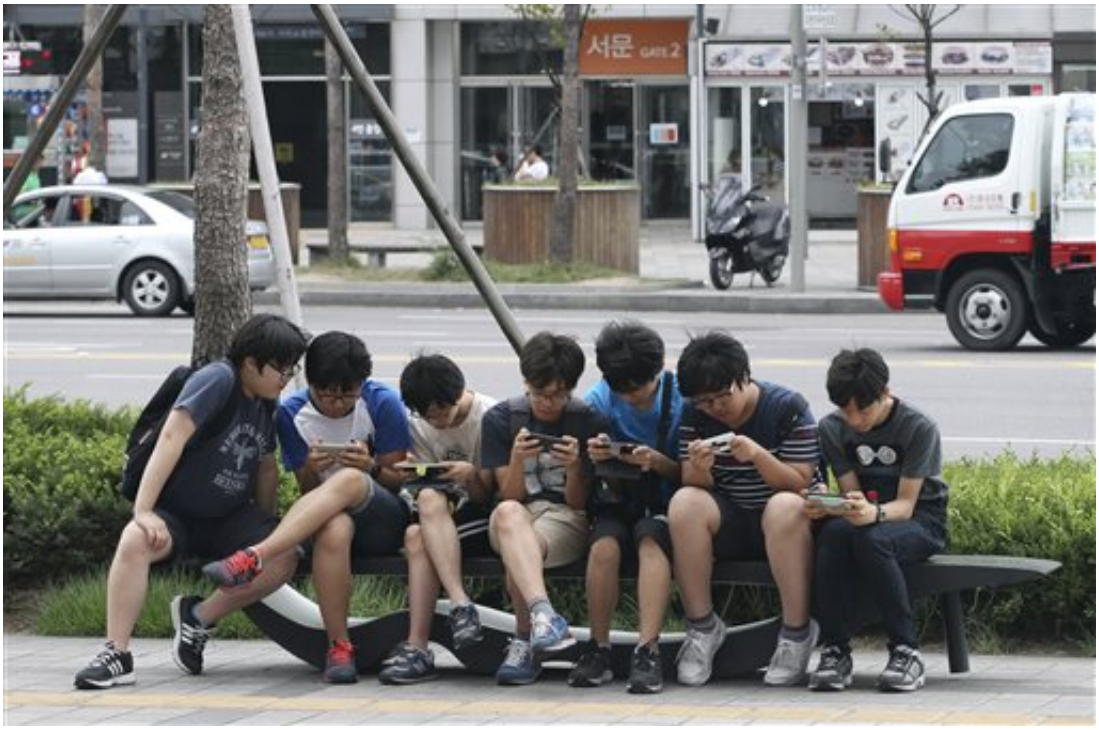
APNewsBreak: South Korea-backed app puts children at risk

September 21 2015, byYoukyung Lee And Raphael Satter



In this July 16, 2015, file photo, South Korean high school students play games on their smartphones on a bench on the sidewalk in Seoul, South Korea. Security researchers say they found critical weaknesses in a South Korean government-mandated child surveillance app, vulnerabilities that could have allowed hackers to easily violate the private lives of the country's youngest citizens. (AP Photo/Ahn Young-joon, File)

Security researchers say they found critical weaknesses in a South Korean government-mandated child surveillance app—vulnerabilities

that left the private lives of the country's youngest citizens open to hackers.

In separate reports released Sunday, Internet watchdog group Citizen Lab and German software auditing company Cure53 said they found a catalog of worrying problems with "Smart Sheriff," the most popular of more than a dozen child monitoring programs that South Korea requires for new smartphones sold to minors.

"There was literally no security at all," Cure53 director Mario Heiderich said. "We've never seen anything that fundamentally broken."

Smart Sheriff and its fellow surveillance apps are meant to serve as electronic baby sitters, letting parents know how much time their children are spending with their phones, keeping kids off objectionable websites and even alerting parents if their children send or receive messages with words like "bully" or "pregnancy."

In April, Seoul required new smartphones sold to those 18 and under to be equipped with such software, a first-of-its-kind move, according to Korea University law professor Park Kyung-sin. The Korean Communications Commission has promoted Smart Sheriff and schools have sent out letters to parents encouraging them to download the app.

Sometime afterward, Citizen Lab, based at the University of Toronto's Munk School of Global Affairs, and Cure53, acting on a request from the Washington-based Open Technology Fund, began sifting through Smart Sheriff's code.

What they found was "really, really bad," Heiderich said.

Children's phone numbers, birth dates, web browsing history and other personal data were being sent across the Internet unencrypted, making

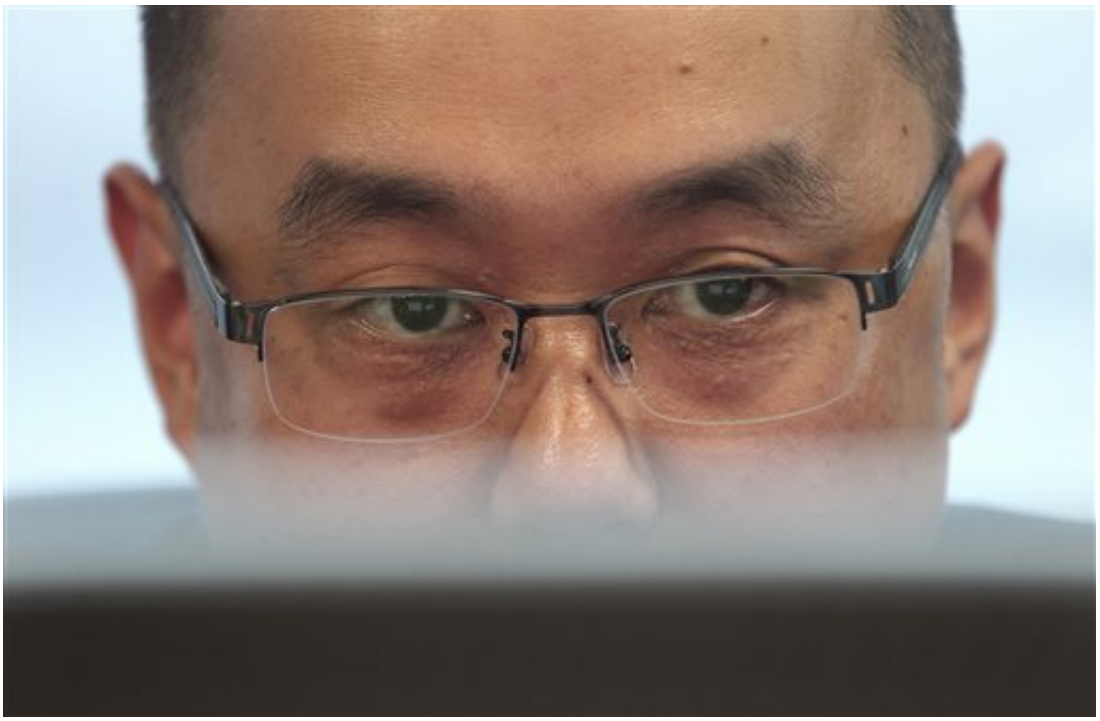
them easy to intercept. Authentication weaknesses meant Smart Sheriff could easily be hijacked, turned off or tricked into sending bogus alerts to parents. Even worse, they found that many weaknesses could be exploited at scale, meaning that thousands or even all of the app's 380,000 users could be compromised at once.

"Smart Sheriff is the kind of baby sitter that leaves the doors unlocked and throws a party where everyone is invited," said Collin Anderson, an independent researcher who collaborated with Citizen Lab on its report.

Citizen Lab said it alerted MOIBA, the association of South Korean mobile operators that developed and operated the app, to the problems on Aug. 3. When contacted Friday, MOIBA said the vulnerabilities had been fixed.

"As soon as we received the email in August, we immediately took action," said Noh Yong-lae, a manager in charge of the Smart Sheriff app.

The researchers were skeptical.



In this Sept. 18, 2015, photo, Ryu Jong-myeong, chief executive of security firm SoTIS, watches a monitor during an interview at his office in Seoul, South Korea. In separate reports released Sunday, Sept. 20, 2015, Internet watchdog group Citizen Lab and German software auditing company Cure53 said they found a catalogue of worrying problems with "Smart Sheriff," the most popular of more than a dozen child monitoring programs South Korea requires for new smartphones sold to minors. (AP Photo/Ahn Young-joon)

"We suspect that very little of these measures taken actually remedy issues that we've flagged in the report," Anderson said, adding that he believed at least one of MOIBA's fixes had opened a new weakness in the program.

Independent experts also weren't impressed with Smart Sheriff.

Ryu Jong-myeong, chief executive of security firm SoTIS, said the app did now appear to be encrypting its transmissions. But he was scathing

about some of the other failures uncovered by Citizen Lab, giving the Smart Sheriff's server infrastructure a security rating of zero out of 10.

"People who made Smart Sheriff cared nothing about protecting private data," he said.

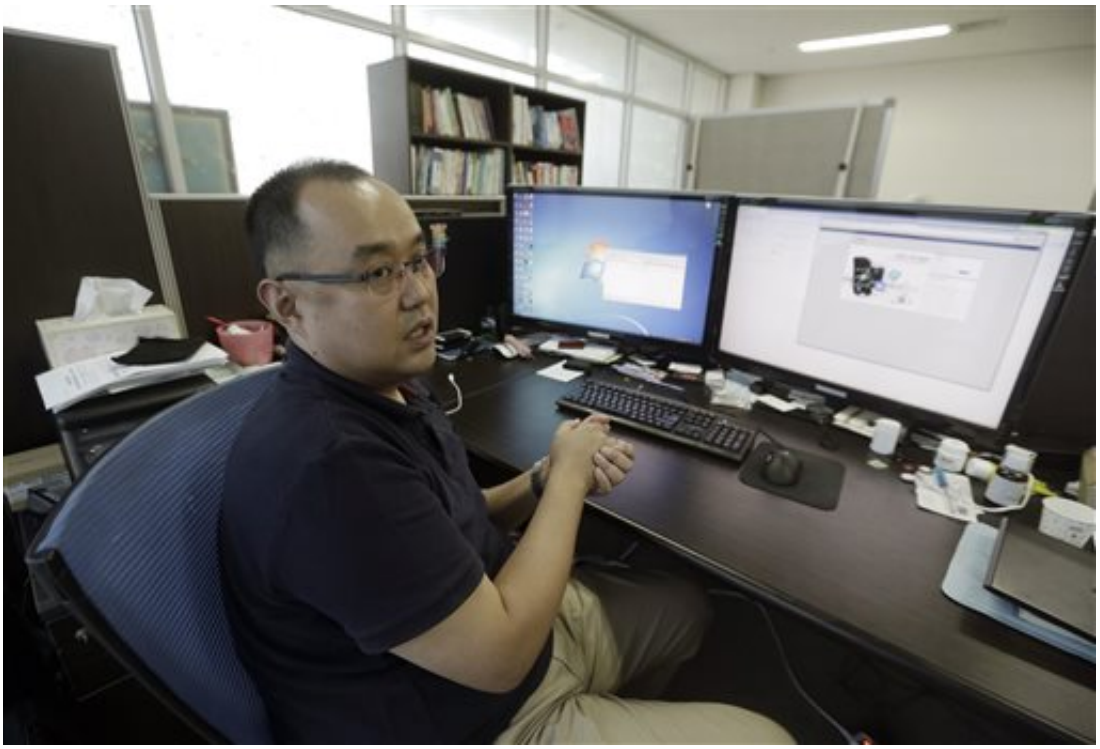
Kwon Seok-chul, chief executive of computer security firm Cuvepia Inc., said the lingering weaknesses meant children's data was still at risk.

"From a hacker's point of view, (the door) stays open," he said.

Many smartphone applications are unsafe, leaking private data or sending or storing it in risky ways.

But Citizen Lab Director Ronald Deibert said Smart Sheriff, a government-mandated program intended to monitor the intimate moments of so many children's lives, merited special scrutiny.

"This is not just a fitness tracker," Deibert said. "It's an application meant to satiate parents' concerns about their children's use of mobile or social media, which is in fact putting them at more risk."



In this Sept. 18, 2015, photo, Ryu Jong-myeong, chief executive of security firm SoTIS, speaks during an interview at his office in Seoul, South Korea. In separate reports released Sunday, Sept. 20, 2015, Internet watchdog group Citizen Lab and German software auditing company Cure53 said they found a catalogue of worrying problems with "Smart Sheriff," the most popular of more than a dozen child monitoring programs South Korea requires for new smartphones sold to minors. (AP Photo/Ahn Young-joon)

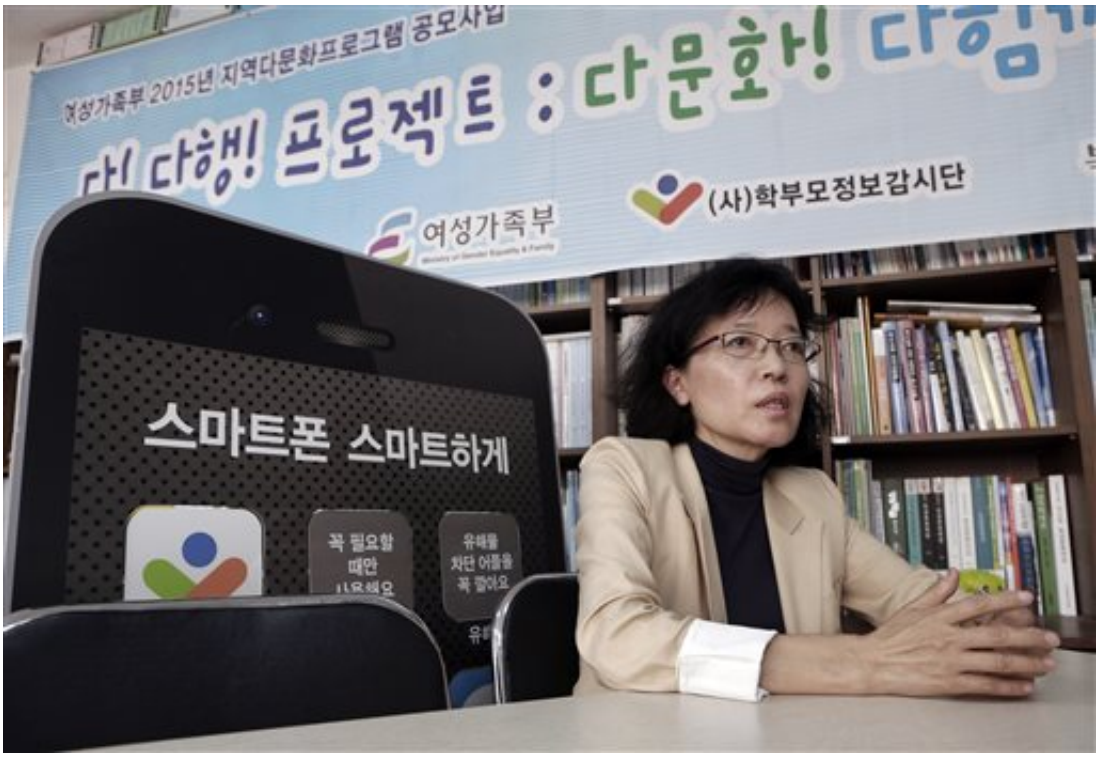
Park, the law professor, said the security flaws should push the government "to revisit the whole idea of requiring a personal communication device to be equipped with software that allows another person to monitor and control that device."

Some South Korean parents may soldier on with Smart Sheriff regardless. Lee Kyung-hwa, a mother of two whose Cyber Parents Union On Net endorses child surveillance, says all the app needs is an upgrade.

"If mothers feel happy thanks to the app, it is still helpful," she said.

But Kim Kha Yeun, a general counsel at libertarian-minded Open Net Korea, predicted that the revelations would turn parents against the technology.

"If they knew that the apps infect and endanger their children, I don't think any South Korean parents would want their children to have this monitoring app," he said.



In this Sept. 18, 2015, Lee Kyung-hwa, a mother of two who is head of Cyber Parents Union On Net, an activist group, which has given lectures to parents to urge them to use the app, speaks during an interview at her office in Seoul, South Korea. In separate reports released Sunday, Sept. 20, 2015, Internet watchdog group Citizen Lab and German software auditing company Cure53 said they found a catalogue of worrying problems with "Smart Sheriff," the most popular of more than a dozen child monitoring programs South Korea requires for new

smartphones sold to minors. Some South Korean parents may soldier on with Smart Sheriff regardless. Lee says all the app needs is an upgrade. (AP Photo/Ahn Young-joon)

The research has already prompted one mother to say she's uninstalling Smart Sheriff.

Yoon Jiwon told The Associated Press that she had previously been put off by the way in which the battery-hungry app kept sending her misleading alerts about her sons being bullied, prompting her to cross-examine them about each chat and text message, breeding frustration and mistrust.

She plans to uninstall the app after learning about the security weaknesses uncovered by Citizen Lab and now says Smart Sheriff was not a good way of interacting with her children.

"It's just not right for a mom to snoop on everything," she said.

More information: Citizen Lab's report: citizenlab.org/2015/09/digital… -korea-smart-sheriff

Cure53's report: cure53.de/pentest-report_smartsheriff.pdf

MOIBA: www.moiba.or.kr

https://phys.org/news/2015-09-apnewsbreak-south-korea-backed-app-children.html