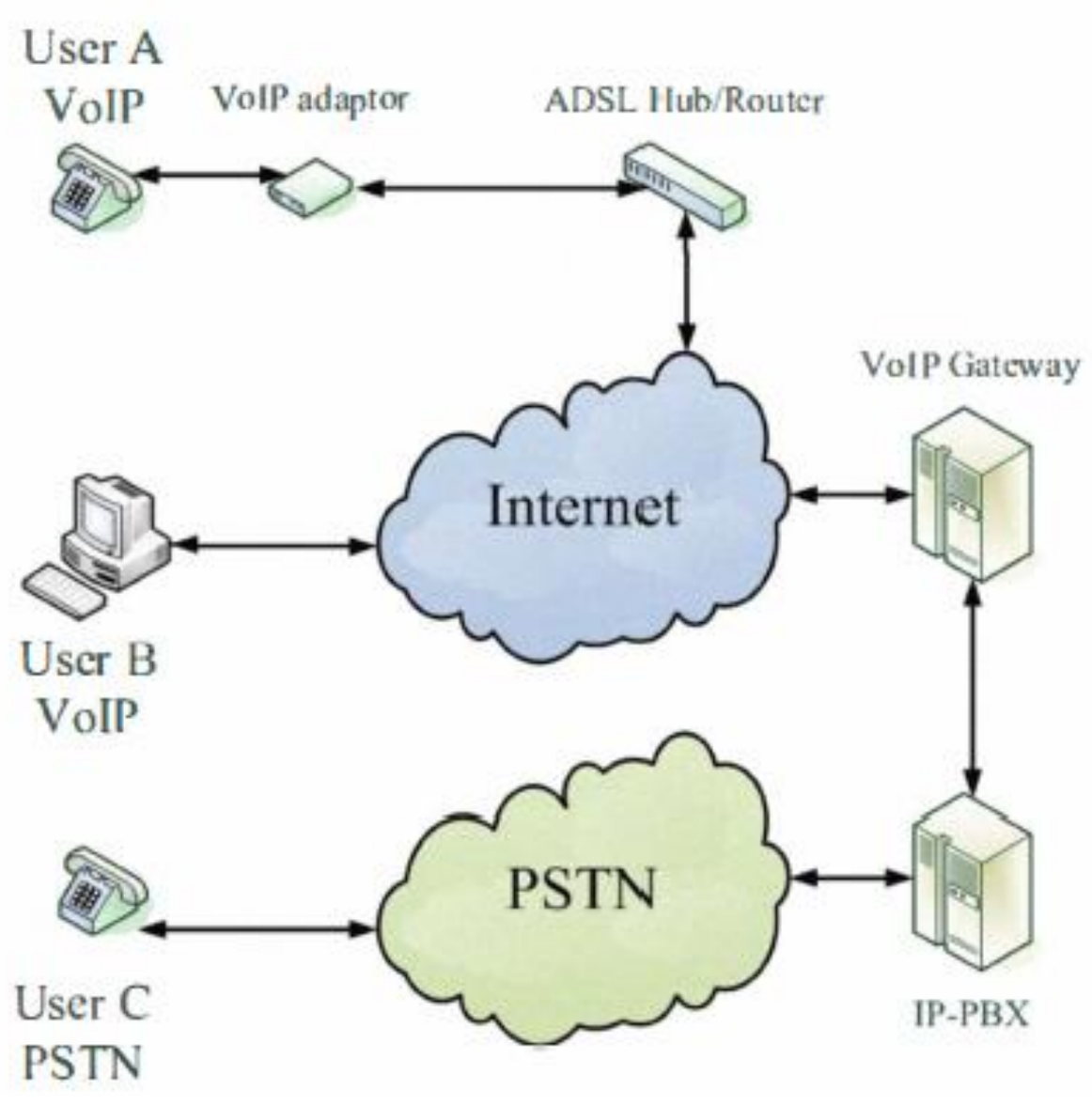
Telefonia Convencional

- Utiliza comutação de circuitos.
- Infraestrutura dedicada entre a central (PSTN) e o usuário.
- Alto custo de infraestrutura.
- Não extensível.



Telefonia VoIP

- Utiliza comutação de pacotes (IP).
- Infraestrutura compartilhada entre o provedor e o usuário.
- Custo reduzido ou inexistente de infraestrutura.
- Altamente extensível.



© Lin et al.

Telefonia VoIP

- Protocolos:
  - Session Initialization Protocol (SIP)
    Real Time Protocol (RTP)
  - Skype
  - GoogleTalk ? (Jabber/XMPP)

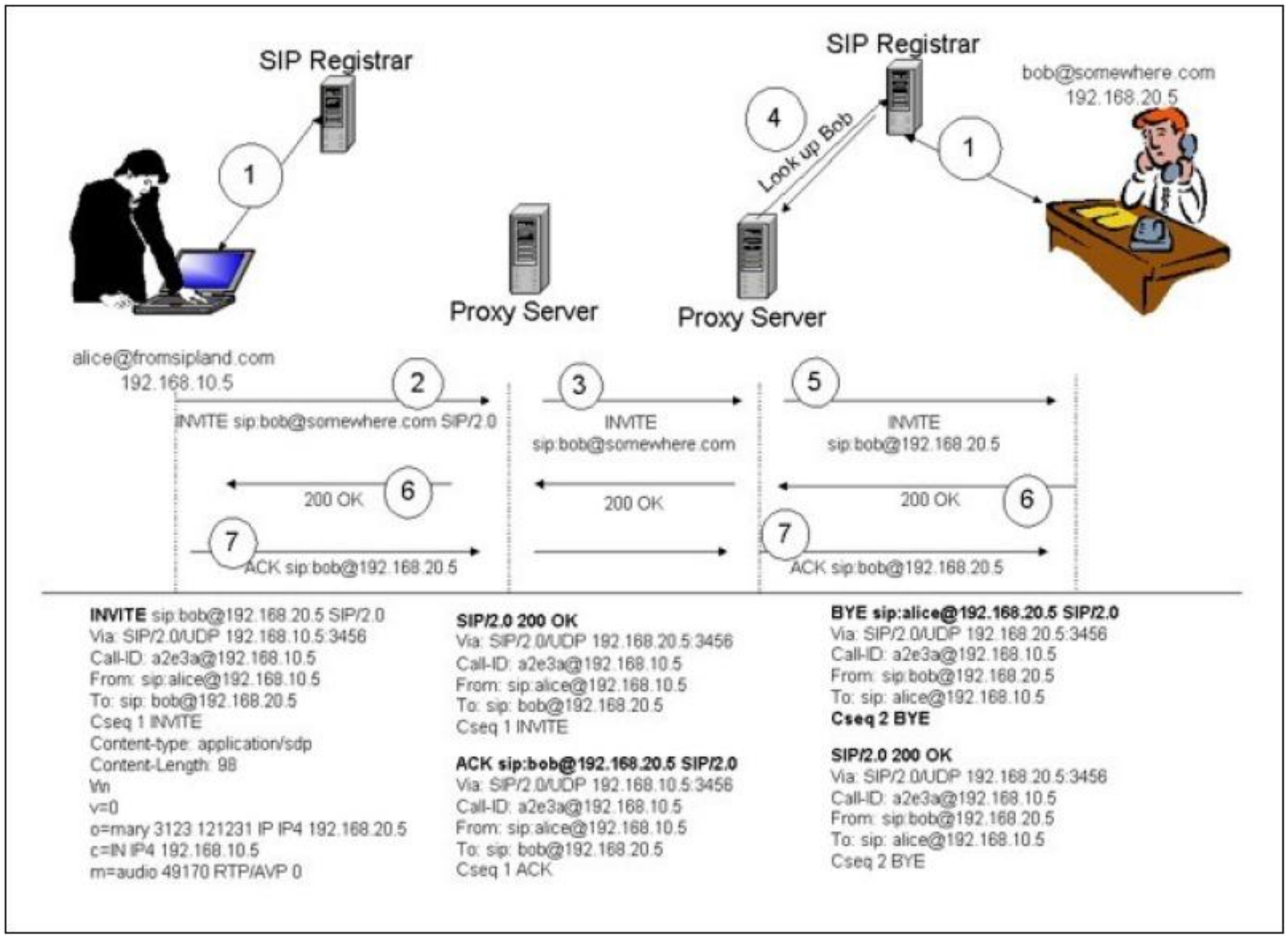
Arquitetura SIP e RTP

- Session Initiation Protocol – SIP
  - Protocolo de sinalização e controle de chamadas
  - Responsável pela inicialização e finalização de chamadas
  - Baseado em mensagens (request/response) textuais
  - Utiliza a porta 5060 TCP e UDP

Arquitetura SIP e RTP

- Real Time Protocol – RTP
- Responsável pelo transporte da mídia.
- Carrega informações de sequência do fluxo
- Utiliza a faixa de portas 1024 – 65535 UDP

Arquitetura SIP e RTP

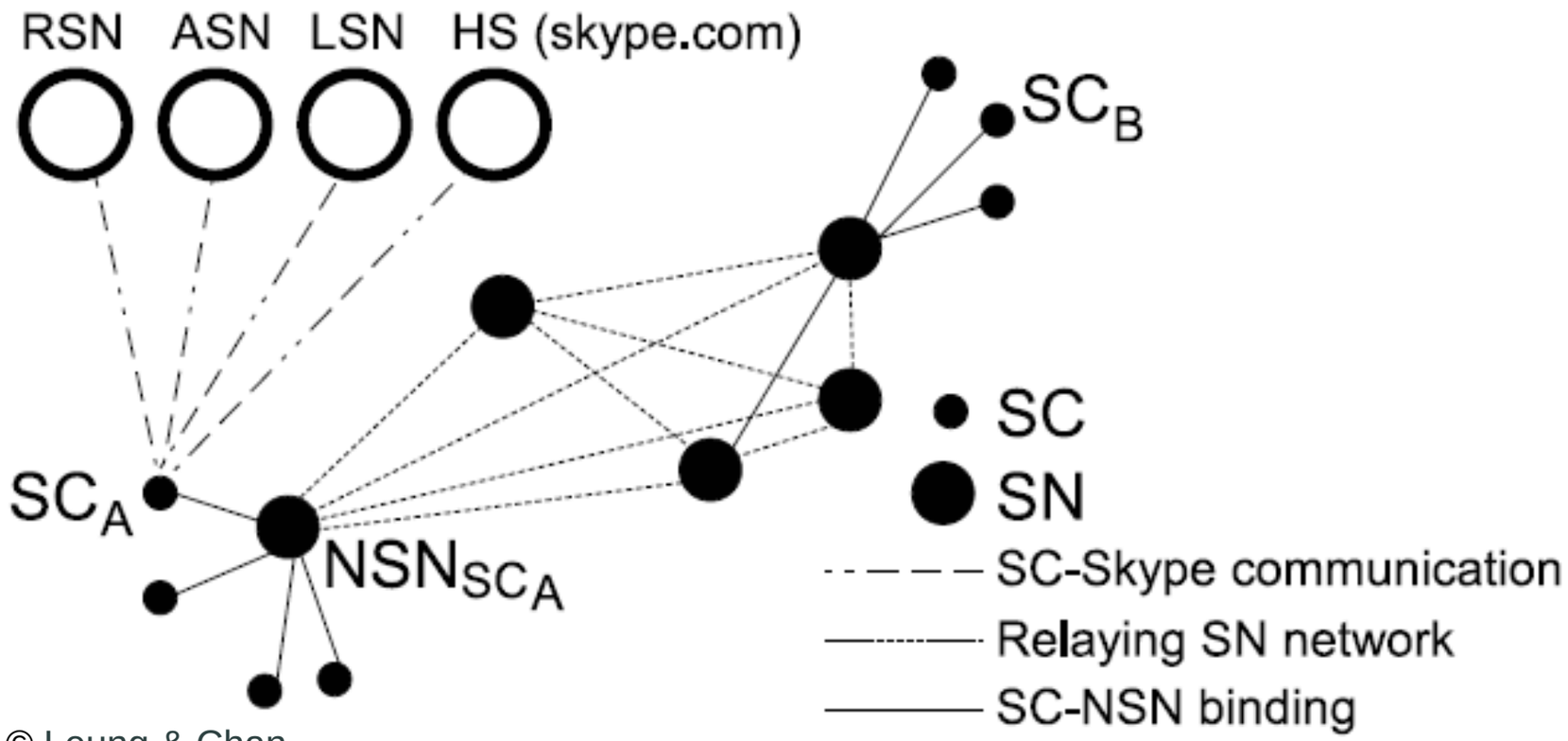


Arquitetura Skype

- Protocolo proprietário
- Dados nativamente criptografados (AES)

Stage	Protocol	Src.Host	Src.Port	Dst.Host	Dst.Ports	Encrypted /Paintext (E / P)	Least no. of Dst.	Typical outgoing packet size	Typical incoming packet size	Average interval of outgoing packets
1. Startup	UDP	SCA	U	RSN	Var	E	1 (or 4)	Var	Var	0.29ms
2. Registration	TCP		T1	RSN	Var (TR)	E	1	Var	Var	Var
3. Authentication	TCP		T2	ASN	33033	E	1	Var	Var	Var
4. SN Handshaking	UDP		U	SN	Var	E	3	Var	Var	0.45ms
5. NAT and Firewall	UDP		U	SN	Var	E	2	Var	Var	Var
6. Skype Latest Version	TCP		T3	HS	80	P	1	Fixed	Fixed	Var
7. NSNs Locating and Binding	UDP		U	NSN	Var	E	9	388B	Var	0.52ms
8. SC Peers Status Update	UDP		U	LSN.	Var	E	1	Var	Var	Var
9. Callee Searching	UDP		U	LSN	Var	E	3+3	Var	464B	0.37ms
10. Add Callee	TCP		T1	RSN	TR	E	1	Var	Var	Var
11. Call Setup	TCP		T4	SCB	Var	E	1	Var	Var	Var
12. Conversation	UDP		U	SCB	UB	E	1	60-181B	60-181B	19-59ms
13. Call Teardown	TCP		T4	SCB	Var	E	1	Var	Var	Var
14. Logout	TCP		T1	RSN	TR	E	1	Var	Var	Var
15. Quit Skype Program	TCP		T1	RSN	TR	E	1	Var	Var	Var
	TCP		T3	HS	80	E	1	Var	Var	Var

Arquitetura Skype



© Leung & Chan

Legislação

- **Communications Assistance for Law Enforcement Act – CALEA**
  - Lei americana aprovada em 1994.
  - Define a obrigação de “cooperação” de operadoras na interceptação de comunicação.
  - Obrigava que toda a infraestrutura de telefonia suportasse a ativação de grampos telefônicos (wiretapping).
  - Em 2004 foi regulamentada a aplicação da lei para provedores VoIP.
  - Devido a suas características o Skype não foi afetado.

Extração de Evidências

Extração de Evidências

- Nos trabalhos [Simon & Slay 2006] e [Slay & Simon 2008], os autores propõem um método de extração de evidências a partir da memória RAM.

- O método deve ser aplicado antes que o computador utilizado para fazer a chamada VoIP seja desligado.

- A análise é feita a partir de um arquivo de imagem da memória RAM que pode ser obtido de duas formas:
  - Através de hardware dedicado instalado previamente no equipamento;
  - Via software.

Extração de Evidências

- Aplicação:
  - A técnica pode ser empregada em situações onde não há outra fonte de informações;
  - O fato da análise ser realizada no computador e não no tráfego de rede minimiza problemas quanto a privacidade de informações.
- Restrições:
  - Necessidade do equipamento permanecer ligado após a realização da chamada;
  - Suporte apenas aos protocolos SIP e RTP;
  - Falta de suporte a protocolos criptografados.

Extração de Evidências

- Resultados:
  - Segundo os autores, foi possível coletar informações de sinalização e mídia em imagens de S.O. Windows XP e MacOS X;
  - Em casos específicos foi possível recriar o áudio.
- Problemas:
  - O trabalho não apresenta nenhuma informação quanto a precisão na localização de evidências;
  - O algoritmo utilizado na busca de informações não foi divulgado por utilizar código proprietário.

Trabalhos Correlatos

Trabalhos Correlatos

- Digital Forensics in VoIP networks [François et al. 2009]
- Speaker Recognition from Encrypted VoIP Communications [Khan et al. 2010]

Trabalhos Correlatos

Digital Forensics in VoIP networks

- Técnica de identificação do dispositivo VoIP a partir do tráfego de sinalização SIP.
- Baseia-se na idéia de que diferentes implementações geram mensagens SIP com características estruturais diferentes.
- O algoritmo proposto gera árvores estruturais a partir de mensagens SIP.
- Foi utilizado o classificador SVM.
- A precisão na identificação dos dispositivos foi de 95%.

Trabalhos Correlatos

- Digital Forensics in VoIP networks
  [François et al. 2009]

- Speaker Recognition from Encrypted VoIP Communications
  [Khan et al. 2010]

Trabalhos Correlatos

Speaker Recognition from Encrypted VoIP Communications

- Técnica de identificação do locutor a partir de dados SRTP criptografados.
- Na verdade, a idéia baseia-se na classificação dos pacotes SRTP em relação a seu tamanho.
- A técnica baseia-se em 2 características:
  - O tamanho da carga de dados SRTP é o mesmo de cargas RTP;
  - Codecs de bitrate variável (VBR) geram bitrates maiores para frequencias mais altas.

Trabalhos Correlatos

Speaker Recognition from Encrypted VoIP Communications

- A técnica permite a identificação e a verificação do locutor.
- Foram utilizados o modelo Ensemble of Nested Dichotomies (END) para a identificação e o classificador SVM para a verificação do locutor.
- Os resultados mostraram que apesar da precisão ser inferior aos conseguidos com dados não criptografados, o resultado final é melhor que a escolha aleatória.

Conclusões

Conclusões

- Apesar do uso difundido da VoIP ainda não existem técnicas forenses eficazes.
- Em todos os trabalhos pesquisados é recorrente a preocupação com a quebra de privacidade.
- Os trabalhos sobre a tecnologia Skype dizem respeito a bloqueio de tráfego e não a coleta de evidências.
- A análise forense em VoIP é uma área que possui um vasto campo a ser pesquisado.

Referências

Referências

1. [Simon & Slay 2006] **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.

2. [Slay & Simon 2008] **J. Slay and M. Simon**. Voice over ip forensics. In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, page 10. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

3. [Leung & Chan 2007] **C.M. Leung and Y.Y. Chan**. Network forensic on encrypted peer-to-peer voip traffics and the detection, blocking, and prioritization of skype traffics. In Proceedings of the 16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pages 401-408. IEEE Computer Society, 2007.

4. [François et al. 2010] **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.

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

6. [Lin et al. 2010] **I.L. Lin, Y.S. Yen, B.L. Wu, and H.Y. Wang**. Voip network forensic analysis with digital evidence procedure. In Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on, pages 236-241. IEEE, 2010.

Obrigado!