All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

What's new in cybersecurity?

At the end of the RSA conference each year, I try to get a sense of what's new. Generally, the answer is “not much”, and in that sense, this year did not disappoint. The same old same old. But there were some interesting things worthy of your attention.

Surveillance and deception going hardware

I wish I didn't have to say this, but surveillance is going to the hardware. One company had a hardware chip that sits between the processor and I/O to intercept all input and output. From a protection perspective, this is essentially a limited form of a hardware security kernel. That is, you can do this with hardware separations mechanisms already present in processors and a secure operating system. So why almost double the hardware on the processor board to add a function that is less capable than a security kernel? The only sensible answer is that surveillance is now completely transparent to and unaffected by the processor and operating system. Whoever controls this chip can examine and alter all signals in and out of the system, without any possibility of user or system intervention. High surety 3rd party deception and surveillance in the hardware. The logical conclusion if this continues is that every system is pre-bugged and remotely exploitable forever, the user/owner has no control, and from a forensics standpoint, who controls this device controls the outcome of the legal process.

Security cases for mobile devices

There is a new iPhone case that can 'go secure' at the slide of a switch. This switch slides a cover over the front and back cameras, covers and induces noise into the microphone, and adds a new microphone that does real-time end-to-end encryption (you have to have one on each side to do this of course). The trend toward independent physical controls to defend against mobile digital devices seems very similar to the hardwareization (new word) of surveillance. Spy vs. spy is alive and well in the mobile device world, where both surveillance and counter-surveillance are in an escalating spiral of increased cost to cure the basic problem that we cannot trust the vendors or the government. Caveat emptor. The lack of transparency forces increased uncertainty and the acts of government to subvert protection drives society toward a fear response. This is very unhealthy for society. Ask George Orwell.

Other issues

Deception for protection is on the rise, with more small companies pushing into the space and angel and venture funding for these companies. Content analysis for mood and other socio- and psycho- logical factors is on the rise, but they still ignore base rates, producing guilt by association, false positives, and all the problems that come with it. Sequential analysis is showing up in some graph-based methods, and this is a good thing, but it remains limited in scope and application, so we will see... Moderate change – normal expansion – same old...

Summary:

At some point society will either decide to stop the idiocy and agree on a sensible future for protection, or pay an eternal price in mindset and finance for the thought police of “1984”.

