# How (M)Secure are You?

/EINPresswire.com/ Phone Call based Authentication is vulnerable to Call Forwarding Exploit.

According to research completed by CS Networks, a global provider of mobile security and messaging products, modern technology is facing dramatic security concerns in approaches of two-step verification. Especially, phone call based one. Results are pointing to serious exploit. “Your calls may be forwarded at anytime without your knowledge”.

Recent developments of technology resulted in merging of legacy SS7 telephone network and Internet with idea to cut down the expenses between mobile operators. There is a wide industry adoption of those hybrid products . However, lack of access control in legacy network protocols now exposed to attacker via internet may come with the price.

According to tests conducted, more then 60% of randomly selected mobile operators are prone to unauthorized call forwarding. An attacker can easy get all required informations such as customer's SIM Card IMSI to authorize himself on the network and send specially crafted packet activating the card forwarding service with destination number of his choice.

In practice, an attacker with the knowledge of valid customer's phone phone number can easy click on “Forgot Password” button and wait for password reset call confirmation PIN. - It's simple as that, according to Stefan Certic, Chief Technologies Officer of CS Networks.

In recent research paper – The Future of Mobile Security, Stefan is describing (M)Secure. A next generation two-step authentication product relaying on patent pending forward-indication technology. “The goal is to prevent bad guys from stealing your sensitive data by preventing a call to active call forwarding subscriber”.

Company executives are calling all interested service providers for a quick demonstration of security exploit.

“All interested companies are more then welcome to apply for live demonstration of forwarding exploit. (M)Secure technology has already found a way in large number of banking and financial institutions after successful presentation at Mobile World Congress. However, recent hacks of major industry players are showing that traditional authentication methods are not enough”.

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.