MIT Technology Review

The Most Controlling Smartphone Ever Made

A custom version of Android exerts total control over what you can do, depending on where you are and what apps or networks you are using.

By David Talbot on December 6, 2012

This is one smartphone your boss and IT guy will love.

New Android models loaded with software from a Boston-based startup, Optio Labs, provide a smart way to secure a device. They control what data you can access and what you can do based on who you're with, what time it is, what other apps you're using, and where you are—right down to the specific room.

The technology's most unusual trick is its room-specific security and access settings: the phone would only show you sensitive company data—or conversely, block things like e-mail, camera, or texting functions—when in range of a Bluetooth beacon sending a cryptographic tether.

Your location in the room (as opposed to a hallway) could be further confirmed through a signal sent via a near-field-communications device—perhaps the one in your boss's phone, which you'd have to bump to get initial access, depending on the settings.

"You can dream up just about any rule—it can be your GPS location, or an indoor location detection: when you are in this specific room you can use these apps and connect to this data, but the moment you walk out we will delete the data, shut down the apps, prevent you from getting access to them," says Jules White, a computer scientist at Virginia Tech and a cofounder of the company.

Companies are struggling with how to leverage employee-owned devices without compromising company data or security (see "IBM Faces the Perils of 'Bring Your Own Device' " and "Bring Your Own Device"). Software from IBM allows a company to erase company data remotely without touching the user's personal data. And software like AT&T's Toggle creates two virtual devices inside your phone, one for work and one for personal use.

The company is already selling the custom Android OS and accompanying policy-management software to undisclosed systems integrators and handset manufacturers, who are expected to bring Android models containing the software to market in late 2013, often targeting federal government agencies. The policies could be customized and downloaded from the cloud, or handled in-house. Part of the software package is a long-running research project at Virginia Tech called Ghostbox.

The technology could prevent data from falling into the wrong hands if a device were lost or stolen. It might also help enforce proper-use policies, such as stopping an anesthesiologist from texting his girlfriend while the patient is getting the catheter snaked up to his heart. That's not a theoretical concern: in one medical journal's survey of cardiopulmonary bypass technicians, almost half admitted they'd texted or taken cell phone calls while managing patients on bypass.

Other security approaches do things like wipe the device when it leaves the country, based on GPS coordinates. And some software applies simple contexts for security, such as asking if a Wi-Fi network should be considered "home," "office," or "a public" network and adapting firewall rules. But blending physical context (such as location) with the context of computing (what network you're on, what data you're looking at) is new, says Doug Schmidt, a computer scientist at Vanderbilt University who was a PhD advisor to White but has no financial tie to the company or technology. "This approach can enforce policies in specific situations where they make sense—rather than all the time."

Some other security researchers point out that the technology—based on a region of Android called Android framework—operates at a level above a more fundamental part, called the kernel. So if the phone fell into the wrong hands, it might still be vulnerable to being compromised, or "rooted," they say, though this does not negate the value of the technology.

"If the owner of a phone is not malicious, this can mean you don't have to rely on the owner knowing 'Should I now open the e-mail here?' because it will do this for him," says Radu Sion, a computer scientist at Stony Brook University. "But I can take any Android phone, and "root" it, and get any access, and do anything I want while I seem to be following policy, unless they have hardware protection that they enforce."

White argues that the technology does provide some protection against rooting, and that Optio Labs's offering will still let customers add trusted hardware or other protections, if desired for things like classified information at the CIA.

Either way, there is plenty of need for good policy-driven controls, whether or not they are bulletproof against the most determined hackers.

David Talbot Chief Correspondent

I'm MIT Technology Review's chief correspondent, keeping an eye most often on the world of information and communication technologies—and asking my kids when I don't understand what's going on. Recent projects have taken me to Kenya to write about mobile-phone-based health initiatives, and... continue »

About David »

Follow @David_A_Talbot