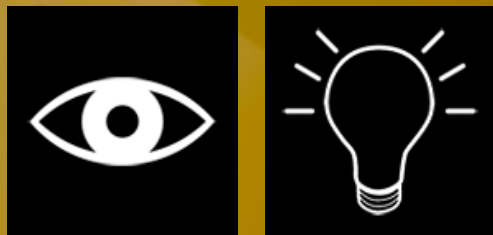




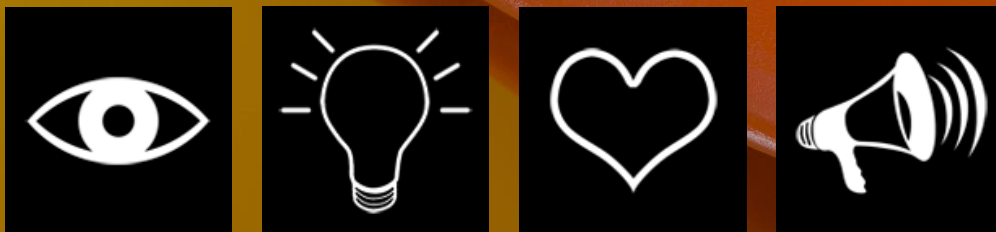
BadUSB

aneb dobrodružství se zviřátky



Michal Altair Valášek

Development & Security Consultant, Altairis
michal.valasek@altairis.cz | www.aspnet.cz | www.secpublica.cz



USB Rubber Ducky

- Keystroke injection tool
 - * 2010, \$ 44.99
 - Slot na MicroSD kartu
 - **www.usbrubberducky.com**
- Vzhled flash disku
 - Emulace klávesnice nebo jiného HW, včetně kompozitního
 - Jednoduchý skriptovací jazyk
- **Payload encoder s podporou české klávesnice:**
 - <https://github.com/ridercz/USB-Rubber-Ducky>
- **Payload build systém:**
 - <https://github.com/ridercz/DuckyBuilder>





demo

Dobrodružství
s gumovou kačenkou



altairis

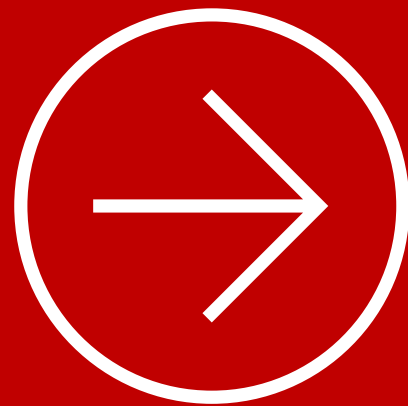
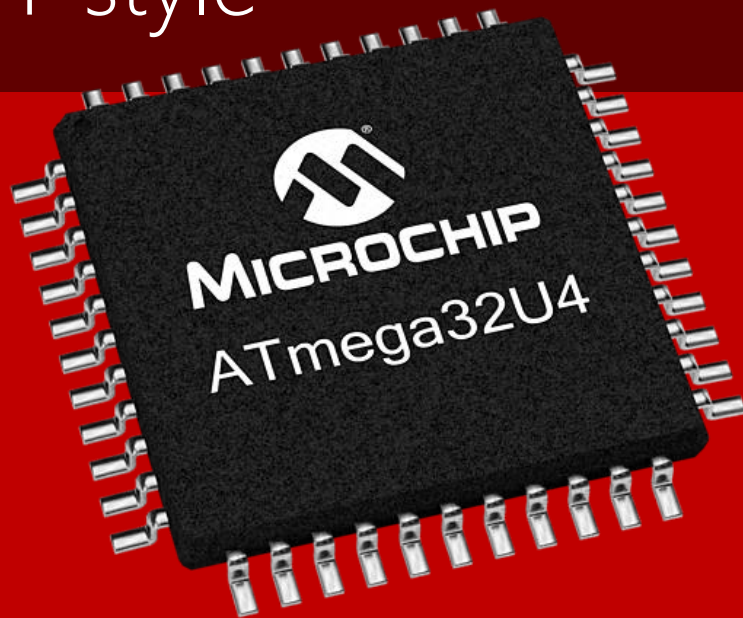








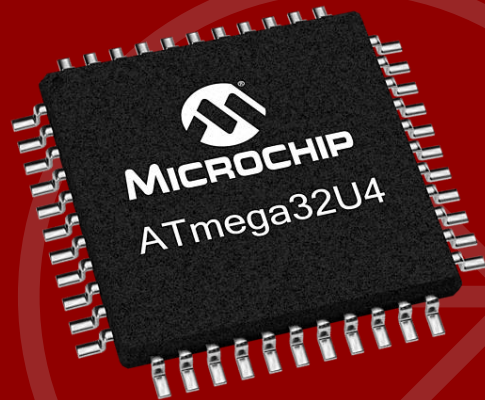
DIY style



 altairis

ATmega32U4

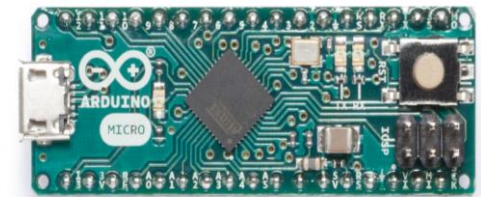
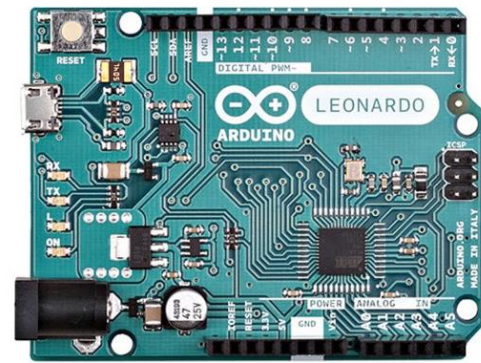
- Osmibitový AVR mikrokontroler
- USB 2.0 Full-speed/Low Speed Device Module
- Podpora emulace jakéhokoliv USB zařízení
 - Klávesnice, myši
 - Ostatní HID (game controller...)
 - Mass Storage Device



<http://www.microchip.com/wwwproducts/en/ATmega32u4>

Arduino Leonardo, Arduino Micro

- SoC: **ATmega32U4**
- Logika: 5 V
- Flash: 32 kB
- SRAM: 2.5 kB
- EEPROM: 1 kB
- Frekvence: 16 MHz
- Rozměry: 53,5×68,6 mm, 20 g
18×48 mm, 13 g



Dostupné na AliExpressu

- Dostupné pod mnoha názvy
 - BadUSB
 - CJMCU Beetle
 - ...
- Varianty s MicroSD slotem, v case nebo miniaturní
- Cena do \$ 10 včetně poštovného



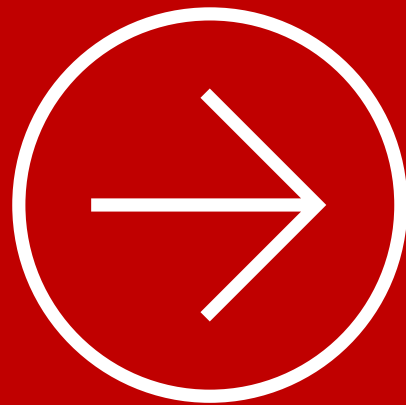


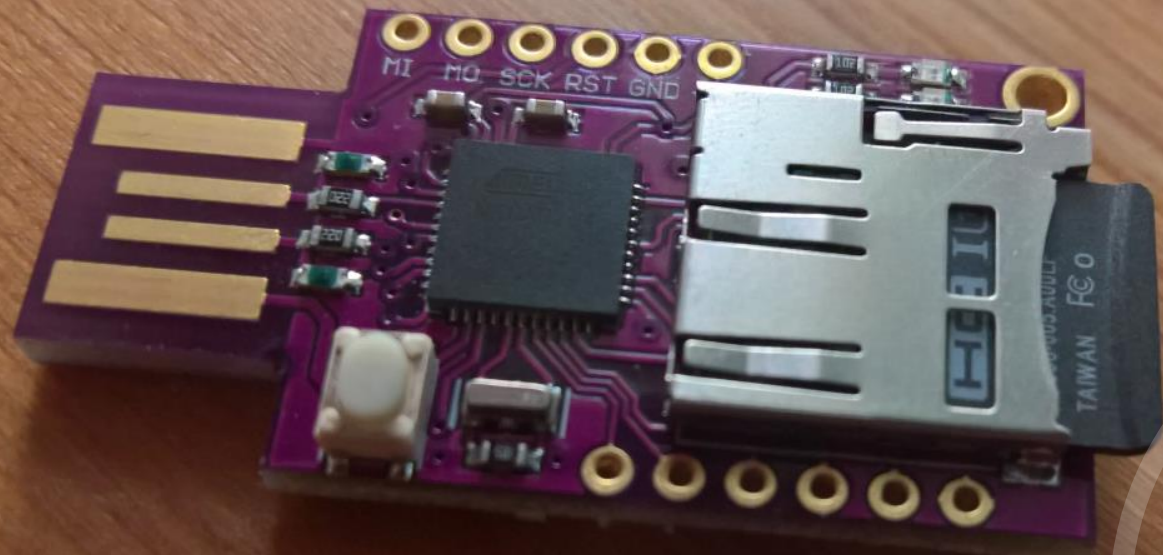
demo

Dobrodružství s broučkem



altairis





SW podpora a odkazy

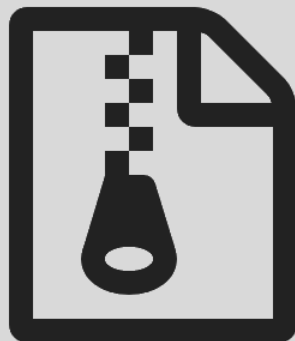
- Obecně o programování Arduina
 - <https://www.arduino.cc>
- Podpora českých klávesnic
 - <https://github.com/ridercz/CzechKeyboard>
- WiDucky
 - WiFi-enabled Rubber Ducky, postaveno na ESP8266
 - <https://github.com/basic4/WiDucky>
- Duckduino
 - Převod Ducky skriptů na Arduino kód
 - <https://nurrl.github.io/Duckduino/>





Download prezentací a příkladů

<https://altair.is/prednasky/20171009-EurOpen.zip>



dotazy ?

www.aspnet.cz

www.rider.cz

facebook.com/rider.cz

twitter.com/ridercz

ask.fm/ridercz

youtube.com/altairiscz

michal.valasek@altairis.cz