Pwn2Own - an International Hacking Competition

Levchenko Michael, Don State Technical University

“Similia similibus curantur” – Paracelsus, 16th century

With the increasing spread of computers and different software penetrating our modern life we became more vulnerable for hackers. Even after dozens of tests flaws in the defense of operating systems and software may be still undiscovered and be useful for malefactors. That is why different hacking contests held. In the race for a prize many large vulnerabilities can be discovered by independent eyes.

Pwn2Own is a software hacking competition held annually at the CanSecWest security conference, beginning in 2007. During the years of successful performance competitors found and sold enormous amount of previously unknown vulnerabilities in the popular wide-used software and noticeably increased the computer defense of the modern software. The competition is used as the stage for the various computer-defense conferences while also providing a checkpoint on the progress made in security since the previous year.

Despite the overall increasing protection of different cyber-systems seems that the cure of the decease is unreachable. Hacker attacks mutate and adapt to the changing defense-principles of software and mobile devices. With the every new update and every new feature of the software there is a chance to get a new vulnerability. The hive mind of the hacker community will find and use in their purpose every bug they can reach. That is why the countless hacking competitions are hold by the large developers of software to test their products “in the field”. The popularity of these events and some scandals with the easy hacks of the most popular and believed to be invulnerable software products attracted the main media agencies in the computer sphere.

Pwn2Own is deservedly one of the most attractive of such competitions, because of its own recognizable style and name. The word “pwn” means “to dominate” or “to get control” in slang of Internet and “2” is read like

“to”, so the whole name of the competition is “hack to own”. And that is the main salt of the competition, distinguishing it from the crowds of others. The main prize is the device you hacked plus cash from the developer as the reward and the unique “Masters” jacket, confirming that you are a high-qualified hacker. Traditionally, competitors can win Apple products such as MacBooks and iPhones as well as Windows-driven laptops and Android devices. The variety of the devices to hack is increasing every year and amount of competitors also growing terribly.

The history of this contest starts in Vancouver, Canada in 2007. That time there was a widespread belief that OS X was significantly more secure than any other competitors, such as Windows. Dragos Ruiu, Canadian programmer was frustrated with Apple's lack of response to the Month of Apple Bugs and the Month of Kernel Bugs, as well as Apple's television commercials that trivialized the security built into the competing Windows operating system. So, Dragos decided to show people the truth about protection of Apple products. He announced about the contest for security researchers on the upcoming CanSecWest information security conference. The contest was to include two MacBook Pros that he would leave in the closed room, hooked up with their wireless access point. Any conference attendee could connect to the wireless network and try to hack or exploit one of the devices. In case of success, he would be able to get the device he hacked. There was no cash reward. Ruiu further said that there would be progressively loosened rules on what exploits were acceptable over the three days of the conference. On the first day of the conference ZDI (Zero-Day Initiative) company joined the contest and announced the 10 000$ flat prize for every successor. ZDI became the regular sponsor of the contest because of similar interests. ZDI has a program which purchases zero-days (term for previously unknown bugs) reports them to the affected vendor and turns them into signatures for their own antimalware system, increasing its effectiveness.

The competition is held for three days. Each day the amount of gain is decreasing, as well as the difficulty of the task. In the vanilla schedule at

the first day competitors try to hack the device through the Wi-Fi without any user interaction with the interface. It was the most hard part of the contest, so hard, that it was removed in the next tours, because the physically lack of control for hacking. The second day allows the competitors to use links that are opened in the browser window to exploit the vulnerabilities in the popular browsers. This is the most popular part of contest because of the frequent updates of browsers that can provide new previously unknown bugs. The first winner of the contest was right in this nomination. And the third part allows direct interacting with the device and execution of your malware. It was later replaced with the mobile devices hacking.

Member of the first contest, Dai Zovi, who had learned about the competition at the end of the first day, had successfully found a vulnerability of the QuickTime plugin for Safari by the 3am. The next day he sent a link to the one of MacBooks and destroyed the belief that the protection of OS X is impenetrable.

Many time passed since that first competition. And Pwn2Own grew from the small local contest to a large international hacking championship with the prize fund of 1 000 000 $, large sponsor base including leaders of the software development such as Microsoft and Google. After 8 years of successful hacking tons of bugs were found and fixed, thousands lines of code were written and dozens of participators grabbed their jackpots. Every year the security and complexity of hacks increases dramatically and new exploits are found every time. Pwn2Own and other hacking contest helps the major software developers to keep people that are using their programs defended against perpetual hacking attempts and help the creators to test their applications and devices in the hardest way.

References

http://www.eweek.com/security-watch/mac-hacked-via-safari-browser-in-pwn2own-contest.html

http://www.computerworld.com/article/2530839/security0/hacker-challenge-takes-aim-at-browsers--smartphones.html

http://www.computerworld.com/article/2501774/security0/google-puts--1m-on-the-line-for-chrome-exploit-rewards.html

https://www.zdnet.com/blog/security/how-long-can-a-mac-survive-the-hacker-jungle/137

http://seclists.org/dailydave/2007/q1/289