OUR PROBLEM IS WITH SMS, NOT SS7

BY ERIC PRIEZKALNS 27 FEB 2019

ORIGINAL ARTICLE PUBLISHED IN COMMS RISK (COMMSRISK.COM)

Would you send somebody the password to your bank account on the back of a postcard? Probably not. You know anybody could read that postcard during its journey from you to its intended recipient. But your actual risk would be small. There are no criminals systematically reading postcards. The likeliest probability is that nobody will read your postcard, even though they could, because it would not occur to anyone that they might gain anything by reading it. And even if somebody did read your postcard, the simple truth is that most people are honest and law-abiding. They might think about stealing your money, but would soon dismiss the prospect because they lacked confidence in how they would do it in practice, and would expect to be caught afterwards.

Now let us imagine another scenario: a bank sends hundreds of letters each day, each communicating account passwords to customers. The letters are inside envelopes which are clearly marked as coming from the bank, with the words "this envelope contains the password of a bank account" written on the outside. The envelope is sealed, but anyone with a kettle could steam it open. Is the password inside this imaginary envelope more secure than the password that you wrote on your imaginary postcard? I would argue it is less secure. Unlike the postcard you thought about, criminals have good reason to target their efforts on finding and opening those envelopes. The criminals are not hopelessly searching for something they are unlikely to find, but systematically overcoming some routine obstacles in order to obtain predictable prizes. They just need to go to the sorting office that first receives the banks' outbound mail, select all the easily-identified letters, and open them all.

By now you have either grasped my point about the dangers of relying on SMS to communicate information securely, or you prefer not to understand it because you would rather focus on postcards and envelopes than the messages being conveyed. SMS is not especially secure, for a wide variety of reasons, but that is a distraction from the real reason why criminals target SS7 vulnerabilities in order to commit crime. Email is not secure either, and some people will email passwords to friends and colleagues, without worrying about the risk that the email will be read by a criminal. Banks do not systematically send passwords by email, but if banks were foolish enough to use email for this purpose then the consequences would be easy to forecast. The ease of intercepting a mode of communication is one factor in determining the risk of using it, but another factor is the frequency and volume of sensitive messages that are sent using that particular mode of communication.

Commsrisk has previously written about the pressure to make SS7 more secure. In 2017 it was reported that a German bank was robbed by hackers who exploited SS7

vulnerabilities to intercept authorization codes sent by SMS. Despite the harrying of telcos, my conclusion was that:

> This debate could go around and around, with everybody keen to find fault with everyone else, but nobody really motivated to find, and fund, a solution that works for all.

This year *Motherboard* reported that criminals stole from a UK bank using the same kind of SS7 exploit as happened in Germany. I believe my previous conclusion still applies: governments, banks and telcos prefer to allow the crime to continue, whilst pointing fingers at each other. The most simplistic response would question why telcos do not improve the security of their networks, but we can just as easily ask why banks keep sending so many SMS messages when they know other banks have been defrauded by criminals with the skills and ability to intercept those messages.

There are ways to address SS7 vulnerabilities, including firewalls and improved threat detection. Telcos should be proactive in adopting them. However, investing in countermeasures like these is like fitting a superior alarm to a car where the driver insists on leaving a pile of banknotes in plain view on the passenger seat. Two factor authentication that relies on SMS messages is grossly inferior to other well-established methods, such as requiring customers to use an authenticator app on their mobile phone. Many businesses are feeding crime because they do not want to change the way they work, and do not want to make their customers change the way they interact with their business. This is near-sighted. Every economy is going to see an increasing proportion of transactions processed across networks. Governments should be telling customers to prefer businesses who use safer methods of communicating with them, just as they tell drivers not to leave valuables where passing criminals will see them. The sooner businesses stop relying on SMS for sensitive communications, the better for all of us.