All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The story behind the story behind the story of Aurora

Every once in a while, it's good to get at the story behind the story behind the story we are reading today. Sometimes it takes a while. This is the back story to the Aurora experiments now the back-story behind other things as well. It's about positive feedback.

Origins

In engineering circles, some of the most famous failures are things like the Tacoma Narrows Bridge collapse. Resonance in the wind effects on the bridge caused an increasingly violent resonance which ultimately destroyed the bridge and killed some folks. The collapse was in the 1940s (Nov 7, I seem to recall), before I was born.

As an electrical engineer I was taught about ringing in switching systems and various other related matters. Under-damped systems tend to grow when interacting with external forces at or around resonant frequencies, leading to electrical destruction of components as the voltages and/or currents exceed design specifications and implementation realities. Find the resonant frequency and you can cause the system to increase energy with each cycle until the energy destroys the system.

In the parlance of some, this generalizes to wave form attacks on systems, wherein induction of wave forms of the right shape and magnitude into a system at the right place and time causes various kinds of mechanical, electrical, informational, or other changes not anticipated or properly mitigated by design and implementation, causing faults resulting in failures, or by intent, attacker desired and defender undesired effects and resulting consequences.

Sympathetic vibration

In studying cyber security, in the early 1990s, I published a book covering the broad areas and, ultimately, produced a database of attack and defense methods that has been available over the Internet since the later 1990s, and the name used for this sort of event was identified as "sympathetic vibration" (with citations from the 1970s-mid-1980s):

> Creating or exploiting positive feedback loops or under-damped oscillatory behaviors so as to overload a system. Examples include electrical or acoustic wave enhancement, the creation of packets in the Internet which form infinite communications loops, and protocol errors causing cascade failures in telephone systems.
>
> *Complexity: In some under-damped systems, sympathetic vibration is easily induced. It sometimes even happens accidentally. In over-damped systems, sympathetic vibration requires additional energy. In logical systems - such as protocol driven networks - the complexity of finding an oscillatory behavior is often very low. A simple search of the Internet protocols leads to several such cases. More generally, finding such cases may involve N-fold combinations of protocol elements which is exponential in time and linear in space. Proving that protocols are free of such behaviors is known to be at least NP-complete.*

 Copyright (c) Fred Cohen, 2018 - All Rights Reserved

UDP viruses

One of the examples of such an attack is the UDP “echo” virus attack where the “echo” protocol is implemented with a forged source and destination port, causing a positive feedback loop which crashes computers. I originally published this in 1996 in the “Internet Holes” series under “UDP Viruses” (http://all.net/Analyst/netsec/1996-07.html)

The President’s Commission, Y2K, and Richard Clark

As part of the efforts surrounding the President’s Commission on Critical Infrastructure Protection, in the late 1990s I was doing assessments of vulnerabilities in power grids. This included, among other things, semi-in-depth reviews of the California ISO and the surrounding and supporting infrastructure, including telecommunications, power generation, delivery, user systems, people, and all manner of related issues. One of the things I identified at the time was the implications of intentional sympathetic vibration attacks on components in and between the power infrastructure, and the potential physical consequences. I considered this to be sensitive at the time, and asked classification folks to verify it should be classified and at what level. I think it was ultimately classified as secret or top secret or whatever.

So the report was sent on, became finalized, and some years later, I was brought into a classified meeting where it was disclosed to me by the then White House guy that there was this classified attack… you guessed it, Richard Clark, was telling me the results of my study from years earlier. It was interesting to hear his misunderstandings and his story of how this was discovered, such being somewhat different from the actual story of how it came to be.

Aurora and Perry Pederson

At some point I got an interesting call over an open line telling me that that thing I had written about some years earlier in the classified study was now being “taken care of”. It was an interesting call and indicated a specific national lab. Generally, a “theoretical” attack has to be demonstrated at some substantial scale before anyone with decision-making power will believe it. As it turned out, Perry Pederson was the person who decided the experiment had to be done and he funded it and got it done. I subsequently got to know Perry in more depth, and he’s a great guy who was trying to help get things moving. This was widely and openly published some time thereafter as “Aurora”. I also heard similar disclosures from other sources over a period of years, usually with a bit of “I’ve got a secret” involved.

Of course I don’t know what was happening in the classified realm of offense in that same time frame, but we all subsequently heard of the same methodology of creating resonance to damage physical systems being used against the Iranian nuclear facilities. But that’s a whole different line of discussion.

Conclusion

Technically, according to the classification guidelines I am aware of, the original work on the power grid vulnerabilities from the late 1990s should now no longer be classified. But I am not going to release details beyond those here, and of course there is no need to do so.

The real story here is the non-story. As recently as the date of this writing, I heard another “new and dangerous” attack technique being discussed publicly as part of a press release by a cyber-security company. It was – you guessed it – an Aurora a.k.a. sympathetic vibration a.k.a. resonance attack. Look in the early 1900s to find the real story behind anything “new”.

 Copyright (c) Fred Cohen, 2018 - All Rights Reserved