Marc Anders
SE 4930
Dr. Schilling
Security Summary #4

I listened to “Show 70, An interview with Ross Anderson” which is part of the Silver bullet podcast. Ross Anderson is a professor of Security Engineering at Cambridge University, and has written a best seller book titled Security Engineering. The interview discussed trusted computing, military and civilian differences in relation to security, Facebook’s new authentication by pictures, and about Stuxnet.

The podcast discussed the idea of trusted computing. Trusted computing is the idea that only signed operating systems and applications will run on the physical computer parts. Anderson talks about the fact that Microsoft and Apple would like this, but that this would shut away almost the entire open source community. In addition to this, Anderson brings up the question of authority. Who or what would be the governing organization that determines which OS is officially signed? It cannot be one country, because no country has authority over another. In addition, any country that had the authority to certify operating systems would be able to create official malware that the computers would run thinking it was safe. This would in effect leave us at the exact same spot as before having trusted computing.

Another topic Anderson talked about was the flaw within Facebooks new authentication. Facebook has discussed the idea that instead of needing a password or username that a person could log into their account based on identifying pictures of their friends. This is flawed, Anderson says, based on the fact that the privacy we desire is normally privacy from those friends. Many people’s friends are friends, and therefore the identifying of friends would potentially be easy for another person. I am

not aware as to whether Facebook will be implementing this, or the exact specifics, but I did find Anderson's point very valid. Most of my close friends all know each other and would not have any issue identifying pictures of them.

A topic that is becoming more and more relevant is the shrinking gap between civilian and military. Anderson points out that as technology increases, the military are using the same software and hardware as the average civilian. This causes problems in the security domain because this means that confidential military information could be leaked even easier. Until recently the production lines for military devices were completely separate from civilian, but as the two start to intertwine major consideration will need to be put into keeping military channels secure.

The final topic that Anderson talked about was Stuxnet. He linked this back to trusted computing, talking about the fact that if the governments really wanted to they could probably cut down the number of major malware applications. He explained though that the governments are not motivated to create more secure systems, because more secure systems mean that their own malware will not perform as well as they would like. This is a pretty scary thought, but I agree with Anderson. I'm not sure how this will be overcome, but as I see Google, Microsoft, Apple, and any other major software/hardware manufacturer working to create more secure systems it causes me to question whether the companies will create a sort of organization that will supersede governments.