GTER
GTS .br

CIDS: Cellular Intrusion Detection System

Sistema de Detecção de Intrusões para Celulares

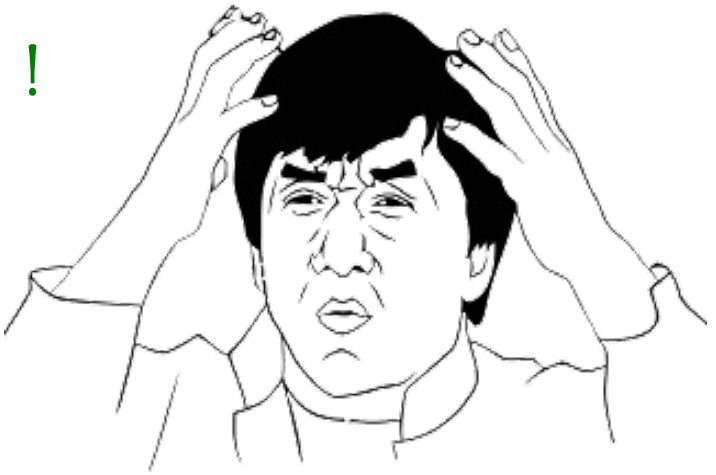
Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System

Contextualizando...

- NIDS presume “grampo” na rede = Fato !
- CIDS é/seria um tipo de NIDS = OK !
- Primeiro (e talvez principal) desafio:

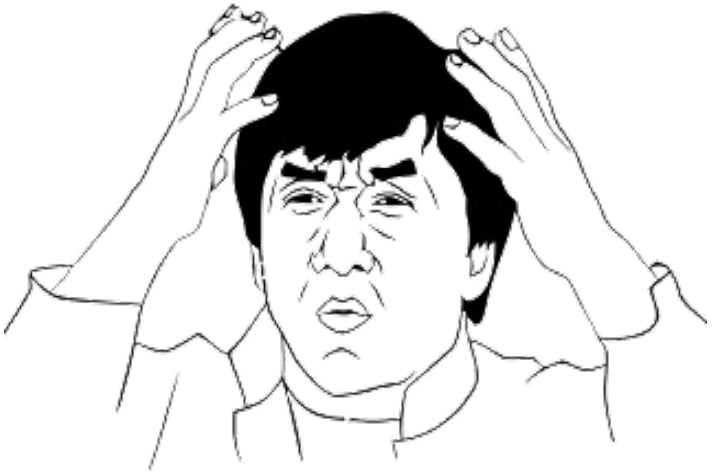


Como “grampear” uma rede de telefonia celular?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System

Contextualizando...



- Do que estamos falando?
  - Captura e análise de tráfego de voz e dados em redes de telefonia celular
- Pra que?
  - Análise no tráfego de dados
    - Malwares (vírus / worms), backdoors, envio “anormal” de dados/informações
    - Busca por padrões (strings e/ou arquivos) no tráfego de dados
  - Análise no tráfego de voz
    - Busca por padrões (citações !?) no tráfego de voz

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
"Grampos" "Oficiais" "Convencionais"

GTER GTS .br

Guardião

- Sistema de escuta telefônica (inclusive celular)
- Fabricante: Digitro (SC)
  - Entre 2002 e 2007 foi adquirido por 12 Estados (RJ, RS, SC, MT, CE, PE, MG, SP, ES, PR, TO e PA), o DF, 04 superintendências da PF (SC, PR, SP e RJ) e pela Procuradoria da República

Fonte:
http://www1.folha.uol.com.br/folha/brasil/ult96u623537.shtml

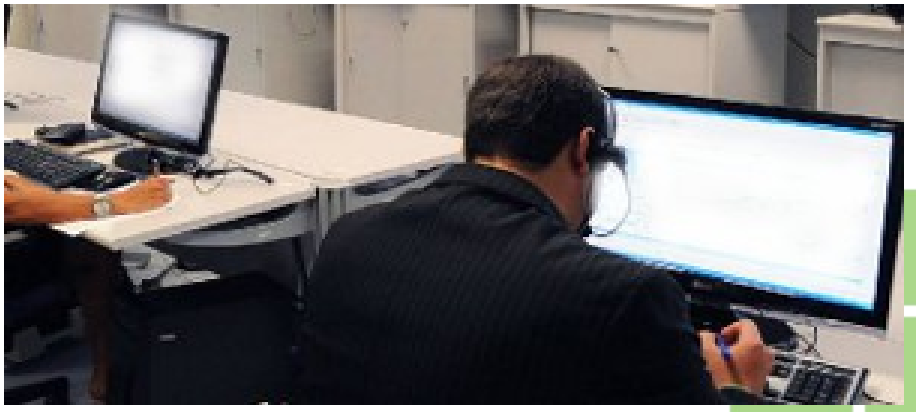
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
"Grampos" "Oficiais" "Convencionais"

Sombra

- Sistema desenvolvido pela Polícia Federal (para não ficar "refém" de empresas)
- Início em 2007

Fonte:
http://www1.folha.uol.com.br/folha/brasil/ult96u623537.shtml



CIDS :: Cellular Intrusion Detection System
"Grampos" "Oficiais" "Convencionais"

GTER GTS .br

SIS = Sistema de Interceptação de Sinais

- Início do planejamento/desenvolvimento: 2010 (implantado em 2012)
- "Menos Burocrático"
- Sistema independente de operadoras de telefonia

  (empresas de telefonia não sabem quem está sendo grampeado)
- Judiciário tem controle informatizado de início e fim de cada escuta

  PF e/ou MP solicitam grampo... juiz autoriza (e monitora) eletronicamente

Fonte: http://www.estadao.com.br/noticias/impresso,novo-esquema-de-escutas-da-pf-deixa-empresas-telefonicas-de-fora,554597,0.htm

Voz e Dados

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
Sistemas Móveis de Interceptação

GTER GTS .br

StingRay

- Também conhecido como:
  - Triggerfish, IMSI Catcher;
    Cell-site Simulator e Digital Analyzer

- Sistema portátil que simula torres falsas de celular para capturar dados de celulares em uma região.
- Fabricação Alemã (Harris Corporation)
- mas vendido nos EUA
  (somente para agências de segurança)

Fonte: http://www.globalresearch.ca/new-hi-tech-police-surveillance-the-stingray-cell-phone-spying-device/5331165

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

StingRay (contramedidas)

- "Hackers" desenvolveram (em 2011) o Catcher Catcher
  - Software que monitora a rede celular em busca de indícios de utilização de StingRays

`http://www.h-online.com/open/news/item/28C3-New-attacks-on-GSM-mobiles-and-security-measures-shown-1401668.html`

CIDS :: Cellular Intrusion Detection System
Análise de Viabilidade

GTER GTS .br

Conclusão:

- Se é possível "grampear" redes celulares (sniffing)...
- ... é possível utilizar um IDS para analisar esse tráfego !!??

Sim !!!

É possível desenvolver um CIDS !!!

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
Análise de Viabilidade

GTER GTS .br

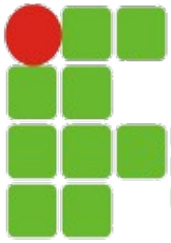
Conclusão:

- Se é possível "grampear" redes celulares (sniffing)...
- ... é possível utilizar um IDS para analisar esse tráfego !!??

É possível desenvolver um CIDS !!!

Mas não é bem assim...

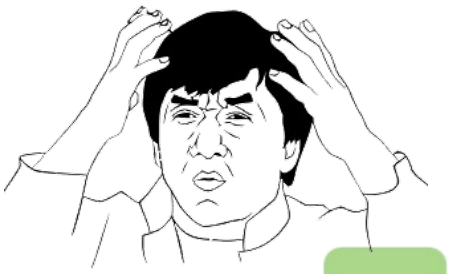
- "grampos" em redes de telefonia celular não são
  - Baratos
  - Acessíveis a "civis"
  - Legalmente autorizados



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
Análise de Viabilidade

- Se “grampos” em redes de telefonia celular não são
  - Baratos...
    - pode-se desenvolver uma solução de baixo custo?
  - Acessíveis a “civis”...
    - pode-se desenvolver uma solução com hardware/software sem restrições de compra/utilização?
  - Legalmente autorizados...
    - pode-se testar/utilizar uma solução com autorização de alguma operadora?



CIDS :: Cellular Intrusion Detection System

Começando a Palestra...

- Você sabe o que é isso?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System

Começando a Palestra...

GTER GTS .br

Femtocell

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

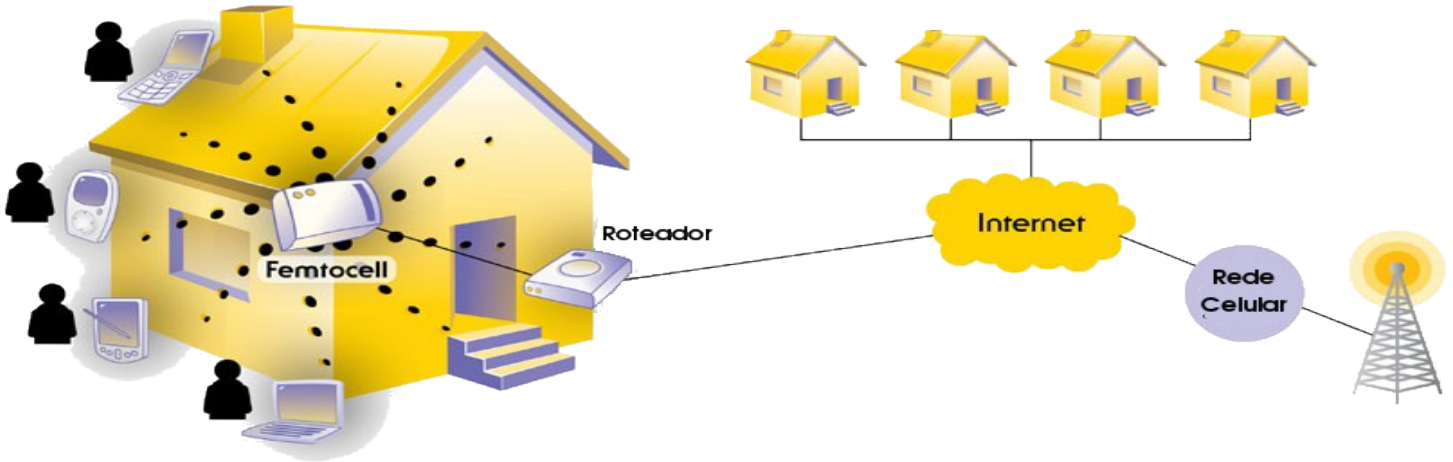
CIDS :: Cellular Intrusion Detection System
Femtocell

- ERB (Estação Rádio-Base) intermediária
  - Posiciona-se entre os aparelhos celulares e as Centrais de Comutação e Controle (CCC) (ou outras ERBs)
  - Também conhecida como Access Point Base Station

Ideal para residências e outros ambientes fechados

CIDS :: Cellular Intrusion Detection System
Femtocell

- Principais Características (1/2)
  - Amplia a área de cobertura "indoor"
  - Solução ideal para regiões de difícil acesso
  - Beneficiam usuários (e operadoras)
  - Conectam-se à rede da operadora através da conexão (banda larga) do ambiente do usuário (ADSL, cabo, etc.)



CIDS :: Cellular Intrusion Detection System
Femtocell

- Principais Características (2/2)
  - Cobertura: 50 a 200 metros;
  - Potência inferior a 1W;
  - Mesmas faixas de frequência das operadoras de celular;
  - Tecnologia: CDMA, GSM e/ou 3G.
- Padrão adotado pelas operadoras
  - Pré-configuradas (usuário não acessa configuração);
  - Gerenciamento e upgrades de software remotos (operadora);
  - Oferta gratuita e/ou com preço subsidiado

CIDS :: Cellular Intrusion Detection System

Femtocell

- Principais Desafios / Discussões
  - Usuário pode adquirir seu próprio femtocell?
    - A utilização, atualmente, está condicionada à oferta e autorização da operadora (e liberação pela agência reguladora)
  - Usuários externos (vizinhos p.ex.) podem usufruir de femtocell sem autorização explícita (sendo usuário da mesma operadora, p.ex.)?
    - Operadoras divergem sobre esse assunto
- Já em uso em vários países:
  - EUA: Sprint, AT&T, Comcast, ~~T-Mobile~~ e Verizon
  - Reino Unido: Vodafone
  - Japão: Softbank
- E no Brasil?
  - Anatel publicou regulamentação em 04/11/2013

CIDS :: Cellular Intrusion Detection System

Voltando à pergunta-chave...

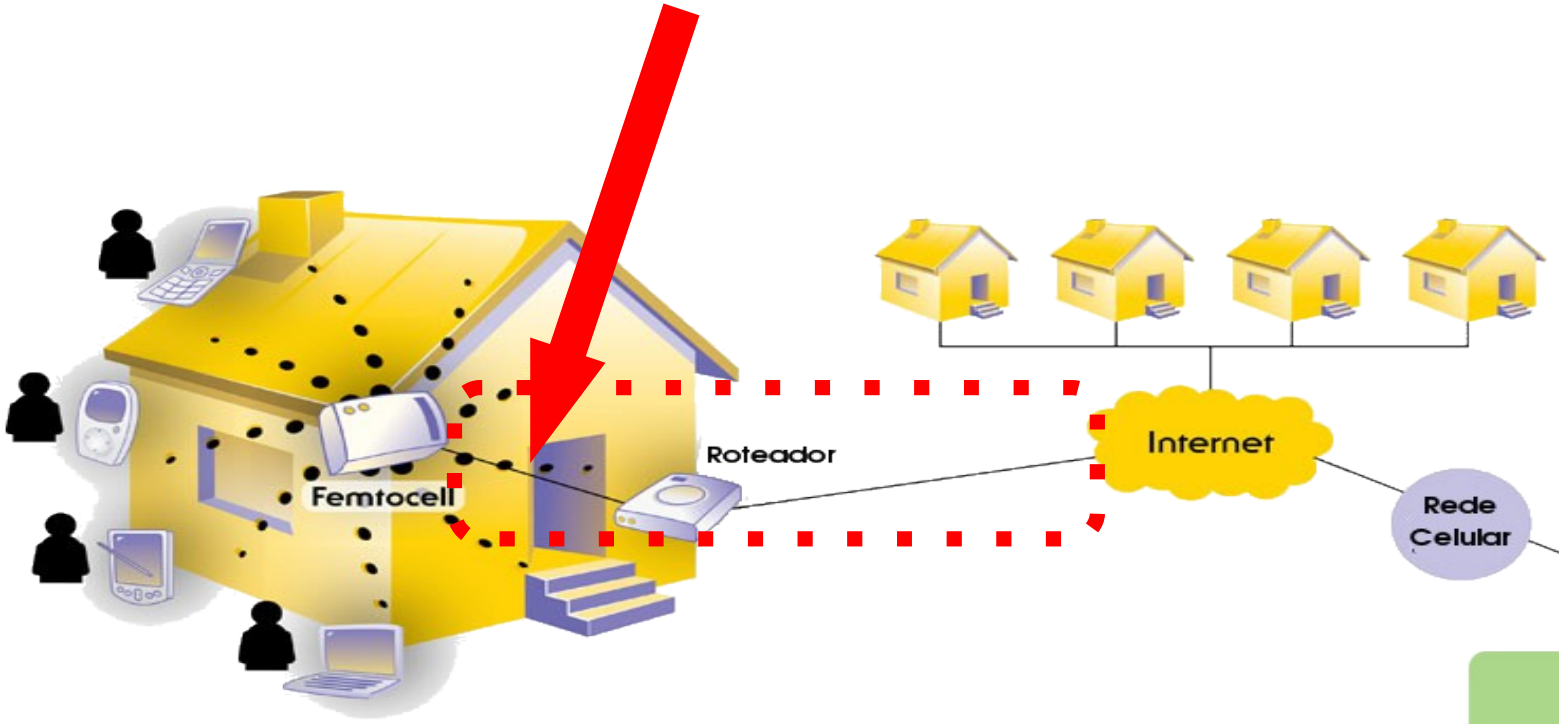
Como "grampear" uma rede de telefonia celular?

CIDS :: Cellular Intrusion Detection System

Onde instalar o "grampo"?

- (1) Entre o femtocell e a rede celular
  - Preferencialmente antes do roteador de acesso (banda larga)

É possível visualizar o tráfego ???



CIDS :: Cellular Intrusion Detection System
Onde instalar o "grampo"?

- (1) Entre o femtocell e a rede celular
  - Preferencialmente antes do roteador de acesso (banda larga)

É possível visualizar o tráfego ???

- Femtocell usa mecanismos/protocolos de segurança comumente utilizados nos sistemas celulares
  - GSM utiliza o protocolo EAP-SIM
    - Estabelece um túnel IPSec (VPN) até o gateway da rede celular
  - UMTS e CDMA 2000 utiliza o protocolo EAP-AKA
    - Baseia-se no mecanismo de autenticação e troca de chaves AKA
    - Gera chaves de sessão mais longas (128bits)
    - Usa um vetor de autenticação gerado a cada processo de autenticação (e mecanismo de re-autenticação)

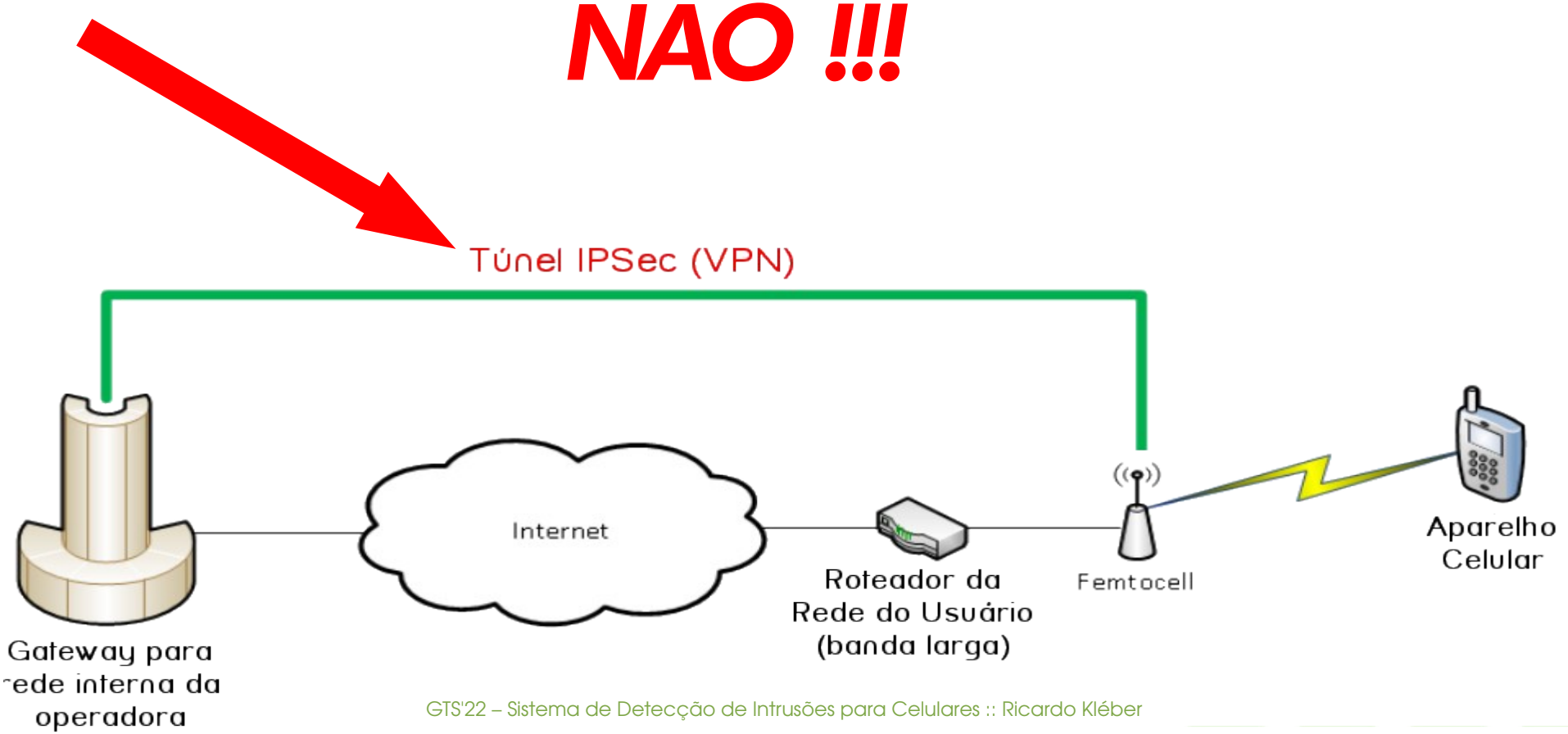
CIDS :: Cellular Intrusion Detection System

Onde instalar o "grampo"?

- (1) Entre o femtocell e a rede celular
  - Preferencialmente antes do roteador de acesso (banda larga)

É possível visualizar o tráfego ???

NÃO !!!



CIDS :: Cellular Intrusion Detection System

Tráfego encriptado (tunelado com IPSec)

No.	Time	Source	Destination	Protocol	Length	Info
386	15:58:38.554631	192.168.1.205	[redacted]	DNS	75	Standard query 0xbae1 A sg.vzwfemto.com
387	15:58:38.560447	[redacted]	192.168.1.205	DNS	161	Standard query response 0xbae1 A 66.174.71
454	15:58:53.370356	192.168.1.205	66.174.71.40	ISAKMP	390	IKE_SA_INIT
458	15:58:53.515946	66.174.71.40	192.168.1.205	ISAKMP	346	IKE_SA_INIT
459	15:58:53.538819	192.168.1.205	66.174.71.40	ISAKMP	314	IKE_AUTH
463	15:58:53.659664	66.174.71.40	192.168.1.205	ISAKMP	170	IKE_AUTH
464	15:58:53.661494	192.168.1.205	66.174.71.40	ISAKMP	154	IKE_AUTH
468	15:58:53.830477	66.174.71.40	192.168.1.205	ISAKMP	186	IKE_AUTH
469	15:58:53.834024	192.168.1.205	66.174.71.40	ISAKMP	170	IKE_AUTH
470	15:58:53.997153	66.174.71.40	192.168.1.205	ISAKMP	122	IKE_AUTH
471	15:58:53.998971	192.168.1.205	66.174.71.40	ISAKMP	138	IKE_AUTH
475	15:58:54.128699	66.174.71.40	192.168.1.205	ISAKMP	282	IKE_AUTH
500	15:58:56.767191	192.168.1.205	66.174.71.40	ESP	142	ESP (SPI=0x9e59ca8d)
502	15:58:56.930664	66.174.71.40	192.168.1.205	ESP	254	ESP (SPI=0x6a5005e9)

```
▷ Internet Protocol Version 4, Src: 192.168.1.205 (192.168.1.205), Dst: 66.174.71.40 (66.174.71.40)
▽ User Datagram Protocol, Src Port: 4500 (4500), Dst Port: 4500 (4500)
    Source port: 4500 (4500)
    Destination port: 4500 (4500)
    Length: 100
  ▷ Checksum: 0x0000 (none)
  UDP Encapsulation of IPsec Packets
▽ Encapsulating Security Payload
    ESP SPI: 0x9e59ca8d (2656684685)
    ESP Sequence: 1
```

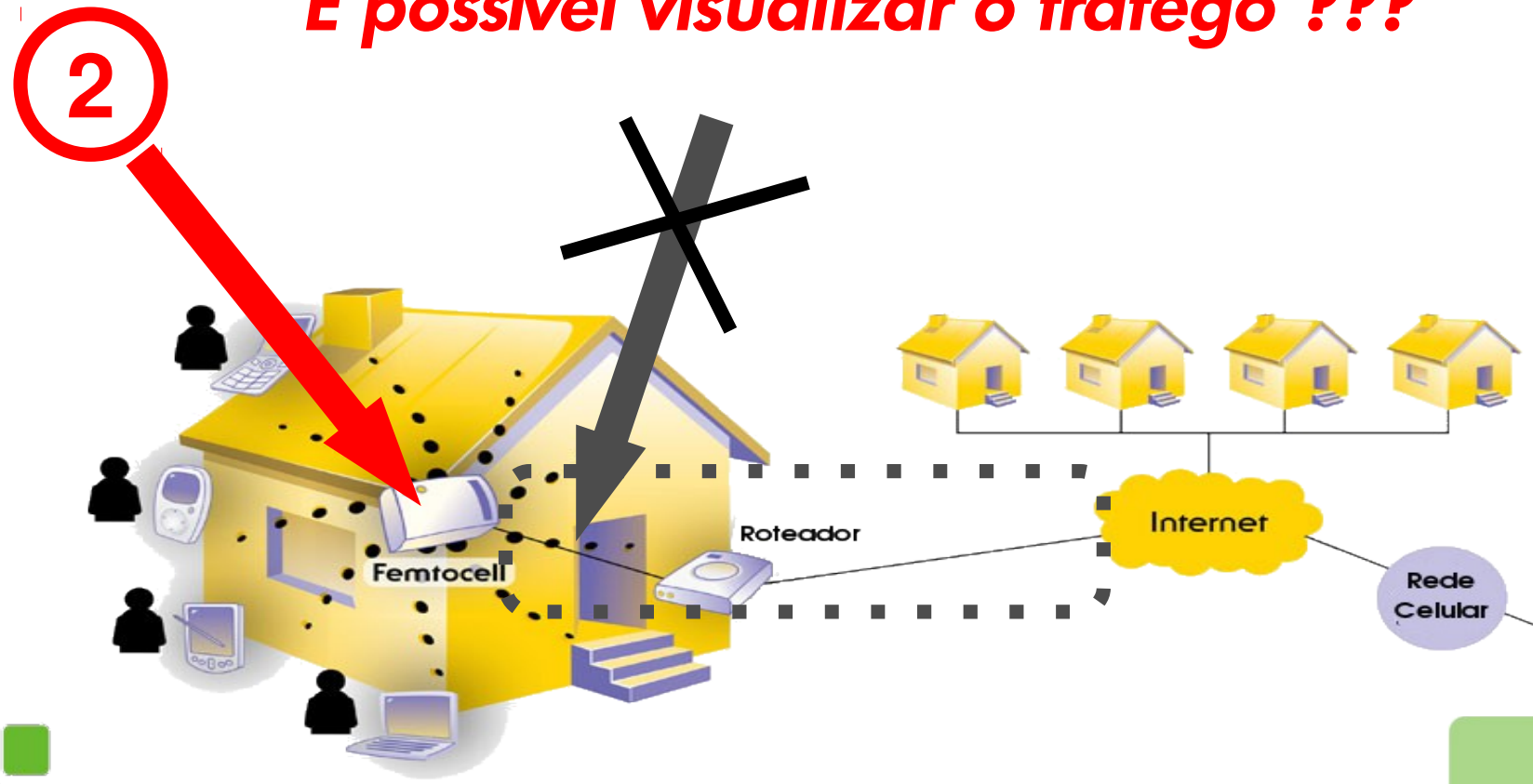
```
0020  47 28 11 94 11 94 00 64  00 00 9e 59 ca 8d 00 00   G(.....d ...Y....
0030  00 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 7d e6 d9 ff 95 39  fb 7f c9 90 c7 75 fb 1b   ..}....9 .....u..
0050  6f a8 7a e2 ca 27 64 21  81 a4 91 5c 2f 1e c5 31   o.z..'d! ...\/..1
```

CIDS :: Cellular Intrusion Detection System

Onde instalar o "grampo"?

- (2) A partir do próprio Femtocell
  - Antes da encriptação dos dados (entrada do "túnel")

É possível visualizar o tráfego ???

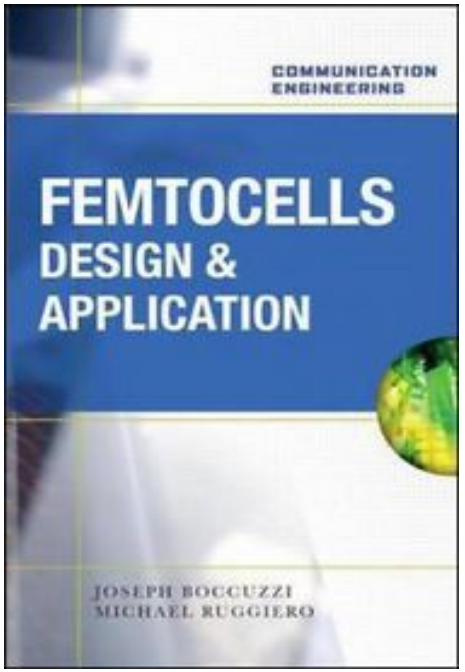


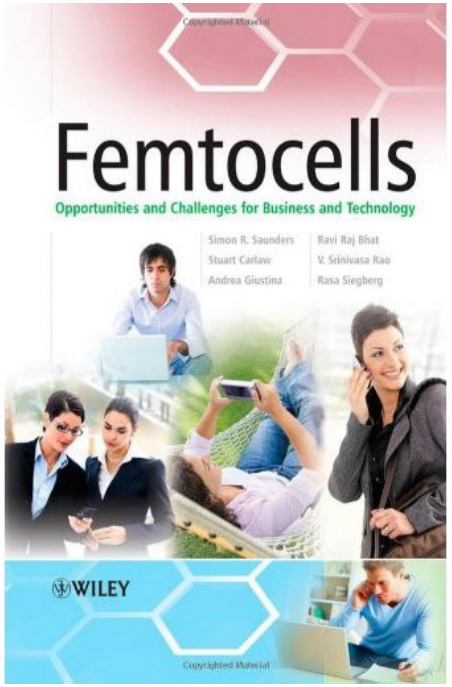
CIDS :: Cellular Intrusion Detection System

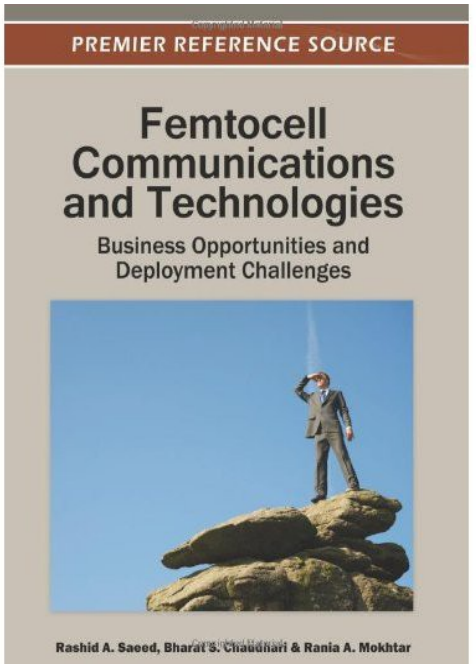
Instalando o "grampo" no Femtocell

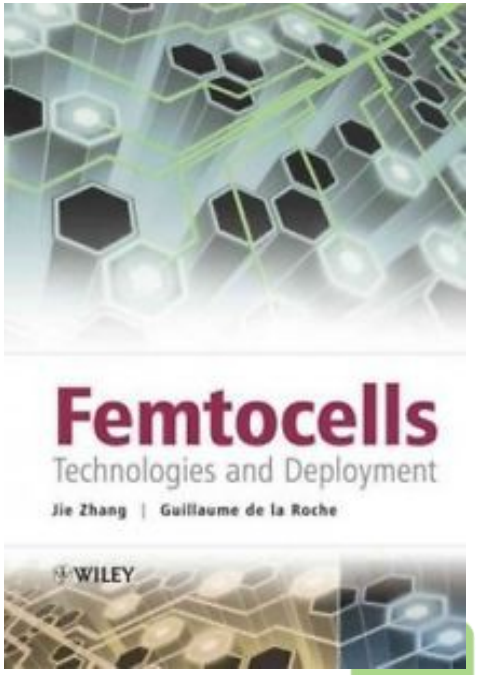
GTER GTS .br

Pra mexer... tem que conhecer...









INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System

Instalando o "grampo" no Femtocell

01) Com o auxílio/autorização da operadora

02) Instalando/configurando o próprio Femtocell

03) Encontrando (e explorando) uma vulnerabilidade no Femtocell

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
Explorando uma vulnerabilidde no Femtocell

- Traffic Interception & Remote Mobile Phone Cloning with a Compromised CDMA Femtocell
  - Doug DePerry | @dugdep
  - Tom Ritter | @TomRittervg
  - Andrew Rahimi

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System
Explorando uma vulnerabilidde no Femtocell

GTER GTS .br

Case da Empresa iSECpartners

iSECpartners part of nccgroup

- Modelo especifico utilizado pela operadora Verizon (EUA)
  - Verizon Network Extenders
    - Samsung SCS-26UC4 e SCS-2U01

- Patch de correção já disponibilizado pela empresa
- Empresa (Verizon) autorizou a iSEC a utilizar o Femtocell sem o patch aplicado e realizar a demonstração
- Após hacking no Femtocell a empresa demonstrou com sucesso:
  - Acesso a chamadas telefônicas
  - Acesso a mensagens SMS trocadas
  - Acesso a mensagens MMS trocadas
  - Ataques Man-In-The-Middle
  - Ataques SSL Stripping
  - Clonagem de Aparelhos

CIDS :: Cellular Intrusion Detection System
Explorando uma vulnerabilidde no Femtocell

Case da Empresa iSECpartners

- Processador Faraday FA626TE ARM v5TE
- Placa Samsung UCMB
- Memória Flash OneNAND
- Antenas GPS e CDMA (2G/3G)
- Porta Ethernet
- Porta HDMI

- Acesso via HDMI (console) | Interrupção do boot e alteração de parâmetros
- Vulnerabilidade: Acesso root via console
- Ativação de acesso SSH como root
- Desativação de regras Iptables
  - Maior Desafio: QuickSec VPN Client
    - Inserido como módulo do kernel (impede exibição de pacotes)
    - Objetivo do “hacking”: Capturar e disponibilizar pacotes antes da encriptação

CIDS :: Cellular Intrusion Detection System
Explorando uma vulnerabilidde no Femtocell

GTER GTS .br

iSECpartners part of nccgroup

Case da Empresa iSECpartners

https://www.isecpartners.com/blog/2013/august/femtocell-presentation-slides-videos-and-app.aspx

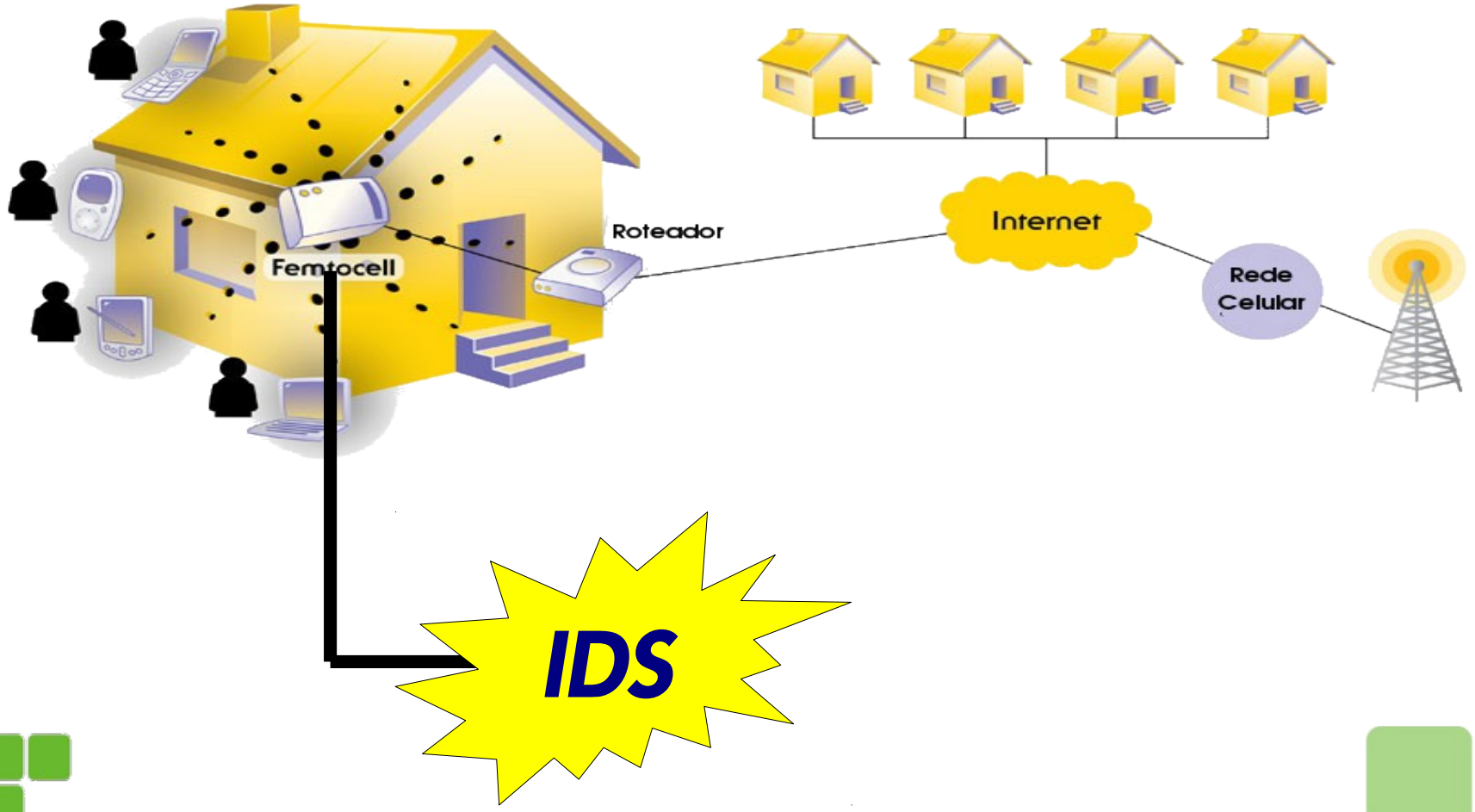
- Vídeo da Interceptação Telefônica:
  - **http://www.youtube.com/watch?v=3FyNB4QmY1Q**
- Vídeo da Interceptação de Mensagens SMS:
  - **http://www.youtube.com/watch?v=R-4fkJiVeE4**
- Vídeo da Interceptação de Mensagens MMS:
  - **http://www.youtube.com/watch?v=uuwsMsvGAYo**
- Vídeo de Ataque Ativo a Tráfego de Dados:
  - **http://www.youtube.com/watch?v=2xjhtDobO8c**
- Vídeo de Clonagem de Equipamento Celular sem Acesso Físico:
  - **http://www.youtube.com/watch?v=Ydo19YOzpzU**

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System

Após definição do local/estratégica do "grampo"...

E o IDS !!??



CIDS :: Cellular Intrusion Detection System
Estrutura do IDS em um Sistema Celular

Artigo escrito pela empresa LMG Security

www.LMGsecurity.com

- Do-It-Yourself Cellular Intrusion Detection System
  - Sherri Davidoff;
  - David Harrison;
  - Randi Price;
  - Scott Fretheim
- Mesmo modelo/operadora explorados pela iSEC = Verizon (EUA)
  - Verizon Network Extenders
- Integração do Femtocell modificado com o Snort IDS
- Infecção (proposital) de Aparelho com Malware
- Captura de tráfego (Femtocell), análise e detecção (IDS)
  - Regra Snort identificou malware implantado

http://lmgsecurity.com/whitepapers/DIY-Cellular-IDS_2013-08-01.pdf

CIDS :: Cellular Intrusion Detection System

Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Malware testado (usado p/infectar celular)
  - Android.Stels Trojan
  - **http://contagiominidump.blogspot.com**
- Assinatura (Snort) desenvolvida a partir da análise do malware
  - Relatório (detalhado) da Dell SecureWorks sobre o malware
  - **http://www.secureworks.com/cyber-threat-intelligence/threats/stels-android-trojan-malware-analysis**
  - Relatório da Symantec sobre o malware
  - **http://www.symantec.com/security response/writeup.jsp?docid=2013-032910-0254-99&tabid=2**

CIDS :: Cellular Intrusion Detection System
Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Regras Snort (específicas para identificar o malware)
  - Comunicação/Tráfego C&C

```
alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels
Possible CnC Server Traffic (95.211.216.148)"; content:"|5fd3d894|";
classtype:trojan-activity; reference:url, www.secureworks.com/ cyber-
threat-intelligence/threats/stels-android-trojan-malware-analysis/;
sid:2000007; rev:1;)

alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels
Possible CnC Server Traffic (31.170.161.216)"; content:"|1FAAA1D8|";
classtype:trojan-activity; reference:url, www.secureworks.com/cyber-
threat-intelligence/threats/stels-android-trojan-malware-analysis/;
sid:2000008; rev:1;)
```

CIDS :: Cellular Intrusion Detection System
Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Regras Snort (específicas para identificar o malware)
  - Acesso a domínios notadamente maliciosos

```
alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels Malicious
Domain (ynfdbdybdd1.freeiz.com)"; content:"ynfdbdybdd1.freeiz.com";
classtype:trojan-activity; reference:url, www.secureworks.com/ cyber-
threat-intelligence/threats/stels-android-trojan-malware-analysis/;
sid:2000010; rev:1;)

alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels Malicious
Domain (androidflashplayer.net.ua)"; content:"androidflashplayer.net.ua";
classtype:trojan-activity; reference:url, www.secureworks.com/cyber-
threat-intelligence/threats/stels-android-trojan-malware-analysis/;
sid:2000009; rev:1;)
```

CIDS :: Cellular Intrusion Detection System
Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Regras Snort (especificas para identificar o malware)
  - Assinatura do Malware (payload) [42bytes]

```
alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels
Known Malware Binary Snippet (first 42 bytes)"; content:"|50 4B 03
04 14 00 08 08 08 00 52 36 61 42 00 00 00 00 00 00 00 00 00 00 00
00 16 00 04 00 61 73 73 65 74 73 2F 68 74 6D 6C 2F 69 6E 64 65 78
2E 68 74 6D 6C FE CA 00 00 35 8E 4F 4B C3 40 10 C5 EF 85|";
classtype:trojan-activity; reference:url, www.secureworks.com/
cyber-threat-intelligence/threats/stels-android-trojan-malware-
analysis/; sid:2000013; rev:1;)
```

CIDS :: Cellular Intrusion Detection System
Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

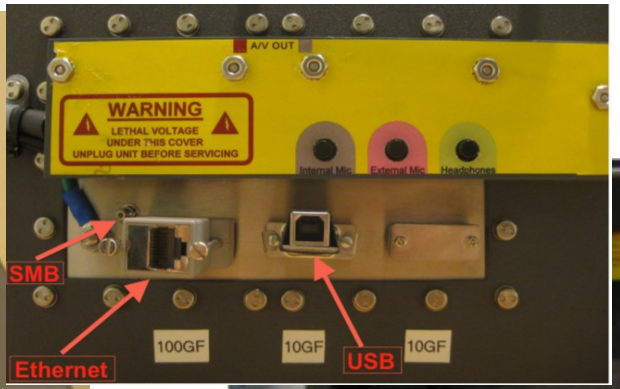
- Regras Snort (específicas para identificar o malware)
  - Busca por nome (padrão) do malware

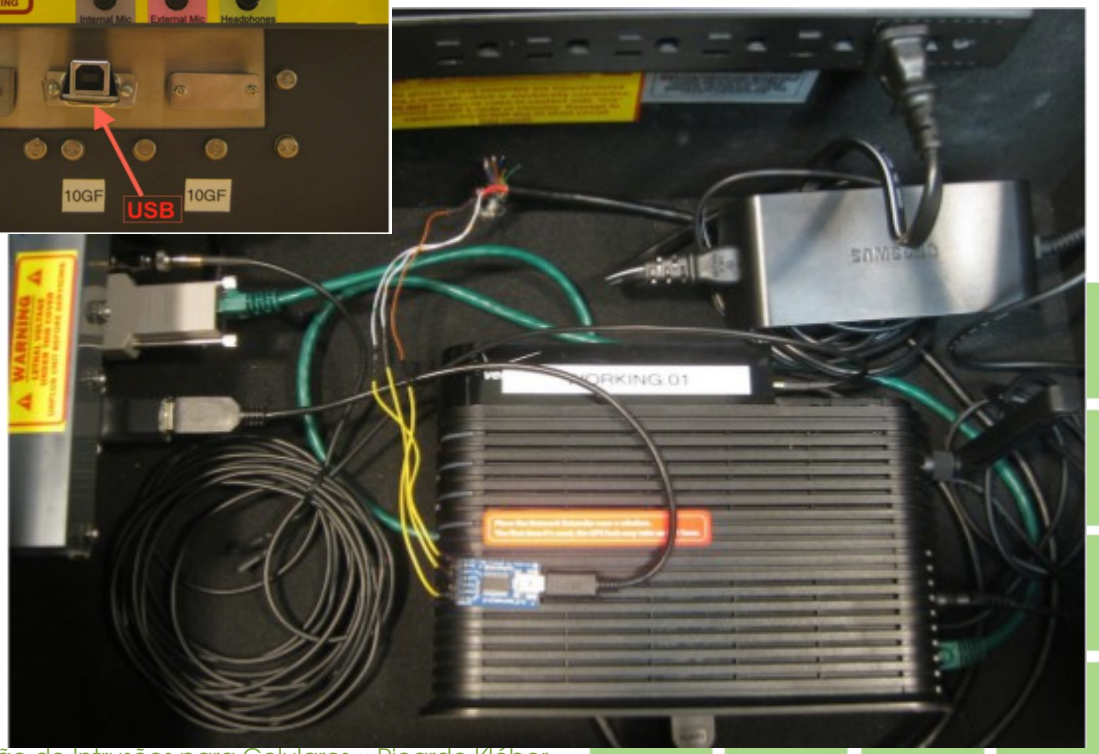
```
alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels Malicious
Domain (ynfdbdybdd1.freeiz.com)"; content:"ynfdbdybdd1.freeiz.com";
classtype:trojan-activity; reference:url, www.secureworks.com/ cyber-
threat-intelligence/threats/stels-android-trojan-malware-analysis/;
sid:2000010; rev:1;)

alert ip any any -> any any (msg:"MOBILE_MALWARE Android/Stels Malicious
Domain (androidflashplayer.net.ua)"; content:"androidflashplayer.net.ua";
classtype:trojan-activity; reference:url, www.secureworks.com/cyber-
threat-intelligence/threats/stels-android-trojan-malware-analysis/;
sid:2000009; rev:1;)
```

CIDS :: Cellular Intrusion Detection System
Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Ambiente Controlado utilizado na pesquisa
  - Câmara de ensaio blindada STE3000-FAV (Ramsey Electronics)





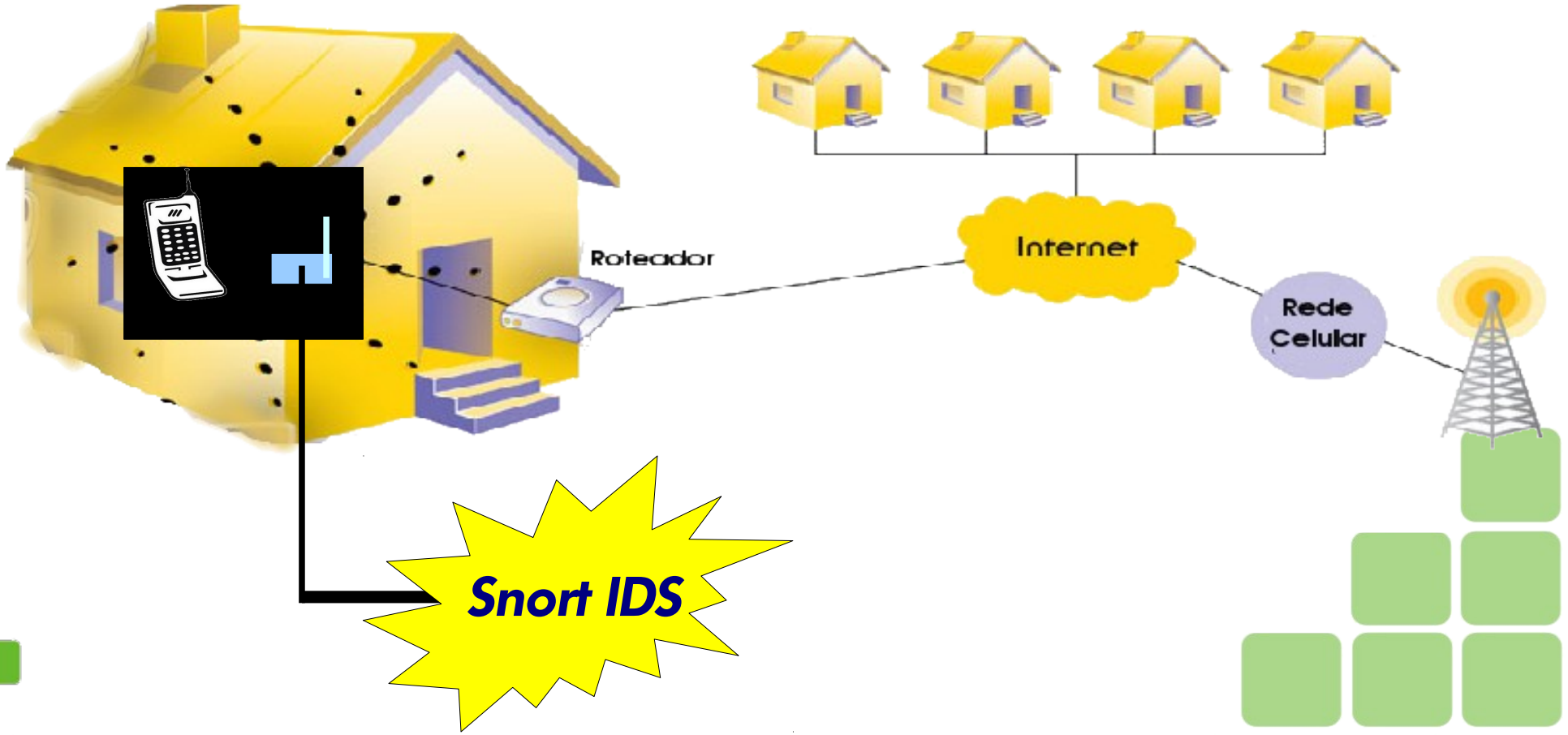
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

CIDS :: Cellular Intrusion Detection System

Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Ambiente Controlado utilizado na pesquisa



CIDS :: Cellular Intrusion Detection System

Estrutura do IDS em um Sistema Celular

Do-It-Yourself Cellular Intrusion Detection System

- Exemplos de Logs Gerados pelo Snort

```
[1:2000010:1] MOBILE_MALWARE Android/Stels Malicious Domain (ynfdbdybdd1.freeiz.com)
[1:2000012:1] MOBILE_MALWARE Android/Stels Known Malware Filename (flashplayer.android.update.apk)
[1:2000000:1] MOBILE_MALWARE Android/Stels botId Phone Home to CnC Server
[1:2000009:1] MOBILE_MALWARE Android/Stels Malicious Domain (androidflashplayer.net.ua)
[1:2000013:1] MOBILE_MALWARE Android/Stels Known Malware Binary Snippet (first 42 bytes)
[1:2000001:1] MOBILE_MALWARE Android/Stels RemoveAllSmsFilters Command From CnC Server
[1:2000008:1] MOBILE_MALWARE Android/Stels Possible CnC Server Traffic (31.170.161.216)
[1:2000006:1] MOBILE_MALWARE Android/Stels POST From Infected Client
[1:2000007:1] MOBILE_MALWARE Android/Stels Possible CnC Server Traffic (95.211.216.148)
```

```
[**] [1:2000012:1] MOBILE_MALWARE Android/Stels Known Malware Filename (flashplayer.
android.update.apk) [**] [Classification: A Network Trojan was detected] [Priority: 1]
07/11-16:52:48.957056 10.184.98.60 -> 10.211.157.205 GRE TTL:64 TOS:0x0 ID:0 IpLen:20
DgmLen:157 DF
```

CIDS :: Cellular Intrusion Detection System

Conclusões

- Sim!!! é possível instalar um CIDS
- O “elo mais fraco” é o Femtocell
  - O “grampo” só pode ser instalado a partir do hacking desse componente
- Pesquisas com CIDS não são brincadeiras de hacking
  - O potencial de colaboração da academia é imenso

Pra pensar...

- Nos EUA já se fala em abolir o uso de Femtocells...
- ... no Brasil as operadoras vão começar a utilizar agora.

CIDS :: Cellular Intrusion Detection System

Slides Disponíveis

www.ricardokleber.com

Palestras:
www.ricardokleber.com/palestras

Vídeos:
www.ricardokleber.com/videos

Twitter:
www.twitter.com/ricardokleber

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE