Google has offered $20,000 for an attack on its Chrome browser that also manages to break out of the protective sandbox. The sandbox is designed to prevent attacks on a system when an exploit has managed to inject and execute code via a vulnerability. The most recent similar hole in Chrome was closed in mid-January – the developer who discovered it received $3133.7 for his find.

Organised by the Zero Day Initiative (ZDI) team at security researchers TippingPoint, the Pwn 2Own
2011 contest offers a further $105,000 for security holes found in Internet Explorer, Safari and Firefox, as well as in Windows Phone 7, iOS, Blackberry 6 and Android, that allow malicious code to be injected and executed. Holes in Symbian have been dropped from the program this year.

For the first time, contestants have also been invited to attack potential firmware holes in wireless modules. Often called "baseband", this hardware includes such components as GSM and UMTS transmitters and receivers, as well as modulators and demodulators, and is implemented via a special processor. The attacks are to reveal holes in the relevant firmware, for instance in the GSM stack.

At the recent Black Hat conference, Ralf-Philipp Weinmann already demonstrated how to use specially crafted GSM packets to inject code into the baseband processor and execute it there – independently of the smartphone operating system in use on the device. Although the researcher's hack requires a dedicated GSM base station, the necessary hardware is available for less than €2,000, and the software (OpenBTS) is open source. For the contest, this equipment will be provided by the organisers.

As usual, the contest takes place during the CanSecWest security conference from 9 to 11 March.