Alexander Cannell

09/30/2016

CSIA 6010

# Internet/Intranet

Evaluate the Dolev-Yao Adversary Model - what are the pros/cons of the model, any shortcomings? If there are shortcomings, what are they and how can they be addressed?

Dolev-Yao Adversary Model or the Dolev-yao model is as the book says, “the standard attack model against messages exchanged over a network.” (Vacca, 2014) This model gives us a better understanding on what an attacker is by giving us several actions we assume an attacker might take. These assumptions are Eavesdrop, Forge, Replay, Delay and rush, Reorder, and Delete. In my book all the assumptions are pros in my book. To be overly cautious with regard to security is a good thing. We are going back to what Anish was talking about in our first discussion, “Information security professionals have a reputation for being the glass half empty types of people...We are conditioned to look for everything that can go wrong”.(Anish, 2013) I think that we need to have a glass half full perspective when looking at security and The Dolev-Yao Model gives us that apply as the industry standard for a threat model. Now the downside with Dolev Yao Model is that we are assuming that everything is insecure, we have to find a good balance between completely secure and usability.

How do you protect against these adversarial attacks?

The easiest way to secure communication is owl post, or smoke signals….haha just kidding. The book talks a lot about Cryptography, which is the art of securing communication. A form of cryptography is encryption; which can be your most reliable defense. Encryption can defend against defend against all of these assumptions listed above, but mostly with eavesdroppers. If Someone(an Attacker) is listening into your communications with your friend Ben, but you and ben speak your own language you guys made up from kindergarten. What uses are those communications to the attacker if he didn't understand the content? Danny Dolev and Andrew Yao put it this way when talking about Public Key Protocols(Which is a form of encryption), “Public key encryption provides secure network communication, usually effective against eavesdroppers.”(PKE, 1983) The company I work for has just made a move from http to https which is the process of encrypting web traffic, another great way to secure communications. The best way to secure communication is to encrypt the communication.

In our CSIA 6200 class we did our own Vulnerability Assessment Model which involved Identify, Analyze, Mitigate, and manage. I think when we are protecting against adversarial attacks we need to do a Vulnerability or risk assessment.

1. Identify
   1. Identify, group, and rank various information functions
   2. Form policies based on these functions and rankings
   3. Perform risk assessment
   4. Prioritize mitigation/prevention activities based on most essential functions first
2. Analyze
   1. Analyze activities/traffic and form baselines for ‘normal’
   2. Perform penetration testing
   3. Monitor for vulnerabilities, compromises, departures from ‘normal’
3. Mitigate
   1. Take measures to fix problems found
   2. Alter policies if needed
4. Manage
   1. Document all fixes/changes to systems
   2. Add/alter policies and groupings/rankings as business grows and changes
   3. Asses implemented fixes and monitor to ensure their success
   4. Repeat process

How can an organization prevent security breaches to their Intranet?

The best way to prevent security breaches to any intranet is to understand your intranet, and identify the risks to that intranet. To properly understand this you will need to perform a Risk assessment. We have to assess the risk of encrypting laptops and mobile devices, using VPN and SSL’s, Malware/spyware, proper internal traffic monitoring, updated Patching, Email vulnerabilities, proper firewall placements and configurations, wireless network security, personal security, and don't underestimate proper password policies. Which are all great ways to better protect ourselves from security breaches.

How would an organization handle an intranet attack?

At my work we do what is called an post mortem. In the post mortem, the incidence response team gives an incident report to the executives one what the incident was, what happened in the incident, when the incident happened, how the incident happened, what damages, and what they did to prevent an incident like this from happening in the future? Kindof nerve racking but it needs to be done. But that is after the incident has occurred. During the incident, it is the responsibility for the network team to have security monitors to know when and what is happening. Then the responsibility for the incident response team to act quickly to resolve the issue, and prevent or circumvent the attack.

<http://www.cs.huji.ac.il/~dolev/pubs/dolev-yao-ieee-01056650.pdf>

<http://nypost.com/2014/11/23/the-shocking-real-life-story-behind-the-imitation-game/>

<https://eprint.iacr.org/2009/079.pdf>

<https://youtu.be/UPmVTPyE5DM>