#### NSA ANT Tastatu, 30C3, Jacob Appelbaum, 30 December 2013

Per Software die Tastenanschläge auf einem gehackten Rechner mitzuprotokollieren, ist den NSA-Spezialisten ohnehin ein Leichtes. Das Hardware-Implantat SURLYSPAWN aber kann selbst dann weitermelden, was der Nutzer gerade tippt, wenn der Rechner gar nicht online ist. Es erzeugt ein unsichtbal Signal, das durch jeden Tastenanschlag verändert wird und sich durch ein von außerhalb des Gebäudes erzeugtes Radarsignal sichtbar machen lässt. Auf diese Weise können Agenten etwa von der anderen Straßenseite mitverfolgen, was auf der manipulierten Tastatur gerade eingegeben wird – ohne dass eine Internetverbindung besteht.

SURLYSPAWN ist ein winziges Hardware-Implantat zur Aufzeichnung von Tastatureingaben, das Daten sammelt und durch Radarwellen-Bestrahlung übermittelt, ohne dass eine Software auf dem Rechner laufen muss. Es verbirgt sich in der Leitung zwischen Tastatur und Prozessor. Es gehört zur ANGRYNEIGHBORFamilie.



# SURLYSPAWN

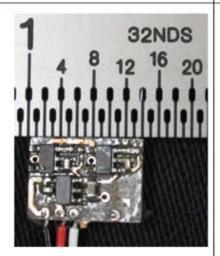
## ANT Product Data

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

07 Apr 2009

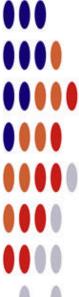
### (U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.



### (U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The signal is re-radiated, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.



Unit Cost: \$30

Status: End processing still in development

POC: , S32243, , , @nsa.ic.gov

Derived From: NSA/CSSM 1-52 Dated: 20070108 Declassify On: 20320108