Ben Collins

1/25/12

SE 4930

Silver Bullet Security Podcast # 69

Website: http://www.cigital.com/silver-bullet/

Speaker: Steve Myers, Assistant Professor of Informatics and Computing in the School of Informatics at Indiana University.

This talk talked of a wide range of security topics but had a main theme that was very interesting. The theme was that there is a major difference between reactive security and Proactive security. He employs trying to teach proactive security, as it provides a better overall solution to the problem of security. He notices that much research has gone into reactive security, where as more research now is being attributed to solving the overall solutions to security. This topic relates to class as we have talked about proactive design, which he talked about as well. This involves analyzing the Architecture you are building, Thread-Modeling and asset identification. He stresses highly in his security classes that as opposed to looking at security attacks such as Cross site scripting, sql injection, and buffer overflows, too look at the root causes. These attack involve input validation, which should be stresses during the design of the product. Another key point he makes is one we discussed in class. He said "security is not a problem you solve, but it is risk management". This meaning we have to study our architecture and figure the weak points and make choices on which targets are the highest security risks, and adjust accordingly.

As well as teaching security, Steve Myers specialty is cryptography. He stressed the points that this is not security, and that sprinkling magically cryptography dust does not make something secure. He looks at it as a tool. Most Cryptographers are not aware of a systems overall security. He used a good analogy that a bank vault maker may not be aware of what it takes to keep a bank secure, he is aware of making sure a bank is hard to access.

Finally, the topic of Malware on phones was discussed. He noted the potential for this to fall under attacks was different because of the type of information it could obtain. Malware could lead to a variety of geographical attacks, phishing, and the ability to use targets wifi identifiers to get information from people who don't even have the malware installed.

This article was a interesting to read because it gave another perspective on the stress of good system design. In class we learned about the ideas behind this, but sometimes its important to hear them in a different phrasing, as it may click more. Overall, I plan to take away the importance of design and architectural analysis, as this is a better system for preventing security risks.