

# TRABALHO 9

Segurança no GSM



Aníbal Afonso Lima Bezerra Alves  
A70859

# GSM – AS MAIORES FALHAS

- Após a leitura do artigo fornecido, foi possível identificar as falhas existentes numa arquitetura GSM e de que forma os atacantes podem explorar essas falhas.
- A maioria destas falhas acontecem ao nível de *software* pois para alterar o *hardware* seria necessário que os atacantes se deslocassem ao local das estações base, ou dos *switching center*, o que não seria tão fácil.

# GSM – ESTABELECIMENTO DE CHAMADA

- Normalmente, o telemóvel está sempre em comunicação com a estação base mais próxima. Essa estação base concorda em ser o intermediário entre o telemóvel e a rede.
- A estação base comunica com uma estação base com a funcionalidade de alocar os canais rádio e coordenar os *handovers* entre as estações base.
- Esta estação por sua vez comunica com o *mobile switching center* e esta vai comunicar com a rede de modo a fazer o processo inverso para estabelecer a comunicação entre os dois terminais móveis.

# GSM – AS MAIORES FALHAS

- As maiores falhas do sistema GSM são:
  - As chamadas telefónicas apenas são encriptadas entre o terminal móvel e a estação base, sendo depois enviados sem encriptação pela rede. A segurança por meio de encriptação também deveria ser garantida na comunicação entre a rede.
  - O facto do sistema RES poder ser utilizado sem o IMS, pois se fossem utilizados em conjunto facilitaria a deteção de escutas ilegais.
  - O utilizador autentica-se a ele próprio numa rede GSM.

- O AXE permite instalar novo *software* sem atualizar o sistema atual, sendo por vezes uma vantagem, também tem desvantagens. No artigo referido, os atacantes utilizaram este facto para conseguirem alterar e esconder o seu ataque na rede.
- A não existência de backup's da informação produzida, como logs e reports.
- Não existência de protocolos que verifiquem o código executado nas estações base, podendo assim ser introduzido código malicioso.

# HOW FREQUENTLY DO YOU THINK THE SECURITY BARRIERS OF THE GSM NETWORKS ARE BROKEN?

- Os ataques à rede GSM são frequentes dado a informação preciosa que pode ser obtida por este meio, apesar de poucos serem de conhecimento público, pois ninguém gosta de ter a sua privacidade invadida.
- O número de tentativas também advém do facto dos *softwares* serem open-source, o que torna possível todos terem acesso aos mesmos.