THE ATHENS AFFAIR

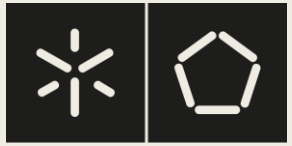
- Rui Freitas, a84121

The Athens Affair

Universidade do Minho
Escola de Engenharia

- **The Athens Affair** é o nome dado ao escândalo ocorrido em 2004/2005 que envolveu a operadora **Vodafone Greece** e utilizadores desta que ocupavam altos cargos do governo incluindo o primeiro ministro e a sua família.
- Através de monitorização ilegal das redes celulares um grupo de hackers teve acesso a conversas privadas sobre assuntos privados relativos ao governo grego.

Origem do escândalo



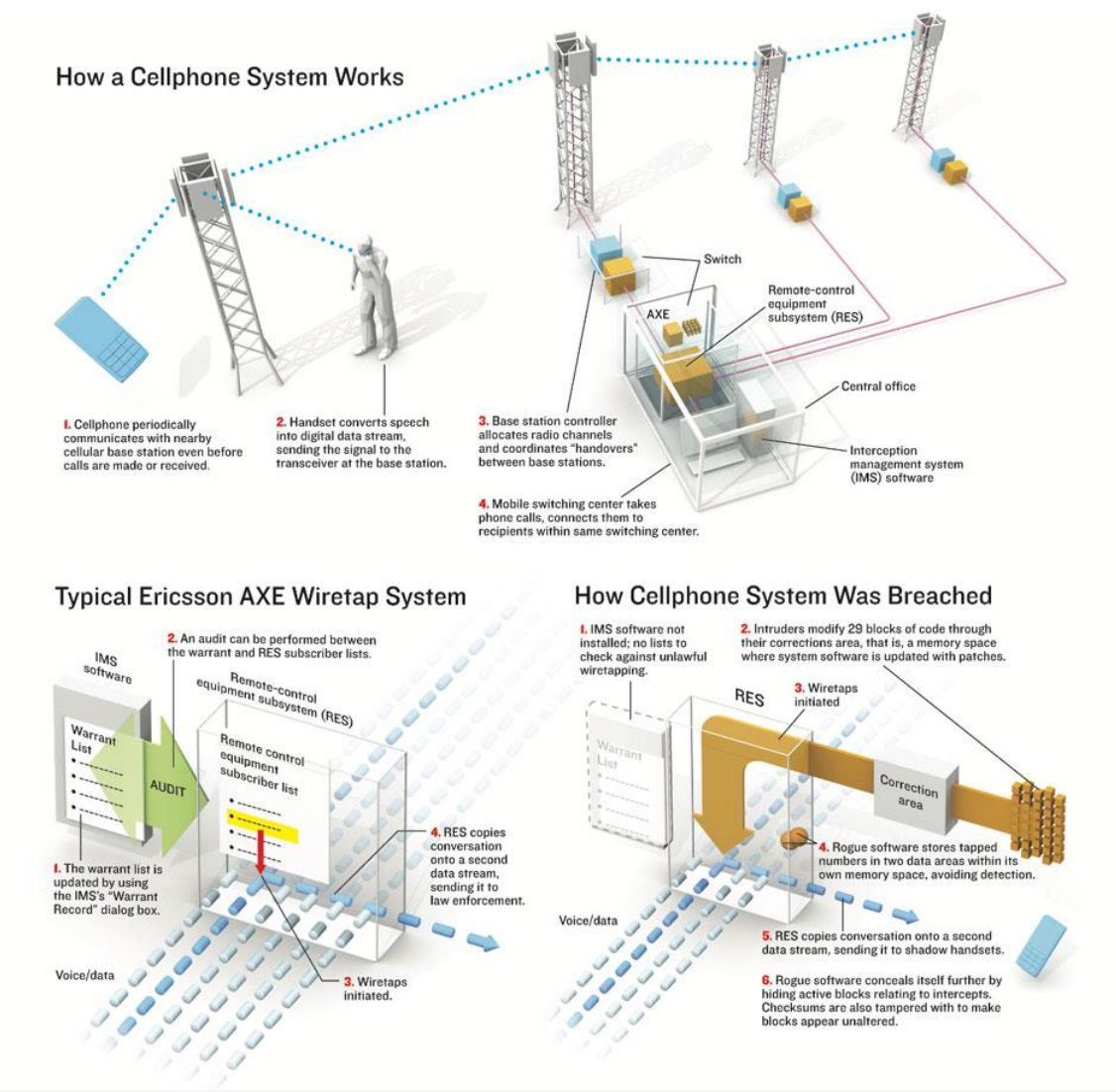
Universidade do Minho
Escola de Engenharia

- Pensa-se que tudo terá começado em 2004, antes do jogos olímpicos de Atenas. No entanto só se veio a descobrir em meados de janeiro do ano seguinte.
- A descoberta deu-se através do controlo de erros de *switches* cujo trabalho é estabelecer a ligação entre 2 telemóveis. Na altura a **Vodafone** pensou que o erro seria dos *switches* e por isso contactou a empresa que os fornecia, a **Ericsson**.
- 5 semanas após estes erros terem sido descobertos a empresa Ericsson alertou a Vodafone de que um software não autorizado teria sido instalado.
- No dia seguinte o CEO da Vodafone Greece ordenou os técnicos a remover o software maligno o que veio fazer com que não fosse possível a descoberta de quem estava por detrás do sucedido.

Como foi modificado o sistema (1)

Universidade do Minho
Escola de Engenharia

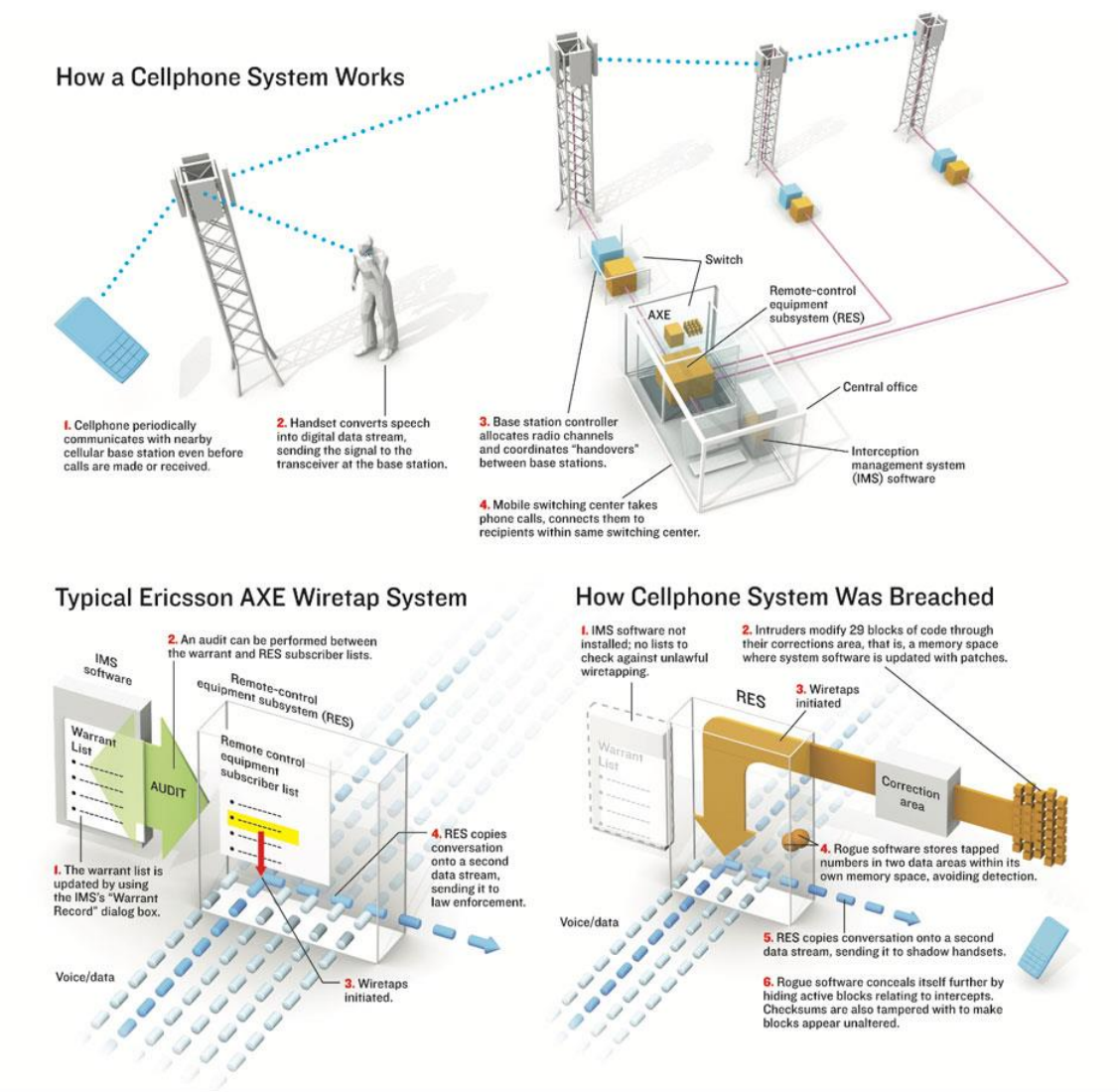
- Para perceber como foi possível os hackers terem acesso às ligações é necessário perceber como é que estas funcionam.
- Em primeiro lugar após a estação mais próxima confirmar a ligação é transformada a *stream* de voz numa *stream* de dados digital.
- As atividades da estação base são geridas por uma estação controladora que tem como principal objetivo controlar os canais rádio e a transferência entre os *transceivers*.
- Este controlador para além disso comunica com um centro de ***switching*** que recebe chamadas e que as conecta a recetores.



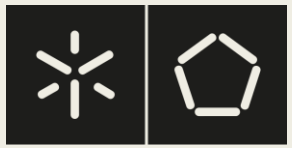
Como foi modificado o sistema (2)

Universidade do Minho
Escola de Engenharia

- Os centros de *switching* são particularmente importantes para o Athens Affair pois era nestes que estava presente o software.
- Na figura podemos observar o **sistema AXE da Ericsson** onde um processador central coordena as operações do *switch*. A chave importante para perceber como foi realizado o ataque é o método '***wiretaps***'.
- Este método consiste na intervenção de um agente de autoridade tendo acesso a todas as chamadas realizadas por um individuo.
- Foi desta forma que os atacantes conseguiram ouvir e talvez gravar todas as conversas realizadas.



Análise ao software dos atacantes



Universidade do Minho
Escola de Engenharia

- O software utilizado pelos atacantes era difícil de detetar internamente pois guardava os dados dentro do seu espaço de memória sendo impercetível aos *switches* qualquer alteração.
- No entanto este era detetável por parte de técnicos da Vodafone caso estes tivessem realizado uma procura pelos vários processos ativos e iriam encontrar um processo suspeito em execução. Para além disso é usual os técnicos procurarem por bloqueios antes de realizar uma atualização, o que não aconteceu.
- Este software foi finalmente descoberto quando os atacantes realizaram um *update* que interferiu no encaminhamento de mensagens que originou erros descobertos pela Vodafone. Isto faz perceber o quão importante é a utilização de ficheiros log.

Quem foi responsável pelo ataque?

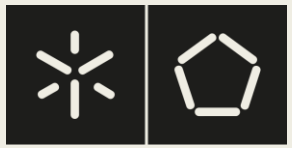
Universidade do Minho
Escola de Engenharia

- Primeiro pensou-se que fosse obra de trabalhadores da Vodafone no entanto não foi possível chegar a tal conclusão. Esta acusação deveu-se ao facto de o diretor de planeamento de redes ter-se suicidado um dia após a descoberta do escândalo. Outra hipótese seria de trabalhadores da Ericsson pois a Vodafone utilizava grande parte do hardware e software da empresa.
- Outra hipótese ainda foi de que se tratava de um trabalho por parte do governo americano visto que as localizações dos telefones monitorizados tinham correlação direta com apartamentos e outras propriedades sob controlo da embaixada americana na Grécia.

vodafone

ERICSSON

O que podemos retirar deste ataque



Universidade do Minho
Escola de Engenharia

- Um dos grandes erros por parte da Vodafone no controlo deste ataque foi não ter realizado técnicas de defesa que permitissem investigar a origem do ataque pois ao terem agido como agiram para além de não ser possível descobrir os culpados também lhes deram tempo para fugirem sem qualquer rasto.
- É normal que países em que estes ataques são raros a equipa que tiver de agir não seja tão experiente pelo que fazia mais sentido existir uma entidade global que pudesse intervir caso algo similar acontecesse.

THE ATHENS AFFAIR

- Rui Freitas, a84121