Future Hacking Concepts

The future of hacking is just a concept right now. While we like to believe that we have a pretty good idea of what that future will be like, there is no way for us to know for sure. And when I mention “the future of hacking”, I do not mean ten, twenty, or thirty years from now. A decade in technology time is like a lifetime for humans. These days most technologies are birthed, manufactured, and set aside within that ten year time frame. So anything beyond five or so years is something I cannot really begin to fathom much less speculate upon. So keeping this in mind, I want to touch on the transitioning of current methods of attack, and the potential of Quantum computing’s effects on current security.

A good way to rev up the thought process on how attackers are transitioning from present day attacks to future methods would be to start with web applications. Web applications span across all enterprises. Things such as banks, online retailers, and web subscriptions all have front ends for a user to touch, and use their personal information to gain a product or resource. A large portion of today’s online markets should be focusing on the security of their websites and online applications. Methods such as SQL injection and cross-site scripting allow attackers to gain information on vulnerable web applications. These methods could allow attackers to gain user information, admin information, and much more if they are successful. The good news is that most web admins know about these techniques and take extra precautions to protect for these. But cyber security is like a leaky boat, when you plug one leak you are likely to spring another. Security evangelist Raf Los from HP Software says, “As organizations understand how to secure their code against programmatic errors, including SQL injection and cross-site scripting (CSS), attackers will inevitably move on to attacking application logic." These days, the designing of web apps is a profitable business. One person can go out and program a web app and sell it to others. These individuals that buy web app APK’s can customize the design very easily to fit their intended use, but now every person who purchased the design has the same logic flaws as the original. I can see this as a big issue for future companies who can’t/won’t take the time and money to build their own web apps. Cookie cutter websites and applications are very easy and neat, but just like everything else in security, convenience != security.

Another future issue that is nearly guaranteed by necessity involves RFID security. RFID is being implemented on a large scale currently. RFID is used in things such as: Keyless door entry for buildings, wireless payment with credit cards at merchants, even bracelets at Disney World that hold all of your personal information and let you pay for food and rides quickly and easily. RFID makes things a little bit more convenient for its users while posing a large security threat. I believe the largest single target for attack is on personal information leading to bank accounts and financial information. Already I have seen wallets with special high-grade materials to block RFID transmissions. Rich Baich of Deloitte & Touche states, “RFID adoption creates a new ability to carry out the current and future goal of any criminal or nation state which is using collection, dissemination and use of data to achieve their goals.” Most people aren’t aware of the potential danger, partially because attacks haven’t really been implemented on a large scale yet, and they aren’t protecting themselves. The market of attack here is mostly untouched.

Now that I have covered some topics on the transition of attacks, it’s time to cover the theoretical implications of quantum computing. Quantum computing is based around the idea data can be crunched exponentially faster when applying quantum physics based ideas to computing. The idea of storing data at a subatomic level, which really shrinks down the size of processors, would also allow computer to send and receive data as qubits instead of bits. While bits are 1’s and 0’s, qubits are 1’s, 0’s, and 1’s and 0’s simultaneously. If each qubit can actually represent a 1 and a 0 at the same time, the processing speed multiplies exponentially each processing step. Concepts aside, insanely fast processing speed makes every single type of encryption method known today completely obsolete. The only vulnerability that is standard through every type of encryption is a brute force attack. Brute force aren’t very feasible against a good number of encryptions today because it would take a long time to eventually stumble across the key. But quantum computing could crack an encryption in minutes that would take modern computers years or decades to break. While quantum computing would absolutely change the world and how it works, it would singlehandedly compromise every security system in existence. According to an article from Bloomberg, the fastest “publically known” quantum computer belongs to Google. Google’s system can generate 512 qubits of processing power, which is quite a ways away from the 10 – 100 million qubits seen as the ideal number. But technology evolves very quickly and, if it isn’t already here, it will be here much sooner than most people are ready for.

There are other concepts that I didn’t touch on that might have been relevant to cover as well, but I feel like just understanding that transitioning itself is a vulnerability is more important. Seeing the potential “Butterfly Effect” that fixing one security flaw can generate is the highest form of security, even when talking about quantum computing.

While it may seem like we are trying to patch a dam with a Band-Aid when it comes to security, understanding what methods of attack were used in the past allow us to detect new vectors of attack today. Just as understanding today’s security flaws gives us insight to what may be headed our way in the future.

Citation:

* Baker, Pam. "The Nightmare Future of Hacking: Page 2." *- ESecurity Planet*. N.p., 21 June 2011. Web. 30 Nov. 2014. <http://www.esecurityplanet.com/trends/article.php/11164\_3936241\_2/The-Nightmare-Future-of-Hacking.htm>.
* King, Ian, and Dune Lawrence. "Defending Against Hackers of the Future."*Bloomberg Business Week*. Bloomberg, 28 Aug. 2014. Web. 30 Nov. 2014. <http://www.businessweek.com/articles/2014-08-28/for-quantum-hackings-threat-startups-offer-futureproofing>.