**Technical Evaluation of DEF CON 21-Evil DoS Attacks and Strong Defenses Video**

DEF CON is a great place to look for educational technology videos that are both mind-blowing and funny. Many masters of technology, and some not, go to DEF CON to present something they found, be it a glitch, a presentation about the history of memes, or to tell a story about a MAC desktop that was stolen and recovered because the owner was a hacker of sorts. Sam Bowne is one of these people. He is a technology expert in the server and networking field. For his presentation, he brought along Matthew Prince, a systems admin who works for CloudFlare. CloudFlare is a company that protects websites from Denial of Service  
(DoS) attacks.

This presentation was about a specific set of attacks that can be done to crash servers and result in Denials of Service. The first part, when Sam Bowne was presenting, contained two attacks. The first was an attack that takes advantage of the TCP handshake by telling the server to open a socket but not send any data because the client’s buffer is full. Doing this many times over will cause the server to open up many, many sockets and consume all the server’s RAM. This makes the server unresponsive and results in a DoS. The second type of attack to advantage of the relatively new IPv6 system by spoofing a router and sending thousands of connect requests. The client machine therefore connects to thousands of fake IPs and consumes all CPU power. Demonstrating on a Windows 2012 Server, Sam was able to crash the machine after about 30 seconds of 100% CPU utilization. Then, Matthew Prince presented. Matthew presented on a single attack and told some stories about it. His attack took advantage of a failure in UDP. Effectively, the client sent a request to the server demanding no TCP response. The server sent back a package about 50 times as big as the request. But, because Matthew had spoofed some machines and a fake IP, that server’s response was actually sent back to itself. Matthew then simulated how a 1 Gbps request attack would result in the server sending itself responses at 50Gbps and taking up its own internet pipes.

The presentation seemed incredibly relevant to the audience because it was DEF CON, the place to show off hacks and glitches and ‘evil’ things like DoS attacks. The crowd who attends DEF CON does not contain any non-technically knowledgeable people because they would not attend an event that has nothing to do with them. The crowd seemed to understand what was going on because they were cheering when the presenters succeeded in their demonstrations.

Being extremely relevant, the presentation could only get better if it was interesting. This is was. The crowd was laughing, and the writer found himself cheering while watching the video. The presenters of DEF CON have a habit of being funny and doing very technical things in such a manner that anybody with minimal technical skill can understand and reproduce. In this regard, Matthew actually challenged the crowd to reproduce a 50 line ‘c’ program which causes machines doing attacks to attack each other rather than the target. He proceeded to state the program he had was not permitted to be shown, and then flashed the code on screen, which may not have been strictly speaking legal, but it was incredibly funny as the crowd decided to cheer very loudly.

Overall, the presentation was very well-done. It was informative, engaging, and funny. As presentations go, it is the writer’s favorite. As well as having learned about networking and potential DoS loopholes, the writer is now engaged in writing the program Matthew challenged the crowd to reproduce.

Source: https://www.youtube.com/watch?v=4BPibf6C35E