Demonstration of Hardware Trojans

Fouad Kiamilev (Dr. K), Ryan Hoover, Ray Delvecchio, Nicholas Waite, Stephen Janansky, Rodney McGee, Corey Lange, Michael Stamat

CVORG

University of Delaware

Who We Are

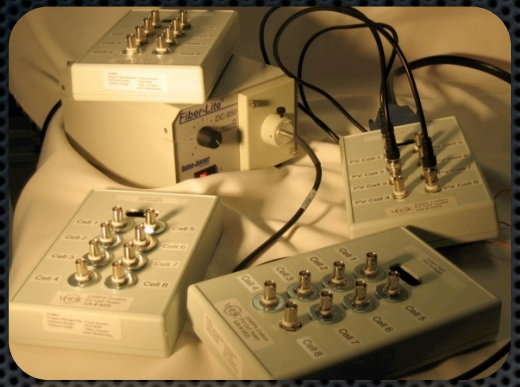
CVORG

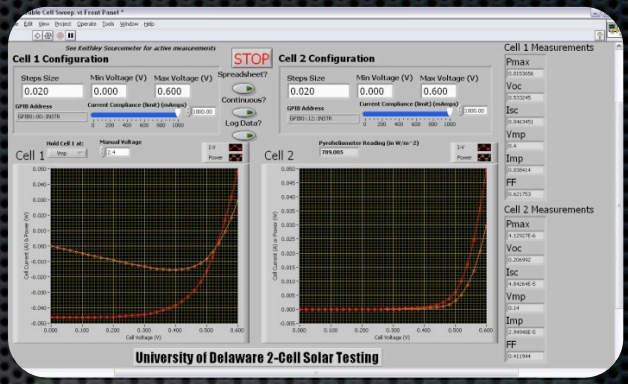


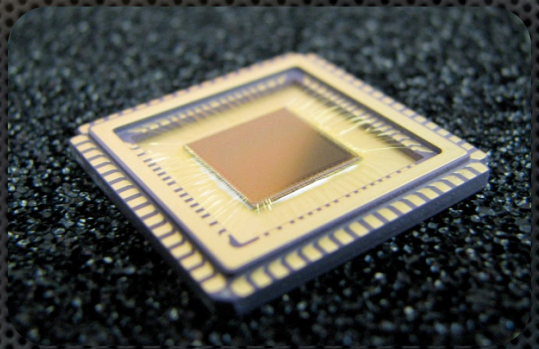
We take pride in our junk drawers.
Crazy ideas are encouraged.
We can't tell you everything but you can still ask.
You simulate it - we build it.
Our mess is a sign of work in progress.
Our toolbox contains more than just MATLAB.
No device is safe from disassembly.
We love what we do.

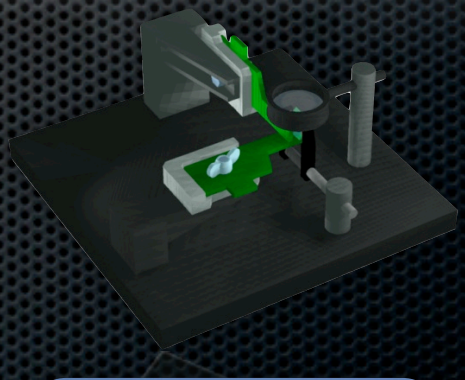
What We Do

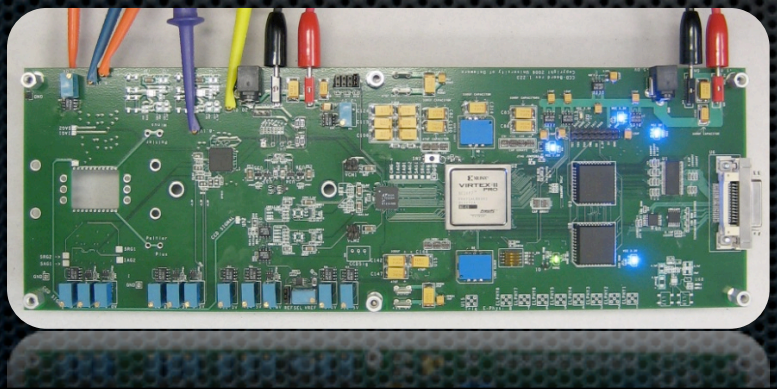
- Software
- Firmware
- FPGA Systems
- Special Instruments
- Reverse Engineering
- Printed Circuit Boards
- Discrete Analog Circuits
- Custom Integrated Circuits
- Mechanical Design
- Gigabit Data Links
- Power Converters

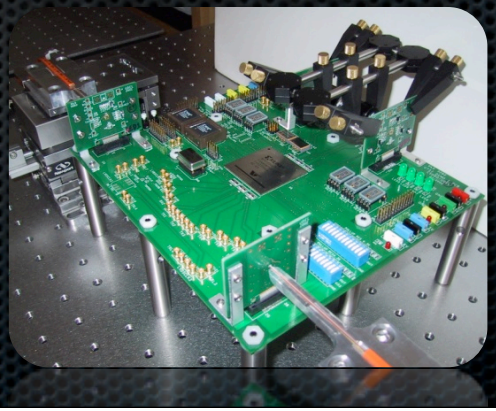














Definitions

- Hardware Trojan: malicious alteration of hardware, that could, under specific conditions, result in functional changes of the system.
- Time Bomb Trojan disables a system at some future time.
- Data Exfiltration Trojan leaks confidential information over a secret channel.

Reference: *Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions*, X. Wang, M. Tehranipoor, and J. Plusquellic, IEEE HOST 2008 Workshop, Anaheim, California, USA

Why is it a threat?

- Electronics plays an important role in:
  - Storage and communication of confidential information
  - Management and control of important equipment
  - Critical national security applications and systems



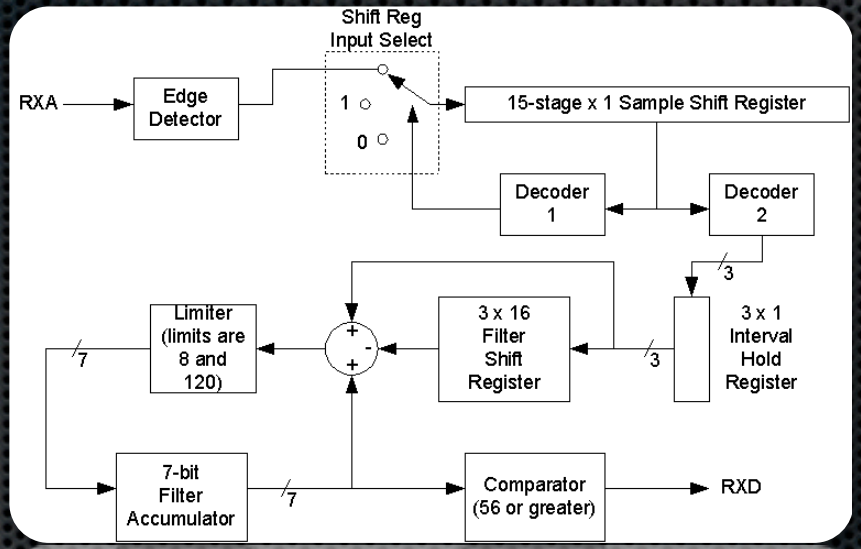
- Because of globalization, chip design and fabrication are increasingly vulnerable to malicious alterations.

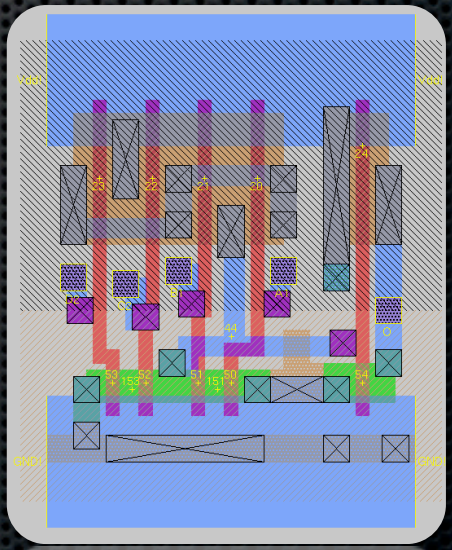
What can be altered?

```
UART_Tx_protocol_120: entity

-- pragma translate_off
generic map (
   instance_name => instance_

-- pragma translate_on
port map (
   clk => clk,
   rst => rst,
   TxClk => SrunIn_0_120_4,
   Disable => SrunOut_1_120_4
   DataTx => SrunIn_2_120_4,
   DataTx_data => SrunIn_2_12
   ParityTest => SrunIn_3_120
   ParityType => SrunIn_4_120
   WordSize => V7_WordSize_12
   StopSize => V7_StopSize_12
   TxRdy => SrunOut_7_120_4,
   SerialTx => SrunOut_8_120_
);
```





HDL Source Code

Circuit Diagram

IC Layout

FPGAs

- Definition: An FPGA is a semiconductor device containing programmable logic components and programmable interconnects.

- To configure ("program") an FPGA you specify how you want the chip to work with a logic circuit diagram or a source code using a hardware description language (HDL).

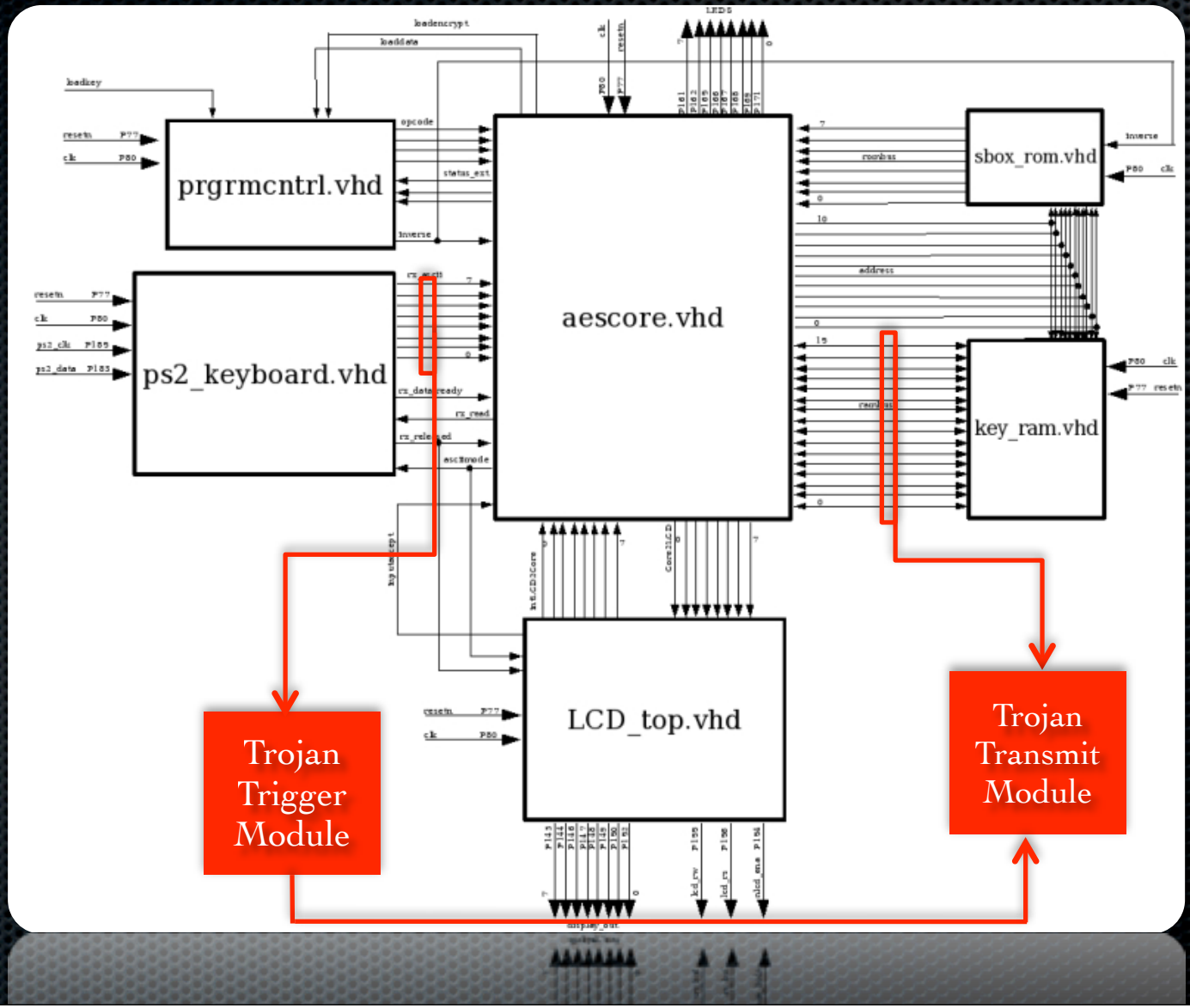


Our Demonstration Platform

- Application
  - AES Encryption engine
- Hardware
  - Spartan 3E FPGA Board
  - PS2 Keyboard (user input)
  - LCD Display (Cipher output)
- Trojan
  - Once triggered by a request to encrypt a special keyword, we transmit AES key on a covert communication channel.



Trojan Insertion



Trojan Demonstrations

- Thermal
  - An external resistor is electrically modulated creating thermal emission.
  - The micro-controller, or other parts of the circuit are quickly saturated with operations, creating thermal emission.
  - The thermal signal is sensed using an IR camera.
- Optical
  - An external LED is electrically modulated at a rate undetectable by human eye.
  - The optical signal is sensed using an optical-to-audio amplifier.
- Radio
  - An external I/O pin is modulated causing radio emission.
  - The radio signal is sensed using radio receiver and post-processing received signal on PC.

To view a video of our hardware Trojan demonstrations please visit this link:
http://www.cvorg.ece.udel.edu/defcon-16

Conclusion

- Hardware Trojans are a new and emerging threat.
- Systems at risk include military systems, financial systems and even household appliances.
- The purpose of our work is to demonstrate the dangers of Hardware Trojans.
- We are also working on Trojan detection schemes.