Memorandum

To:

From:

Date: 15th March, 2010

Re: Persuasive Essay

The essay's target audience is readers of *The Guardian* newspaper.

It is about the issue of G.S.M security and how Karsten Nohl has found a way to listen in on other people's mobile pho ne calls. I will be **agreeing** that Nohl's research is important and necessary.

Shonak

Persuasive Essay

So you're on your mobile phone to your bank discussing changing your account details. The next day you find that a fraudulent transaction was made u nder that same account. What happened? Welcome to what is likely to be an unexpected twist in the practicality of using mobile phones, where the intrusion of mobile phone conversations could become as commonplace as security threats on your computer. And what's worse about it is: there's little you can do to defend yourself. Research conducted by German computer scientist Karsten Nohl suggests giving tools to customers in order to research more into the issues with GSM (Global System for Mobile Communicati ons, the standard of which most mobiles phone use). Whilst some may deem research of this kind 'illegal', I believe it is imperative that this research is undertaken to better understand the vulnerabilities in GSM.

GSM is a standard of mobile communic ation which was developed and implemented into mobile phone technology in 1988. The information transmitted is encrypted with an algorithm known as the A5/1 function that uses a 64 bit key to provide privacy to the calls one makes from their mobile phone. In December 2009, Karsten Nohl broke the encryption of this function using a table of functions (called rainbow tables), to allow him to listen in on people's phone calls.

It is important to understand the wider significance of the problem. Issues with co mputer security today in businesses, public institutions, and even governments would become trivial compared to the highly worrying concern of widespread usage of the technology developed to break GSM technology. Another issue is the scale of phones potentially at risk. The fact that most major mobile phone operators around the world are affected and that "approximately 80%" (Anon, n.d) of mobile phones on these networks use the GSM technology, there is clearly a very large scope for breach of privacy among st many consumers.

With the scale of the security hole so widespread, it's fundamental that adequate research is undertaken in order to resolve it. It would only be a matter of time until a team of hackers decrypt the 22 year old G.S.M. technology and subs equently misuse it for intercepting private (and potentially significant) communication. The founders of G.S.M have been given a n opportunity to work alongside Nohl in avoiding this situation and co - ordinating with other researchers to truly scrutinise the effectiveness of the A5/1 security

specification, by making the tools more widespread to the public. Though instead, they deem the work "highly illegal" (Kang, 2010), yet there is no example, evidence or explanation as to how any legislation is being broken.

Some critics of Nohl's research team may argue that the further research that he and his team intend on taking is unethical, due to the fact that he is giving the necessary tools to customers to try to intercept phone calls themselves. This is certainly not the case: Nohl is simply suggesting that people extend the research that he has already made, by trying it for themselves and "go[ing] to their operators and create demand for improvements" (Mills, 2010). Some may question the legality of Nohl's actions. These accusations of illegal practise are unjustified considering he has not intruded a private phone call without one's permission. Instead, he has researched solely for the purpose of providing a mechanism to demonstrate the vulnerability of GSM to others, and has stated that "intercepting the phone calls of others should be illegal everywhere", and "security research is still legal" (Mills, 2010). Given his intentions in investigating GSM, it becomes difficult to understand how any research he is conducting can be regarded as illegal.

Resolving the G.S.M security issue may never occur without further research taking place. The solution would involve convincing network operators, who historically have been slow to adapt to changes in network transmission technology, to update to the newer and more secure A5/3 128 bit technology that Nohl admits his team "cannot crack" (Mills, 2010). These network operators would not spare much concern if isolated cases of attack arise (in the case of Nohl); since the number of incidents would be far less than if the public are provided the technology to create an attack themselves. Only this customer demand will force an upgrade in the current encryption function to A5/3, so it is essential that customers have the necessary resources required to conduct the research – albeit performing within the constraints of the law.

How can we let such a profound and pressing security threat to "about 3.5 billion" (O'brien, 2009) people's privacy pass by without the need to research more into its solutions? We live in a complex world where the need for secure communication is equally important as the information being communicated. The first phase of Nohl's research has been completed: the security problem has been identified to the public. It's now up to us to persuade our mobile phone network operators - through possessing the very technology that would cause it's infrastructure to collapse – that the need to update the technology is of utmost importance in order to keep mobile phone technology as a secure mode of transmission that we have always trusted it to be. I feel Nohl has provided an important and necessary framework for the public to mount a challenge to network operators, persuading them to update their insecure networks to the secure A5/3

standard. It's imperative that his research in this field continues with other professionals and the public at large in order to safeguard the future integrity of our mobile networks.

Bibliography

Anon (n.d) GSM World Services . *GSM World.* **Online.** <http://gsmworld.com/technology/services/index.htm#nav -6> [accessed 12 March 2010]

Kang, M (2010) German computer scientist breaks mobile phone codes. *Ethiopian Review*. **Online.** (3 January) <http://www.ethiopianreview.com/news/8122 > [accessed 15 March 2010]

Mills, E (2010) Researcher Karsten Nohl on mobile eavesdropping . *CNET News*. **Online.** (1 January) < http://news.cnet.com/8301-27080_3-10423219-245.html?tag=newsLeadStoriesArea.1 /> [accessed 14 March 2010]

O'Brien, K (2009) Cellpho ne Encryption Code is Divuldged. *The New York Times*. **Online**. (28 December) < http://www.nytimes.com/2009/12/29/technology/29hack.html?_r=2 > [accessed 12 March 2010]

Number of Words: 924