

New device to beat wire-tapping

■ *Sirivish Toomgum*
The Nation

IF THE JUNTA's leading members are worried about foreign governments eavesdropping on their confidential calls, they can ask for help from a research team at King Mongkut's Institute of Technology Ladkrabang.

Assoc Prof Pitikhate Sooraksa and Asst Prof Kitdakorn Klomkarn showcased their anti-wiretapping device yesterday.

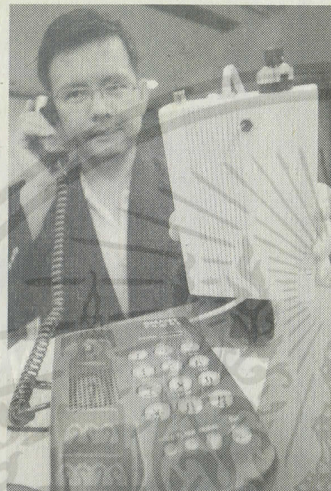
Their prototype, which is due to receive an international patent, has been funded by the Thailand Research Fund (TRF).

When connected to the fixed-line telephones of the caller and receiver, the device will convert their voices into a "complex chaotic signal" via encryption. While the callers will hear each other as normal, a wiretapping third party will hear only a hissing sound.

Pitikhate and his team from the institute's Faculty of Engineering started the project several years ago. "The device can be further tweaked to fit with mobile phones. If needed, we can morph it into a mobile-phone accessory," Pitikhate said.

When asked if Singapore could easily intercept or decode calls encrypted by their device, Pitikhate said that it might take a year and Kitdakorn was confident that a decipher would be impossible.

"I don't think our researchers are less capable than those in foreign countries and I'm confident



ASSOC PROF Pitikhate Sooraksa demonstrates the anti-eavesdropping device.

that they cannot crack our code. As the device is part of my ongoing doctorate thesis, if they can crack ours, it means I fail the exam," Kitdakorn said.

Pitikhate said the method could be applied to encrypt the transmission of faxes or pictures.

Recently, Council for National Security chief General Sonthi Boonyaratglin voiced concern that Singapore could be listening to confidential calls after its state-linked Temasek Holdings purchased Thai telecom firm Shin Corp last year.

Both researchers said that though many foreign countries

Panel to check on telecoms

The government moved yesterday to put the country's telecom networks under the microscope, following reports about local or foreign operators listening in on conversations.

Information and Communications Technology (ICT) Minister Sitthichai Pookaiyaudom said he had authorised a panel to look for any secret or unlawful operations embedded in the entire telecom system - wireless or wired, whether run by authorities or companies on concessions.

The task force - led by ICT Ministry permanent secretary Kraisor Pornsutee and staffed with technicians from TOT and CAT Telecom - will try to uncover any activities that detracted from the public's use of telecommunications or illegally or unfairly exploited users.

It has 60 days to report its findings.

Local mobile-operators insist they have never eavesdropped on local customers, but the government is taking nothing for granted.

"If they say no, we'll take it as a no for now, but the panel will look into that after setting up technical measures needed for inspection," Sitthichai said.

The government might consider taking back telecoms from foreign operators, but for that to happen, their sales contracts must include buy-back options, or else those operators must breach major deal conditions. "Otherwise, it will badly hurt foreign investors' confidence in Thai authorities and Thai companies in all industries," he said.

have sophisticated devices to prevent message interception, they consider them as militarily strategic and prohibit their export.

"It's important for Thailand to invent its own state-of-the-art tool," Pitikhate said.

Piyaporn Manthachitra, TRF's public relations consultant, said the fund had worked with the Thai Army on many projects but the

brainchild of Pitikhate's team had not been part of them.

She said that, if requested by the government, the TRF could include the device's development in its military project.

Pitikhate said several international inventors had used a similar technique of a chaotic signal to encrypt messages but with different application methods.

New device to beat wire-tapping, *The Nation*. 26 Jan 2007, p.2A

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้