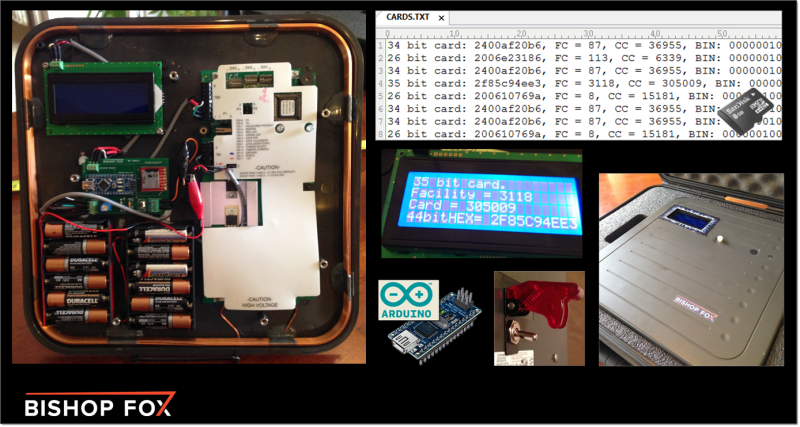
# Attack Tools

Practical guide to RFID hacking for penetration testers. Investigates the latest attack tools and techniques available for stealing and using RFID proximity badge information to gain unauthorized access to buildings and other secure areas.

# RFID Hacking Tools

Tastic RFID Thief



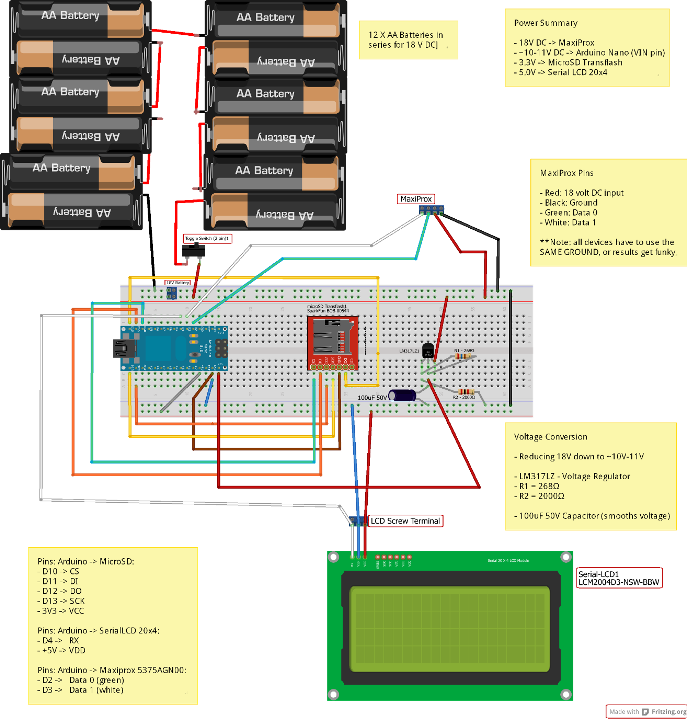
The Tastic RFID Thief is a silent, long-range RFID reader that can steal the proximity badge information from an unsuspecting employee as they physically walk near this concealed device.  Specifically, it is targeting **125KHz, low frequency** RFID badge systems used for physical security, such as those used in [HID Prox](https://www.hidglobal.com/products/Cards-and-Credentials/HID-Proximity) and [Indala Prox](https://www.hidglobal.com/products/Cards-and-Credentials/Indala) products.  Alternatively, the PCB could even be used to weaponize a **13.56MHz**, **high frequency** RFID reader, like those for [HID iCLASS](https://www.hidglobal.com/products/readers/iclass) access control systems.

Our goal is to make it easy for security professionals to re-create this tool so that they can perform RFID physical penetration tests and better demonstrate the risks posed by these technologies to their management.  The hope is that they can get up and running quickly, even if they don’t have an RFID or electrical engineering background.

Downloads of the code, parts list, and PCB designs can be found below, all of which are **free** for download and use.

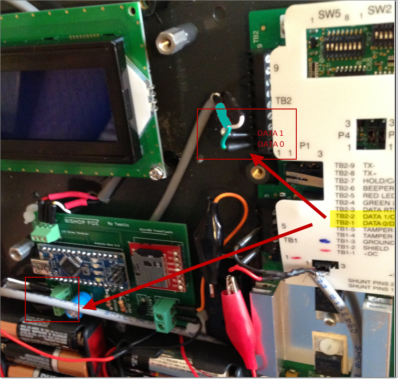
Design

We used an [Arduino microcontroller](http://arduino.cc/en/Main/ArduinoBoardNano) to weaponize a commercial RFID badge reader (the [HID MaxiProx 5375](https://www.hidglobal.com/products/readers/hid-proximity/5375) – bought on eBay) – effectively turning it into a custom, long-range RFID hacking tool.  This involved the creation of a small, portable [PCB](http://en.wikipedia.org/wiki/Printed_circuit_board) (designed in [Fritzing](http://fritzing.org/)) that can be inserted into almost any commercial RFID reader to steal badge info.

[](http://www.bishopfox.com/wp-content/uploads/2013/08/Tastic-Custom_RFID_Stealer_PCB-30Jun2013_bb.png)

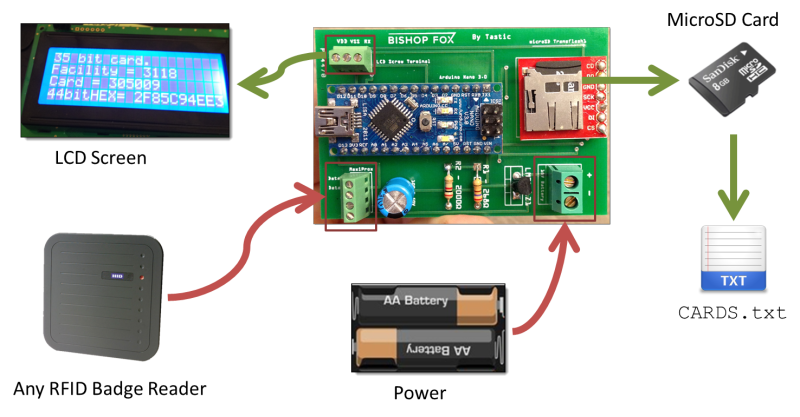
Tastic RFID Thief – Designed in Fritzing

Note, this PCB can alternatively be inserted into an Indala reader for testing Indala Prox deployments (e.g. [Indala Long-Range Reader 620](http://www.hidglobal.com/prod_detail.php?prod_id=92)).  Alternatively, the PCB could even be used to weaponize a high frequency (13.56MHz) RFID reader, such as the [iClass R90 Long Range reader](http://www.mobileidsolutions.com/resources/product-info/hid/iclass-r90-long-range-readers.pdf).  The PCB can be inserted into any RFID reader that supports the standard [Wiegand DATA0/DATA1 output](https://en.wikipedia.org/wiki/Wiegand_interface) (which is pretty much all of them).

[](https://www.bishopfox.com/wp-content/uploads/2013/08/Tastic-RFID_Thief-Wiegand_Inputs-Green_White.png)

Tastic RFID Thief – Wiegand DATA0/DATA1 – Green/White Input Taken from Reader

The tool steals badge information silently, and conveniently saves it to a text file (CARDS.txt) on a microSD card for later use such as badge cloning.

[](http://www.bishopfox.com/wp-content/uploads/2013/08/Tastic_RFID_-_PCB_InputsOutputsv2.png)

Tastic RFID Thief – PCB Inputs and Outputs

This solution allowed us to read proximity cards from up to 3 feet away, making the stealthy approach an actual reality.  A typical attack would involve placing the weaponized reader into a messenger bag or backpack, walking by someone in line at the local Starbucks, and capturing the RFID badge info on their person.  A visualization of what the attack would look like is captured in the image below:

[](http://www.bishopfox.com/wp-content/uploads/2013/08/RFID-StealingCardInfo.png)

Visualization of the RFID stealing attack from up to 3 feet away.

You can use the Tastic RFID Thief’s PCB files in the Tastic RFID – PCB Design.zip from the **Downloads** section below to have a nice PCB printed cheaply at any major site that prints custom boards.  A couple cheap pcb printers I’d recommend :

* 4pcb.com: ~$30 for 1 board with student discount:
  + <http://www.4pcb.com/>
  + <http://www.4pcb.com/pcb-student-discount.html>
* Fritzing Fab: ~30 Euro per board
  + [Fritzing Project – Bishop Fox – Tastic RFID Thief – long-range RFID reader](http://fritzing.org/projects/bishop-fox-tastic-rfid-thief-long-range-rfid-reade)
  + <http://fab.fritzing.org/fritzing-fab>
  + <http://fab.fritzing.org/pricing>

**Videos**

[**RFID Hacking: Intro to Tastic RFID Thief - 05Sept2013**](https://www.youtube.com/watch?v=gP9f_TiKHIY)

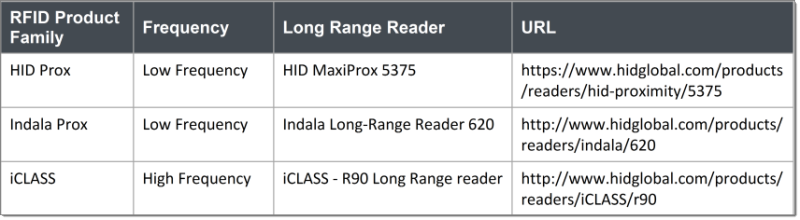
[**RFID Hacking: Look at Insides - Tastic RFID Thief**](https://www.youtube.com/watch?v=Hc4y7givo_o)

[*By PoseLab*](http://poselab.com)

For more of our RFID Hacking videos, see our [RFID Hacking: Media Gallery](http://www.bishopfox.com/resources/tools/rfid-hacking/media-gallery/).

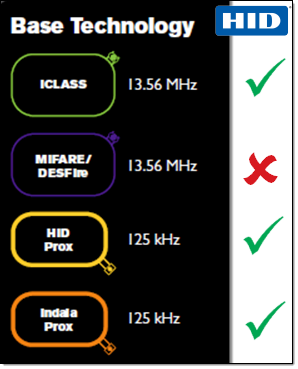
Long Range Readers to Weaponize

The table below provides links to the 3 long range RFID readers sold by HID Global, that can be weaponized by the Tastic RFID Thief PCB. You can typically find all 3 available for purchase on eBay.

[](http://www.bishopfox.com/wp-content/uploads/2013/08/TasticRFIDThief-CommercialReadersToWeaponize-1.png)

HID Global – Long Range RFID Readers to Weaponize

Tastic RFID Thief’s PCB can be inserted into almost any commercial RFID badge reader.  It has been successfully tested with the long-range readers sold by HID Global for 3 of their 4 [major RFID product families](http://www.hidglobal.com/sites/hidglobal.com/files/resource_files/hid_full_product_catalog_en.pdf).

[](http://www.bishopfox.com/wp-content/uploads/2013/08/HID_Global-3of4_RFID_Product_Families_Covered.png)

HID RFID – 3 of 4 Product Families Covered

For the [Black Hat USA 2014 – Tool Arsenal](https://www.blackhat.com/us-14/arsenal.html#Brown), we demonstrated using the Tastic RFID Thief’s PCB to weaponize both an [Indala – Long-Range Reader 620](http://www.hidglobal.com/products/readers/indala/620) and an [iCLASS – R90 Long Range Reader](http://www.hidglobal.com/products/readers/iCLASS/r90). Illustrated in the photo below, we can see that we simply hooked up the black/red power cables and the green/white standard [Wiegand DATA0/DATA1 output](https://en.wikipedia.org/wiki/Wiegand_interface) cables to our PCB to effectively weaponize those readers.

[](http://www.bishopfox.com/wp-content/uploads/2013/08/TasticRFIDThief-iClassR90_and_Indala620-Aug2014.png)

Tastic RFID Thief – PCB used to weaponize both the Indala 620 and iCLASS R90 long range readers.

The folks over at ToolsWatch.org caught a good photo of the demo on their [tool arsenal day 1 wrap up post – 06Aug2014](http://www.toolswatch.org/2014/08/black-hat-arsenal-usa-2014-wrap-up-day-1/).

[](http://www.bishopfox.com/wp-content/uploads/2013/08/BlackHat2014-BishopFox-Photos-Fran-1.jpg)

Tastic RFID Thief – Demo of Weaponized HID Indala and iCLASS long-range readers at Black Hat USA 2014 – Tool Arsenal – 06Aug2014.

Optimizing Read Range

Greater read distances can be achieved by reducing interference and providing clean, high voltage. For more details on improving read range, see the following resources:

* [HID – MaxiProx 5375 – Product Page](https://www.hidglobal.com/products/readers/hid-proximity/5375)
* [HID – MaxiProx 5375 – Installation Guide PDF](https://www.hidglobal.com/sites/hidglobal.com/files/maxiprox_ins_en.pdf)
* [HID – Installing the HID MaxiProx for optimum read range – AppNote 010 – (PDF)](http://www.hidglobal.com/sites/hidglobal.com/files/0010_an_en.pdf)
* [HID Whitepaper – Achieving Optimal Read Range – It’s all in the Frequency (PDF)](https://www.hidglobal.com/achieving-optimal-read-range-whitepaper)
* [Gorferay.com – Installing the HID MaxiProx for Optimum Read Range](http://www.gorferay.com/installing-the-hid-maxiprox-for-optimum-read-range/)

**Install Notes – Arduino Sketch**

**Note 1**: The design was compiled and loaded onto the [Arduino Nano v3.0](http://arduino.cc/en/Main/ArduinoBoardNano) using the [Arduino v1.0.1 software](https://www.arduino.cc/en/Main/OldSoftwareReleases#1.0.x) with the added [sdfatlib (05Dec2011)](https://web.archive.org/web/20150101142121/http:/sdfatlib.googlecode.com/files/sdfatlib20111205.zip) library to handle the microSD card writing.  See [Arduino – Libraries](https://web.archive.org/web/20130426132017/http:/arduino.cc/en/Guide/Libraries) for more info on adding additional Arduino libraries. Unzip the sdfatlib20111205.zip file and copy the “SdFat” folder to “/arduino-1.0.1/libraries/SdFat/” (starting at location where your arduino.exe program is located).  If there was already an “SdFat” folder there, delete it and copy over from the zip cleanly.

Set Tools->Board value to “Arduino Nano w/ ATmega328“. Go to File->Upload to upload our sketch: Tastic\_RFID\_Arduino\_Code.ino.

**Note 2**: Make sure to format the filesystem of the microSD card to [FAT](http://en.wikipedia.org/wiki/File_Allocation_Table) (not [FAT32](http://en.wikipedia.org/wiki/File_Allocation_Table#FAT32)). This will require you to use a smaller size microSD card, [2GB or less](http://support.microsoft.com/kb/118335). See: a [cheap microSD card example](https://www.amazon.com/gp/product/B000VOU91U/) product that works well [here](https://www.amazon.com/gp/product/B000VOU91U/).

**Note 3:** Shubham Shah was kind enough to put together a blog post providing a detailed assembly guide for the Tastic RFID Thief. This guide, which is full of step-by-step instructions and photos can be found at: <https://shubh.am/guide-to-building-the-tastic-rfid-thief/>

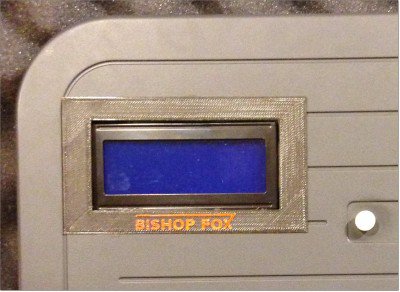
**Note 4:** For tips on how to completely silence your [HID MaxiProx 5375 reader](https://www.hidglobal.com/products/readers/hid-proximity/5375), see our blog post: [Tastic RFID Thief: Silent RFID Hacking – Bishop Fox](http://www.bishopfox.com/blog/2014/09/tastic-rfid-thief-silent-deadly/).

**Downloads**

|  |  |
| --- | --- |
| [Tastic RFID - Parts List.txt](https://www.bishopfox.com/download/778/)  List of part names and URLs used to create the Tastic RFID Thief. | [Tastic RFID - PCB Design.zip](https://www.bishopfox.com/download/817/)  Fritzing and related design files needed to recreate the PCB used to weaponize RFID readers, creating the Tastic RFID Thief. |
| [Tastic RFID - Arduino Code.zip](https://www.bishopfox.com/download/814/)  Code to load onto the Arduino Nano v3.0 to control the logic of the Tastic RFID Thief. |  |

**LCD Faceplate - 3D printable**

A 3D printable LCD 20×4 faceplate to cover the LCD rectangular hole on the front of the Tastic RFID Thief.  The example below was printed using a [Makerbot Replicator 2 – 3D printer](http://store.makerbot.com/replicator2).

[](http://www.bishopfox.com/wp-content/uploads/2013/08/LCD_Faceplate-BishopFox-TasticRFIDThief-2.jpg)

3D printable LCD faceplate for cover of Tastic RFID Thief.

If you are like me, you may have made a mess of cutting out the rectangle for the LCD on the plastic cover of your [**HID MaxiProx5375 RFID Reader**](https://www.hidglobal.com/products/readers/hid-proximity/5375).

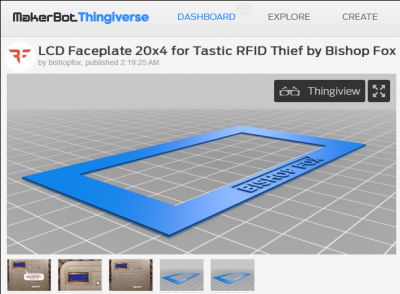
If so, no worries.  This extremely thin (0.5mm), [3D printable LCD faceplate](http://www.thingiverse.com/thing:346531) and a little **[krazy glue](http://www.amazon.com/gp/product/B000M7RZG8/)** is all you’ll need to make that LCD hole look nice and clean.

[](http://www.bishopfox.com/wp-content/uploads/2013/08/LCD_Faceplate-BishopFox-TasticRFIDThief-1a.jpg)

Clean cover of Tastic RFID Thief with 3D printable LCD faceplate.

You can also find details on the 3D printable object at our Thingiverse.com page at:

* [Thingiverse.com – LCD Faceplate 20×4 for Tastic RFID Thief by Bishop Fox](http://www.thingiverse.com/thing:346531)

[](http://www.bishopfox.com/wp-content/uploads/2013/08/LCD_Faceplate-BishopFox-Thingiverse-1.png)

Thingiverse.com – LCD Faceplate 20×4 for Tastic RFID Thief by Bishop Fox