Centro Federal de Educação Tecnológica do Rio Grande do Norte
Unidade de Ensino Descentralizada de Currais Novos
Departamento Acadêmico em Gestão Tecnológica

SPIT

Spam over Ip Telephony

(A Nova Praga Virtual)

Ricardo Kléber Martins Galvão
rk@cefetrn.br
http://www.ricardokleber.com.br

GTS
Grupo de Trabalho em Segurança

São Paulo, 27/10/2007

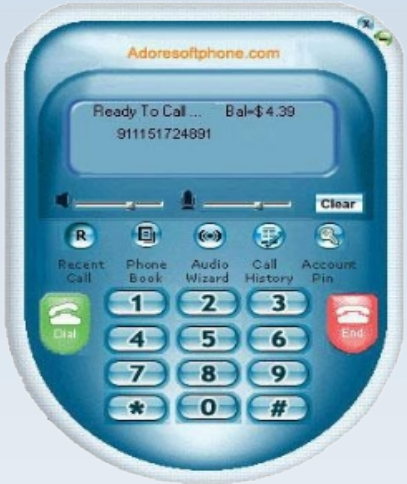
VoIP :: Visão Geral

- Criada para permitir o tráfego de voz sobre uma rede de dados.
- “Digitalização” de voz e “empacotamento” de dados para a transmissão em uma rede que utilize os protocolos TCP/IP.

VoIP :: Visão Geral

- Apresentação:
  - Softphone
  - Telefone VoIP
  - Telefone convencional

    + adaptador (ATA)
  - PABX VoIP
  - VoIP sobre Wireless



VoIP :: Breve Histórico

- Primeiros produtos lançados em 1995
- Foco inicial: Mercado Corporativo

Atrativo: Redução de custos de telefonia através da utilização compartilhada da infra-estrutura das redes de dados já existentes, para transmissão integrada de voz e de dados.

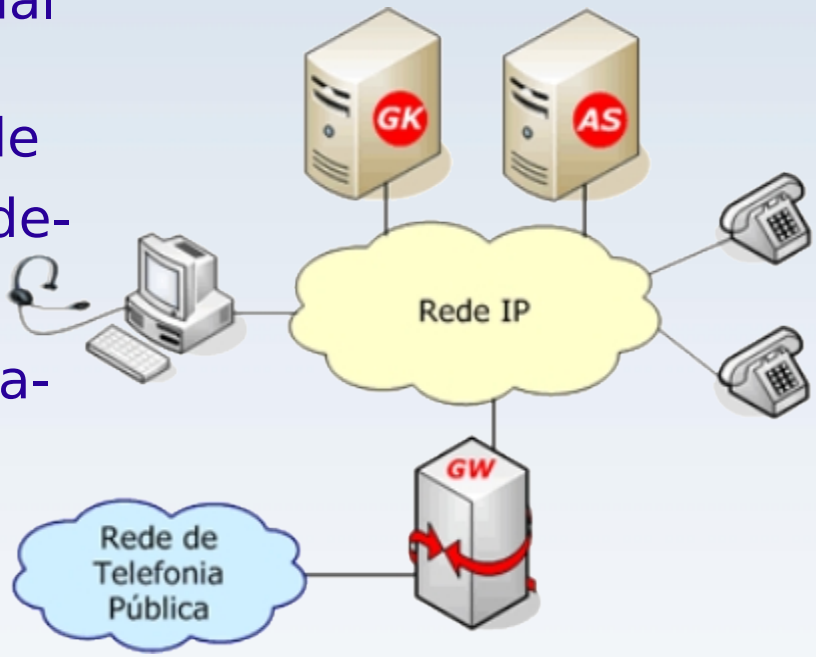
VoIP :: Requisitos

- Transmissão de voz em tempo real com tempo de latência (atraso) menor que 300ms;
- Procedimentos de sinalização para estabelecimento e controle de chamadas e fornecimento de serviços adicionais (conferência, chamada em espera, identificador de chamadas, etc).

- Interface com os sistemas públicos de telefonia comutada e móvel.

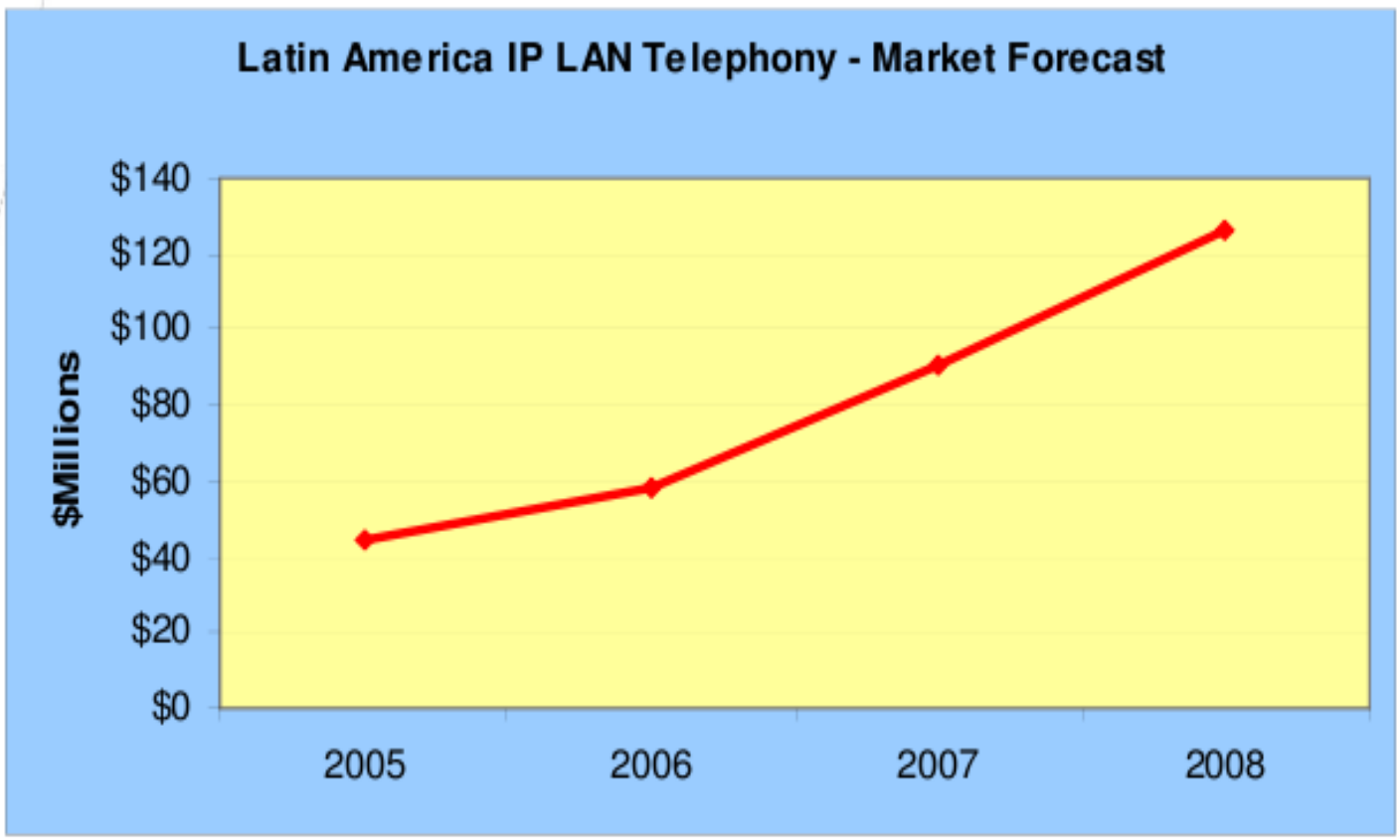
VoIP :: Arquitetura Básica

- **Terminal :** Telefone IP, analógico com ATA ou softphone
- **Gateway (GW)** : Ponte entre a rede VoIP e a telefonia convencional
- **Gatekeeper :** Gerenciador de telefones IP (tradução de endereços de terminais), controle de acesso, controle de chamadas e banda utilizada



- **Application Server (AS) :**
  Fornece os serviços adicionais da rede VoIP
  - agenda, conferência, chamada em espera, voicemail...

VoIP :: Estimativa para América Latina



Fonte: Synergy Research, 2005

VoIP :: Estimativa para os EUA

- 2003 = 131.000 assinantes VoIP
- ...
- 2008 = 17,5 milhões de assinantes VoIP

Fonte: Yankee Group (www.yankeegroup.com)

OBS: Mais ou menos o mesmo número de pessoas que usavam e-mail em 1995, quando popularizou-se o SPAM !!!

VoIP x Telefonia Convencional

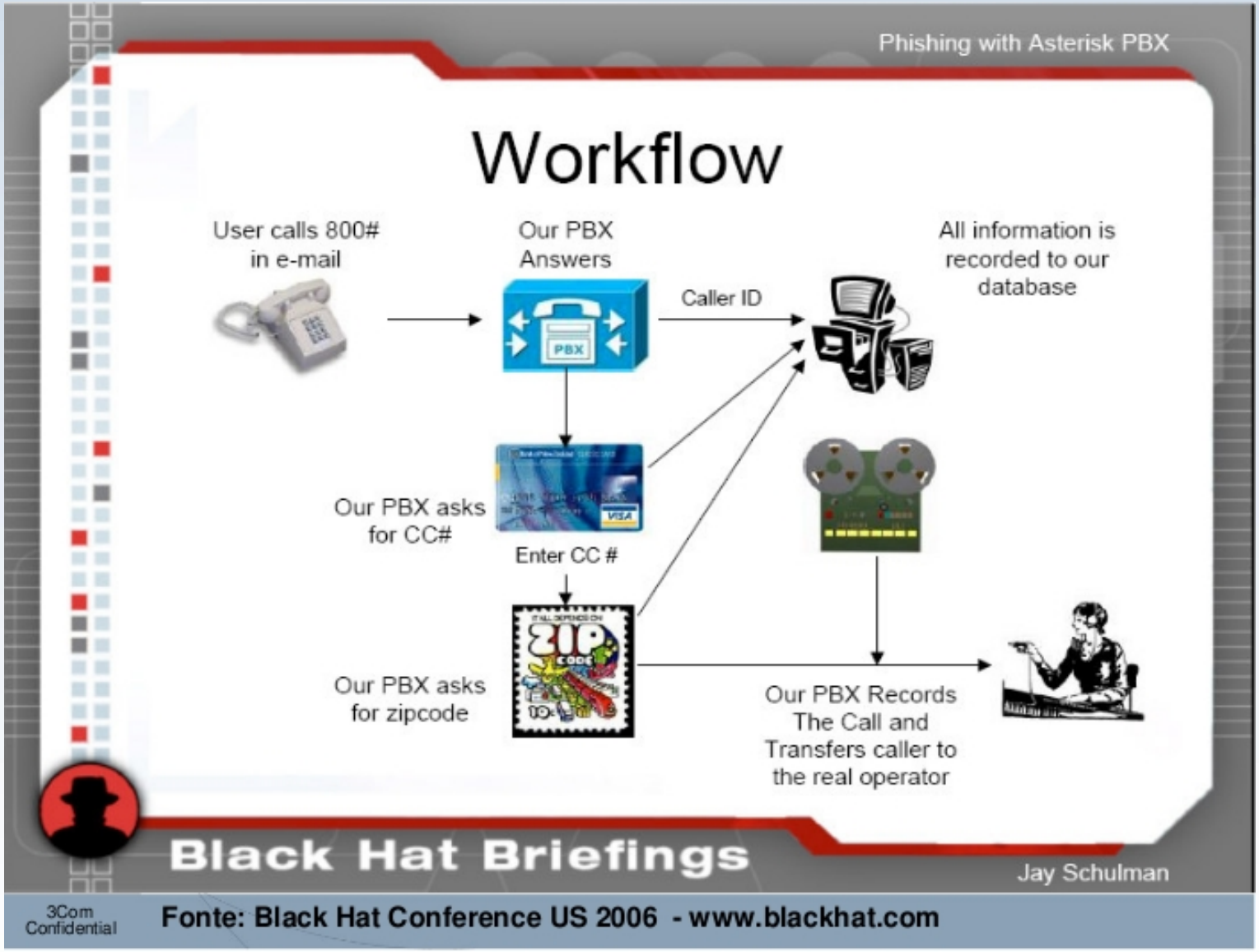
- Substituto natural (tendência) (custo x benefício)
- Exemplo do impacto do uso de celulares na telefonia convencional (pesquisa nacional – PNAD – IBGE):
  - Abrangência: 51,7 milhões de casas
  - **16,7% usam apenas celular**

Novos Conceitos... Novos Problemas...

E a (in)Segurança no uso do VoIP ??

(in)Segurança no uso do VoIP

- Interceptação (“Grampo”) Digital



(in)Segurança no uso do VoIP

- Dependência da rede (DDoS !!??)

10 ANOS
IDG NOW!
tecnologia em primeiro lugar

IDG BRAS

20 de agosto de 2007

Home | Mercado | Internet | Segurança | Co
Telecom e Redes

IDG Now! » Telecom e Redes » Serviços

TELECOM E REDES

SERVIÇOS

Após mais de 48 horas com falha de conexão, Skype volta a funcionar

Por Gregg Keizer, para o IDG Now!*
Publicada em 20 de agosto de 2007 às 08h49
Atualizada em 20 de agosto de 2007 às 10h58

E-mail | Imprima | Comente | Erros? | del.icio.us | Digg

a a a

Framingham - Empresa anunciou no final da sexta-feira (17/08) que todos os usuários podiam novamente se autenticar no serviço de voz sobre IP.

O Skype anunciou no final da sexta-feira (17/08) que todos os usuários podiam novamente se autenticar no serviço de voz sobre IP, marcando o final do problema que deixou milhões de pessoas sem serviço por mais de 48 horas.

O GLOBO ONLINE | TECNOLOGIA

CAPA | PLANTÃO | MEU GLOBO ONLINE | BLOGS | GLOBOONLINERS | EU-REPÓRT
PAÍS | RIO | SÃO PAULO | ECONOMIA | MUNDO | CIÊNCIA | ESPORTES | CUL

Publicada em 17/08/2007 às 19h01m

RETOMADA

Skype aponta normalização dos serviços e nega ataque de crackers

O Globo Online com agências internacionais

NOVA YORK e RIO - Pouco mais de 24 horas após apresentar problemas na oferta de ligações de voz via internet, a empresa de telefonia pela web Skype exibe como normalizados os principais serviços de voz (VoIP). Na noite desta sexta-feira, um gráfico que acompanha a qualidade dos serviços prestados ao usuário, no blog "Heartbeat" , foi publicado e exibia mensagens "funcionando normalmente" ("All working normally") para os serviços. Até as 19h, apenas os canais de cadastro de novos usuários e de acesso a redes de compartilhamento (peer-to-peer) apresentavam problemas.

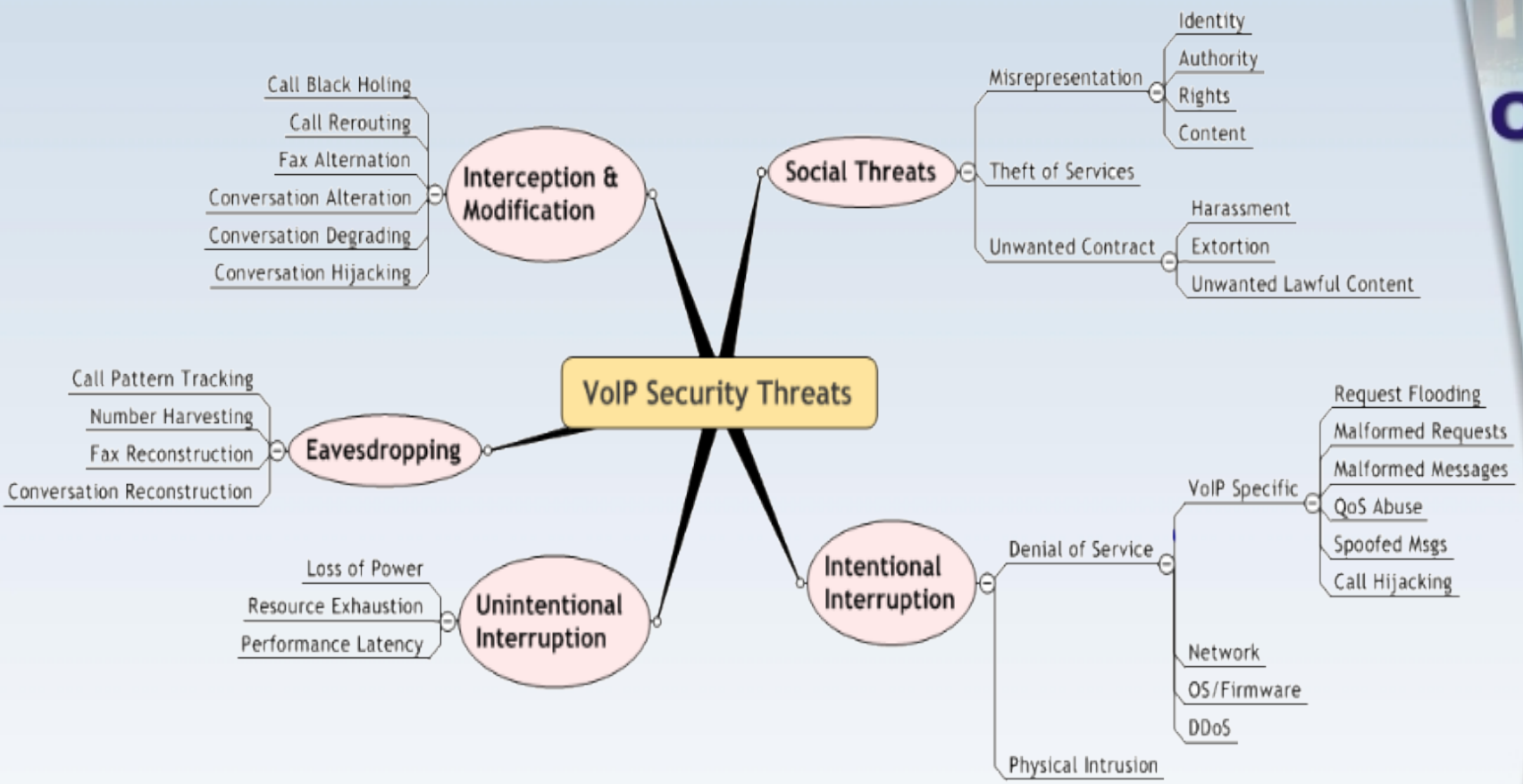
Na manhã dessa sexta-feira, a Skype, propriedade do eBay, reconheceu em nota que não havia conseguido consertar os problemas de acesso dos usuários a seus serviços, iniciados na quinta-feira, e que os ajustes poderiam levar o dia inteiro.

(in)Segurança no uso do VoIP

É só isso ???

Não !!!

(in)Segurança no uso do VoIP :: Ameaças



Fonte: VoIP Security Alliance (www.voipsa.org)

(in)Segurança no uso do VoIP
:: Nosso foco... SPIT

Spam over Ip Telephony

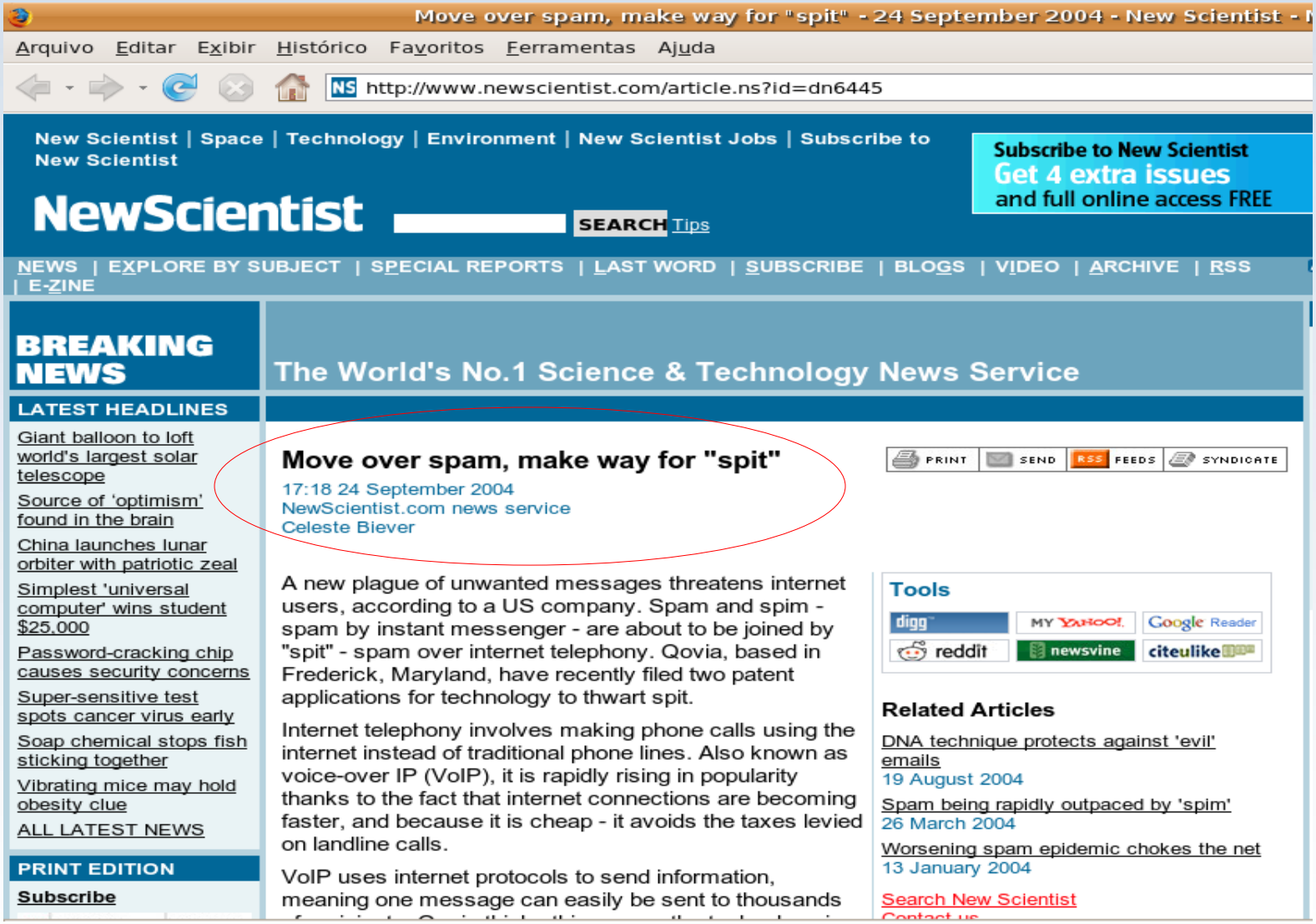
Origem Divulgada

- 13 de maio de 2005
- Bruce Schneier
- Blog “Schneier on Security” (www.schneier.com/blog)

SPIT :: Citação Mais Antiga

http://www.newscientist.com/article.ns?id=dn6445

Celeste Biever :: 24/09/2004



SPIT :: Citação Mais Antiga

http://www.pctoday.com/editorial/article.asp?article=articles%2F2005%2Ft0305%2F11t05%2F11t05.asp

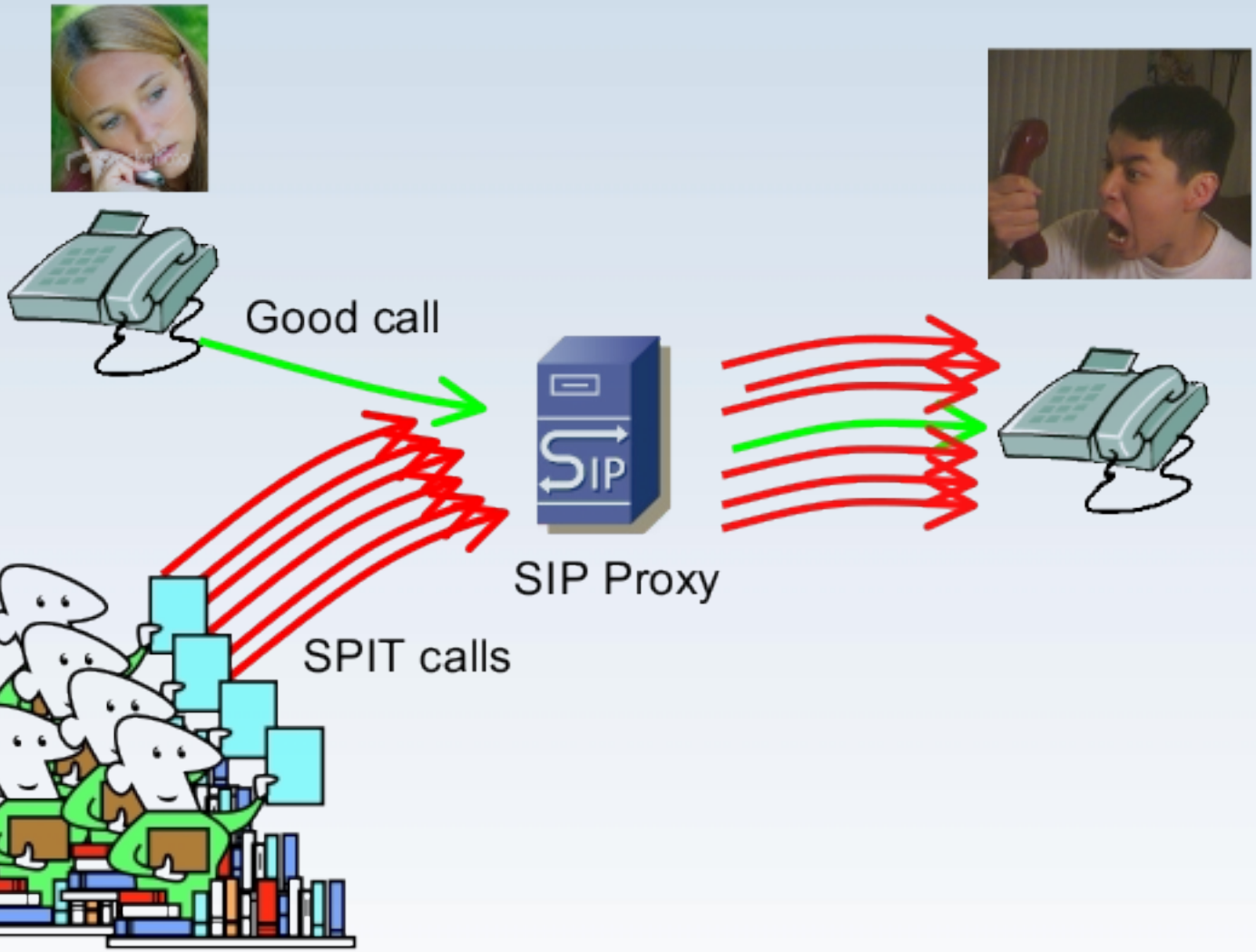
*"**Spit (short for spam over Internet Telephony)** is a type of spam or solicitation made over VoIP. **Qovia (www.qovia.com)** a leading developer of VoIP monitoring and management technologies and products, **stated in its June 2004 press release** that **"VoIP Spam is a combination of telemarketing calls and email spam in which a single 'caller' uses Internet technology to send thousands of voice messages simultaneously into callers' VoIP voice mailboxes."** Experts, including the U.S. Telecommunications Association, concur that spit presents a critical challenge to the telephony industry as it exists today."*

www.qovia.com

- Fundada em 2002
- Testes de envio de 1000 mensagens por minuto (VoIP)
- IP Telephony Manager (2006)
- *Site sem informações atualmente*

A Praga do SPAM

SPIT :: SPam over Ip Telephony



SPIT :: SPam over Ip Telephony

- Mensagens **não solicitadas** que chegam por meio de receptores de VoIP (softphones, aparelhos VoIP ou aparelhos convencionais utilizando ATA).
- Derivada do SPAM tradicional
- Utilização em massa para trotes e telemarketing

  Mensagens indesejáveis em momentos indesejáveis com propostas indesejáveis de origens (geralmente) desconhecidas...
- Atrativos ao telemarketing convencional
  - Gratuidade
    - baixo custo de meio de transmissão e número de funcionários
  - Automatização
  - Volume (abrangência de “alvos”)

SPIT :: SPam over Ip Telephony

- Fundamento semelhante
  - Envio de mensagem não desejada (geralmente de conteúdo comercial)
- Diferencial: Análise de conteúdo
  - Possível e implementável contra o SPAM
  - SPIT: Conteúdo só disponível após atendimento da chamada
    - Possível, porém, em caso de uso de caixa-postal VoIP
- SPAM :: Soluções “paliativas”
  - Problema não resolvido definitivamente
  - Uso de quarentena não reduz tráfego (apenas bloqueia suspeitas)
  - Criatividade burla (mesmo que momentaneamente) filtros convencionais (spam em links, imagens e pdf's p.ex.)

SPIT :: Uso no Telemarketing

- Gravação da mensagem

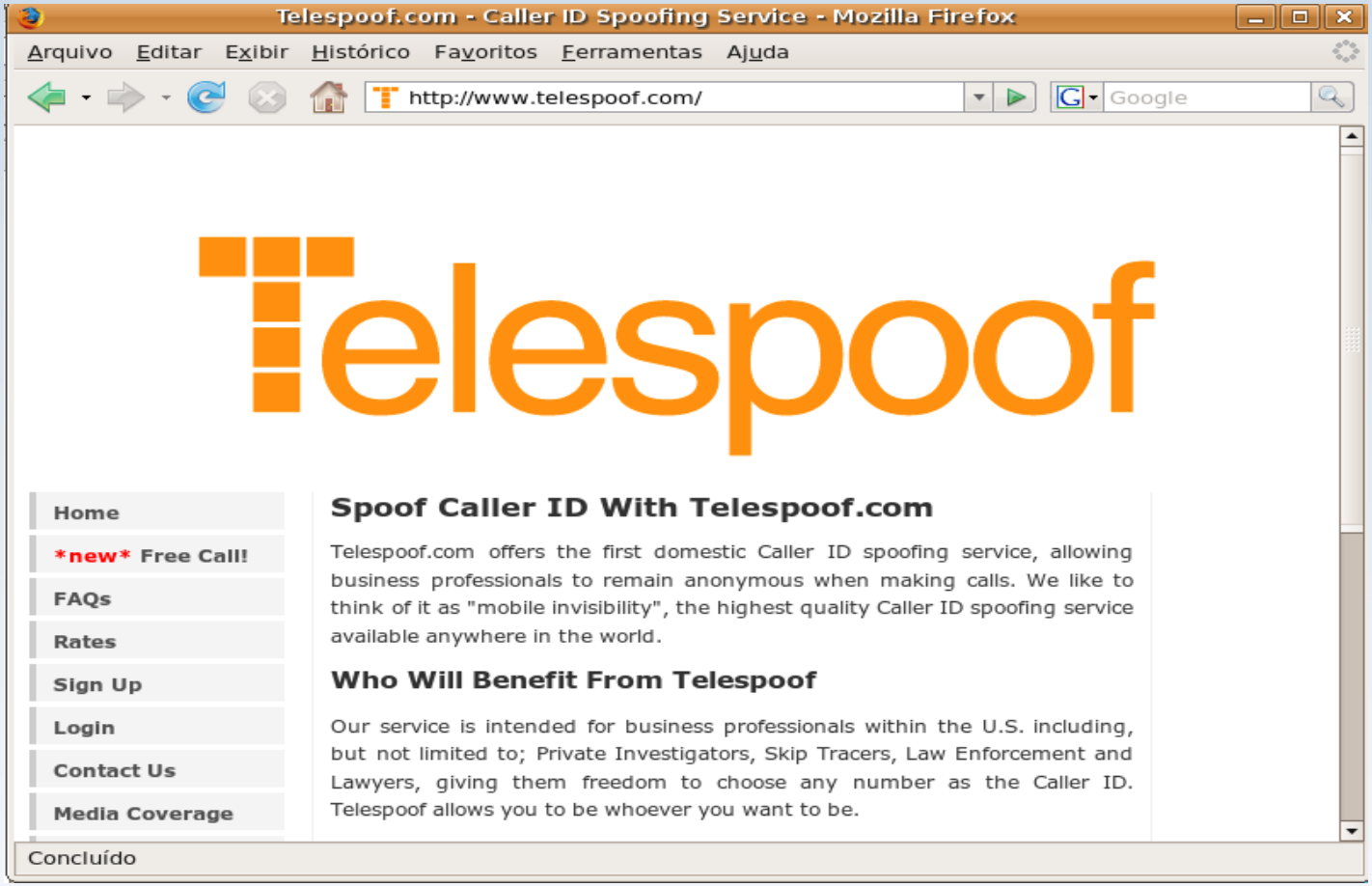
  (uso de ferramentas específicas para reduzir custos);
- Envio automatizado “em massa” para diversos

  destinatários
  - ... com perfis específicos (telemarketing direcionado); ou
  - ... aleatoriamente (produtos de abrangência geral).
  - A cada atendimento, o sistema dispara a gravação da mensagem
  - É possível a personalização da mensagem (adaptação automática baseada em perfis) incluindo nomes ou características do “alvo”.

SPIT :: Prejuízos

- Pessoais
  - Tempo
    - ... até a identificação do SPIT
    - ... para bloquear número de origem (identificável !!??)
  - Psicológicos
    - Raiva... Angústia... Stress...
      - Você lê e-mails quando quer... e telefonemas? (Aperitivo: SMS)
      - O anonimato estimula golpes...
        - Na telefonia convencional... bina diminuiu incidência...
- Corporativos
  - Custos
    - ... com armazenamento (caixas-postais VoIP)
    - ... com banda de comunicação
      - Consumo indevido
      - Concorrência/atraso em pacotes de clientes

SPIT :: Anonimato !!??



Empresas de Voip Caller Spoofing !!!

VoIP :: Soluções antigas para novos problemas

Uso de Criptografia

- Alguns sistemas dispõem de solução com criptografia
- Caso não exista utilizar VPN's (OpenVPN !!??)
- “Grampos” VoIP são uma realidade (VOMIT !!??)

Uso de IDS (Sistema de Detecção de Intrusões)

- Agentes monitorando redes de dados VoIP;
- Assinaturas de ataque específicas;
- Soluções de acordo com “o bolso”;
- Falta de proatividade (elemento passivo)
- Solução mais adequada... IPS !!!

Combate com IPS
(Intrusion Prevention System)

- Análise de tráfego e bloqueio em tempo real
- Proteção DDoS
- Soluções baseadas em hardware
- Filtros de vulnerabilidades (SIP, H.323)
- Latência de microssegundos (< 150ms)
- Custo !!??
- HLBR promete...

Severity	Name
Major	2588: H.225: Source Address URL Length Anomaly
Major	2590: H.225: Source Address h323-ID Length Anomaly
Major	2591: H.225: Source Address h323-ID Value Anomaly
Major	2592: H.225: Source Address dialedDigits Length Anomaly
Major	2593: H.225: Source Address Email Length Anomaly
Major	2595: H.225: Destination Address Choice Anomaly
Major	2598: H.225: Destination Address h323-ID Length Anomaly
Major	2599: H.225: Destination Address URL Length Anomaly
Major	2600: H.225: Destination Address URL Value Anomaly
Major	2601: H.225: Destination Address h323-ID Value Anomaly
Major	2602: H.225: Destination Address dialedDigits Length Anomaly
Major	2604: H.225: Source Address Choice Anomaly
Major	2605: H.225: Protos Suite Attack
Critical	2818: SIP: Method Anomaly
Critical	2819: SIP: URI Anomaly
Critical	2820: SIP: Version Anomaly
Critical	2821: SIP: Via Host Anomaly
Critical	2822: SIP: Via Version Anomaly
Critical	2823: SIP: Via Tag Anomaly
Critical	2824: SIP: From Field Anomaly
Critical	2825: SIP: Contact Field Anomaly
Critical	2827: SIP: Call-ID Field Anomaly
Critical	2829: SIP: Cseq Field Anomaly
Critical	2830: SIP: Content-Type Field Anomaly

Fonte: 3Com

SPIT :: O que aprendemos com o SPAM

- SPAM :: Resolver x Aprender a conviver
  - Lists
    - Whitelists;
    - Blacklists;
    - Greylists
  - Filtros
    - Globais;
    - Institucionais;
    - Pessoais

Soluções (com adaptações) implementáveis para amenizar o SPIT

Combate ao SPIT

E os novos problemas ???

Solução (comercial) Interessante...

- **VoIP Seal (NEC)**
  - **Solução comercial...**
    - **... Idéias implementáveis**
      - **Saverio Niccolini, NEC**
        - *Vários artigos publicados !!!*

Combate com VoIP Seal
(Filtro de Spit)

- Apresentado pela NEC no Congresso 3GSM (Barcelona, **12 a 15/02/2007**)
- Separação de chamadas originadas de softwares geradores de SPIT de ligações feitas por pessoas
- Bloqueio realizado antes mesmo do telefone tocar
- Estrutura modular adaptável a novas técnicas de SPIT
- Simulações feitas pela empresa identificaram e bloquearam **99%** dos SPIT enviados

Combate com VoIP Seal
(Filtro de Spit)

- Característica Básica:
  - **Em todos os casos... Interceptação prévia (Greeting)**
  - Técnicas de Detecção: **Interação com o chamador**
    - *Captcha (de áudio)*
      - **Desafios como: *"Digite um número de 1 a 5..."***
        - *Impossibilidade (pelo menos inicialmente) de interação a partir de mecanismos automatizados (SPIT)*

Combate com VoIP Seal
(Filtro de Spit)

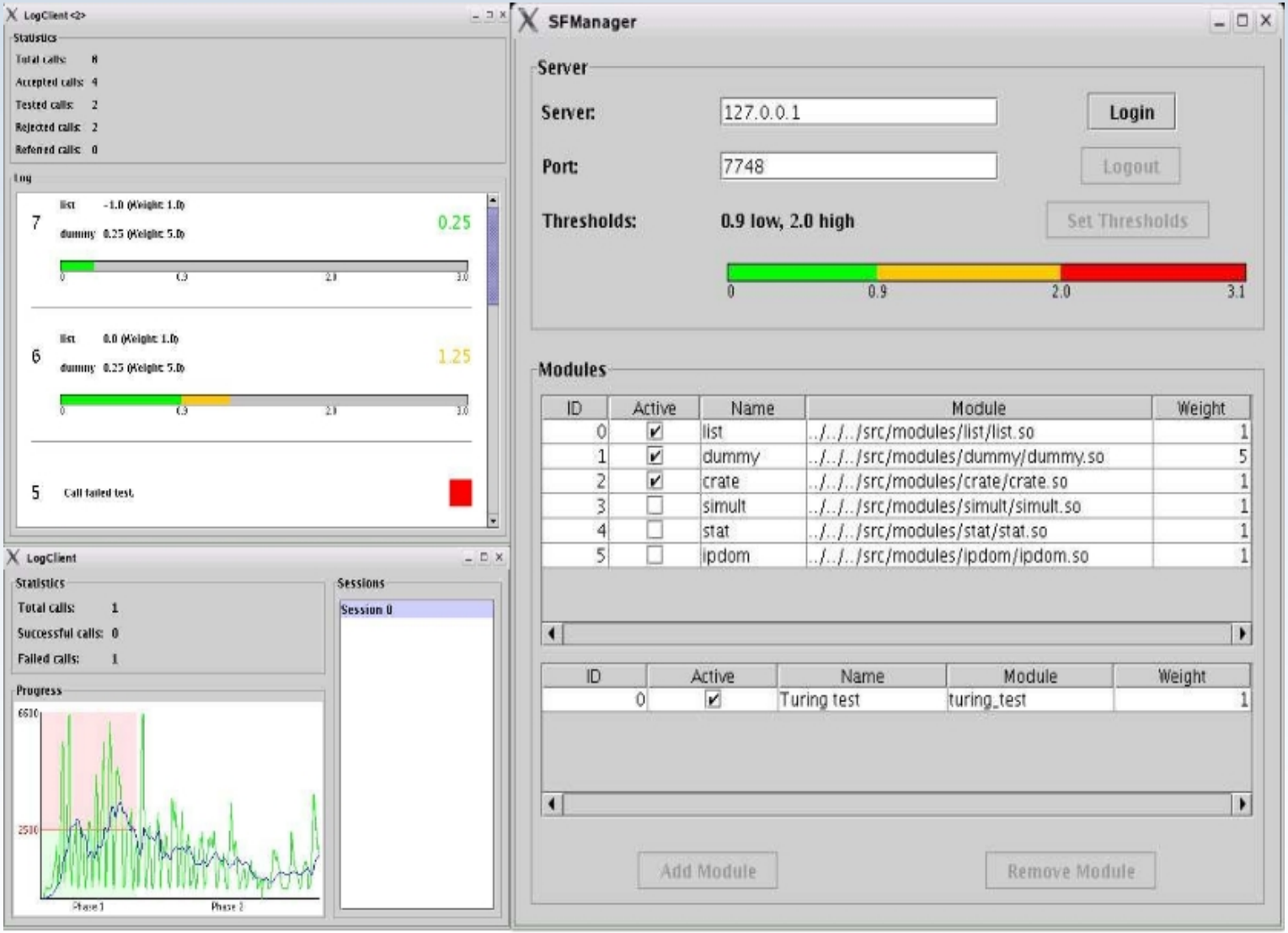
- Outras Técnicas de Detecção:
  - Simulação de atendimento e análise de áudio
    - Teste Básico : **Toques Adicionais**
      - **Humanos** entenderiam como se não tivesse havido o atendimento e **parariam de falar**...
      - **Mecanismos automatizados** iniciariam a reprodução de gravações (SPIT) **sem cessar**...
        - A ausência de som representaria um usuário humano
          - A ligação seria completada
        - O áudio contínuo (ignorando os toques adicionais)...
          - SPIT » Encerramento da chamada sem acionar destinatário

Combate com VoIP Seal
(Filtro de Spit)

- Outras Técnicas de Detecção:
  - Simulação de atendimento e análise de áudio
    - Teste Avançado: ***Turing Test***
      - Interceptação de áudio inicial (sem completar ligação)
      - Utilização de técnicas de detecção de tipo de áudio
        - **Humano » Mensagem Automática » Completa Ligação**
        - **Gravação » Encerramento sem completar ligação**

Combate com VoIP Seal
(Filtro de Spit)

- **Interface VoIP Seal :: Turing Test**



Fonte: NEC

Combate com VoIP Seal
(Filtro de Spit)

- **Outras características do VoIP Seal**
  - Compatibilidade com soluções VoIP corporativas e residenciais (pabx, ata e/ou softphone).
  - Promessa de integração com anti-virus/personal firewall

VoIP Seal incorporado a soluções Skype

Skype Puts Its Seal on VoIP Gateway from VoSKY

http://ipcommunications.tmcnet.com/hot-topics/gateway/articles/6568-skype-puts-its-seal-voip-gateway-from-vosky.htm

02/05/2007

- VoSKY Exchange (gateway PBX)
  - Solução VoIP Seal embutida

Motivação... Ratificando !!!

- VoIP SEAL (NEC)
  - Solução comercial...
    - ... Idéias implementáveis

Third Annual VoIP Security Workshop
(Berlin, Germany 01, 02/06/2006)

- **SPIT Mitigation by a Network-Level Anti-Spit Entity**
  - *Bertrand Mathieu, Yvon Gourhant; Quentin Lourdier*
    - *France Telecom R&D, France*
- **Incorporating Active Fingerprinting into SPIT Prevention Systems**
  - *Hong Yan, Carnegie Mellon University, USA*
  - *Kunwadee Sripanidkulchai, IBM, USA*
  - *Hui Zhang, Carnegie Mellon University, USA*
  - *Zon-yin Shae, Debanjan Saha, IBM T. J. Watson, USA*
- **Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT**
  - *Markus Hansen*
    - *Independent Centre for Privacy Protection, Germany*
- **SPIT and SPIM**
  - Saverio Niccolini, NEC, Germany

Reconhecimento de Padrão de Voz Humana

Detecting SPIT Calls by Checking Human Communication Patterns

Quittek, J.; **Niccolini, S.**; Tartarelli, S.; Stiemerling, M.; Brunner, M.; Ewald, T.

IEEE International Conference on Communications, 2007 (ICC)

Volume , Issue , **24-28 June 2007** Page(s):1979 - 1984

Prevention of Spam over IP Telephony (SPIT)

*Juergen QUITTEK, **Saverio NICCOLINI**, Sandra TARTARELLI, Roman SCHLEGEL*

- Paper publicando no NEC Technical Journal (2006)
- Apresenta uma arquitetura genérica de um sistema de prevenção a SPITs

SPIT Prevention: State of Art and Research Challenges

Saverio NICCOLINI

- Apresentado no Voip Security Seminar (2006)
- Esquemas de proteção e screenshot do VoIP Seal

Voice Over IP – Security and SPIT

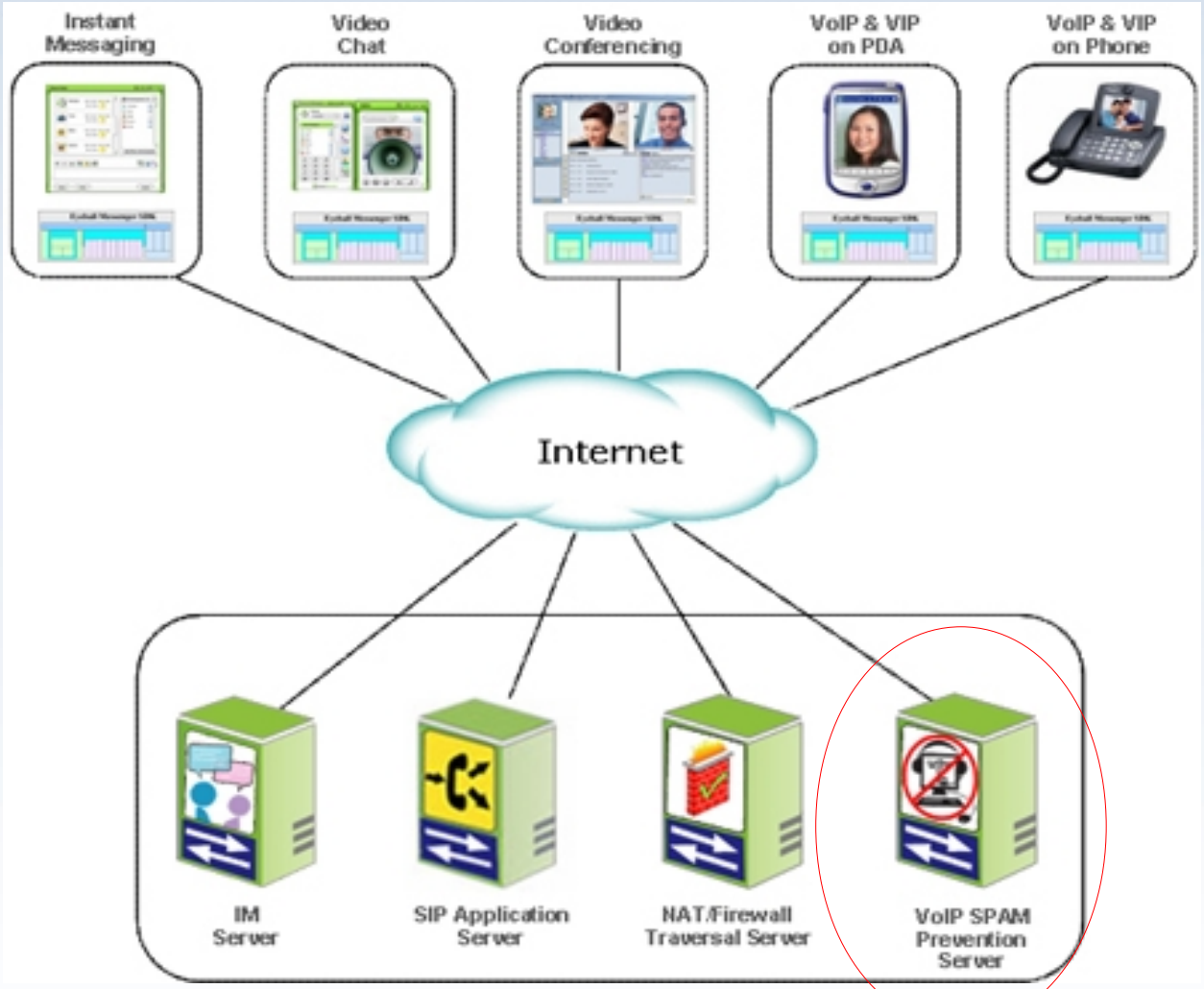
Rainer Baumann, Stéphane Cavin e Stefan Schmid

- University of Berne (Zurich/Switzerland)
- 24 de Agosto de 2006
- 12 soluções para o SPIT;
- Principais problemas;
- "*A Biometric Framework for SPIT Prevention*"

Eyeball AntiSPIT Server

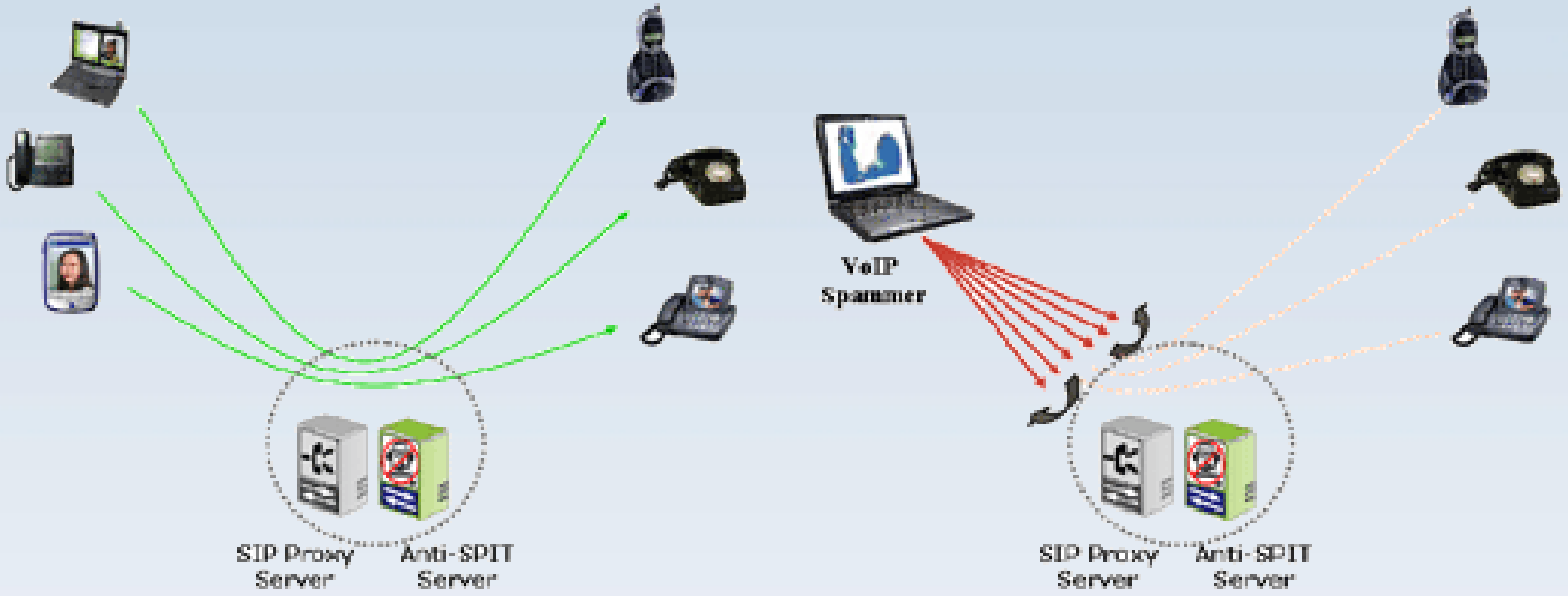
www.eyeball.com

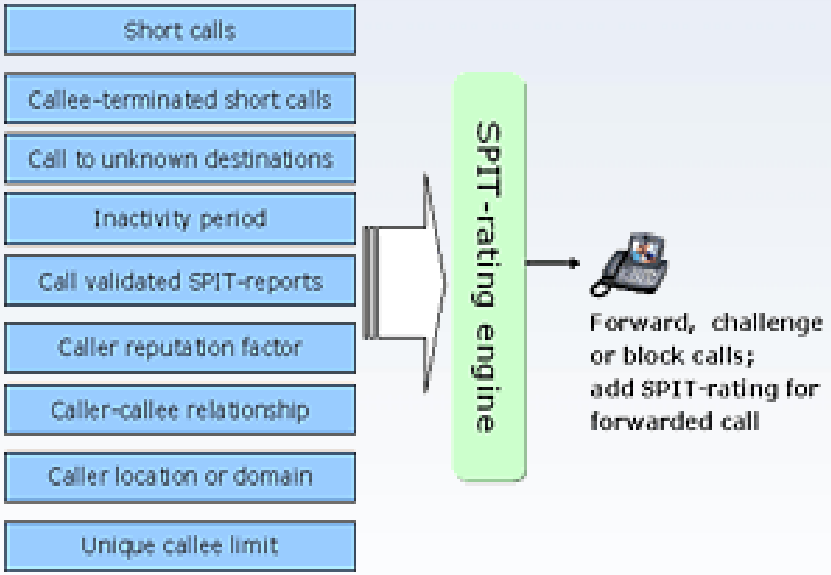
Eyeball Networks



Eyeball AntiSPIT Server

www.eyeball.com





- Prêmio 2007 Internet Telephony Excellence Award (Setembro/2007)
  - Internet Telephony Magazine
  - www.itmag.com

"Combatendo SPIT em 10 Lições"

http://www.voipnow.org/2007/04/10_tips_to_filt.html

- ***VoIP Provider Filtering***
- ***Strong Authentication***
- ***Reputation Based Systems***
- ***Central Black Lists***
- ***VoIP SEAL***
- ***Automated Challenge***
- ***VoIP Firewall***
- ***Voice Recognition***
- ***Calling Rate Limit***
- ***Secure Your VoIP***

"Combatendo SPIT em 10 Lições"

- **1/10 :: VoIP Provider Filtering**
  - Alguns provedores VoIP (como Skype e Vonage) mantêm estruturas proprietárias para o tráfego VoIP;
  - Estrutura facilita a aplicação de filtros;
  - Filtros dos provedores VoIP são a primeira linha de defesa !!!

"Combatendo SPIT em 10 Lições"

- **2/10 :: Strong Authentication**
  - Forçar os usuários de VoIP a se submeterem a processos de autenticação antes da realização de chamadas;
  - Uso de relações de confiança;
  - Necessidade de "roubo de identidade" ou criação de identidade falsa para atacantes;
  - Aprovação de lista de solicitações antes de liberação para recebimento de chamada.

"Combatendo SPIT em 10 Lições"

- **3/10 :: Reputation Based Systems**
  - Atribuição de pontuação aos usuários (baseada em histórico do usuário como originador de chamadas);
  - Pontuação negativa em caso de notificação de SPIT;
  - Compartilhamento de "ranking" pelas operadoras;
  - Problemas para novos usuários;
  - Possibilidade de burlar método melhorando pontuação com chamadas entre contas de geradores de SPIT.

"Combatendo SPIT em 10 Lições"

- **4/10 :: Central Black Lists**
  - Uso de sistemas semelhantes as Listas Negras de E-mail;
  - Identificação de números e redes geradoras de SPITs;
  - Lista cresce e evolui de acordo com a abrangência de utilizadores;
  - Também necessária a cooperação entre provedores VoIP.

“Combatendo SPIT em 10 Lições”

- **5/10 :: VoIP SEAL**
  - Uso da solução da NEC e/ou soluções semelhantes de contenção (interceptação) e testes de chamadas;
  - Processo “two-step”;
  - Estabelecimento de grau de suspeita de SPIT;
  - Liberação de acordo com grau de suspeita (configurável);
  - Solução já detalhada.

“Combatendo SPIT em 10 Lições”

- **6/10 :: Automated Challenge**
  - **Baseado no Captcha (solução eficientemente utilizada para evitar acessos a páginas web por mecanismos automáticos);**
  - **Resposta a desafio antes da liberação da chamada;**
  - **Perguntas simples para humanos inviabilizam o SPIT;**
  - **Números com êxitos anteriores podem ser liberados para novas chamadas (não submetidos a novos testes).**

"Combatendo SPIT em 10 Lições"

- **7/10 :: VoIP Firewall**
  - A filtragem de pacotes VoIP pode ser implementada de várias maneiras (inclusive todas elas de uma só vez):
    - Filtragem por endereços de origem;
    - Filtragem por conteúdo;
    - Integração Firewall+IPS;
    - Blacklists, Whitelists, Greylists...

"Combatendo SPIT em 10 Lições"

- **8/10 :: Voice Recognition**
  - Análise da voz do interlocutor;
  - Identificação de parentes, amigos, conhecidos pela comparação de padrões de voz;
  - Soluções como a V-Priorities (Microsoft) garantem 90% de acerto nestes testes.

"Combatendo SPIT em 10 Lições"

- **9/10 :: Calling Rate Limit**
  - Mecanismo leva em conta histórico de chamador e receptores para ajustar taxa de chamada;
  - Interfere diretamente sobre o número de chamadas permitidas a partir de um mesmo chamador;
  - Ao exceder a taxa de limite de chamadas, o chamador tem suas chamadas obstruídas e é submetido a testes específicos para identificá-lo ou não como *SPITTER*

“Combatendo SPIT em 10 Lições”

- **10/10 :: Secure Your VoIP**
  - **Participação do usuário VoIP é fundamental;**
  - **Escolha de provedores com mecanismos de combate a SPIT;**
  - **Pressão para uso de soluções de combate nas instituições;**
  - **Uso de soluções disponíveis (que necessitem da interação com o usuário para instalar/configurar/utilizar).**

Conclusões

- O SPIT é uma ameaça real e merece grande atenção neste momento de consolidação do VoIP;
- Técnicas de combate ao SPAM podem (e devem) ser adaptadas e utilizadas para o combate ao SPIT;
- As técnicas convencionais, porém, não são suficientes;
- A análise de conteúdo é a melhor técnica atual para a identificação e bloqueio do SPIT, porém, não é tão simples quanto a análise de e-mails em busca de SPAM;
- O uso de soluções de retenção de chamadas e análise de conteúdo é a recomendação do momento (retardo da interceptação tem que ser encarado como inevitável).

Centro Federal de Educação Tecnológica do Rio Grande do Norte
Unidade de Ensino Descentralizada de Currais Novos
Departamento Acadêmico em Gestão Tecnológica

SPIT

Spam over Ip Telephony

(A Nova Praga Virtual)

Ricardo Kléber Martins Galvão
rk@cefetrn.br
http://www.ricardokleber.com.br

GTS
Grupo de Trabalho em Segurança

São Paulo, 27/10/2007