

Medienmitteilung

Bern, 16. Juni 2009

„Keykeriki“ – Dreamlab Technologies entwickelt zusammen mit dem Team remote-exploit.org den ersten Open-source-Universalempfänger für Schnurlostartaturen. Damit lässt sich das Funksignal einer beliebigen Schnurlostartatur abfangen und verarbeiten. Ausserdem können damit – für Ausbildungszwecke – Hackangriffe demonstriert werden.

Schnurlose Tastaturen gehören heute in vielen Büros und Privathaushalten zur Standardausrüstung und werden gerne auch im Front-Office-Bereich, beispielsweise an Bankschaltern, eingesetzt. Sie stellen jedoch – darauf hat die Dreamlab Technologies AG die Hersteller und die Öffentlichkeit bereits 2007 in einem White Paper hingewiesen – ein grosses Sicherheitsrisiko dar, weil damit Daten zum Teil unverschlüsselt per Funk übermittelt werden. Mit dem neu entwickelten, portablen Universalempfänger lässt sich das Signal mühelos abfangen und aufzeichnen; mit dem richtigen Antennen-Equipment auch aus grösserer Distanz. Die zum Abfangen des Signals notwendige Software lässt sich unter <http://www.remote-exploit.org> kostenlos herunterladen. Auch die Baupläne für die Hardware sind hier kostenlos online erhältlich.

Die Hardware

Die Hardware sollte, das war das Ziel, klein und portabel sein, sich zudem leicht erweitern und an zukünftige Bedürfnisse anpassen lassen. Keykeriki basiert auf einem Texas Instruments TRF7900-Chip, der von einem ATMEL ATMEGA Mikrokontroller kontrolliert wird. Für das Logging wurde ein SDCard-Interface eingebaut und zusätzlich ein zweiter USART-Channel für zukünftige Hardware-Erweiterungen („Backpacks“) angebracht. Das ganze Board kann direkt über den USB-Bus oder über eine stabile 5-Volt-Spannungsquelle versorgt werden. Keykeriki wird via USB-Port an einen Computer angeschlossen und entweder über eine Terminal-Applikation oder über die mitgelieferte KeykeriCTL-Software gesteuert. Geplant ist, in Zukunft auch vorgefertigte, bestückte Boards als Bausatz zum Selbstkostenpreis anzubieten.

Die Software

Weil die Hardware relativ flexibel gestaltet ist, können die meisten Features mittels Software eingebaut werden. In diesem ersten Release werden verschiedenste Funktionen angeboten, beispielsweise das Umschalten von Funkfrequenzen, die Ausgabe der Signalstärke, die Handhabung von Verschlüsselungen (rudimentäre statistische Analysen zur Berechnung des Schlüssels), Entschlüsselung und Speicherung der Daten und insbesondere eben das Mitlesen und Dekodieren von Microsoft 27MHz basierten Tastaturen.

Erweiterungen

Erweiterungen der Hardware sind ohne größere Umstände zu realisieren, da verschiedene Schnittstellen wie ein zweiter USART, I²C/TWI sowie das SPI nach außen geführt wurden. Somit können z. B. sogenannte Backpacks, etwa ein LCD Display Controller, über die USART-Schnittstelle angeschlossen werden. Hierbei müsste lediglich die frei verfügbare und dokumentierte Firmware im Quellcode modifiziert werden.

Geplante Erweiterungen der bestehenden Hardware sind eine Antennenverstärkung, Support für weitere Microsoft-Keyboards und die Produkte anderer Hersteller, die ständige Verbesserung von Hardware und Software sowie insbesondere das Ermöglichen der parallelen Verarbeitung von Signalen mehrerer Keyboards in der Nähe. Ausserdem ist auch das Entwickeln eines sendefähigen Keykerikis geplant, das Maus- und Tastatursignale an einen PC übermitteln kann.

Details zur Entschlüsselung werden in der Dokumentation auf der Webseite <http://www.remote-exploit.org> publiziert.

Dreamlab Technologies AG ist ein auf IT-Security spezialisiertes und international ausgerichtetes IT-Sicherheitsunternehmen. Seit 1997 führt Dreamlab Technologies High-End-Sicherheitstests, Beratungen und Schulungen durch und realisiert Lösungen basierend auf „best-in-class“-Open-Standard-Technologien. Dreamlab Technologies ist offizielle Schulungspartnerin und Repräsentantin von ISECOM (Institute for Security and Open Methodologies) für Frankreich, Deutschland, Österreich und die Schweiz. ISECOM ist die Herausgeberin von OSSTMM, der heute wohl am meisten verbreiteten Methodik für umfassende Sicherheitsaudits.

Kontakt für allgemeine Informationen	Rahel Schwab Dreamlab Technologies AG CH –3011 Berne Switzerland	+41 31 398 66 66 rahel.schwab@dreamlab.net http://dreamlab.net
Kontakte für technische Details	Max Moser, Senior Security Expert Thorsten Schröder, Senior Security Expert Dreamlab Technologies AG CH –3011 Berne Switzerland	+41 31 398 66 66 max.moser@dreamlab.net thorsten.schroeder@dreamlab.net http://dreamlab.net