Greg Baker
Senior Design Project
Current Events Essay

Guide to Breaking Cell Phone Security Revealed

This AP article is about the release of lookup tables that allow for quick decryption of the GSM protocol. It talks about the security researcher, Karsten Nohl, who released the information to the public. There are a number of ethical concerns about doing this; Does it expose people to undue risk from information loss? Will the increased short-term risk push phone companies to replace GSM in 80% of the world's phone? Groups such as the GSM Association, law enforcement agencies and legislators questioned the motives. A lot of the ethical questions about Nohl are questions that led to our project to begin with.

This article relates directly to our project; The weakness of GSM was one of the inspirations of the project we work on. Many of the concerns over the capability this gives organized criminals are concerns that our project was meant to address. Oddly, with anything involving cryptography, one of the larger ethical concerns was what capabilities that the use gives criminals. In our case, the concern was criminals using the technique to hide crimes. In the case of the release of GSM information, the concern is using the technique to commit crimes. In an interesting twist, the success of our project will defend against the usage of the information the article is about.

The event addressed in the article impacts my personal and professional life considerably. I know that when involved in a high enough level of organization not to use a phone provider that uses GSM, preferring a 3G or later network. This impacts my purchasing, and further pins me into more advanced and expensive phones. A further goal is to be more careful should I need to implement a cryptographic system, I will be more careful in the selection of algorithms and the method in which I implement it. On the other hand, releasing information that can compromise the security of large numbers of people must be done carefully. The controversy surrounding Nohl illustrates that fact.