Have Script, Will destroy

Interview with the hacker Clara G. Sopht

February 2000, Berlin

F: Clara, would you call yourself a hacker?

C: No. [laughs] Always the same stupid question. But there are some hackers who call me a ‚hacker', others call me ‚cracker' and others just 'lazy-assed destroyer'. There is a big variety of swaerwords (Schimpfworte) around for people like me.

F: But these different terms actually describe very different activities. Are there any precise definitions, and to which one would you like to refer?

C: There is something like a dictionary, called the ‚Jargon File'. It has been put together by many different people from the hacker scene since the 70s. It is a perfect reference book for all terms around hacking. There you can find anything you are looking for.

To answer your question in short: After hackers had gotten quite a bad press, the scene came up with the idea to distinguish between good and bad hackers-the bad ones are the crackers. I'm not sure if this was a good idea. Anyway, this distinction never made it's way to a broader public, and it is more or less a ‚feel-good' strategy for the ones who consider themselves as the good ones. I match with all of these terms or noone, depends.

F: You came to Europe for the Chaos Communication Congress in Berlin. Did you enjoy it?

C: Oh, ja. It's always worth going to such places. You meet lots of interesting guys, get some bits of hot information. And there was excellent stuff in the program, like about ‚Information Warfare' or ‚Information Operations' how they prefer to call it, and Echelon which is a part of the Project 415.

F: That sounds as if you were mostly interested in the political aspects of information technology?

C: Each aspect of information technology is political. But it is definitely true that I'm very much concernd with the idea of resistance and political activism on the net — the electronic underground. Hackers are the spearhead of this new forms of resistance. They have an enormous political potential, although most of them do not even realize that. And there are also other political activists who fight for goals outside the net, and use the net as the site for their contestation.

F: What are the forms electronic resistance takes today?

C: Hm, this is a very delicate question. In the end, there aren't many, and the few existing are very controversial. Let me give you an example. In the mid 90s the group CriticalArtEnsemble published a book called Electronic Civil Disobedience. The basic assumption of the book is that power and representations of power are no longer located in the real world but shifted into the nets. That's why resistance against power also has to take place in the nets. In the following they developed a model by transferring Civil Disobendience from the real life in the virtual world, and called it Electronic Cicvil Disobendience. It is about blocking the flow of information rather than the flow of personnel, and it takes place at the sites of military, corporate, or governmental institutions. That CAE's basic assumptions were right, you see in the extent these locations are defended, and the extent to which trespassers are punished. The greater the intensity of defense and punishment, the greater the power-value. And as you certainly know, hackers are heavily punished for what they do. Which means they are operating at the right sites!

F: So what is the controversy about?

C: The controversy is about the direct translation of this theoretical model into pratice. The name of this concrete form is Denial of Service attack, DoS. Basically that means to remotely disable machines by flooding them with more traffic than they could handle. You can effectively cripple any network, regardless of size or bandwith with this method. In minutes, all network activity of the attacked server is shut down as the attack consumes all available network resources. To automate this processes scripts are used which generate endless traffic.

F: I guess almost everybody has heard of the recent attacks on some e-commerce sites. They were also committed with the same tools. To me it sounds like a very targetted attack. Why is it contested by most hackers?

C: There are various forms of DoS attacks which all work slightly different, and they use different scripts. So-called Distributed Dos attacks are most common. That means they are launched from different servers, use spoofed IP-numbers as senders, and involve millions of packets. These attacks consume bandwith, not just of the targetted network, but also of all customers who share the bandwith. So the execution is not very precise. That's why it is accused to show an inkling of grace. And instead of ensuring the free flow information, which is one of the basic principles of hacking, DoS attacks do the opposite. This are the more rational reasons against Dos, but there are also many irrational. The perpetuaters are named childish, malcontent and lacking technical skil, and they are accused to do it just for revenge. The attacks are considered as worthless.

F: But what do you personally think of these methods?

C: First of all, I would like to note something general. People who own computers, and especially hackers are gaining more and more power. The computer networks are one big power-tool, and somehow by mistake, the industries have sold millions of computers to the people. We made them rich by buying those machines, but now we have these weapons. Obviously, they didn't think much when they sold us the tools, because the last thing governments want is ‚power to the people'.

Concerning the Dos attacks: All people I know who carry out such attacks do have real hacker abilities. Second is, that those people think about whom they attack and why. So, it's not just stupid script-kiddies who don't know what they're doing. For these people it is one form of resistance amongst others. They also work on free software concerns, cryptography etc. I do not exactly want to promote DDos as the best one, but we do not yet have the 'best one'. It still has to be developped, and it gets developped out of trial and error. The good point about it certainly is, that it attracks a lot of attention, it makes evident where power accumulates and — the executers usually don't get busted. If you do it intelligently, it is very secure. And blocking information access is the best means to disrupt any institution, whether it is military, corporate, or governmental.

F: Let's have a word about the attacks on the e-commerce sites mid february.

C: History repeats itself, as this takes us back to the first instance of a successful DDoS, back in '94 or so against the Mexican government by the Electronic Disturbance Theater which sent port 80 requests for bad pages looking for 'Human_Rights' and such. From a technical point of view the attacks were no surprise, at least not for professionals. The tools to do such things are around for a while, it was just a question of time that someone would use them for a major attack. And as it worked so well, it will certainly be copied.

Interesstingly the attacks came some days after Clinton's proposal to massively expand the budget for electronic law enforcement. This made some smarties detect that the Secret Services themselves must have launched the attacks, in order to create a panic which would make it easier to pass the budget. For me, it is the other way round. If the government cries out for ‚alternative wars', for ‚cyberterrorism', they should get it. (gespielt bedrohlich): The envisioned ‚New and Deadly' threat became true. This was just the beginning.

No, seriuosly: The way the technical infrastructure works today, but also the way how insecurities are handled do not at all ensure a stable working of the internet. And the interesting point is, that the actual stability of the internet is in no relation to the huge values being projected onto it. I think it is quite healthy to shake things a little, and make some bubbles burst! Cyberspace is not secure, and never will be! It doesn't make sense to make a belief-system out of any technology, be it for commercial or power reasons or to improve the world.

F: I would like to switch to another aspect, Clara. You are operating in a dominantly male domain. Does that cause problems for you? Do you have to fight for equal rights? And would you consider yourself as a feminist?

C: Uh! Aehm, that's a hard one. Well, my experience is that most hackers hate feminists. That would be reason enough for me to call my self a femist. In general I'm not a big fan of isms - like hackism - but fact is that we are far away from having equal rights for men and women. That's for sure. The big question is what strategies actually could make sense today.

F: Did you ever hear of cyberfeminism? And what do you think of it?

C: Oh, cyberfeminism seems to be quite funny. These girls tend to be fresh and cheeky, but I would recommend them to get their hands more dirty with technology and transform their rhetoric strategies into technological attacks which would hit much deeper.

F: Do you have a vision? What makes you work?

C: I'm not sure. As the things you love most can easily become the things you hate most, I sometimes have the vision to take down the whole internet - of course with the help of some friends - and then become a musician and a dancer.

Published in artbyte, The Magazin of Digital Culture, New York, Jul-August 2000

This text is related to the project *Women Hackers*: http://artwarez.org/projects/womenhackers