



## High-grade encryption used in malicious mobile apps

[Dan Raywood](#)

October 14 2011

Malicious application writers are using high-level encryption to communicate securely from the app to the command and control centre (C&C).

Speaking to SC Magazine, Axelle Aprville, senior computer security engineer at Fortinet, said attackers are encrypting traffic from the application so that when an SMS is sent, it is hidden from the device owner.

She said that strong encryption such as DES or AES is making it more difficult to analyse the communication.

“It is getting more technical; we have seen cryptographic malware, and mobile malware uses the best cryptography. There is a shift from writing malware that sends an SMS or dials a premium number,” Aprville said.

“This is becoming more and more advanced to achieve privilege escalation by using cryptography or botnets for mobile. It is much more advanced than the state of mobile malware from two years ago.”

Asked how users are becoming infected initially, Aprville said there are more risks due to users attempting to download applications without checking their safety, or doing so via pop-ups from malicious pages viewed on a phone.

She said: “The mobile malware explosion began three years ago when I could go in-depth on every sample, but now I am seeing a new family every week.”

Asked about the encryption technology being used, Aprville said “these are not things cryptographers would approve of”.

Source: <http://www.scmagazineuk.com/high-grade-encryption-used-in-malicious-mobile-apps/printarticle/214353/>