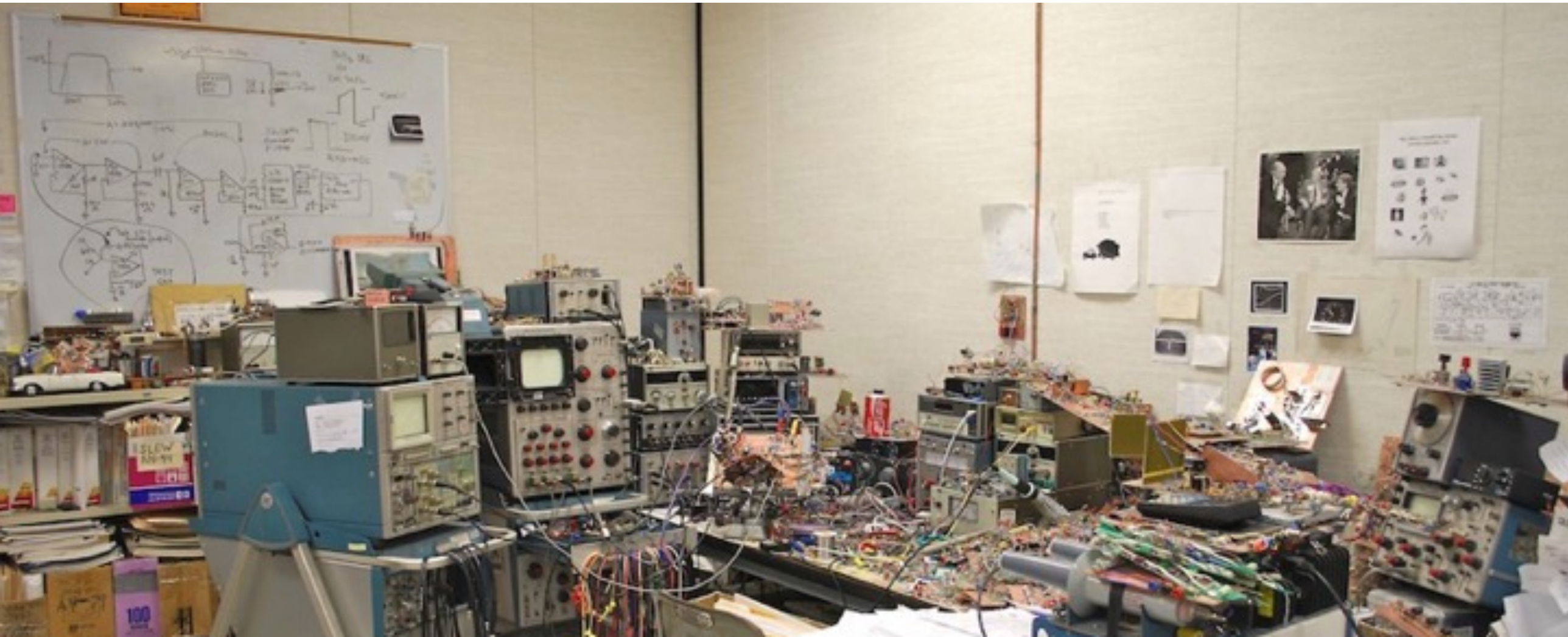
Hardware Hacking Basics

DEFCON 26 Workshop

Joe Grand (@joegrand)



Workshop

- Gain skills to reverse engineer, modify, and/or attack products on your own
  - Soldering / Desoldering
  - Circuit Board Modification
  - Signal Monitoring / Analysis
  - Memory Extraction
- Subset of Joe Grand's Hands-on Hardware Hacking 2-day training
  - **`www.grandideastudio.com/portfolio/hardware-hacking-training/`**



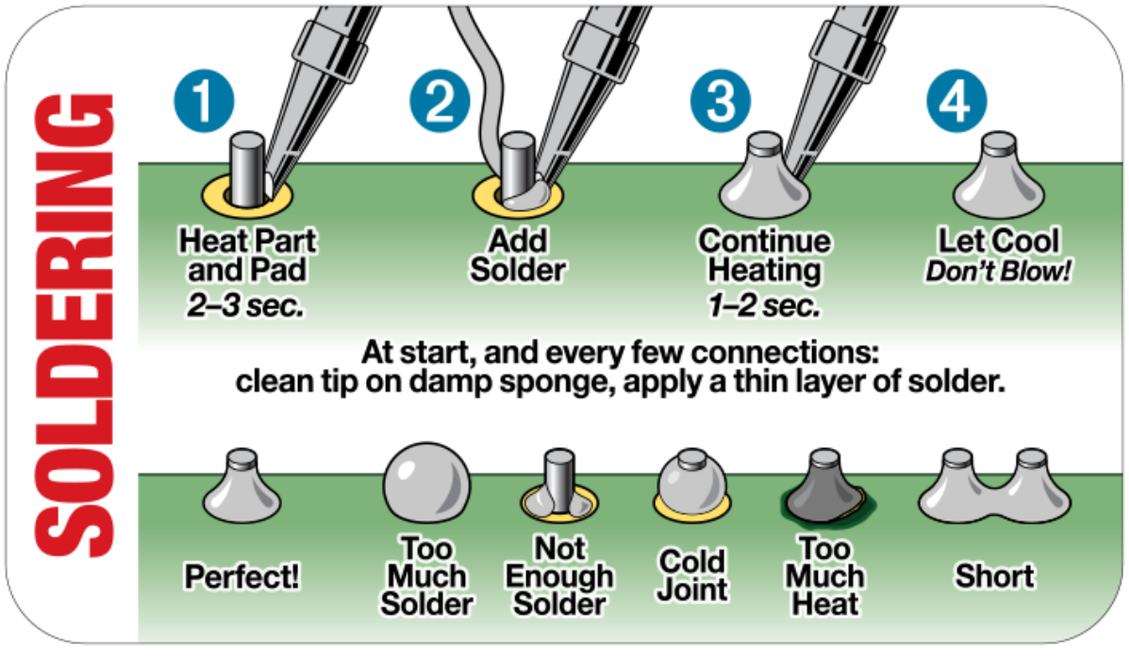
© 2018 Grand Idea Studio, Inc.

Soldering / Desoldering

© 2018 Grand Idea Studio, Inc.

Soldering

- Process to hold components together and/or mount them to a surface
- Melting and putting a filler alloy (solder) between the target surfaces
- Requires sufficient heat distribution



© 2018 Grand Idea Studio, Inc.

Soldering Iron

- Provides focused heat to melt solder
- Range from a simple stick iron to a full-fledged rework station (~$10-$5k)
  - Interchangeable tips, adjustable temperature, reflow
  - Ex.: Weller, Metcal, Hakko, Aoyue
- Heat comes from the *edge* of the iron





© 2018 Grand Idea Studio, Inc.

Soldering Accessories

- Solder: Alloy (Tin/lead or lead-free), 0.025-0.031" diameter ideal, melting temperature ~700-750°F
- Tip cleaner: Helps to keep the solder tip clean for even heat distribution
  - Ex.: Sponge, braid







© 2018 Grand Idea Studio, Inc.

Lab:
Soldering

© 2018 Grand Idea Studio, Inc.

Desoldering Accessories

- Solder Sucker/Pump: Manual vacuum device that pulls up molten solder into its chamber
- Braid: Wicks molten solder into copper braid
- Flux: Assists in heat transfer and removal of surface oxides







© 2018 Grand Idea Studio, Inc.

Desoldering: Surface Mount

- ChipQuik, **`www.chipquik.com`**
- Provides quick and easy removal of surface mount (and multi-pin through hole) components
- Primary component is a low-melting temperature alloy (< 200ºF)
  - Reduces the overall melting temperature of the solder
  - Allows you to lift/slide the part right off the board



© 2018 Grand Idea Studio, Inc.

Lab:
Desoldering

© 2018 Grand Idea Studio, Inc.

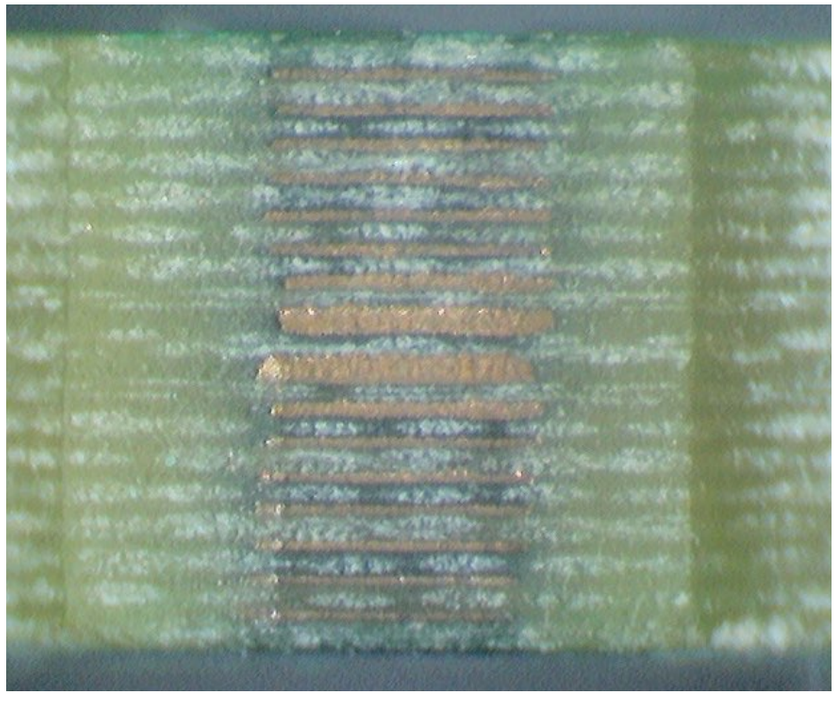
Circuit Board Modification

© 2018 Grand Idea Studio, Inc.

PCB Construction

- Layers of thin copper foil (conductive) laminated to insulating (non-conductive) layers
  - "Circuit board sandwich"
- Form the physical carrier and electrical pathways for components

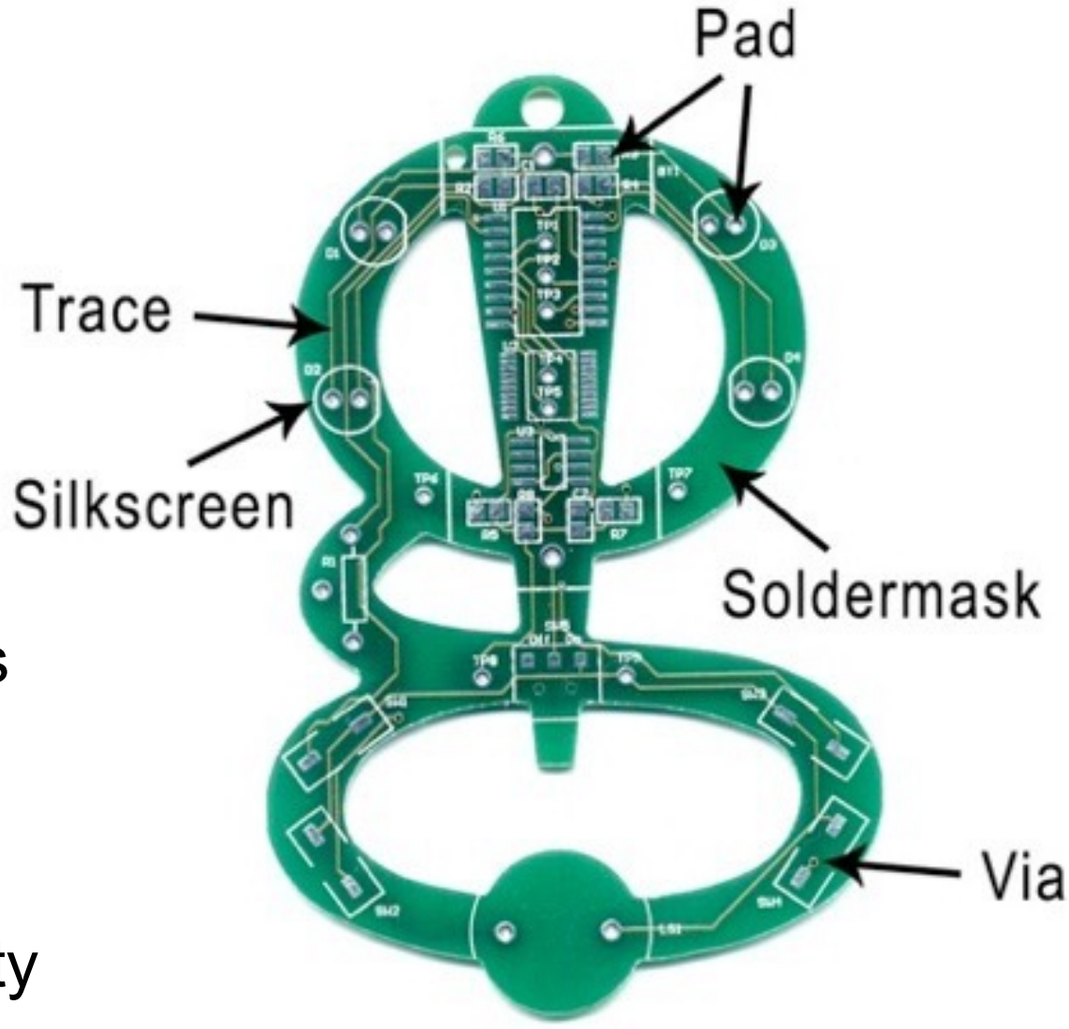


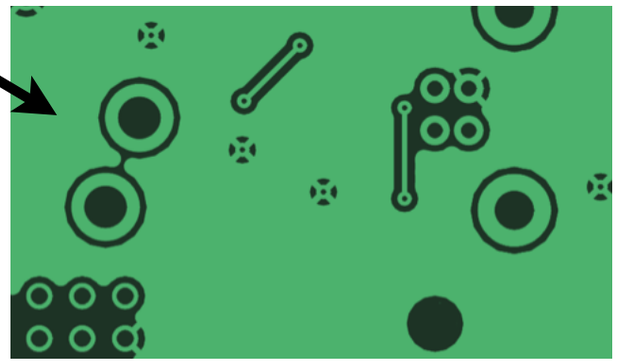


© 2018 Grand Idea Studio, Inc.

PCB Construction 2

- Silkscreen (Component Legend)
  - Epoxy or printable ink
  - Part designators, symbols/logos, manufacturing/test markings
- Soldermask
  - Protects PCB from dust/moisture
  - Provides access to desired copper areas
- Copper
  - Thickness = weight of copper/sq. ft.
  - Surface finish provides better solderability
- Substrate
  - Insulating layer
  - Rigid and/or flex, fiberglass/epoxy weave or specialized composite

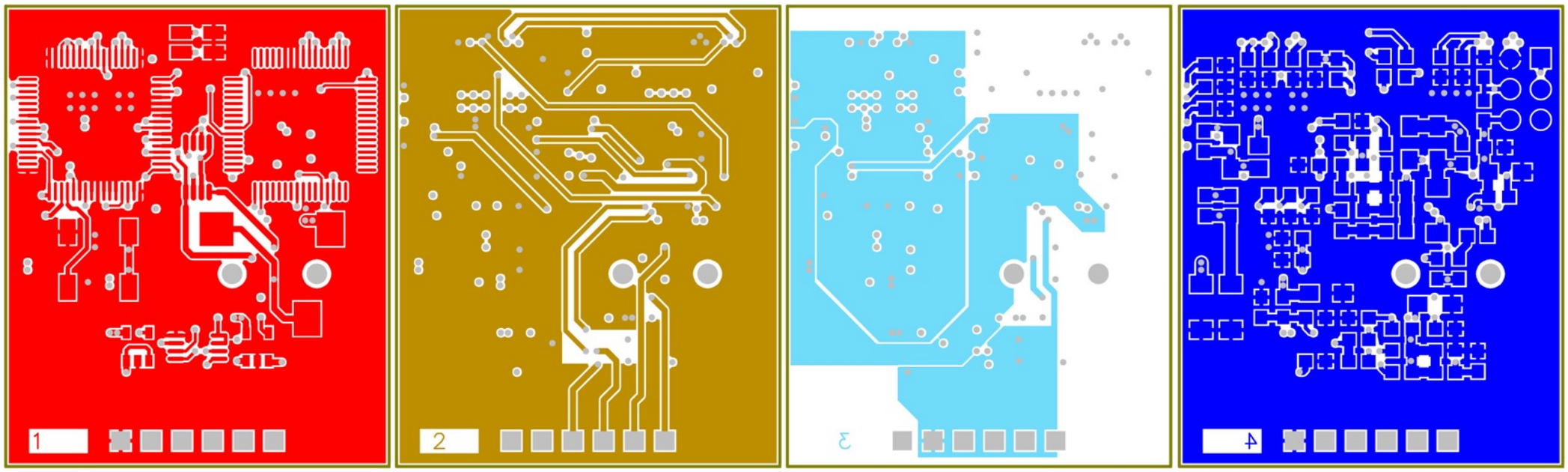




© 2018 Grand Idea Studio, Inc.

PCB Deconstruction

- Complete circuit layout and schematic can be recreated
- Solder mask removal, delayering, imaging
  - **`www.grandideastudio.com/portfolio/pcbdt/`**



© 2018 Grand Idea Studio, Inc.

Solder Mask Removal

- Gain access to a specific trace/pad/via
  - Ex.: Unpopulated footprint/connector
- Repair a damaged/broken trace/pad
- Physical abrasion is most efficient
  - X-Acto/hobby knife
  - Sandpaper
  - Dental tools
  - Wood carving tools (miniature chisel)
  - Fiberglass scratch brush

© 2018 Grand Idea Studio, Inc.

Trace Cutting

- Isolate signal to prevent communication
  - Ex.: Intentionally cause failure, MITM
- Change state of signal (high v. low)
  - Ex.: Affect bootstrap pin settings
- Beware of damage to surrounding traces/ components/PCB layers

© 2018 Grand Idea Studio, Inc.



Lab:
PCB Modifications

© 2018 Grand Idea Studio, Inc.

Signal Monitoring / Analysis

© 2018 Grand Idea Studio, Inc.

Signal Monitoring / Analysis

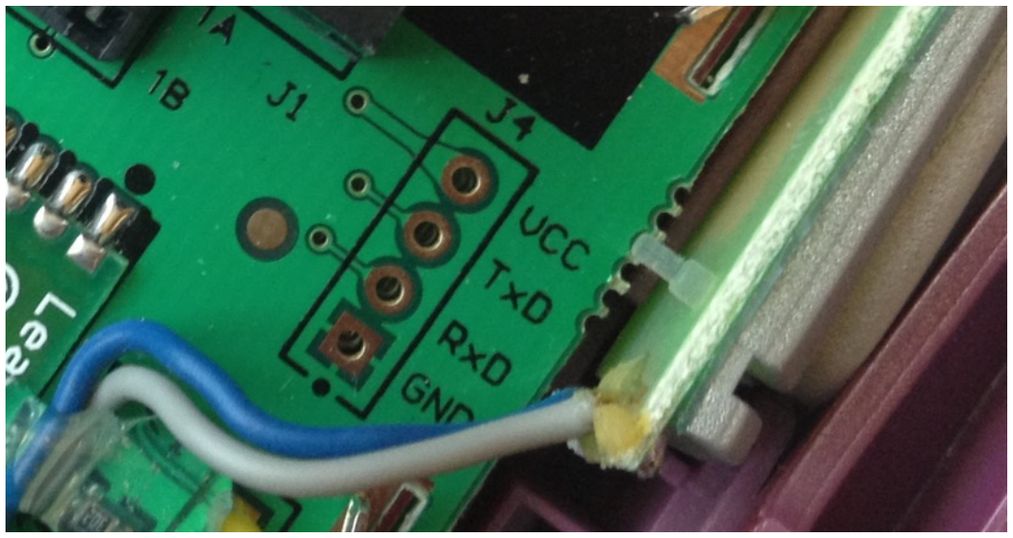
- Acquire, analyze, and decode communications
- Off-the-shelf tools exist for most interfaces
  - Engineers need tools for development, debugging
    - Ex.: Oscilloscope, Logic Analyzer, Protocol Analyzer
  - If not, may require custom circuitry and/or manual decoding of data

© 2018 Grand Idea Studio, Inc.

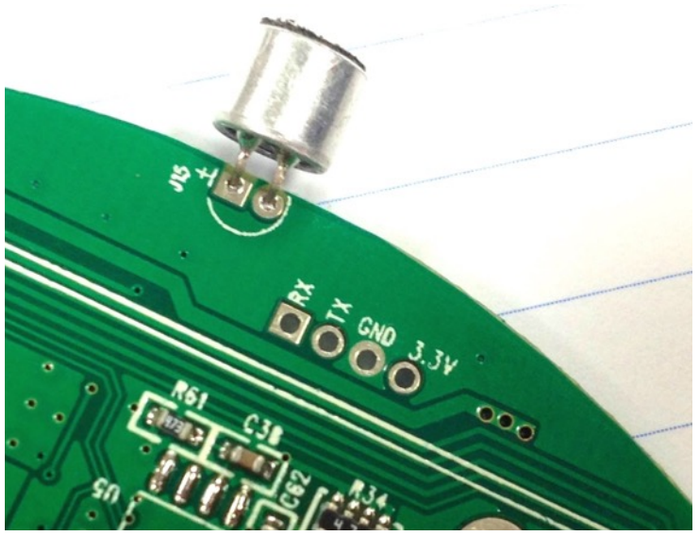


Serial / UART

- Universal Asynchronous Receiver/Transmitter
- Many embedded systems use UART as a console
  - Ex.: Boot log, debug output, bootloader menu, recovery interface, login prompt, root shell
  - Monitor signals on power-up w/ scope/logic analyzer







© 2018 Grand Idea Studio, Inc.

Serial / UART 2

- Asynchronous serial interface
  - → TXD = Transmit data (to target device)
  - ← RXD = Receive data (from target device)
  - ↔ DTR, DSR, RTS, CTS, RI, DCD = Control signals (uncommon for modern implementations)
- Transfer speed (baud rate) "built in" to the signal
  - Vendor may implement non-standard speed to thwart discovery

© 2018 Grand Idea Studio, Inc.



Serial / UART 3

- NRZ (Non-Return-To-Zero) coding
- Data bits sent LSB first (D0)
- Voltage range depends on system
  - Logic level (Ex.: 1.8V, 3.3V, 5V)
  - RS232: +/-3V to +/-25V (+/-15V typical)

1	2	3	4	5	6	7	8	9	10	11
Start bit	**5–8 data bits**								**Stop bit(s)**	
Start	Data 0	Data 1	Data 2	Data 3	Data 4	Data 5	Data 6	Data 7	Stop	

*** Start bit + Data bits + Parity (optional) + Stop bit(s)

© 2018 Grand Idea Studio, Inc.



Serial / UART 4



© 2018 Grand Idea Studio, Inc.

Lab:
Signal Monitoring & Decoding

© 2018 Grand Idea Studio, Inc.

Memory Extraction

© 2018 Grand Idea Studio, Inc.

Memory

- Try to retrieve contents of all available memory devices in a product
  - Regardless of technology
  - Most MCUs contain internal RAM, ROM, Flash
- Many methods of extraction
  - Device programmer (in-circuit or removed from board)
  - Programming/debug interface
  - Installing a custom program onto target
  - Firmware upgrade package (vendor website or MITM/ proxy)

© 2018 Grand Idea Studio, Inc.



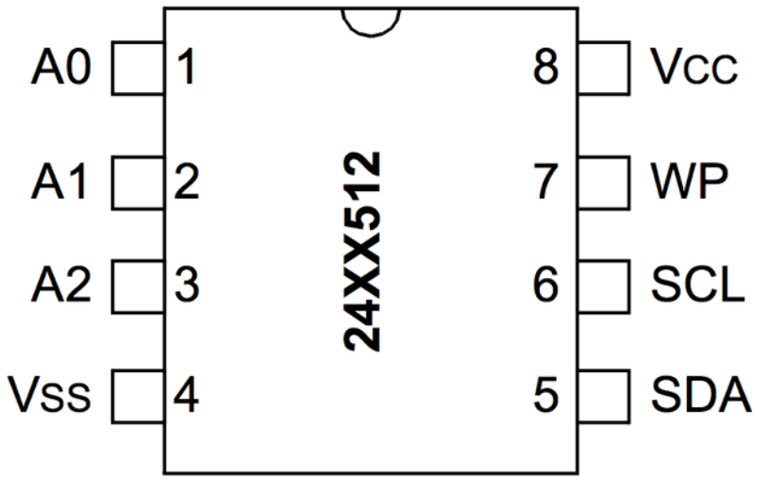
Memory 2

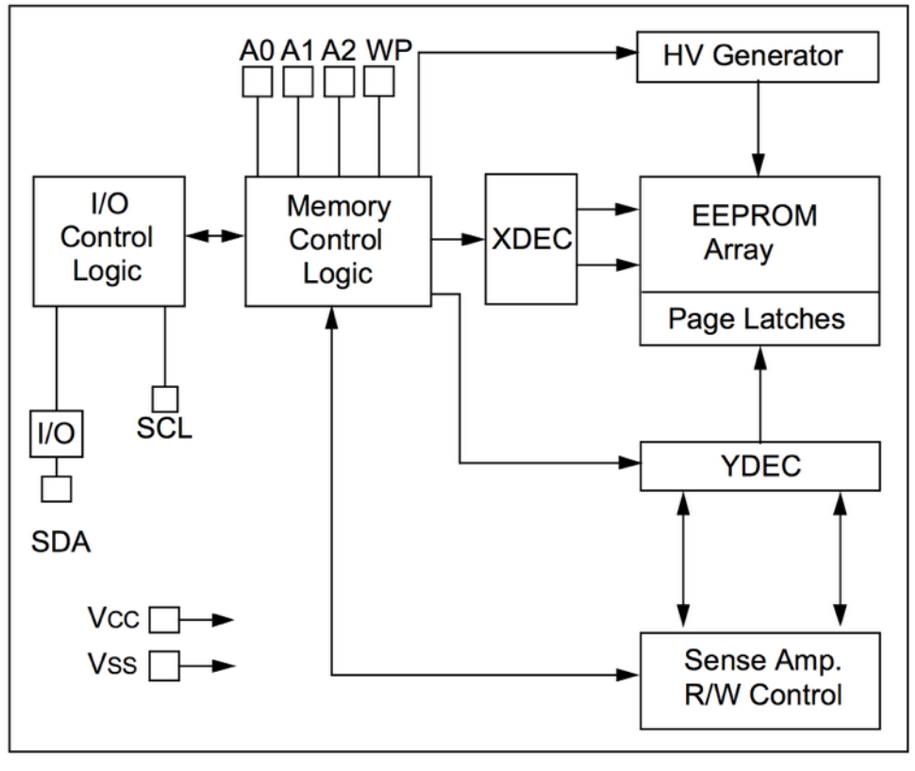
- Then, it (usually) becomes a software problem!
  - Embedded systems are general purpose computers programmed to perform a specific task
  - Analysis (static/dynamic), code execution, file system mounting, modification, reprogramming, discover elements/credentials for pivot

© 2018 Grand Idea Studio, Inc.



Lab:
Data Extraction from EEPROM





© 2018 Grand Idea Studio, Inc.

The End

© 2018 Grand Idea Studio, Inc.