Secure Precinct Scanner Counter

Inherently secure by design

Craig Schiro on behalf of
Louisiana Citizens for Election Integrity
Jan 9, 2022

CITIZENS FOR
ELECTION
INTEGRITY

IT vs Life Critical

- Critical application demand high integrity because of the risk / consequences of failure or compromise is unacceptable
- Risk must be as low as reasonably possible, IT commercial Off-The-Shelf (COTS) technology is not fit for such purpose. COTS Windows or Linux technology is not designed for life critical applications and therefore is not acceptable for such applications.
- Voting systems is such a critical application that justifies integrity and zero trust. Ballot Marking Devices are not suitable for example see : “Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters”

The following is a list of the most critical Windows 10 vulnerabilities for 2021:

1. Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
2. Windows Remote Desktop Service Denial of Service Vulnerability
3. Windows Kernel Elevation of Privilege Vulnerability
4. Windows Hyper-V Elevation of Privilege Vulnerability
5. Windows Spoofing Vulnerability
6. Windows Print Spooler Remote Code Execution Vulnerability
7. Group Policy Elevation of Privilege Vulnerability
8. Microsoft Graphics Components Remote Code Execution Vulnerability
9. Windows TCP/IP Denial of Service Vulnerability
10. NetBT Information Disclosure Vulnerability

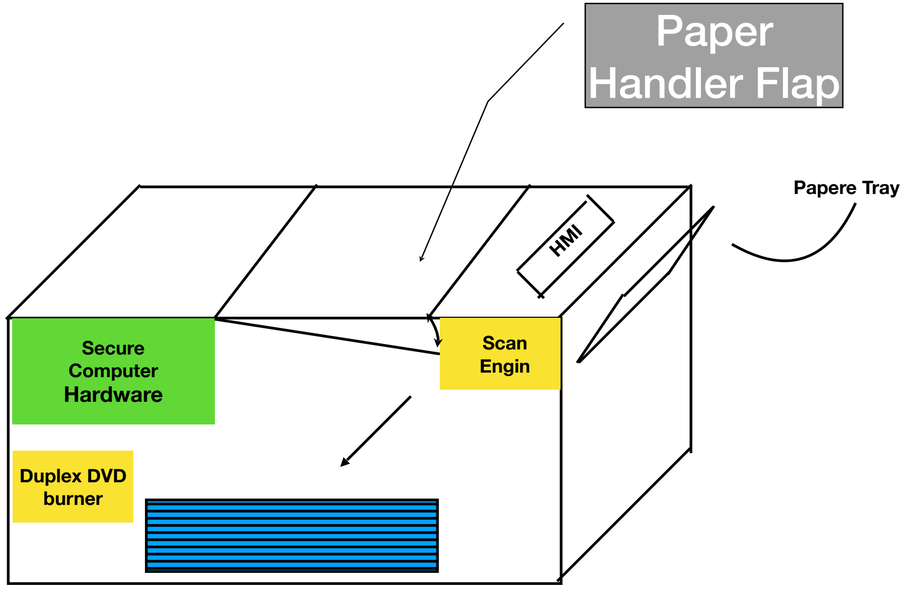
- Superfluous hardware and software, including peripherals that include co-processors provide huge and well known attack surfaces to exploit
- Vast international domain knowledge in COTS including enemy nation states with unlimited resources develop day-zero attacks to capture, control and exploit COTS infrastructure
- Application Security such as encryption, digital signing of code, digital certificates and firmware signing is optional rather than a fundamental requirement before systems can operate
- Lack of secure boot allows code modification that goes undetected
- Just a few examples of venerabilities too numerous to catalog

Safe, Secure, Reliable

- Battle proven secure by design GHS Integrity® Real Time Operating System (RTOS) is engineered for mission critical applications for military, Avionics,Industrial, and other life critical applications including as automotive safety
- Secure Digital lifecycle management to secure software and hardware assets are signed to ensure trusted chains of custody
- Secure boot and application signing by digital signatures and certificate ensure valid and authenticated executables, hardware devices including identity of all secure network communications
- For fit for purpose life critical hardware see Bedrock Automation for secure by design hardware that uses GHS Integrity® learn more at Bedrock Automation

Secure by Design

- Mission critical applications must be Inherently secure by design
- Security must not be “bolt on” after thought but a fundamental design requirement
    - Must be a primary design objective that addresses hardware, software OS, and Software applications.
        - Must include physical security and electronic hardware security repelling physical and cyber attacks



- **Secure Computer Hardware** to contain the Integrity Green Hill Software secure OS
  - The OS runs
    - Ballot counterfeit prevention and authentication
    - Critical optical mark identification and integer counting code
    - High resolution image scan that allows digital forensic analysis marked with evidence “finger” print to meet legal digital evidence requirements
    - Ballot 2 dimensional mark identification matrix (identified valid marks)
    - ballot Over / under vote return ballot to the voter by paper handler flap to handle multi page ballots validations
- Human Man Interface (HMI), Duplex DVD burner
- An example of secure hardware that uses Green Hill Software OS see Bedrock Automation
- Packaged in a double locked metal case that provides faraday shielding to preventing full spectrum, electromagnetic radiation

“It takes 20 years to build a reputation and few minutes of cyber-incidents to ruin it.”

— Stephane Nappo