Summary of Discussion on 11/6/02
Brian Kellogg

The discussion started with some confusion on what an intrusion detection system actually does. It was brought up that it checks attacks, why doesn’t it look for attacks like the replay attack. Also, intrusion detection is not proactive, why can’t it do more to prevent an attack when a partial attack is detected. Intrusion detection systems are designed to detect intrusions. These intrusions in general are normal activities, but done in a certain way or certain combinations can constitute an attack. So usually, the activities that are detected are just logged where more severe attacks will notify a security officer. It was mentioned that one downfall of the paper’s method is that there is no way to find out what are information variable and what are correlation variables. Chad though IDS should focus more on common effects so that it can resist attacks. Michelle mentioned that some IDS do have this classification. It was also pointed out that if responses were too severe, the IDS might create new attacks. An example of this is if for a certain attack, the IDS will cut off that port from the network. If an attacker knows this, they can spoof a legitimate router and in effect cause a denial of service attack. One response to an intrusion that many companies use is just to unplug the machine from the network. This is the only true way to be assured there will be no more intrusions until the problem is dealt with. It was mentioned there are hacker tools out there that specifically focus on making IDS go berserk. It was pointed out that IDS only can detect known attacks, so maybe intrusion signatures need to be updated like virus software. There is one IDS called zone alarm that start out the system not allowing any external connections. It will ask every time if you are willing to connect or let someone connect. So nothing is allowed that isn’t manually accepted. There are other approaches to IDS like LISYS (Lightweight Intrusion detection SYStem) which first defines normal network activity in a training period and can detect attacks by comparing new data to the old data. Also, there are approaches using neural nets. This paper did not really talk about the complexity of their pruning methods. If it is too complex, it will still cause the choking attacks described in the paper. Dr. Cheng asked if there was realistic application for this. Different communities have different standards. Some accept just theories. Others like software engineering are extremely demanding and require tool support. This is because it is too difficult to try to do without tool support. It needs to be based on a sound theory and reproducible by others. For example, many have tech reports that instruct how to reproduce a result. Software engineering a new field, but since it requires validation it shows that it is a maturing field. Dr. Cheng closed by saying there is a big push for empirical research. It is not new or ground breaking, but very valuable. Software factory was an example of a company that did empirical research that is now shut down.