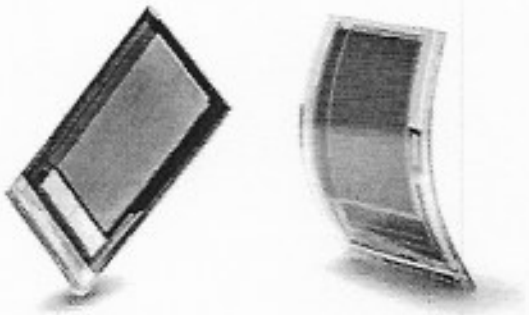
NEXT Flexible Sensors Reach Mass Production

Posted on June 20, 2017

NEXT Biometrics has succeeded in its aim of being ready for mass production of its flexible fingerprint sensors in Q2, the company has announced.



It's the result of a partnership with Taiwan-based display maker Innolux established last July, along with considerable investments in new production equipment. Now, everything is in place and up to spec, and NEXT says it's already "collaborating with customers on smart card projects," according to a statement from the company.

Commenting on the achievement, NEXT CEO Ritu Favre said, "We are not aware of any other fingerprint supplier able to mass produce flexible sensors," adding later that "[t]he smart card market represents endless opportunities". Indeed, it's one that has lately seen a steep ramp-up in activity, with Mastercard having recently announced successful trials of its biometric payment card, and Zwipe getting its first orders for its own biometric smart card solution, to name a couple of major examples.

As for NEXT, Innolux's enthusiasm attests to the company's prospects, with EVP Chin-Lung Ting having asserted in a presentation to investors that "NEXT's flexible panels will become the cash cow of Innolux."

Cybersecurity Fact vs. Fiction

Based on popular media, it's easy to be concerned about the security of smart cars, homes, medical devices, and public utilities. But how truly likely are such attacks?

Today's security industry is plagued with misinformation and FUD (fear, uncertainty, and doubt). Is your car safe to drive? Could that insulin pump you rely on give you a deadly dose? Could your power go off and never come back on? Is someone watching you through your smart home devices? Unfortunately, it's getting harder to identify the real threats from the exaggerated ones these days. I'd like to separate fact from fiction by addressing a few questions these headline-grabbing hacking tactics might prompt.

#1. Is my car secure?
Malicious hackers remotely hijacking cars is a frightening proposition, especially with the automotive industry rapidly moving toward automated driving. The recent CIA-related dumps on WikiLeaks listed car hacking as a "potential mission area" and films like the *Fate of the Furious* feature dramatic displays of hacked cars wreaking havoc at the command of criminals. Is remote car takeover really a threat?

The short answer is no. There's more fiction than fact when it comes to car hacking. Remote car takeover hacks usually target either the entertainment system or the onboard diagnostic (OBD) port and both have serious limitations. Targeting the OBD port requires either physical access to the port (i.e., sitting in the back seat with a laptop) or exploiting a third-party dongle connected to the port. Bosch Drivelog Connecter recently patched a vulnerability in its OBD dongle that could have allowed attackers within Bluetooth range to remotely kill a car's engine. But this physical proximity requirement (either in the car or within Bluetooth range) is a huge limitation for attacks.

Security researchers Dr. Charlie Miller and Chris Valasek put the automotive industry on notice in 2015 by hacking a Jeep Cherokee using a vulnerability in the entertainment system. Since then, manufacturers have focused more on securing the technology systems within cars. So don't expect to see a self-aware red Plymouth out on killing spree anytime soon.

.

#2. Is my smart home stupid when it comes to security?
If you're a fan of the hacker drama series *Mr. Robot*, you may recall the season 2 premiere that showed the worst-case scenario for a hacked smart home. The attackers controlled everything from the home audio system to the shower's water temperature. Fortunately, a full home takeover is extremely unlikely. But hacking individual Internet of Things (IoT) smart devices in the home is very much a concern today. So there's both fact and fiction when it comes to smart home hacking.

For example, hackers often target smart cameras and DVR systems when building botnet armies. Attackers use these IoT botnets to launch massive distributed denial-of-service attacks, such as the assault that took down DNS hosting provider Dyn in October 2016. The same vulnerabilities could easily be exploited to add remote access capabilities, potentially giving attackers full control over the devices and enabling them to use the device as a pivot point for launching further attacks. Consumers can limit the opportunities for a hostile takeover of smart home devices by not opening unneeded ports on their network firewall and configuring strong management passwords during device setup.

But the reality is that the amount of effort an attacker would have to put in to take over a smart home simply isn't worth it. So although you probably don't need to worry about someone taking over

your home, you should still be concerned about malicious hackers adding your smart devices to a botnet and using them to launch further network attacks.

#3. Could my healthcare device kill me?

There have been some big headlines over the years relating to healthcare hacks, like Dick Cheney's pacemaker or the more recent Johnson & Johnson insulin pump security vulnerability. The reality is that healthcare device manufacturers have been slow to design products that take security into consideration. This means the public is indeed at risk, making this threat more fact than fiction.

Network-connected medical equipment running embedded versions of Windows and Linux are common in the healthcare industry. These devices are often so highly specialized and sensitive to modification that they aren't patched or updated. We've already seen cybercriminals exploit these weaknesses with network worms spreading ransomware such as the WannaCry attack in May 2017. Unfortunately, these types of attacks are likely to continue.

The WannaCry ransomware did have one perk. It raised awareness of the risks associated with legacy and highly specialized healthcare systems. With many major hospitals completely shut down for most of the day by ransomware infections, we are likely to see changes to network security practices to protect healthcare systems against similar attacks.

#4. Are my utilities safe?

An attacker taking down the electric grid or another public utility would absolutely cripple the country's ability to function. These attacks are possible, but coordinating them on a nationwide scale is unlikely, so this threat is also a mix of fact and fiction.

There have already been several reported instances of intrusion over the past few years targeting public utilities within the United States. In one case, attackers brute-forced a valid password to an Internet-exposed Web portal. In another event, malware potentially linked to the Grizzly Steppe operation (the same group believed to be behind the recent attacks against the U.S. Democratic party) was detected on a laptop used by a Vermont utility. And in yet another instance, attackers successfully compromised the control system network for an unnamed U.S. public utility.

However, an attacker could most likely not shut down the entirety of our country's electric grid or water supply. Although the nation is moving toward a fully connected megagrid, overall electric utilities are still largely separated by region. Water utilities are often even more localized, meaning a failure in one likely won't affect another.

As you can see, most of these Hollywood hacks aren't viable in the real world, but most do contain a kernel of truth — sometimes a kernel you should be worried about.