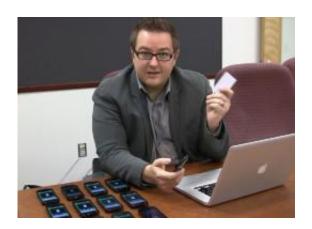# Cybersecurity breakthrough keeps sensitive data confined in physical space (w/ video)

October 17 2011

(PhysOrg.com) -- In a breakthrough that could aid spies, keepers of medical records, and parents who want to prevent their kids from "sexting," a team of Virginia Tech researchers has created software to remotely put smart phones under lockdown. The phones are given permission to access sensitive data while in a particular room, but when the devices leave the room, the data is completely wiped.

"This level of complexity and security, nobody else has," says Jules White, assistant professor in the Department of Electrical and Computer Engineering. "There are commercial products that do limited versions of these things, but nothing that allows for automating wiping and complete control of settings and apps on smart phones and tablets."

A general, for example, could access secret intelligence while visiting a secure government facility without fear that his or her smart phone or tablet computer might later be lost or stolen, White said. "This system provides something that has never been available before. It puts physical boundaries around information in cyberspace."

Medical caregivers could review patient information during a doctor visit, but – safeguarding patient privacy – doctors or nurses couldn't walk out of the examination room with the patient's records.

The software also enables central control of phone features such as preventing a smart phone's camera or email from working.

"For instance, you could keep certain apps from working in the operating room so surgeons wouldn't get distracted, or you could prevent nurses from taking patient photos and putting them on the Internet," White said. "In that same way, parents could restrict when and where children could send text messages to prevent distraction at school. Parents could also limit to whom messages with images could be sent in order to prevent 'sexting.'"

White and his team, in research underwritten by Virginia Tech Applied Research Corporation, modified Google's Android operating system to create the security features.

The team recently demonstrated the software for an inside-the-beltway group, Virginia Tech Intelligence and Defense Executive Alumni, or VT IDEA, composed of Virginia Tech alums who are interested in research that may benefit intelligence and military agencies.

"It was exciting to connect the VT IDEA group with Jules White and his team," said John Provo, director of the Virginia Tech Office of Economic Development. "Technology like this may be ripe not only for

commercialization, but it could also improve our nation's defense and security."

Provided by Virginia Polytechnic Institute and State University