Sam Yarcho

SE-4930 – Software Security

Podcast Summary

1/23/12

Show 058 – An Interview with John Savage

http://www.cigital.com/silver-bullet/show-058/

A little about John Savage – John Savage is a professor of Computer Science at Brown University. He earned his PHD in '65. He co-founded the department of Computer Science in 1979 and chaired it from 1985 – 1991. He has deep roots in theoretical computer science and also computational nano-technology, and has written three books, the latest being Models of Computation.

I could try to blend the interview questions into paragraph form, but I think readers will get more out of the episode by reading it in a summarized interview format:

What is the state of cyber security as a discipline?
It 25-30 years old, still in its early stages. We have a long way to go. Cyber security challenges are very hard, intellectually very challenging, and are of great practical importance. Not enough progress on this field.

What issues are top of mind when it comes to cyber security and other cyber issues?
Setting a good policy and process to deal with issues of cyber security. The country has been developing one and it has started to pick up steam in 2009 and 2010

How are the technical skills of the policy makers? Do they seem to understand what the policy is about or is it magic to them?
They are people that John worked with in Computer Science and they are very intelligent people who are "quick studies". They have come to grips with cyber security issues over time and have a good depth of knowledge to be able to address the policy issues. They have not yet dealt with profound issues however. He believes you have to have technologists and policy makes at the table at the same time, because both need to work together with the things they know.

Does it make sense to form military units in cyberspace as a reaction to our worrisome dependence and systematic vulnerability?
Short answer - yes. This is unavoidable. 20 nations are preparing for cyber conflict. It should be attacked like radio communication was. We should invest very large efforts to reduce risks and tension, and should demilitarize it, although it might be beyond that now. We have to raise the alarm and bring the attention to the public that these threats are real and could have a significant effect on the economy.

Is wiki leaks part of the press that should be protected by the first amendment or is it a new beast or is it in fact a terrorist organization as some politics have said?
Not a terrorist organization. His question is - how did they not notice that somebody was grabbing all the files out of the database and being put on a USB drive? Shouldn't they have noticed such a large volume being taken off, and raised a red flag? Maybe put a limit to the number of items per day a person can download.

Why does the government focus all of their attention on offensive weaponry these days?
The government is proactive. They are there to protect the country. They get the best and brightest minds and confront a brand new challenge, so they prepare for the possibility of an attack and also prepare for defense.

Don't they focus more on offense than defense?
If they're doing superbly on defense, they won't tell you.

Policy makers are focusing more on how to react if something happens, and not on how to build programs securely to avoid it from happening in the first place. Why is this?
This is partially because they aren't extremely technical and don't know what options they have available. John starts talking about how he thinks that the vendors/creators of software should be responsible for not securing their software completely, and for the damage it might make to someone's computer. But when you buy someone's software, you agree that they are not responsible for any damage done, and he thinks this needs to change.

Is using stuxnet as a cyber weapon morally justified?

Yes, it is. He believes it is as morally justified as it is to sabotage a piece of equipment that you know is going to be used against you.

What implications do nano technology have for cyber security?
On the surface - none, except for the fact that as we make our components smaller, we put more on a chip, this allows us to change the way we write code, and the way we implement chips.

What's the best book of fiction you've recently read?
The Girl with the Dragon Tattoo, only the first volume. He understands she is quite a geek, and wants to read the rest of them.

What's the most interesting non-fiction book you've read recently?
The solution to the crypto computing problem due to Craig Gentry which is Homomorphic encryption. Craig Gentry has shown is that it is possible to encode data so that when you compute on the data, it remains encrypted. And you never have to decrypt until you bring the results home. The technique is very intellectually challenging, and is very inefficient currently. It is right now impractical to use due to some challenges.