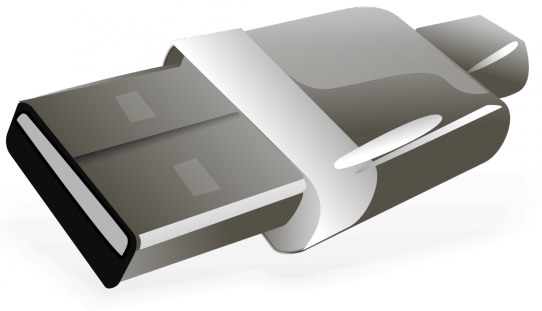
USB connections make snooping easy

10 August 2017



Credit: CC0 Public Domain

USB connections, the most common interface used globally to connect external devices to computers, are vulnerable to information leakage, making them even less secure than has been thought, Australian research shows.

University of Adelaide researchers tested more than 50 different computers and external USB hubs and found that over 90 percent of them leaked information to an external USB device. The results are being presented at the USENIX Security Symposium in Vancouver, Canada next week.

"USB-connected devices include keyboards, cardswipers and fingerprint readers which often send sensitive information to the computer," says project leader Dr Yuval Yarom, Research Associate with the University of Adelaide's School of Computer Science.

"It has been thought that because that information is only sent along the direct communication path to the computer, it is protected from potentially compromised devices.

"But our research showed that if a malicious device or one that's been tampered with is plugged into adjacent ports on the same external or internal USB hub, this sensitive information can be captured. That means keystrokes showing passwords or other private information can be easily stolen."

Dr Yarom says this 'channel-to-channel crosstalk leakage' is analogous with water leaking from pipes. "Electricity flows like water along pipes – and it can leak out," he says. "In our project, we showed that voltage fluctuations of the USB port's data lines can be monitored from the adjacent ports on the USB hub."

The leak was discovered by University of Adelaide student Yang Su, in the School of Computer Science, in collaboration with Dr Daniel Genkin (University of Pennsylvania and University of Maryland) and Dr Damith Ranasinghe (Auto-ID Lab, University of Adelaide). They used a modified cheap novelty plug-in lamp with a USB connector to "read" every key stroke from the adjacent keyboard USB interface. The data was sent via Bluetooth to another computer.

Dr Yarom says other research has shown that if USB sticks are dropped on the ground, 75 percent of them are picked up and plugged into a computer. But they could have been tampered with to send a message via Bluetooth or SMS to a computer anywhere in the world.

"The main take-home message is that people should not connect anything to USB unless they can fully trust it," says Dr Yarom. "For users it usually means not to connect to other people devices. For organisations that require more security, the whole supply chain should be validated to ensure that the devices are secure."

Dr Yarom says the long-term solution is that USB connections should be redesigned to make them more secure.

"The USB has been designed under the assumption that everything connected is under the control of the user and that everything is trusted – but we know that's not the case. The USB will

never be secure unless the data is encrypted before it is sent."

Provided by University of Adelaide