The second day of the Pwn2Own competition, organised by the Zero Day Initiative (ZDI) team at security researchers TippingPoint, was devoted to iPhone and BlackBerry. Charlie Miller exploited a vulnerability in the mobile version of the Safari web browser on iOS 4.2.1 to delete the address book when a manipulative website was visited. However, the first attempt failed when the browser merely crashed. But the second attempt succeeded and earned Mr Miller $15,000 and an iPhone. Miller had help from Dion Blazakis.

To get around data execution prevention (DEP) on the iPhone, Miller used Return-Oriented Programming (ROP), in which no code is placed on the stack; instead, addresses that call existing code fragments are. Miller says his exploit does not, however, work on the recently published iOS version 4.3, where Apple has implemented Address Space Layout Randomization (ASLR) for the first time. Libraries are now loaded to random addresses, thereby preventing ROP from working without further work. However, the vulnerability that Miller exploits remains in iOS 4.3.

It took three people to hack a BlackBerry Torch 9800. Unfortunately, the main hurdle was not special security, which BlackBerry doesn't have, but a lack of publicly accessible documentation about the system and a lack of tools. As a result, Vincenzo Iozzo, Willem Pinckaers and Ralf Philipp Weinmann had to work their way through the system by trial and error.

In the end, however, they managed to exploit a number of vulnerabilities to get at a hole in the WebKit-based browser, which RIM recently brought to BlackBerry. While the team only needed to demonstrate that it had access to the address book to win the competition, they nonetheless also showed how a file could be written into the file system.

As well as attacks on mobile devices, attacks on Firefox were also on the agenda but the candidates for that competition did not show up, just as no one did on the first day for

Chrome.