Ryan Breuer
Article #1
Silver Bullet Podcast - Show 050 - An Interview with Richard Clarke
Article Date: June 1st, 2010

What was discussed in the podcast?

The main focus of this podcast was on cyberterrorism. One of the first things mentioned was that the odds of a single individual causing a catastrophe with a cyberattack was not very likely. The main threats are instead nation states or criminal cartels that would have the capability to take down much more than just a few websites like being able to take down a power grid. Unfortunately, little knowledge is needed to successfully pull off a cyberattack. This was proven when North Korea, who has little to no cyberspace, was able to take down websites in the U.S. with a cyberattack.

A lot of today's attacks are much more subtle than they were in the past. People are able to access and steal a lot of information from under someone or some company and they may never even realize anything is happening. Even though some attacks are stealthy and subtle, there are still many simple attacks, that although they've been around for a while, are still an easy thing to do that almost always works. An example would be the DDOS attack which may not work on large companies like Google or Amazon, but most other websites, it could still be a threat.

Next comes software security. As Clark says in the interview, "We've made progress, but we've made progress from a really low beginning, [and] there's a lot more that has to be done." Basically, they are saying that everything that has happened is good and is helping the security of software, but because there was so little to begin with, any progress that is made looks even better. They also mention that there is a cost to software security. If you want extremely secure software, you will have to invest a lot more time and money into it. The example they give is that NASA supposedly spends $25,000 per line of code to make their code secure. That would be insane for pretty much any other project and it would not gain you much.

The challenge is to find a perfect balance of how much time and money to spend on security and what you can live without.

The next focus is regulations of software security. It seems to only come up in certain situations such as when the government is invading too much into your privacy like when they were allowed to tap into phones without a warrant or when they are asked in a way that makes people think differently about it. One such example was asking a parent if they wanted regulations on toys having lead based paint that their children would be licking the paint on. Until confronted with that regulation, they probably didn't care what kind of paint was on the toy, but when informed, they appreciate that the regulation is there. Unfortunately, it again comes down to being able to balance the freedoms that we have with the cybersecurity to stop attacks from affecting you.

What you learned from the podcast?

Cybersecurity is a huge issue even in today's world with ever growing technology to fight against it. Even the simple things are still concerns when it comes to security and some things that should have more security do not, such as the power grids, that if attacked would affect a large number of people with fairly little effort from the attackers.

How this material will help you in your software development?

I will be watching out for the security issues that pose a threat to everyone or just to any and all products that may be overlooked normally. Simple things, such as the DDOS attacks, have been able to be mitigated by larger companies, but are still possibly to handle by smaller ones if you plan for such things properly.