Serial Offenders

Widespread Flaws in Serial Port Servers

HD Moore

Serial Port Servers

- Devices that provides remote IP access to serial ports
  - Known as serial-to-ethernet converters or terminal servers
  - Used for remote management, logging, out-of-band access
  - Widely used for industrial, point of sale, and transportation

Serial Port Servers: Components

- Embedded processor
  - ARM, MIPS, x86
- Embedded OS
  - NET+OS, Evolution, eCOS, VxWorks, or Linux
- Management UI
  - Telnet, SSH, HTTP
- Serial ports
  - RJ45, DB25, DB9, DIN
- Network ports
  - Ethernet, GSM, 3G, LTE, WiFi

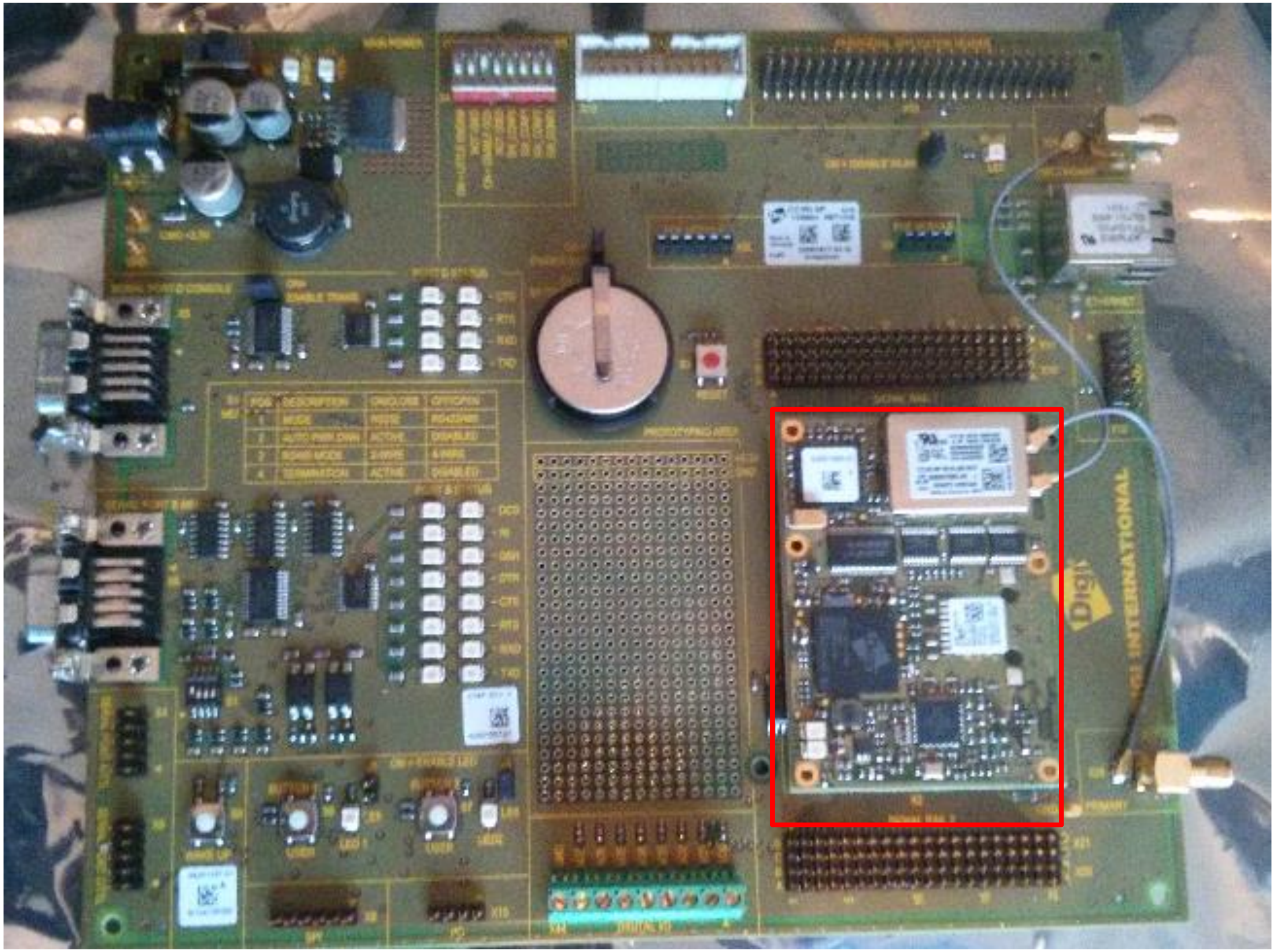
Serial Port Servers: Features

- Remote serial port access
  - Interact with target ports through telnet, SSH, and HTTP
  - TCP socket proxy ports provide direct pass-through
  - Proprietary protocols for virtual COM port drivers
- Serial port monitoring and automation
  - Some products offer basic automated interaction
  - Use expect-style logic, can alert, send commands
  - Stream to remote hosts when criteria are met

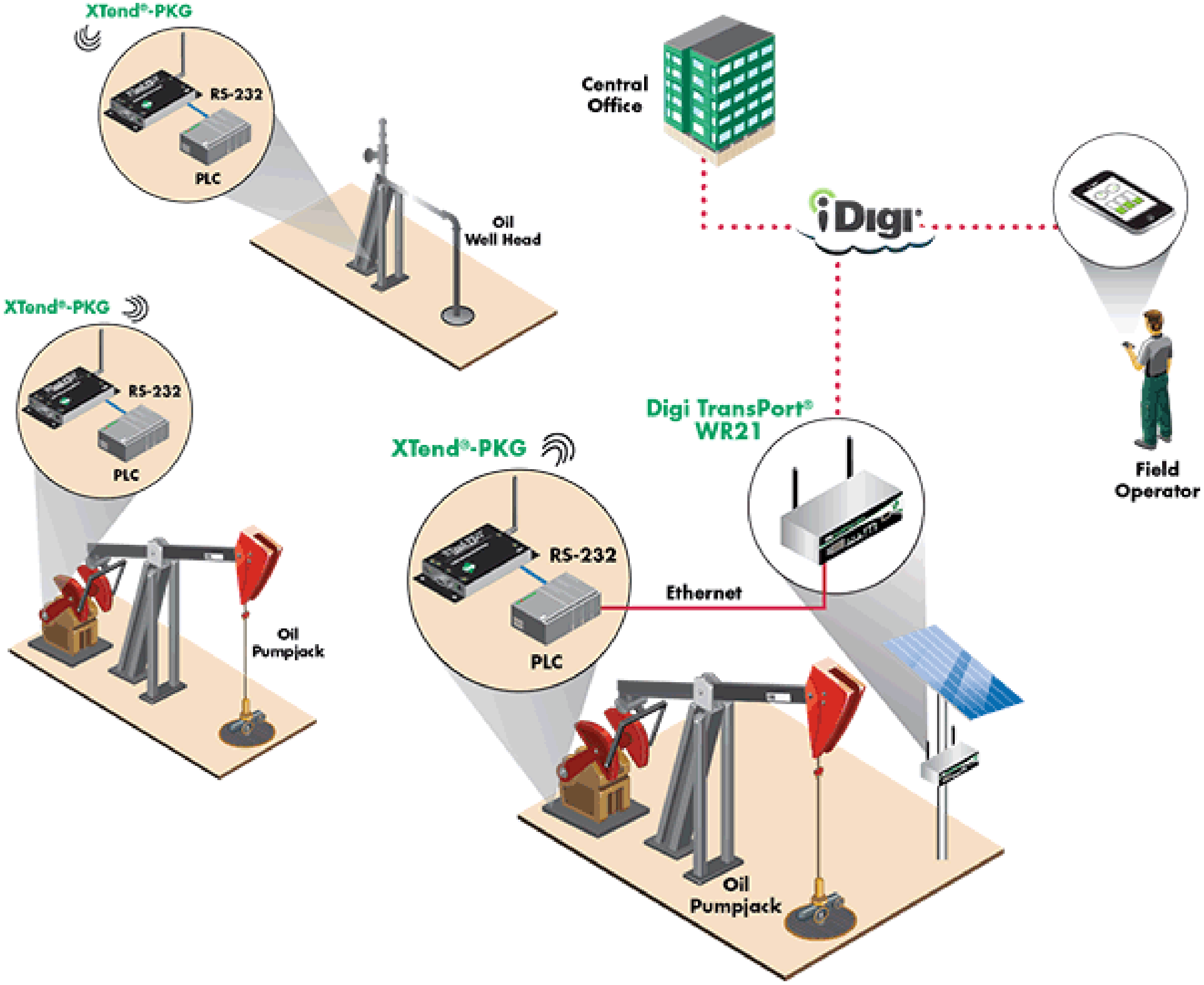
Serial Port Servers: Development

- Sold as kits for proprietary implementations
  - Integrators buy devices, create custom code, and resell
  - Custom automation for industrial, medical, and telco
  - Development is typically in C, Python, or scripts
- Expanded use beyond serial ports
  - GPIO pins used for custom hardware integration
  - Wireless support for Zigbee and other RF serial
  - Support for MODBUS and other IA protocols

Digi Connect SP Development Kit

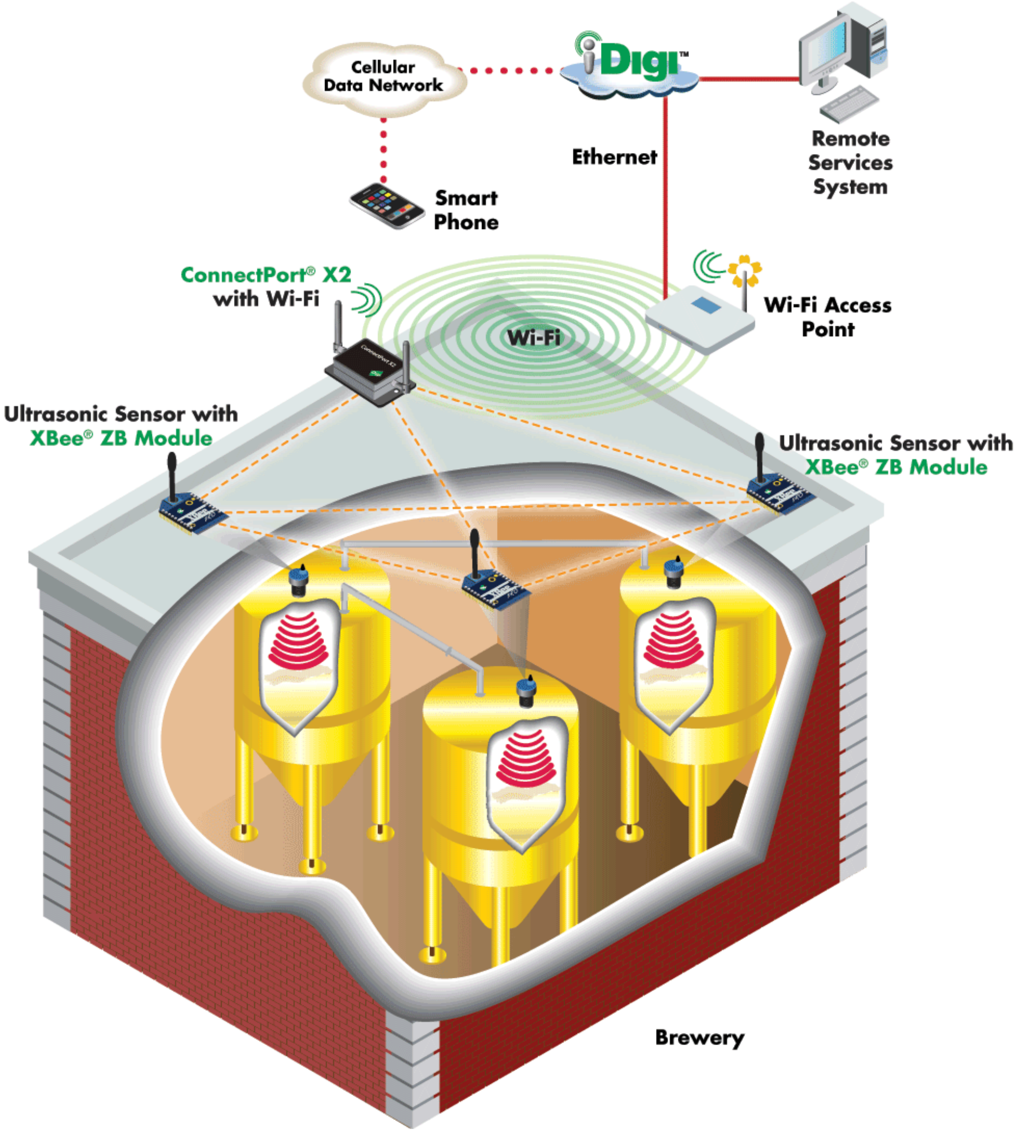


Use Cases: Oil and Gas Monitoring



http://www.digi.com/learningcenter/stories/monitor-oil-field-equipment-with-rf-modems

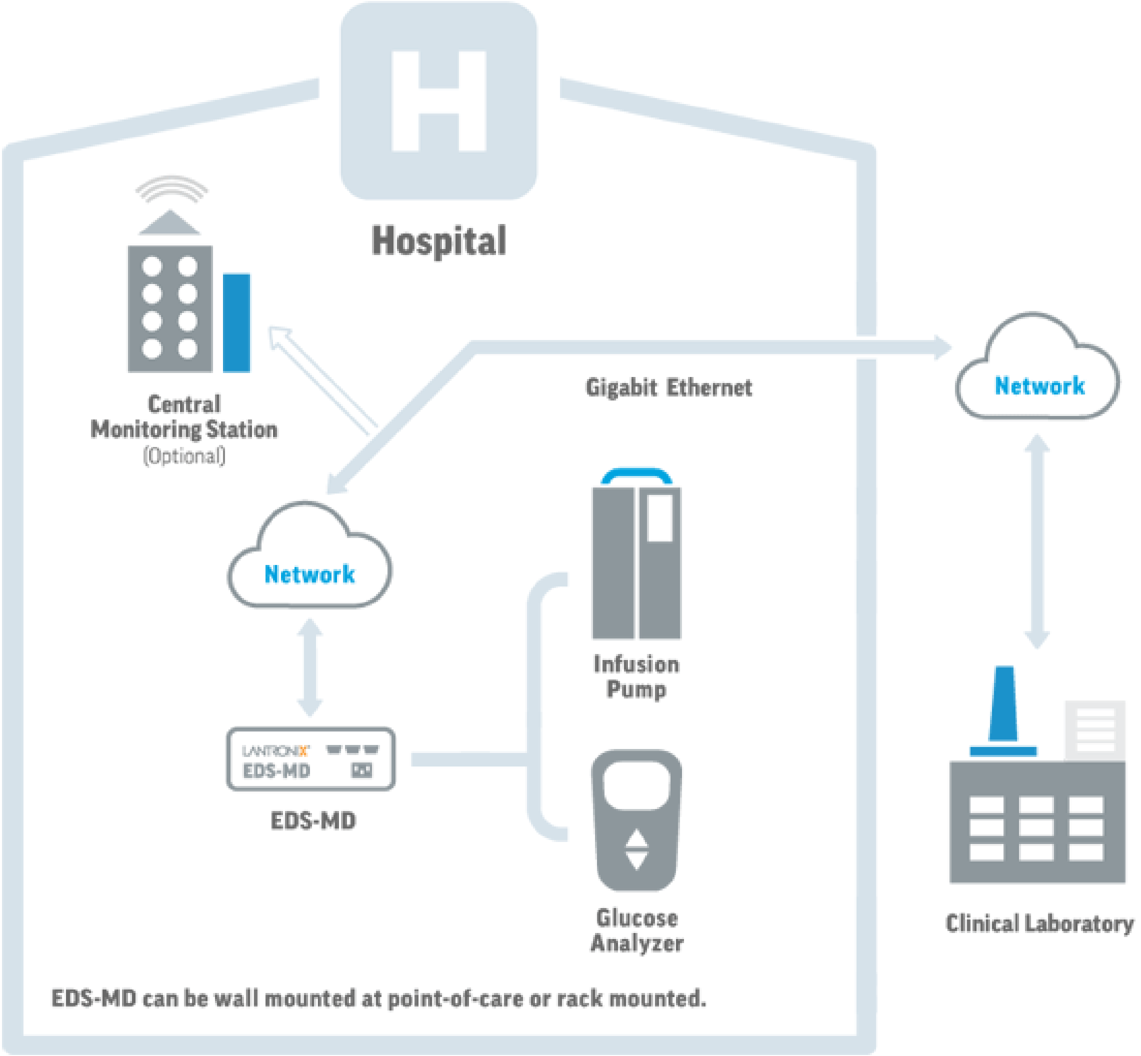
Use Cases: Brewery Tank Monitoring



RAPID7

http://www.digi.com/learningcenter/stories/measuring-tank-levels-in-a-brewery

Use Cases: Medical Device Monitoring



RAPID7

http://www.lantronix.com/device-networking/external-device-servers/eds-md.html

Use Cases: Internet Power Meter Monitoring

http://www.lantronix.com/solutions/power-case-automated_energy.html

Use Cases: Even More

Transportation

- Remote traffic signal monitoring and management
- Remote tracking of vehicle location via 3G + GPS
- Remote management of fleet fueling stations

IT Systems

- Remote access to UPS and PDU for remote reboot
- Remote access to servers, routers, and switches
- Out-of-band equipment access via GSM & 3G/LTE

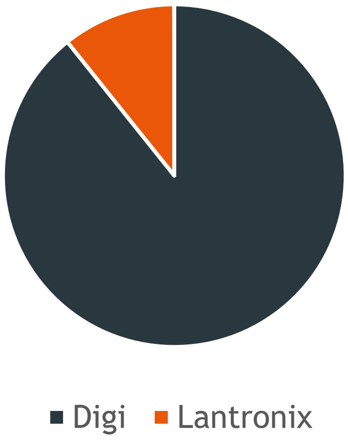
Internet Exposure

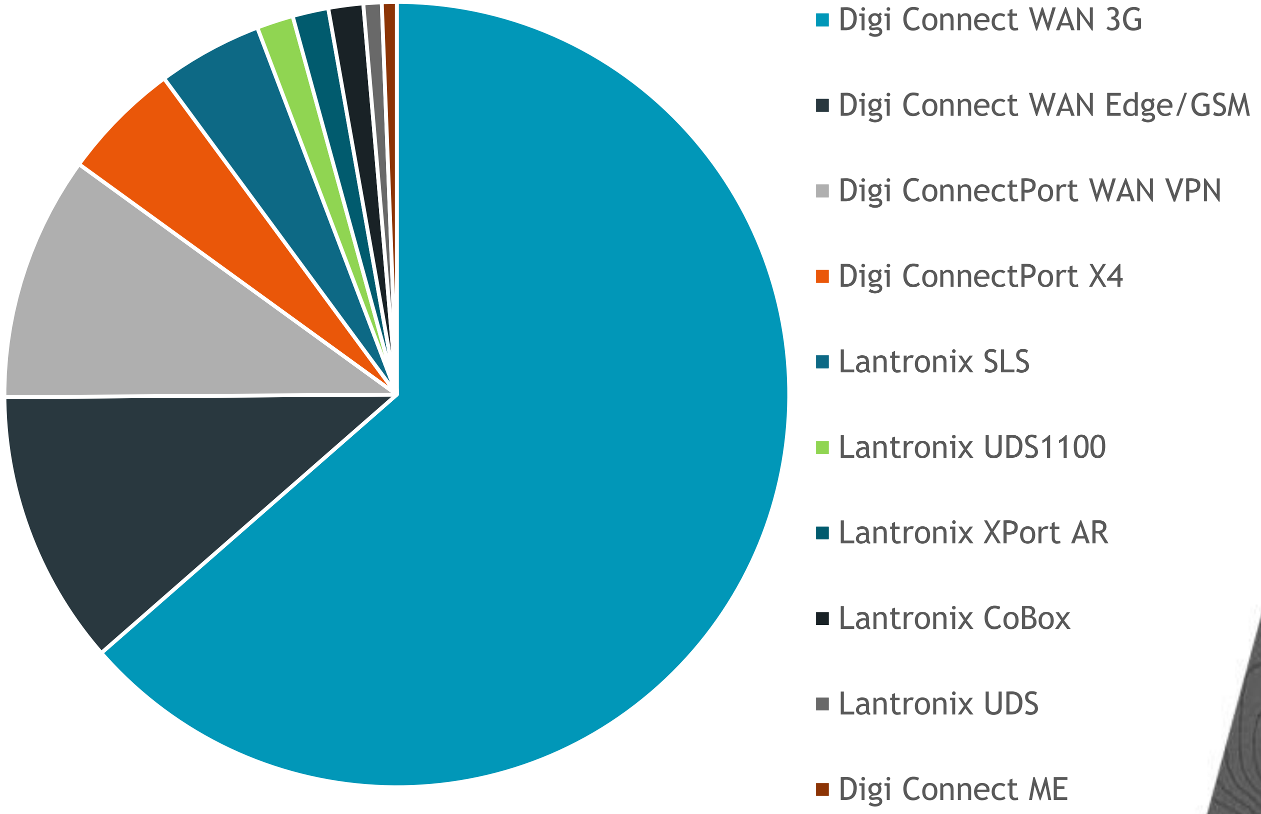
SHODAN, Internet Census 2012, Critical.IO

- Internet-facing devices identified using 3 data sets
  - http://www.shodanhq.com/
  - http://internetcensus2012.bitbucket.org/
  - Critical.IO (private)
- Try to detect to servers using multiple protocols
  - Digi Advanced Device Discovery Protocol
  - SNMP “public” System Description
  - Telnet, FTP, and SSH banners
  - Web interface HTML
  - SSL certificates

Serial Port Device Exposure: SNMP

- SNMP “public” System Description
  - Over 114,000 Digi and Lantronix devices expose SNMP
  - Over 95,000 Digi devices connected via GPRS, EDGE, & 3G





RAPID7

Serial Port Device Exposure: TCP

- Telnet, FTP, SSH, HTTP, and SSL detection
  - Less reliable than SNMP and smaller sample sizes
  - 8,000 Digi devices found with FTP exposed
  - 500 Lantronix systems detected via Telnet
  - Telnet & FTP ambiguous for some devices
  - HTTP and SSL also ambiguous

```
Certificate chain:
  s:/CN=192.168.0.60
  i:/CN=192.168.0.60
```

```
HTTP/1.1 302 Found
Location: https://127.0.0.1:8080/home.htm
Content-Length: 0
Server: Allegro-Software-RomPager/4.01
```

```
Trying 192.168.0.60...
Connected to 192.168.0.60.
Escape character is '^]'.

login:
```

Serial Port Device Exposure: ADDP

- Digi devices support a custom discovery protocol
  - ADDP: Advanced Device Discovery Protocol
  - Obtain the IP settings of a remote Digi device
  - Metasploit scanner module implemented

```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_addp_version
msf auxiliary(digi_addp_version) > set RHOSTS 192.168.0.60
msf auxiliary(digi_addp_version) > run

[*] Finding ADDP nodes within 192.168.0.60->192.168.0.60 (1 hosts)
[*] 192.168.0.60:2362 ADDP hwname:Digi Connect WAN Edge10 hwrev:0
    fwrev:Version 82001160_J1 01/04/2007
    mac:00:40:9D:2E:AD:B2 ip:192.168.0.60 mask:255.255.255.0
    gw:192.168.0.1 dns:0.0.0.0 dhcp:false
    ports:1 realport:771 realport_enc:false magic:DIGI
```

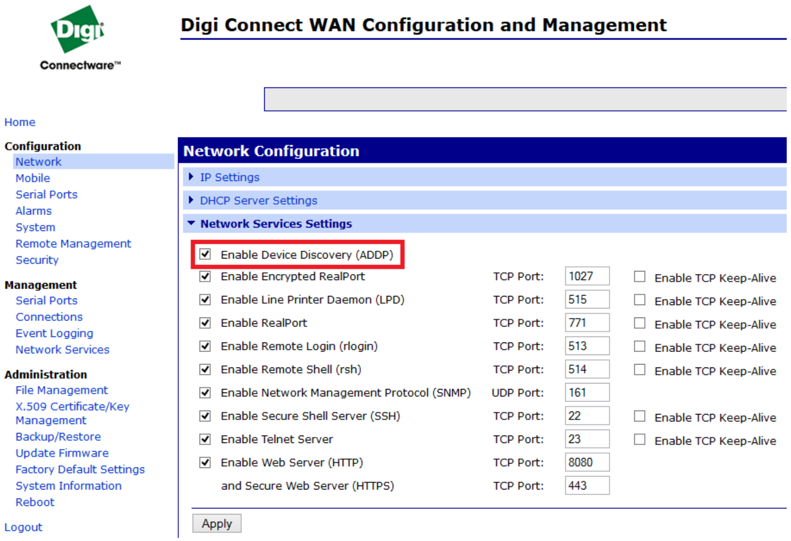
http://qbeukes.blogspot.com/2009/11/advanced-digi-discovery-protocol_21.html

Serial Port Device Exposure: ADDP

- 14,000+ devices respond to Digi ADDP probes
  - Enabled by default only on some equipment
  - Three “magic” strings: DIGI, DVKT, and DGDP
  - DIGI magic is used for “normal” Digi products (87%)
  - DVKT magic is used for third-party builds (13%)

Serial Port Device Exposure: ADDP

- Digi ADDP allows for configuration changes
  - Requires the root password, which defaults to “dbps”
  - Change the running network configuration (DNS, IP, etc)
  - Change the DHCP and WiFi configuration
  - Reboot the device



Digi Connect WAN Configuration and Management

Network Configuration

Network Services Settings

☑ Enable Device Discovery (ADDP)			
☑ Enable Encrypted RealPort	TCP Port:	1027	☐ Enable TCP Keep-Alive
☑ Enable Line Printer Daemon (LPD)	TCP Port:	515	☐ Enable TCP Keep-Alive
☑ Enable RealPort	TCP Port:	771	☐ Enable TCP Keep-Alive
☑ Enable Remote Login (rlogin)	TCP Port:	513	☐ Enable TCP Keep-Alive
☑ Enable Remote Shell (rsh)	TCP Port:	514	☐ Enable TCP Keep-Alive
☑ Enable Network Management Protocol (SNMP)	UDP Port:	161	
☑ Enable Secure Shell Server (SSH)	TCP Port:	22	☐ Enable TCP Keep-Alive
☑ Enable Telnet Server	TCP Port:	23	☐ Enable TCP Keep-Alive
☑ Enable Web Server (HTTP)	TCP Port:	8080	
and Secure Web Server (HTTPS)	TCP Port:	443	

Serial Port Device Exposure: ADDP

- Third-party products using Digi development kits
  - Found on the internet and responded to ADDP

TrippLite SNMP Card
NS7520 Development Board
BP880 TNA-IP1-1
TechNode-MMP500
ES1A
Lonbox PID4000
EtherLink/3
Konwerter PD8
AnywhereUSB/2
xEPI 2
Vitylan /2.0.0
Vaisala WLAN Interface
SP1490-9232 Dual PSU Ethernet
PROFline STR (CC75)
Netcom V3.0
RSLAN
PicoGate
PD8 Converter
Informer-IP
OpenNET Max
LPD401A

ME-NS9210
ECOLOG-NET LAN
ADA-13110
Pinnacle(tm) / LANLink™
Profi42
EDI Ethernet Port
2010ECLip Signal Monitor
SQ20XX
Stulz WIB 8000
A900-LAN 9210
DOMIQ D-BL-1B
Endress+Hauser NEMA X4
Sabre SNMP Module
Rotronic HygroWeb
3M Detection System Model 9100
WEB Remote Control
GridStream IP Radio
Nightshift SeCo
Grathic XBox2
Q.gate IP

Serial Port Device Exposure: ADDP

- Third-party products are often hardcoded for ADDP
  - No configuration interface to disable the ADDP protocol
  - Often no way to change the “dbps” password
  - Metasploit includes an ADDP reboot module

```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_addp_reboot
msf auxiliary(digi_addp_reboot) > set RHOSTS 192.168.0.60
msf auxiliary(digi_addp_reboot) > run
```

Serial Port Server Authentication

Remote Management

- Username and password is required to manage the device
- Typically done via the web interface or telnet
- Some support HTTPS and SSH management

Default Passwords

- Digi equipment defaults to root:dbps for authentication
- Digi-based products often have their own defaults (“faster”)
- Lantronix varies based on hardware model and access
  - root:root, root:PASS, root:lantronix, access:systemn

Serial Port Access Authentication

- Serial port access methods
  - Authenticated encrypted TCP multiplex ports
  - Authenticated, encrypted ssh or web consoles
  - Authenticated, clear-text telnet or web consoles
  - Authenticated clear-text TCP multiplex ports
  - Unauthenticated clear-text TCP multiplex ports
  - Unauthenticated TCP pass-through ports
  - Unauthenticated encrypted TCP multiplexed ports
  - Unauthenticated UDP mapped ports

Serial Port Access Authentication

- Guess which are most common?
  - Authenticated encrypted TCP multiplex ports
  - Authenticated, encrypted ssh or web consoles
  - Authenticated, clear-text telnet or web consoles
  - Authenticated clear-text TCP multiplex ports
  - **Unauthenticated clear-text TCP multiplex ports**
  - **Unauthenticated TCP pass-through ports**
  - Unauthenticated encrypted TCP multiplexed ports
  - Unauthenticated UDP mapped ports

Serial Port Passthrough Services

- Port range depends on the vendor
  - Lantronix uses 2001-2032 and 3001-3032
  - Digi uses 2001-2099
- Connect and immediately access the port
  - Linux root shells sitting on ports 2001/3001

```
[root@localhost root]#
```

Serial Port TCP Multiplexed Services

- Digi uses the RealPort protocol on port 771
  - The encrypted (SSL) version is on port 1027
  - 9,043 unique IPs expose RealPort (IC2012)
- Digi can expose up to 64 ports this way
  - Client must know (or guess) the line speed

Serial Port TCP Multiplexed Services

- Scanning for RealPort services via Metasploit

```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_realport_version
msf auxiliary(digi_realport_version) > set RHOSTS 192.168.0.60
msf auxiliary(digi_realport_version) > run

[*] 192.168.0.60:771 Digi Connect WAN ( ports: 1 )
```

Serial Port TCP Multiplexed Services

- Scanning for RealPort shells via Metasploit

```
$ msfconsole
msf > use auxiliary/scanner/scada/digi_realport_serialport_scan
msf auxiliary(digi_realport_serialport_scan) > set RHOSTS 192.168.0.60
msf auxiliary(digi_realport_serialport_scan) > run

[*] 192.168.0.60:771 [port 1 @ 9600bps] "[root@localhost root] # \r\n"
```

Serial Target Shells

- Approximately 13,000 shells were found online
  - Direct-mapped via 2001/3001 or via RealPort multiplexer
  - One 16-port Digi exposed 16 shells across FreeBSD & IOS
  - The target devices DO support authentication…

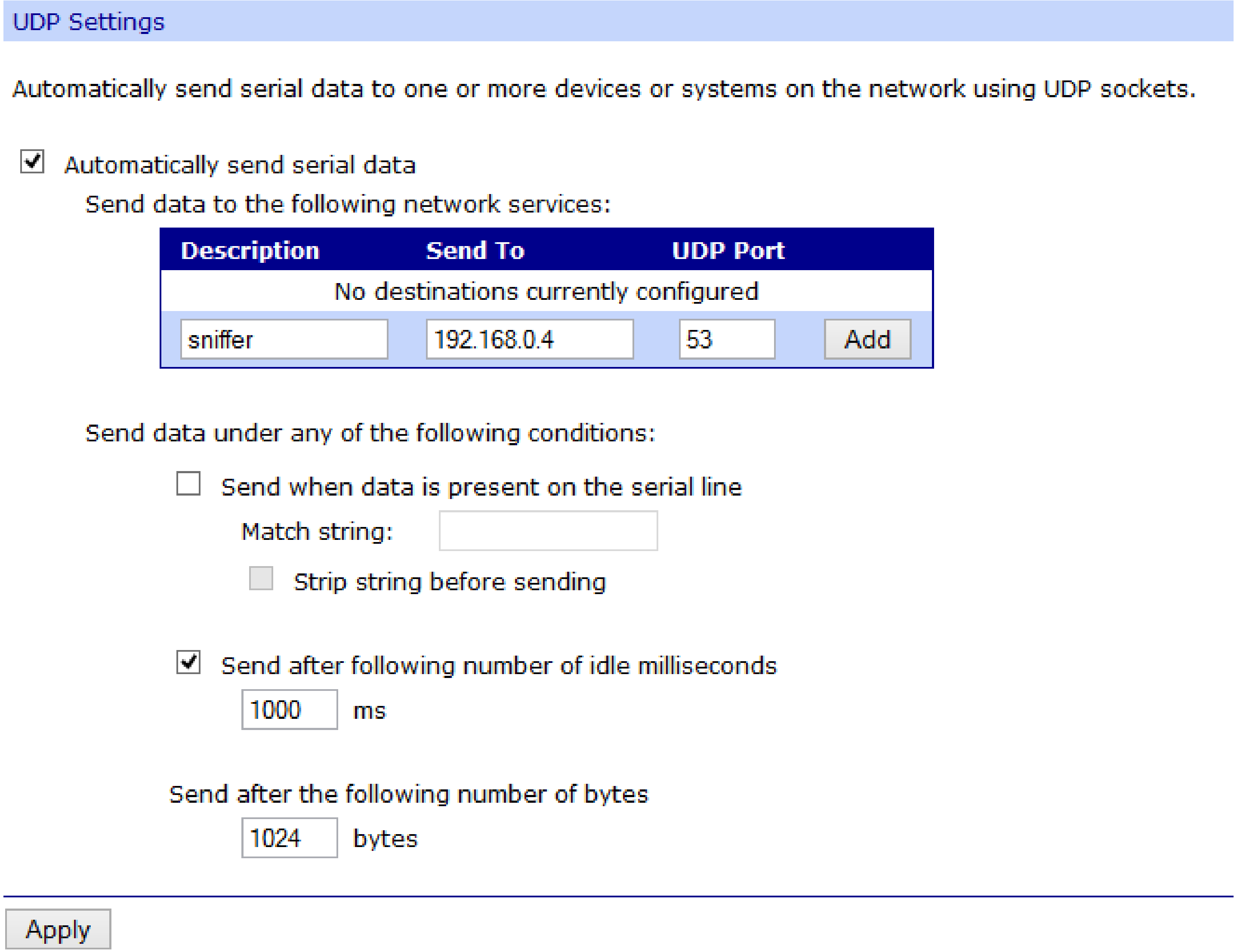
Serial Target Authentication

- Administrators will connect and authenticate
  - No such thing as “disconnecting” from a serial port
  - Some network devices enforce inactivity timeouts
  - Others stay authenticated until an explicit logoff

Exploitation & Beyond

- Getting access to the web interface is step one
  - Default, missing, or weak passwords make this easy
  - Used Metasploit to bruteforce purchased gear
  - Passwords were “dbps”, “digi”, & “faster”
- Lantronix exposes a full Linux environment
  - All of the standard tricks apply (sniffers, scripting)
- Digi provides remote data logging
  - Send all serial data to an external IP (UDP/TCP)
  - Trigger based on content, data, timing

Digi Remote Data Logging



UDP Settings

Automatically send serial data to one or more devices or systems on the network using UDP sockets.

☑ Automatically send serial data

Send data to the following network services:

Description	Send To	UDP Port	
No destinations currently configured			
sniffer	192.168.0.4	53	Add

Send data under any of the following conditions:

□ Send when data is present on the serial line

Match string:

□ Strip string before sending

☑ Send after following number of idle milliseconds

1000 ms

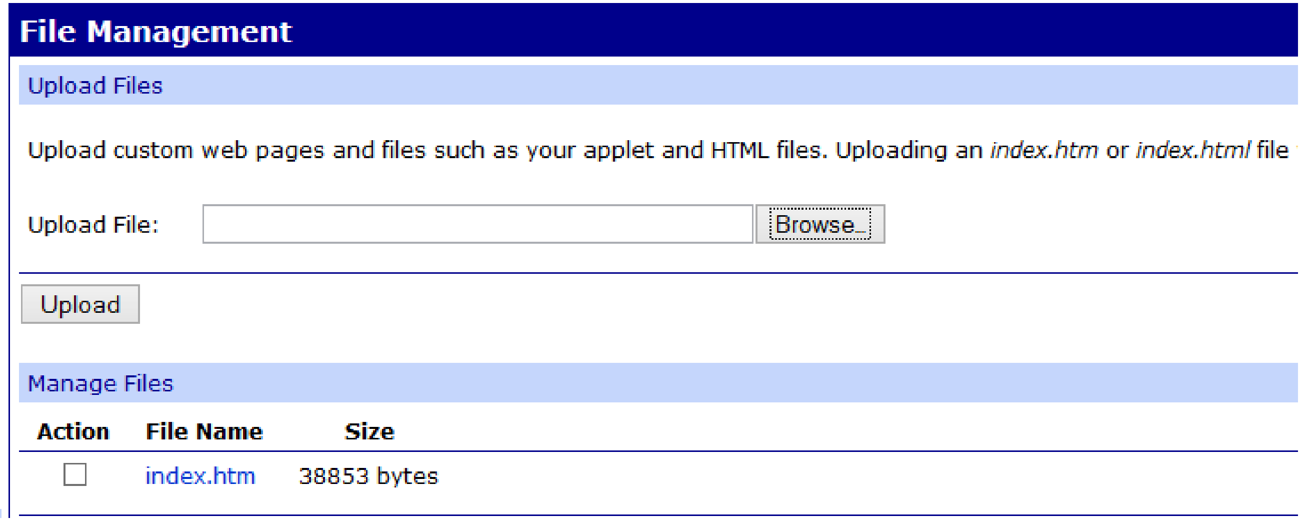
Send after the following number of bytes

1024 bytes

Apply

Digi File Manager

- Upload static exploits to the web interface
  - Use the device as a drive-by host or target the admin
  - Automatically shows index.htm to the admin



File Management

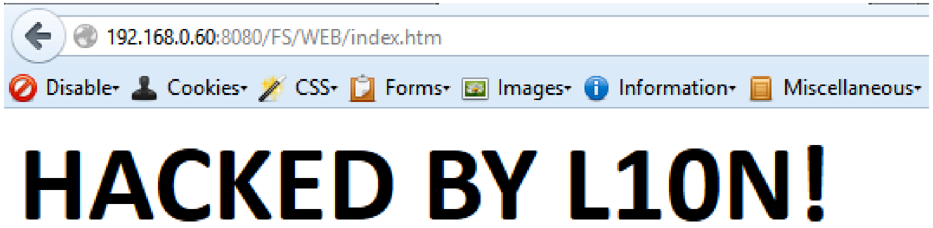
Upload Files

Upload custom web pages and files such as your applet and HTML files. Uploading an *index.htm* or *index.html* file

Upload File:

Manage Files

Action	File Name	Size
☐	index.htm	38853 bytes

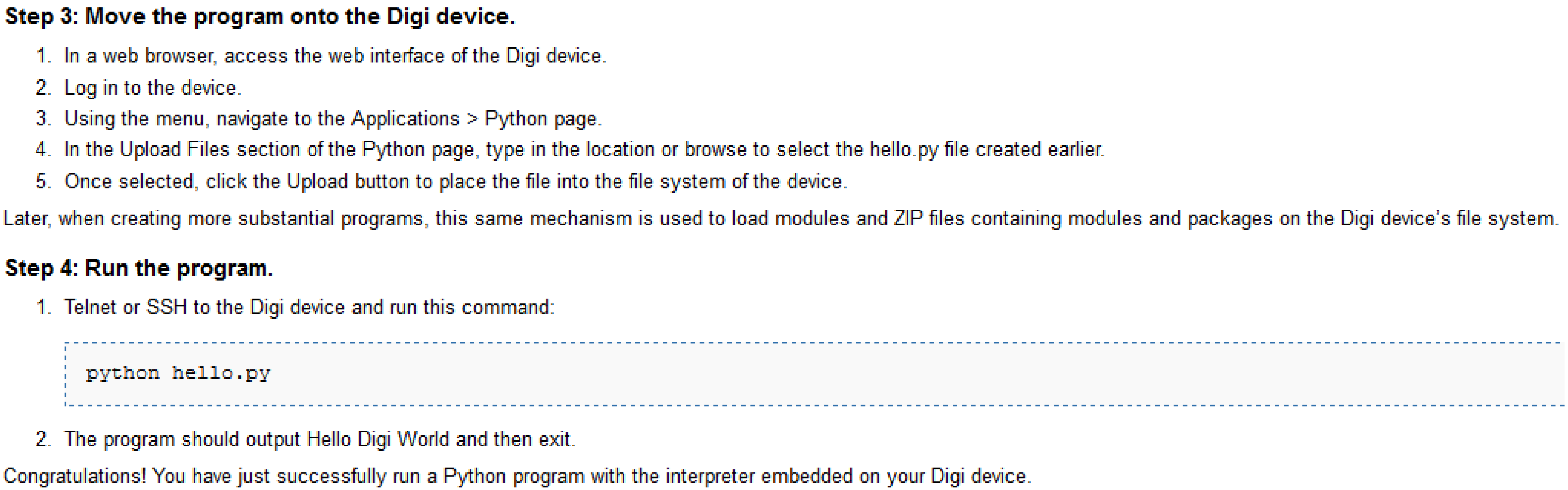


192.168.0.60:8080/FS/WEB/index.htm

HACKED BY L10N!

Digi File Manager: Python

- Newer Digi systems support on-device python
  - Used for things like meter monitoring and MODBUS
  - Can just as easily create a persistent backdoor



Step 3: Move the program onto the Digi device.

1. In a web browser, access the web interface of the Digi device.
2. Log in to the device.
3. Using the menu, navigate to the Applications > Python page.
4. In the Upload Files section of the Python page, type in the location or browse to select the hello.py file created earlier.
5. Once selected, click the Upload button to place the file into the file system of the device.

Later, when creating more substantial programs, this same mechanism is used to load modules and ZIP files containing modules and packages on the Digi device's file system.

Step 4: Run the program.

1. Telnet or SSH to the Digi device and run this command:

```
python hello.py
```

2. The program should output Hello Digi World and then exit.

Congratulations! You have just successfully run a Python program with the interpreter embedded on your Digi device.

Remediation

- Only use encrypted management services (SSL/SSH)
- Set a strong password and non-default username
- Scan for and disable ADDP wherever you find it
- Require authentication to access serial ports
  - Enable RealPort authentication and encryption for Digi
  - Use SSH instead of telnet & direct-mapped ports
- Enable inactivity timeouts for serial consoles
- Enable remote event logging
- Audit uploaded scripts

Next Steps

- Audit of embedded web server & ssh services
- Audit of the RealPort protocol stack
- Audit of Lantronix devices
- Metasploit session support
- Metasploit payloads

Serial Devices in the Wild

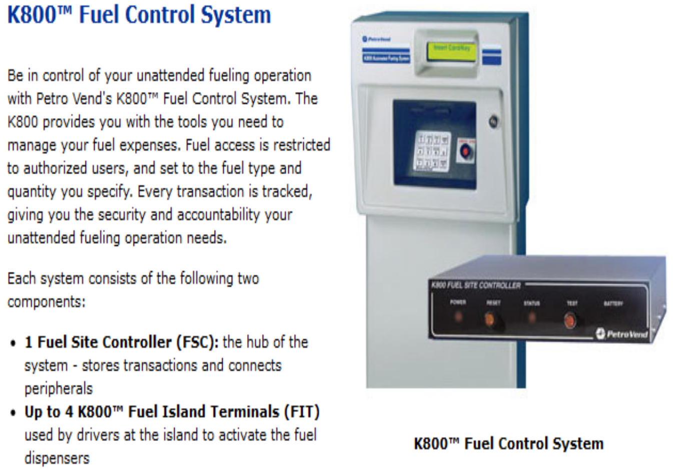
Extracted from Internet Census 2012 data on 2001/3001 TCP

EDI Traffic Signal Monitors

- Based on Digi development kits, exposes ADDP
  - Default password is “dbps” as a result
  - ~40 or so identified in the Internet Census 2012 data

K800 Fuel Control Systems

- Often connected through Digi serial port servers
  - Appears to be a x86 board managed via serial



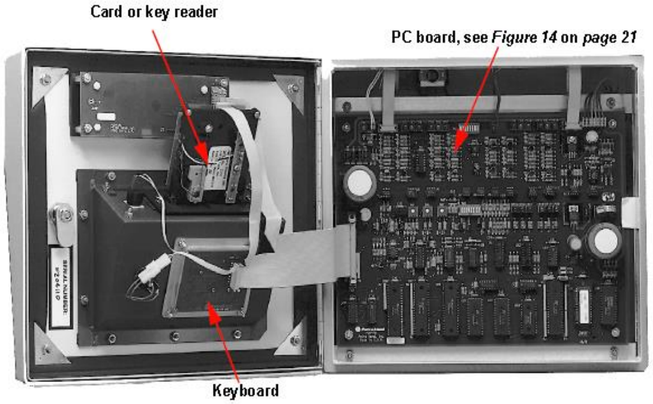
K800™ Fuel Control System

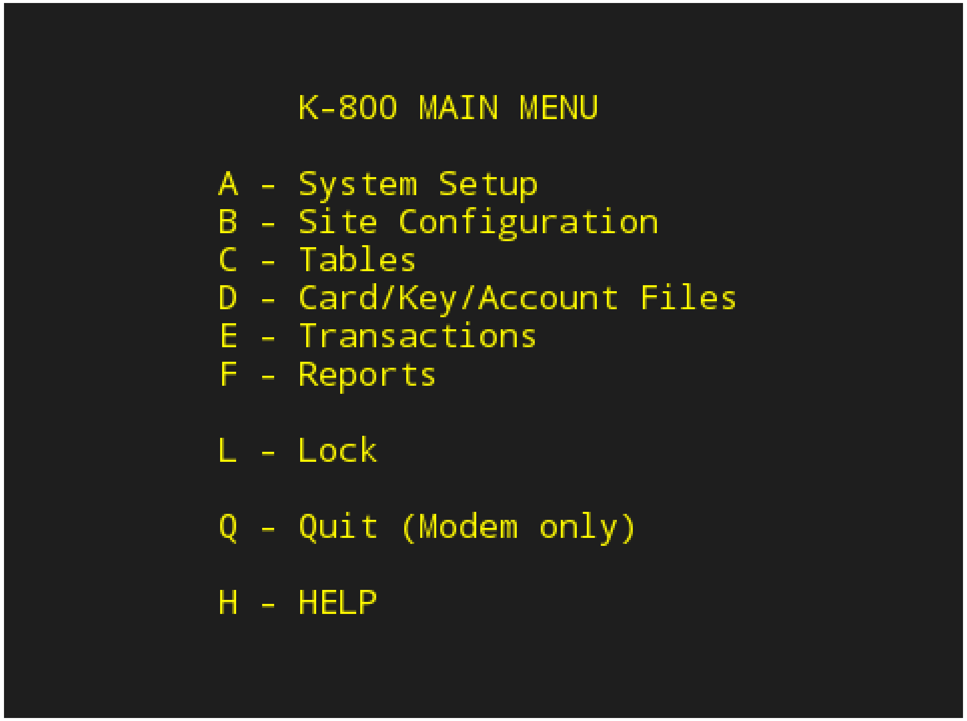
Be in control of your unattended fueling operation with Petro Vend's K800™ Fuel Control System. The K800 provides you with the tools you need to manage your fuel expenses. Fuel access is restricted to authorized users, and set to the fuel type and quantity you specify. Every transaction is tracked, giving you the security and accountability your unattended fueling operation needs.

Each system consists of the following two components:

- **1 Fuel Site Controller (FSC):** the hub of the system - stores transactions and connects peripherals
- **Up to 4 K800™ Fuel Island Terminals (FIT)** used by drivers at the island to activate the fuel dispensers

K800™ Fuel Control System

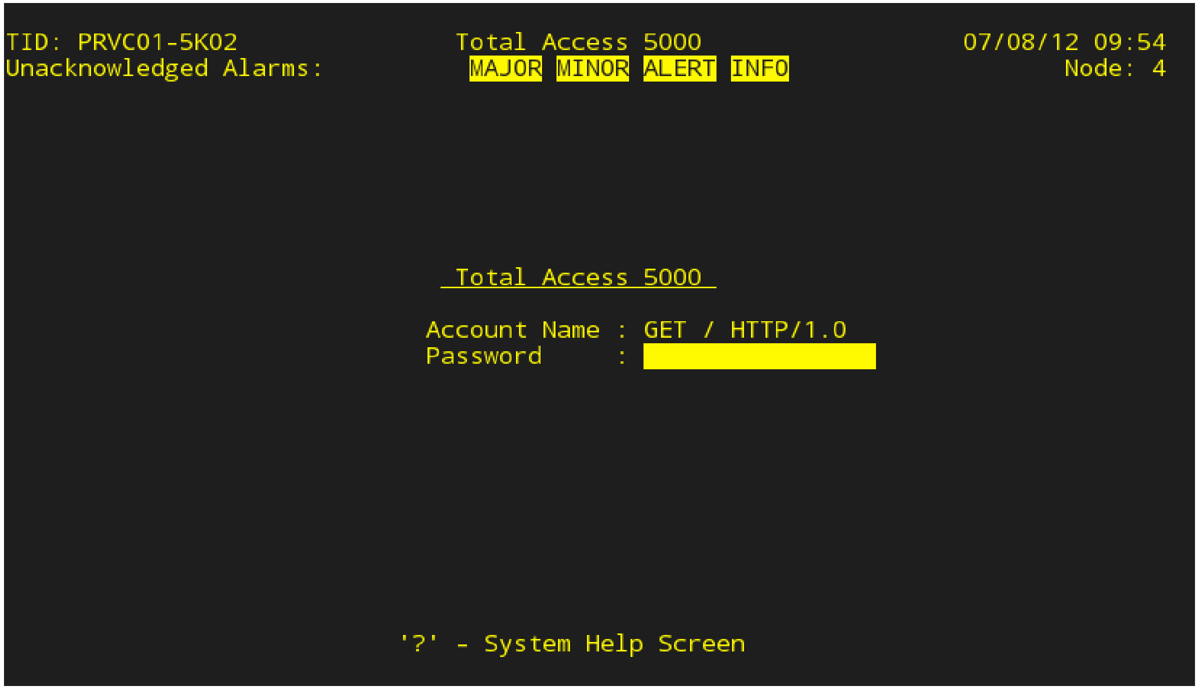




```
      K-800 MAIN MENU

  A - System Setup
  B - Site Configuration
  C - Tables
  D - Card/Key/Account Files
  E - Transactions
  F - Reports

  L - Lock

  Q - Quit (Modem only)

  H - HELP
```

Adtran IPTV Headend Systems

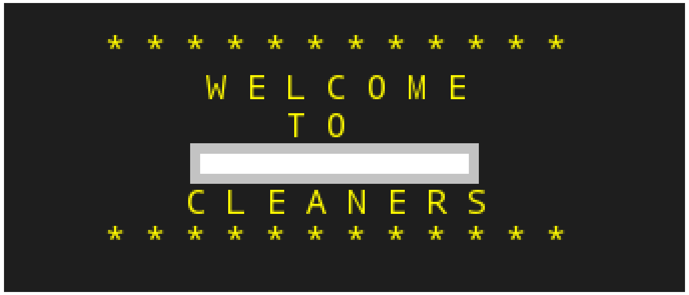
- Actually required authentication
- Except when left logged-in



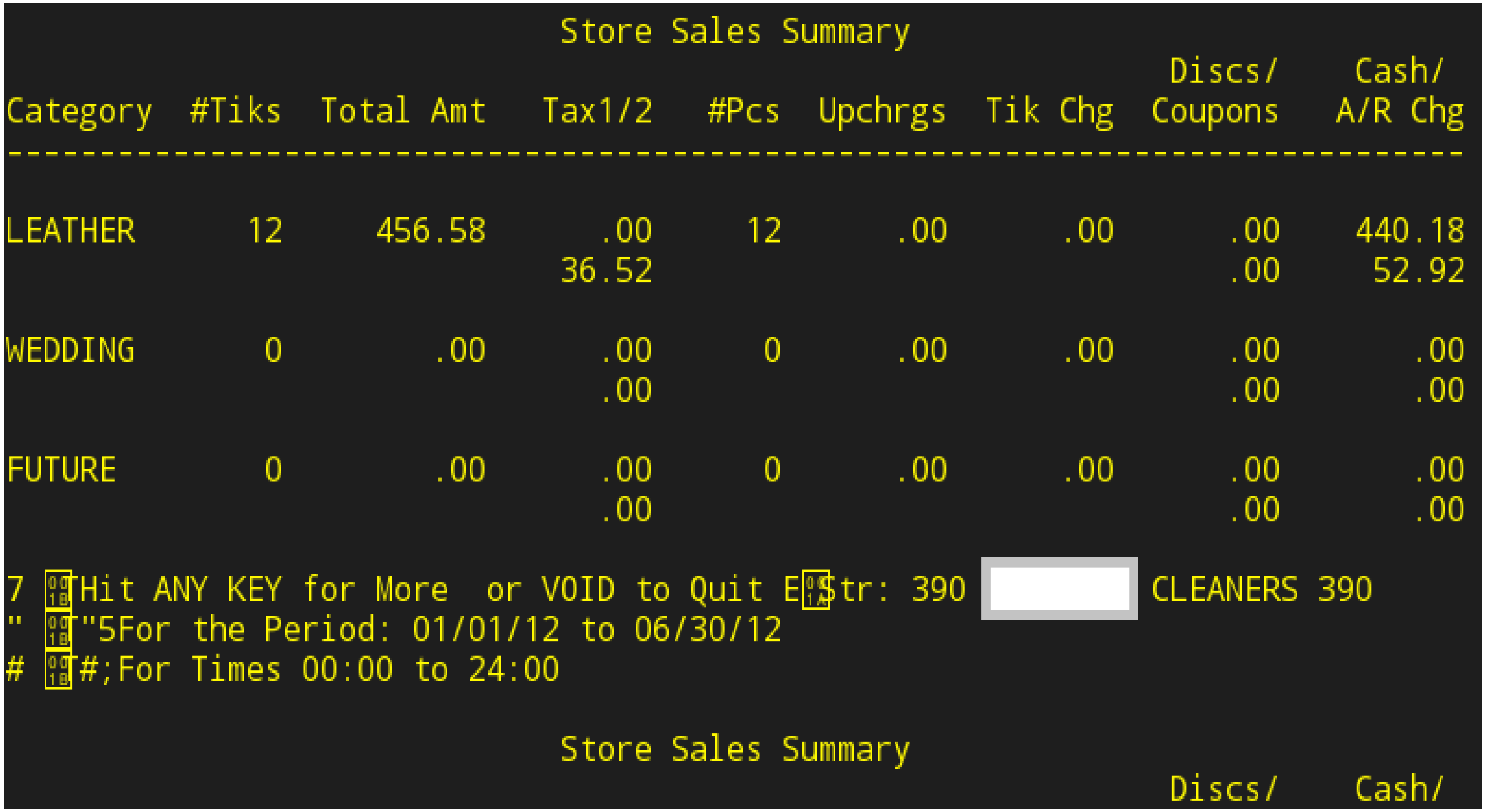
```
TID: PRVC01-5K02                 Total Access 5000                   07/08/12 09:54
Unacknowledged Alarms:            MAJOR MINOR ALERT INFO                    Node: 4



                                 Total Access 5000

                             Account Name : GET / HTTP/1.0
                             Password     :



                           '?' - System Help Screen
```

National Dry Cleaner Chains

- Full access to PoS systems
- No authentication



```
* * * * * * * * * * * *
      W E L C O M E
          T O
      [redacted]
    C L E A N E R S
* * * * * * * * * * * *
```



```
                            Store Sales Summary
                                                              Discs/     Cash/
Category  #Tiks  Total Amt   Tax1/2   #Pcs  Upchrgs  Tik Chg  Coupons    A/R Chg
---------------------------------------------------------------------------------

LEATHER      12     456.58      .00     12      .00      .00      .00     440.18
                              36.52                               .00      52.92

WEDDING       0        .00      .00      0      .00      .00      .00        .00
                                .00                               .00        .00

FUTURE        0        .00      .00      0      .00      .00      .00        .00
                                .00                               .00        .00

7  ▯THit ANY KEY for More  or VOID to Quit E▯$tr: 390 [redacted] CLEANERS 390
"  ▯T"5For the Period: 01/01/12 to 06/30/12
#  ▯T#;For Times 00:00 to 24:00

                            Store Sales Summary
                                                              Discs/     Cash/
```

Conclusions

Summary: Exposure

- Over 114,000 serial port servers on the internet
- 95,000 are on mobile connections, no firewall
- Concentrated within a few mobile ISP subnets
- Discoverable via SNMP, ADDP, RealPort scans
- Network configuration exposed through ADDP
- Indexed by Internet Census 2012 & SHODAN

Summary: Authentication

- Weak, default, and missing management credentials
- Third-party Digi kits may hardcode ADDP password
- Most servers do not authenticate the serial port
- Most serial devices do not automatically logout
- 13,000 serial ports lead to authenticated shells

Summary: Systems

- Industrial automation equipment is most exposed
- Serial servers a gateway to Zigbee and MODBUS
- Exposes important hardware
  - Traffic signal equipment
  - Electrical monitors
  - Medical systems

Thanks!