When USB devices attack

Manchester Grey Hats

PRESENTED BY:
Tim Wilkes

@mcrgreyhats

Disclaimer: Please don’t be a dick. I accept no responsibility.
Ever.
For Anything.

1997 was not a good year...

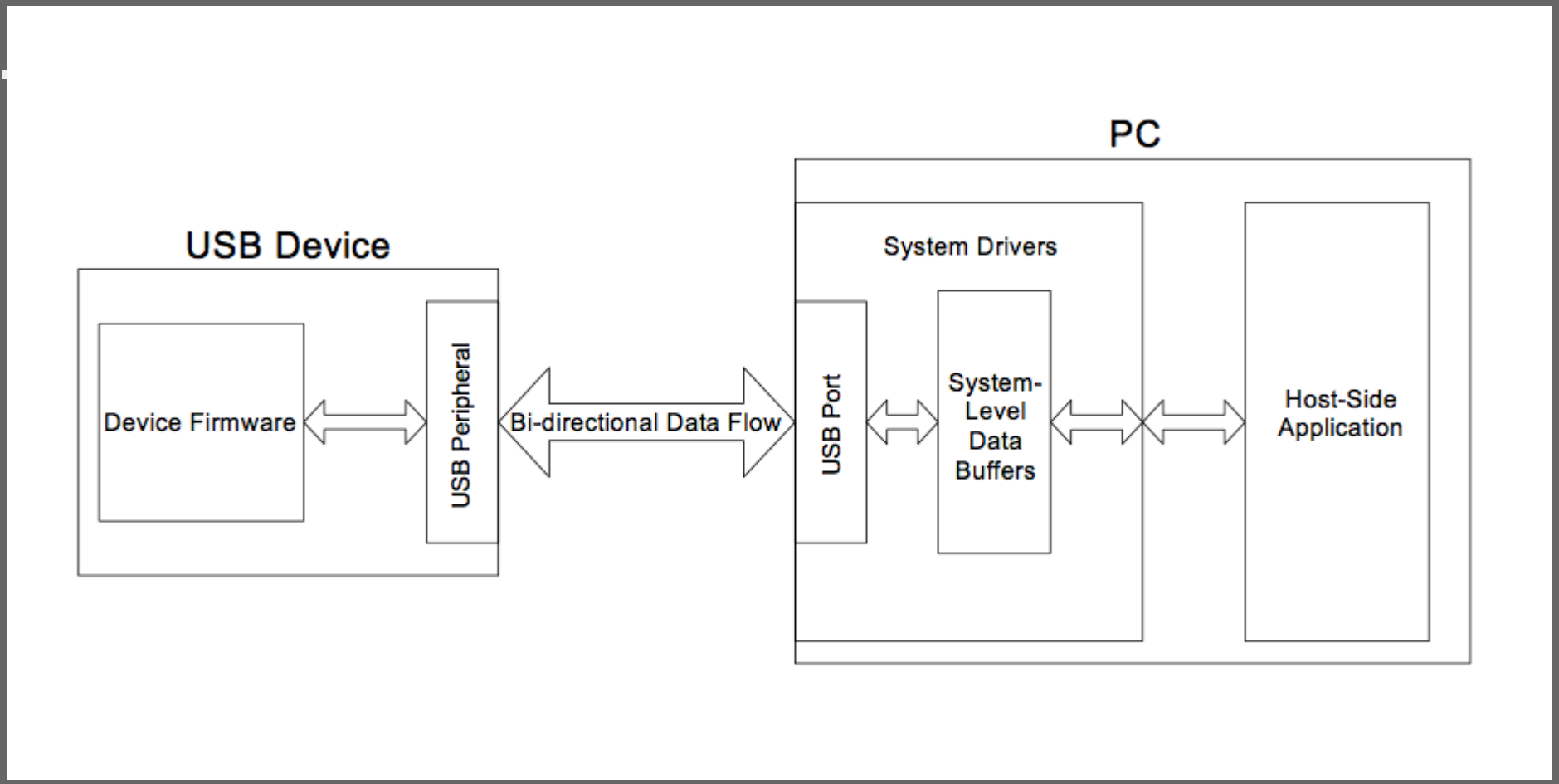
- Windows 95 OSR 2.5 came out
- Different connectors for different devices
- USB Support
- Autorun was a thing
- Clippy...

Fast forward to 2017...

- USB Keyboards
- USB Storage
- USB Network
- USB Serial Interfaces
- USB fans ?
- USB gimmicks

So USB does quite a bit...

- How does the computer know what device is attached?



Interested in USB Development?

- Try the HIDIOT by Rawhex.
- Rawhex is not Digistump
- The HIDIOT is not a digispark
- They are compatible
- The HIDIOT is awesome for USB development
- Rawhex are awesome – We have 2 HIDIOTS to give out

Just to back up a little

- Season 2 (Episode 3) of Hak5 released the USB Switchblade based on USBdumper (2006)
- Later USB-hacksaw
- Utilized Autorun with the USB storage.
- Later became the basis for the...

USB Rubber ducky

Must be a good idea...

- Many imitators
  - Peensy / Teensy
  - Digispark / ATTiny based
  - BAD USB
- Now the Bash Bunny is also available
  - Network / storage /keyboard / serial

Also The Lan turtle

- Network based attacks
  - Imitators too
  - Poison tap

Enter Mr Robot

- USB drops
  - Rubber ducky costs $50
  - Bash Bunny costs $150
- Not cheap / disposable

Way too expensive

- So what about the alternatives?
  - Teensy is around £10
  - Peensy is more (+ soldering)
  - BADUSB – PITA (if you can find the drive)
  - Digispark is £1 – We have a winner!

Downsides

- Looks – requires camouflage
- Limited memory
  - Can’t type out meterpreter (directly)
  - Has no feedback (but none of the devices do)

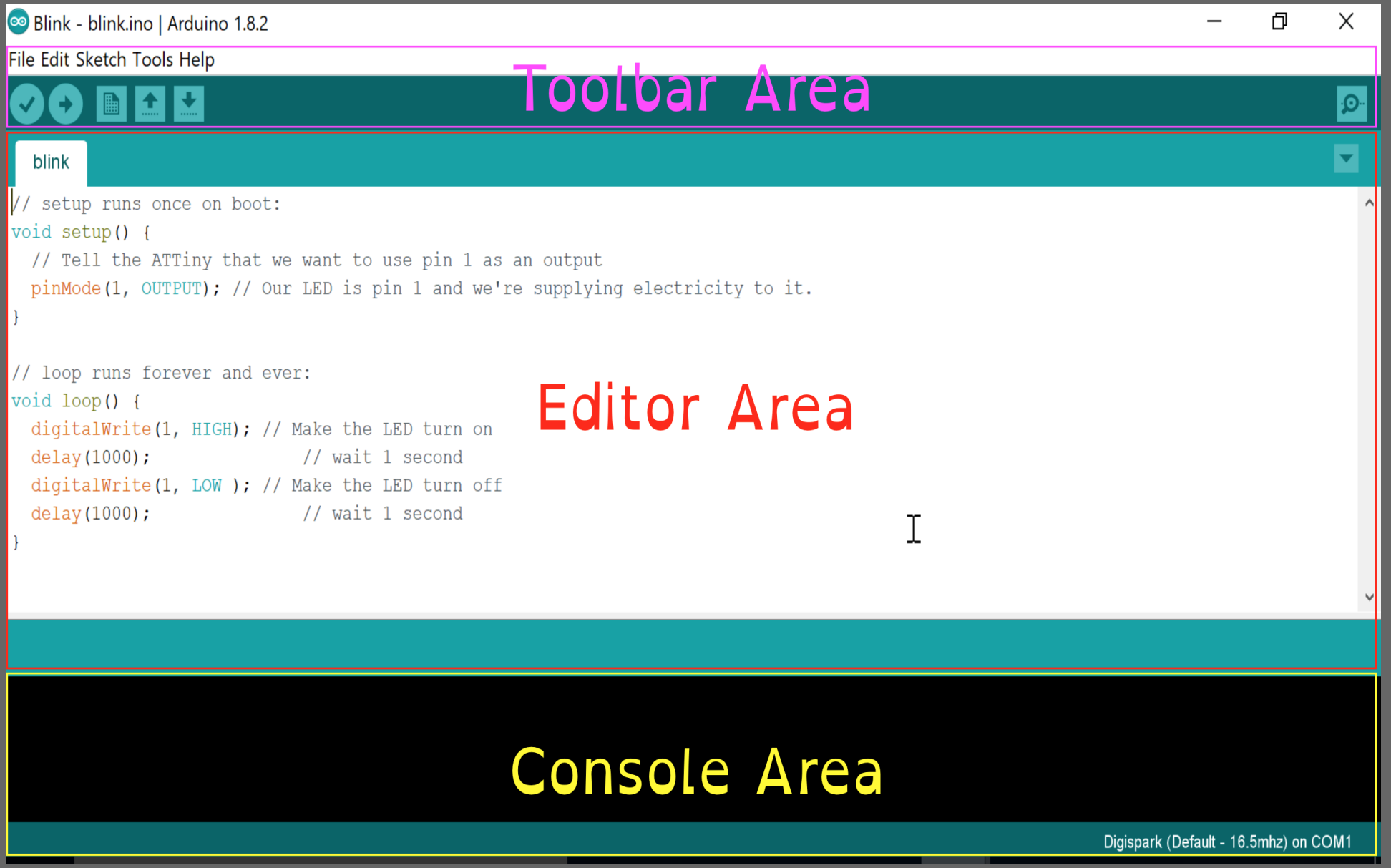
Speaking of Feedback...

- If you enjoy the workshop, please leave feedback on meetup.com

Is everyone set up for the Workshop?

- Do you have the Arduino software installed?
- Do you have the digispark board installed?
- http://digistump.com/package_digistump_index.json
- Drivers?

The IDE


Blink - blink.ino | Arduino 1.8.2
File Edit Sketch Tools Help
Toolbar Area
blink
// setup runs once on boot:
void setup() {
// Tell the ATTiny that we want to use pin 1 as an output
pinMode(1, OUTPUT); // Our LED is pin 1 and we're supplying electricity to it.
}
// loop runs forever and ever:
void loop() {
digitalWrite(1, HIGH); // Make the LED turn on
delay(1000); // wait 1 second
digitalWrite(1, LOW); // Make the LED turn off
delay(1000); // wait 1 second
}
Editor Area
Console Area
Digispark (Default - 16.5mhz) on COM1

Ex 1 - Blinken Lights

Ex 2 – Text in Notepad

Ex 3 - Fakeupdate

Ex 4 – Web deploy

Ex 5 - Random Number Gen

- Don’t use in anger!

Ex 6 – Rubber Ducky Payload

Questions?

CONTACT:
usb@php-systems.com