International Journal of Computer Engineering and Sciences Research

VOL. 01, NO. 01, January 2019
Pages 01–06
Available online at: www.ijcesr.com

# Dark Notes Press, LLC: A New Architecture

Mr. Kurt Amacker[1]Dr. Syed Adeel Ahmed[2]

[1]*School of Professional Advancement, Tulane University, New Orleans, 70118, Louisiana, United States*
[2]*Xavier University of Louisiana, 1 Drexel Drive New Orleans, 70125, Louisiana, United States*

**Abstract:** Dark Notes Press, LLC is a small publishing house established by Kurt Amacker in November 2013. The business and most of its assets are housed in his residence, which functions as a legally designated home office within Orleans Parish and the City of New Orleans. However, the information technology architecture of the business relies on consumer-grade equipment, much of which is host to vulnerabilities and is often unreliable. This piece seeks to map and inventory the current architecture and identify gaps and vulnerabilities. Following that, a new and more secure architecture will be proposed, explained, and budgeted.

**Keywords**Enterprise Architecture, SOHO, Small Business

## I. Introduction

Dark Notes Press's (DNP) current architecture layout was assembled ad hoc from consumer-grade hardware, with little consideration for router security or even basic cybersecurity principles, outside of maintaining WPA2 encryption on its two wireless networks—affectionately dubbed The Ninth Gate (5GHz, 1300Mbps) and The Ninth Gate 2 (2.4GHz, 600Mbps). As such, it should be considered a CMMI Level 1 organization. A cursory inspection on DNP's Small-Office-Home-Office(SOHO) architecture immediately reveals vulnerabilities and areas for improvement. This initiative began when founder and publisher Kurt Amacker encountered programmer Michael Horowit'z blog *Router Security*. Horowitz explains that consumer-grade routers are generally insecure compared to their business-class counterparts.Horowitz's writes "If you care about the security of your router, and you should, it is best to avoid consumer grade routers. On the whole, the software in these routers is buggy…"[1]. This led Amacker to consider the entirety of DNP's SOHO architecture, and whether it might contain vulnerabilities that would open up the network to malicious actors. What this line of questioning uncoversis disconcerting to say the least. Several hardware components within the network are not only lacking current firmware, but are fundamentally and irreparably vulnerable. Here, DNP's current and flawed SOHO architecture is inventoried and diagramed, with each appliance's vulnerabilities (or lack thereof) annotated. Then, the paper proposes an alternate architecture, with a proposed inventory, accompanying diagram, and cost.

## II. Materials and Methods

DNPfaces many of the same challenges as other small businesses. As Bradley Mitchell at *Lifewire*writes, "Security challenges impact SOHO networks more than other kinds of networks. Unlike larger ones, small businesses generally cannot afford to hire professional staff to manage their networks. Small businesses also are more likely targets of security attacks than households due to their financial and community position"[2]. Fortunately, DNP's network has never been the subject of a major attack (that the company knows of). However, the network is still subject to the same risks as any other. Cybersecurity specialists at the Interhack Corporation provide a basic primer for network security that outlines the kinds of attacks even a SOHO network may experience. These include, but are not limited to:

- Denial-of-service attacks
- Unauthorized access attempts
- Illicitly executed commands

- Confidentiality breaches
- Destructive behavior and/or "cyber-vandalism," including clandestinely modifying or deleting data[3].

With Amacker as DNP's sole employee, a secure network is imperative. The following outlines DNP's existing architecture, with cursory notes on each, including gaps, shortfalls, and security concerns.

### 2.1 Current Architecture

1. **Hardware:** MSI GT70
   - Desktop replacement "gaming" laptop from 2012
   - Processor is 3.2GHz Intel Core i7-4700MQ
   - RAM is 24GB DDR3
   - Memory speed is 1600MHz
   - Hard drive is 1024GB flash memory solid state

   **Observations:** The unit is functional, with occasional glitches consistent with Windows 10.A wipe/reload, cleaning, and firmware upgrade is recommended.

2. **Hardware:** Microsoft Surface Pro 4
   - Portable tablet/PC from 2017
   - Processor is 3.4GHz Intel Core i7
   - RAM is 16 GB
   - Memory speed is 2.2 to 3.4 GHz
   - Hard drive is 1 TB flash memory solid state

   **Observations:** The unit is currently non-functional due to a known hardware flaw, in which is overheats and causes visual artifacts and distortion. It will be replaced via Microsoft's trade-in program for an equivalent unit.

3. **Hardware:** Linksys Business LGS116 16-PortDesktop Gigabit Ethernet Unmanaged Network Switch
   - "Plug-and-play" network switch purchased in 2016
   - PoE+ functionality in ports 1-8
   - Maximum speed per port is 1 Gbps
   - No web-based user interface

   **Observations:** The unit is functional. Its current internet speed is 150Mbps download/10Mbps upload.

4. **Hardware:** TP-Link AC1900 Smart Wireless Router
   - Wireless router purchased in 2015
   - Speed up to 1900 Mbps
   - CPU Processor is 1GHz dual core
   - Contains 4 Gigabit ethernet ports (only one used for switch)
   - Broadcasts two networks (2.4GHz 600Mbps and 5GHz 1300Mbps) using WPA2 security

   **Observations:**The unit seems prone to drops in service, but this is informal observation.*SecurityFocus*also reports a longstanding directory traversal vulnerability in multiple TP-Link products, including the TP-Link AC1900 running the current firmware, last updated in 2/2018[4].

5. **Hardware:** TP-Link AC1750 WiFi Range Extender
   - Wireless range extender purchased in 2016
   - Extends both 2.4GHz and 5GHz networks

   **Observations:**Cybersecurity firm*ReFirmLabs* reports a major security vulnerability in many TP-Link range extenders.Using the Centrifuge platform, the site demonstrated a major command injection bug, albeit one that requires administrative access to exploit.However, it allows the hackers to download the config.bin file without authentication.This configuration backup file can be decrypted using a common password among TP-Link devices.The router's user ID and password are stored in plain text, and there is an MD5 hashcode for the administrative password.With the MD5 hashcode, the hacker can gain access to the router functions[5].

6. **Hardware:** ARRIS SURFboard DOCSIS 3.0 HighSpeed Broadband Cable Modem
    - Cable modem purchased in 2016
    - Has 32 download channels and 8 upload channels, up to 1.4 Gbps

    **Observations:** Arris is subject to a class action lawsuit in California over this modem for using the faulty Puma 6 chipset from Intel, which causes latency jitters and drops in service.The lawsuit is ongoing[6].

7. **Hardware:**HP PageWide Pro 477dw Multifunction Printer/Copier/Scanner/Fax Machine
    - Networked, multifunction printer purchased in 2017
    - Provides both wireless and ethernet access to multiple devices on network

    **Observations:**The unit is prone to dropped wireless connections and occasional glitches within normal operating parameters.Otherwise unit is functional. There was a vulnerability allowing for arbitrary code execution reported in January 2018, but it has since been corrected in firmware upgrade[7].

8. **File Storage:**Dropbox Plus
    - Cloud-based file storage
    - 1TB of space allotted, with 92.2GB in use
    - Allows for access to synched files across multiple devices

    **Observations:**Like all cloud-based file storage, Dropbox is vulnerable to lost data and attacks by malicious actors. Writing for *StickyPassword*, cybersecurity blogger Cassie Phillips documented "Previous Scandals and Breaches" that have plagued the service. These include a shifting policy on customer information sharing, a bug that caused files to be deleted, and the company's failure to notify customers about a security exploit that surfaced (the vulnerability was repaired in May 2014 after the media alerted the public). Philips also points out that using Dropbox on public networks without a VPN is doubly dangerous, because files targeted by hackers can synch across multiple devices, creating local copies seeded from their potentially infected cloud counterpart. From the beginning, she emphasizes that Dropbox has become a significant target for hackers because of the volume of information stored and shared there[8]. While this does not render Dropbox wholly unusable for DNP's proposed architecture, it identifies a need for a more stable and secure storage platform—ideally, one locally hosted.

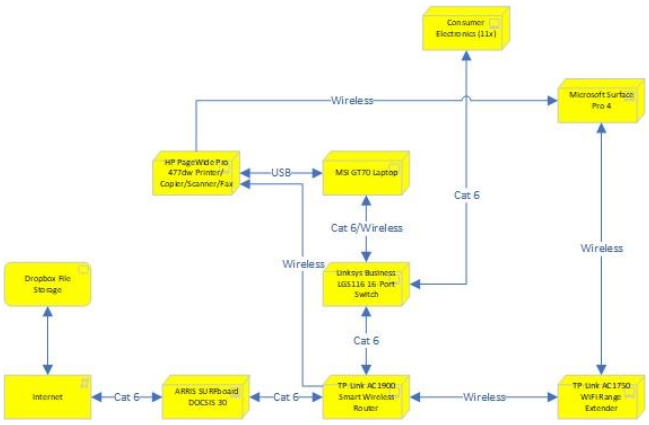


**Figure 1.** Current Architecture

### 2.2 Proposed Architecture

1. **Hardware:** MSI GT70
    - See**Section 2.1**

    **Observations:** No changes.

2. **Hardware:** Microsoft Surface Pro 4
    - See **Section 2.1**

    **Observations:** No changes.

3. **Hardware:** Linksys Business LGS116 16-PortDesktop Gigabit Ethernet Unmanaged Network Switch
    - See **Section 2.1**

   **Observations:** No changes.

4. **Hardware:** Peplink Balance One 600Mbps Dual-WAN Router with Dual-Band 11ac Wi-Fi
    - Wireless router released in 2014
    - Speed up to 600 Mbps
    - CPU Processor is unreleased
    - Contains 10 ethernet ports; 8 LAN and 2 WAN (only one used for switch)
    - Broadcasts two networks (2.4GHz 300Mbps and 5GHz 866Mbps) using WPA2 Enterprise security

   **Observations:**Peplink products are emphatically endorsed by Michael Horowitz of *Router Security*.The emphasis is not on their speed, but their security and configurability. The unit also maintains a backup of previous firmware to ensure functionality. Guest networks are isolated from devices on the network and other users[10].
   **Price:** $499.00
   **Availability:** Amazon.com

5. **Hardware:** Pepwave AP One Enterprise Ceiling Mountable 11AC AP (x2)
    - Ceiling mounted wireless access point
    - Extends both 2.4GHz and 5GHz networks at speeds up to 450Mbps and 1300Mbps, respectively
    - Works with Power-over-Ethernet (POE)
    - Requires professional installation

   **Observations:** There is limited information about the device available online, outside of Pepwave's own website. Some older reviews express concerns, but these may have been mitigated by firmware upgrades or newer iterations of the hardware.
   **Price:** $249.00
   **Availability:** Amazon.com

6. **Hardware:** NETGEAR DOCSIS 3.1 Gigabit Cable Modem (CM1000)
    - Cable modem released in 2016
    - Has 32 download channels and 8 upload channels, up to 6Gbps on paper; given that current home speeds top out at 1Gbps this only future-proofs it
    - Uses the updated Intel Puma 7 chipset, and was part of a firmware upgrade to correct earlier issues

   **Observations:**There are no known security vulnerabilities.Some review sites still prefer ARRIS products, but DNP is less inclined to support them given the ongoing class action suit.
   **Price:** $179.99
   **Availability:** Amazon.com

7. **Hardware:**HP PageWide Pro 477dw Multifunction Printer/Copier/Scanner/Fax Machine
    - See **Section 2.1**

   **Observations:** No changes.

8. **File Storage:**Synology 6 Bay NAS DiskStation - DS1618+
    - 6-bay network access server released in 2018
    - 4GB DDR4 memory, expandable up to 32GB
    - Maximum capacity with expansions 192TB

   **Observations:** In order to circumvent the need for cloud-based storage, DNP intends to move its data on to a private file server with remote access, connected to the SOHO network. Synology's NAS Diskstation is an ideal solution, with a simple web-based interface that can act as a "private cloud" of sorts. While DNP may rely on services like Dropbox for large file transfers, the cloud should not be used as a permanent storage solution for such a large amount of data. The Diskstation will allow for access both within the DNP home office and online.
   **Price:** $749
   **Availability:** Amazon

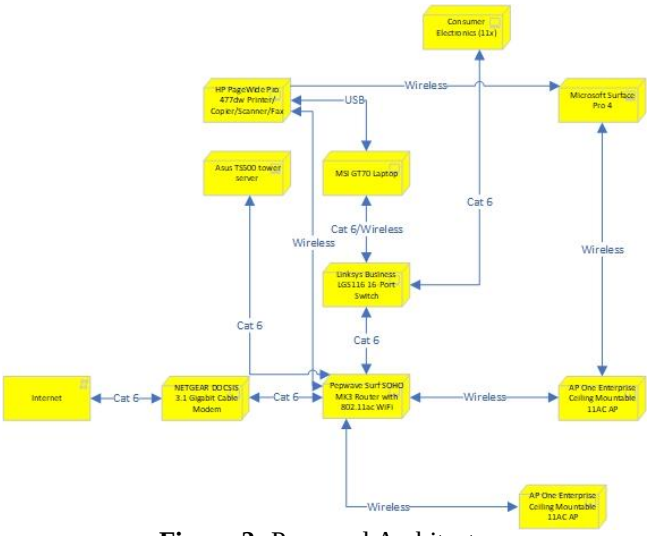


**Figure 2:** Proposed Architecture

| **Hardware** | **Price** |
|---|---|
| MSI GT70 | N/A |
| Microsoft Surface Pro 4 | N/A |
| LinksysBusiness LGS116 | N/A |
| Peplink Balance One 600Mbps | $499.00 |
| Pepwave AP One Enterprise Ceiling Mountable 11AC AP (x2) | $498.00 |
| NETGEAR DOCSIS 3.1 Gigabit Cable Modem (CM1000) | $179.99 |
| HP PageWide Pro 477dw | N/A |
| Synology 6 Bay NAS DiskStation | $749.00 |
| **Total** | $1925.99 |

**Figure 3:** Budget

### 2.3 Implementation

Most of the proposed hardware outlined in **Section 2.2** can be installed by Amacker himself at no additional cost. The Pepwave AP One Enterprise Ceiling Mountables require professional installation in the ceilings around the DNP SOHO. Electricians from Plauche Electrical will carry Cat-6 cable back to the router through the attic, connect it through a hole in the ceiling, and secure it as needed. The cost for installation is TBD.

## III. Conclusion

The observations presented within this report should explain the necessity of upgrading and otherwise correcting DNP's SOHO architecture. And, for the purposes of avoiding even common cybersecurity pitfalls, it should be done sooner rather than later. The availability of a personal file server such as the Synology 6 Bay NAS DiskStation also negates the need for using Dropbox or other cloud-based services as a primary means of file storage and sharing. While using Dropbox is not typically dangerous or insecure, any cloud-based solution suffers from an increase in vulnerability by its very nature.

In order for DNP to reach CMMI Level 2, it must follow the proposals outlined here, and then continue refining and cementing its business and technology processes. To do otherwise is to continue on a path at the mercy of not only its own vulnerabilities, but mediocrity itself.

**REFERENCES**

[1] Horowitz, Michael. "Router Bugs Flaws Hacks and Vulnerabilities." *Router Security*, Michael Horowitz, n.d., routersecurity.org/bugs.php.

[2] Mitchell, Bradley. "How SOHO Routers and Networks Differ From Ordinary Ones." *Lifewire*,Dotdash, 6 Nov. 2018, www.lifewire.com/soho-routers-and-networks-explained-3971344.

[3] Curtin, Matt. "Introduction to Network Security." *Interhack Corporation*,Interhack Corporation, Mar. 1997, www.interhack.net/pubs/network-security/network-security.html#SECTION00040000000000000000.

[4] "Multiple TP-LINK Products CVE-2015-3035 Directory Traversal Vulnerability." *SecurityFocus*,SecurityFocus, 10 Apr. 2015, www.securityfocus.com/bid/ 74050/info.

[5] Heffner, Craig. "From Bad to Worse: Firmware Vulnerability Detection with the Centrifuge Platform." *ReFirm Labs*,ReFirm Labs, Inc., 13 Aug. 2018, www.refirmlabs.com/blog/exploiting-command-injection-bugs-tp-link-wl-wa850re-wifi-range-extender.

[6] "A Vulnerability in HP Printer Products Could Allow for Arbitrary Code Execution." *Center for Internet Security*, Center for Internet Security, Inc., 30 Jan. 2018, www.cisecurity.org/advisory/a-vulnerability-in-hp-printer-products-could-allow-for-arbitrary-code-execution_2018-013/.

[7] "A Vulnerability in HP Printer Products Could Allow for Arbitrary Code Execution." *Center for Internet Security*, Center for Internet Security, Inc., 30 Jan. 2018, www.cisecurity.org/advisory/a-vulnerability-in-hp-printer-products-could-allow-for-arbitrary-code-execution_2018-013/.

[8] "A Vulnerability in HP Printer Products Could Allow for Arbitrary Code Execution." *Center for Internet Security*, Center for Internet Security, Inc., 30 Jan. 2018, www.cisecurity.org/advisory/a-vulnerability-in-hp-printer-products-could-allow-for-arbitrary-code-execution_2018-013/.

[9] Philips, Cassie. "Is Dropbox Really Safe?" *Sticky Password Blog*,Lamantine Software, 14 Jan. 2016, www.stickypassword.com/blog/is-dropbox-really-safe/.

[10] Horowitz, Michael. "Pepwave Surf SOHO Router." Router Security, Michael Horowitz, 10 Nov. 2018, routersecurity.org/pepwavesurfsofo.php.