What is Our Greatest Cyber-Security Threat?

OT vulnerability explained and national conversation about security and privacy urged at ASU Biodesign presentation

Where is the U.S. most vulnerable to cyber-security attack? And, what is the greatest need that we have regarding cyber-security, privacy and cyber-warfare? Those non-trivial questions were recently addressed by a distinguished military cyber-security expert, U.S. Navy Commander, Zachary Staples.

Commander Staples, who is the Director of the Naval Postgraduate School, Center for Cyber Warfare, in Monterey, California, spoke as an invited guest April 12, 2017, at the ASU Biodesign Institute. I was invited by a friend at the institute and decided to attend, hoping that it would yield some insight into a topic that I write about frequently.

I was not disappointed.

The Biodesign Institute at ASU takes on global challenges in healthcare, sustainability and security by developing nature-inspired solutions, and translating them into commercially viable products and clinical practices. With security as one of the three stated challenges on its 21st century agenda, Commander Staples' visit served to advance the institute's ambitious mission.

Not knowing what to expect at the presentation, I learned some very interesting things. First, the Navy is way cooler than I thought. In addition to projecting some impressive photos of U.S. Navy ships and planes, Commander Staples deftly pointed out that the Navy created Siri at its Office of Naval Research and that the military had invented long-distance hacking.

LTE Defect

A couple of relevant consumer issues also surfaced during his congenial, 75-minute address. First, the ubiquitous LTE mobile technology that we use every day has no location privacy—because of a technical compromise. Apparently, anyone can triangulate your location from cell phone tower data.

> *“Should electrical engineers (EEs) decide our privacy?” Staples asked.*

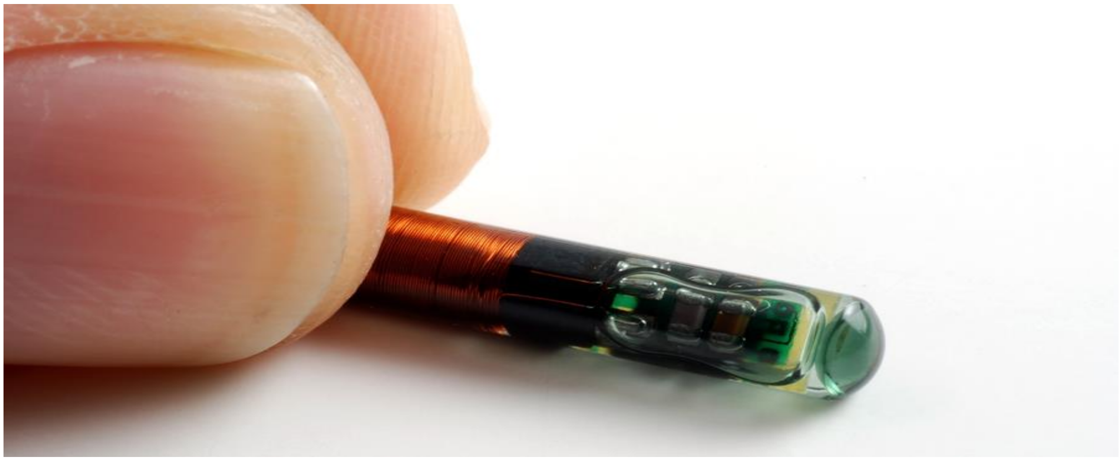
The other revelation I suspected (I’ve been writing about consumer intelligence-gathering technology in the banking industry). But, being among a group of mostly young adults, the reality of it hit home. That is,

> *“Target knows you are pregnant before your relatives do.” We are that transparent to skilled digital marketers.*

Every Computer at Risk

He presented some societal concerns as well. For example, he pointed out that the Internet is the equivalent of a Model T in terms of safety. In addition, he emphasized what everyone in cyber-security knows but won’t admit, that every computer is connected, whether by network or humans, and…

> *“Every computer is hackable.”*



Tracking Implants

Then, there were some surprising admissions—at least surprising to me. When asked about the financial services industry using intelligence community technology to track individuals for marketing purposes, he stated that he is not worried about that kind of technology transfer to the private sector. In fact, he said that he would like to see it increase through additional channels. Continuing pleasantly, he conjectured that:

> *“Personnel tracking will become the norm.”*

We may even have implants inserted under our skin at some future date, so that we are always tracked, he related. Sounds like a ‘safety and convenience vs. privacy’ debate is coming on that one.

Other surprises:

- Startups can get funds from the military to develop new technology.
- The best way to take down a network of terrorists (rather than smart bombs) might be an Information targeting strategy where deception is used to divide the group and they attack each other.
- The line where the government steps in to protect an American business under attack is not well-defined. The military intervened with the Somali pirates and Captain Phillips ($60 million at risk), but not between North Korea and Sony ($300 million lost).

Infrastructure Vulnerability Greatest Risk

Commander Staples proved to be an articulate ambassador of the military who demonstrated his practical knowledge of the cyber-security landscape. He also showed impressive skill at handling controversial questions and opinions from the partly student audience.

So, what keeps Commander Staples up at night? What does he, a decorated, battlefield-wise, military cyber-security expert, believe is the biggest cyber-threat to our country? Or, put another way, where is the greatest risk of damage? He stated it early in the presentation and then repeated it later for emphasis.

> *“The greatest current cyber-security threat to the U.S. is the vulnerability of the nation’s operational technology (OT).”*

He explained OT as the computers and machines that are controlling our industrial, agricultural and traffic infrastructure. All these systems are operated by computers or computerized machines. For example, only one of several harvesting combines is manned. The others follow along using GPS technology.

Because our industrial technology is older (we get new smartphones every 2-3 years), it is more vulnerable to damaging and constantly-evolving cyber-attacks (picture blastware and headless worms). The difficulty in securing it lies in the economic and technical inconvenience that much of it requires bolt-on security, if it has any at all.

Time for the Conversation

Along the way, Commander Staples pointed out that our digital laws are out of date (1986). Thus, it's time to have public conversations, a national discussion, on digital privacy, cyber-security and cyber-warfare to consider such issues as:

- What levels of privacy do we want and how will they be controlled?
- Where is the line between a private and a national response to an attack?
- Who has the responsibility for cyber-warfare, and a sensitive related issue,
- What levels of violence will we tolerate on the cyber-battlefield?

He stated very clearly that we need an open and civil debate on these issues. “The FBI vs. Apple is not a collaborative way to solve cyber-security problems,” he stated. I very much agree. Let's not let the EE's, attorneys, judges and terrorists decide our national privacy and security policy. So, join in the debate. There is so much to talk about.