The BEACON

West Mountain RADIO

CBA V Available Now

Updated CBA Software available

New Life for an Old Analog Scanner

By Sholto Fisher, K7TMG

I'm sure many of you have an old analog VHF/UHF scanner gathering dust somewhere in your house?
In my case a 1980's vintage Uniden Bearcat BC-145XL was found lurking in a closet so I started thinking about what it could be used for in 2021.

Back in its day the BC-145XL (and similar scanner) were very useful and simple to operate and program. It covers 29MHz to 512MHz in several bands and has a WX button for quick access to NOAA WX. 16 channels does not sound like a lot but it is fine for this application.

Every year there are less and less analog signals to be heard on the VHF/UHF bands. There is still the NOAA WX stations, 2m and 70cm ham bands and GMRS/FRS channels of course, but a lot of what we used to buy a scanner for has "gone digital".

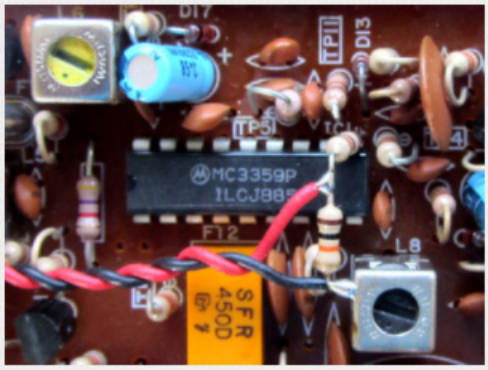
Is there a way to listen to digital traffic with an old dinosaur like my BC-145XL? I began to wonder and do a little research.

Some of the digital systems in use may be familiar to you such as D-STAR (Icom) and MotoTRBO (DMR) which are widely used on our ham bands.

A little searching on the internet and I stumbled across a remarkable computer program called DSDPlus which decodes many of these digital systems and outputs the recovered audio to your computer speakers.
This sounded promising so I looked into it some more and found that it will decode the following types of digital transmission: D-STAR, NXDN4800, NXDN9600, DMR/MotoTRBO, P25 Phase 1, X2-TDMA, and ProVoice. There does not seem to be any support for Yaesu Fusion (C4FM) but this is not a big loss (at least in this part of the world) as I do not think there are any Fusion repeaters in range.

The next surprise was that DSDPlus is free software. There is a modest cost to get the latest versions of the software as and when they come out but the freeware version (1.101) is perfectly adequate. I do encourage you to join the so-called DSDPlus Fast Lane Program. Visit https://www.dsdplus.com/
These digital signals have very different channel/bandwidth characteristics than traditional analog voice signals so simply hooking up the audio from my old scanner to the computer line-in jack isn't going to work. We need to take audio from the discriminator (i.e. before any filtering is done inside the scanner).
In case you didn't know there's a very useful web site which covers making discriminator taps on popular scanners (isn't it amazing what you can find on the web?) so I quickly located the page on the Bearcat BC-145XL at https://www.discriminator.nl/ubc145xl/index-en.html

Pin 10 of the MC3359 contains the unfiltered audio



The components at pin 10


Chassis socket in the scanner's back

Follow the next steps to make the discriminator output:

- Install a 3.5 mm mono socket in the scanner's back
- Solder a 10 k resistor to pin 10 of the receiver IC
- Connect another 10 k resistor to the other lead of the resistor connected to pin 10
- Solder the other lead of the second resistor to the metal shield of the IF coil.
- Connect the junction of both resistors with the signal solder lug of the chassis socket (red wire)
- Connect the chassis socket's ground lug with the metal shield of the IF coil (black wire)

As you can see, making a discriminator tap on this scanner is as easy as installing a 3.5mm panel jack fed by a resistive divider connected to the receiver IC (MC3359) and ground.

I had this completed in short order so now I hooked up the scanner's new audio output to my computer sound card input and fired up DSDPlus.

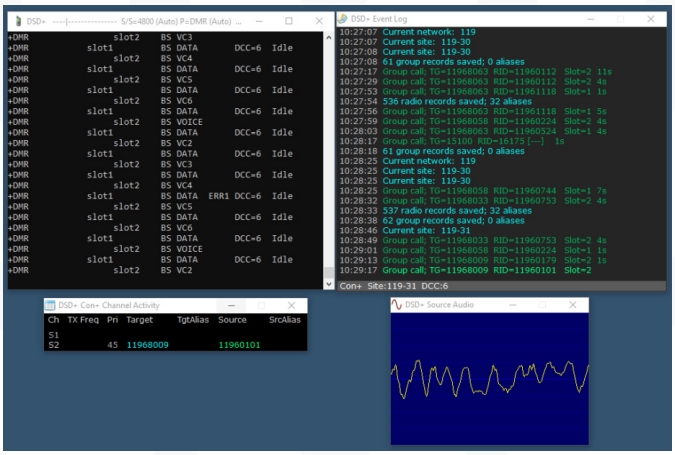
There's a nice tuning indicator with the software that shows the level of the input signal. Using the Windows volume control I could adjust this level. DSDPlus seems to work over a wide dynamic range so I am not sure this is particularly critical.

Next I needed some signals to test it on. I find Radio Reference to be invaluable for finding scanner frequencies in my local area so I headed over to https://www.radioreference.com/ and entered my state and county.

This gave me a bunch of frequencies to try where I may expect various digital signals. Many are up around 760MHz unfortunately (the BC-145XL tops out at 512MHz) but luckily there is simulcasting on lower UHF frequencies (around 460MHz).

Many of these signals are trunked and of course the BC-145XL has no trunking capabilities but you can simply park the scanner on one of the frequencies and wait for a signal. I found that by programming the most likely candidates into the scanner and scanning through all 16 channels was the best strategy. DSDPlus quickly synchronizes on the signal type and starts playing audio through the computer speakers.

Some signals are encrypted (typically law enforcement P25 Phase 1) so you're not going to hear those but even on these encrypted networks you will occasionally hear a radio that presumably hasn't had encryption enabled on it.



DSDPlus decoding a DMR (MotoTRBO) signal

There are other types of signals you can use your modified scanner for too. The discriminator audio can be used for:

- 9600 bps Packet Radio. Use UZ7HO Sound Modem http://uz7.ho.ua/packetradio.htm
- ATCS (Advanced Train Control System) decoding. Use https://www.coaa.co.uk/trainplotter.htm
- AIS (Automatic Identification System) Maritime decoding. Use https://www.coaa.co.uk/shipplotter.htm or MultiPSK http://f6cte.free.fr/multipsk_e.htm
- Pagers (POCSAG, FLEX, etc). This may be illegal in your country to monitor however!. Use https://discriminator.nl/pdw/index-en.html or MultiPSK http://f6cte.free.fr/multipsk_e.htm
- NWR SAME (Weather Alerts)*. Use MultiPSK http://f6cte.free.fr/multipsk_e.htm

I have not tried it yet but I believe you might also have a shot at NOAA WX satellite images on 137MHz using the WXtoIMG software from https://wxtoimgrestored.xyz/
The discriminator modification doesn't alter the audio coming out of the scanner's internal speaker so you can also continue to use it for analog signals.
While my scanner and software isn't going to compete with the latest trunking digital scanners available, it also didn't cost $1000 to be able to decode many of the newest digital systems! I hope you will give it a try yourself.

** NWR SAME decoding doesn't technically require discriminator audio but it's another fun thing to try when you're looking for something to decode on VHF!*

A Report from Greece

By Miroslav Skoric (YT7MPB)

My last conference travel to Greece was in early September 2021. It was linked to IEEE ISCC 2021. There I met a Greek radio amateur (Fig. 1, 2) who brought his portable antenna (as disassembled in two bags), and assisted me in assembling & mounting it on my hotel room's balcony (Fig. 3, 4, 5).

Fig. 1

Fig. 2

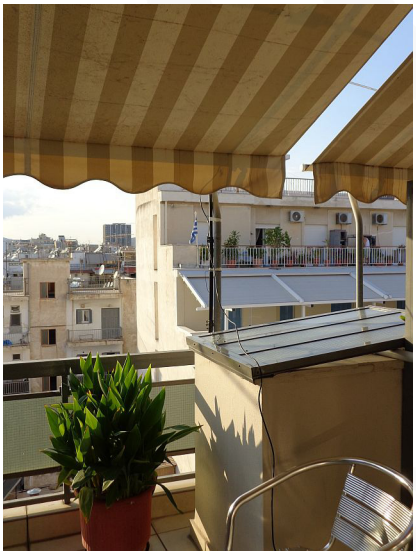


Fig. 3

Fig. 4

Fig. 5

The plan was to test VHF and 'old' HF packet-radio for APRS positioning purpose, as well as other 'data' communications with my forwarding partners. The antenna cable was fed into a portable HF radio that was placed in my hotel room, over an antenna tuner. The RIGblaster Advantage was used for HF part. But at first, the WMR RIGblaster Plug and Play was attached to a VHF handy radio and a laptop computer running a node/BBS/Winlink software. I used my home-made cable adapter to attach the 6-pin mini-DIN input/output of RIGblaster Plug and Play to the 3.5mm and 2.5mm jacks of the handy radio (Fig. 6, 7).

Fig. 6

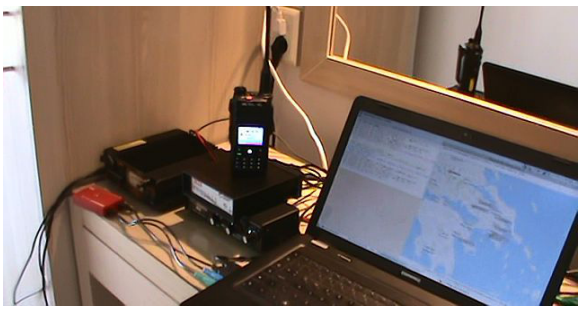


Fig. 7

At first, I made experiments with VHF APRS traffic in the room, but realized that signals were much better when moved the radio to the balcony, Fig. 8-9.

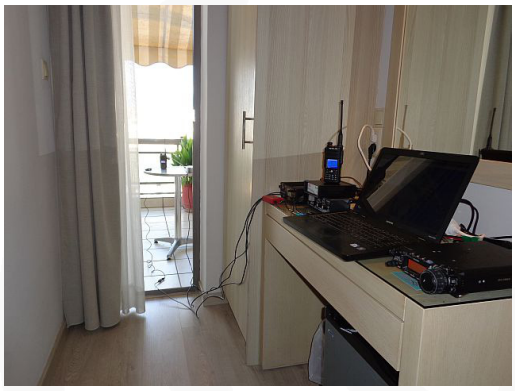


Fig. 8

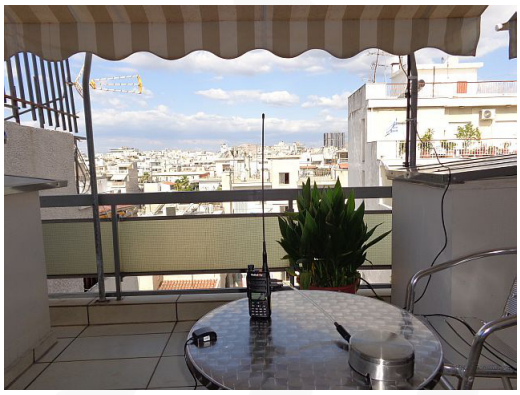


Fig. 9

At first, I made experiments with VHF APRS traffic in the room, but realized that signals were much better when moved the radio to the balcony, Fig. 8-9.

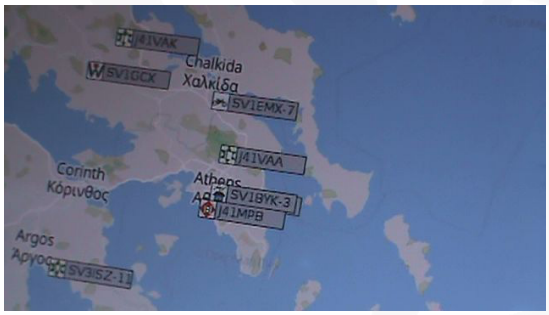


Fig. 10

Left: YT7MPB (J41MPB) Right: SV1IW
Fig. 11

Our lecture was held in the conference hotel in central Athens where I shared my time for talk with the other ham co-author, Fig. 12 and 13.

Fig. 12

Fig. 13

During our talk, I organized a good display of my instruments and described their features. Of course, both the WMR RIGblaster Plug and Play, and the RIGblaster Advantage were there on the table (Fig 14-15).

Fig. 14

Fig. 15

Our session took some 1.5 hours and we presented most important features of ham radio hardware & software used in RF email exchange, positioning systems, and cases of emergency. When finished, we took some time for a coffee on the hotel's roof, having a nice view to Acropolis (Fig 16, 17).

Fig. 16

Fig. 17

That was the last day of the conference itself, which was held in 'hybrid' format because of pandemic situation, so our session was the only one held 'in-person' and in real time!

The following week I spent in Piraeus near Athens, by performing more tests in HF packet, VHF packet, and other data transmissions (Fig. 18-19). Even though the conditions were far from perfect, the overall impressions were positive.

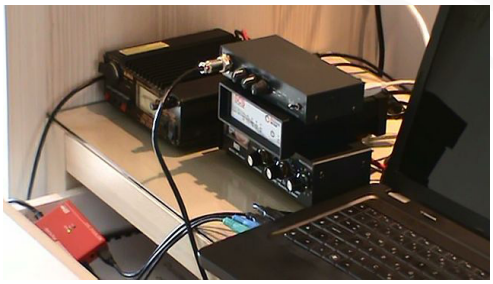


Fig. 18

Fig. 19

There is a chance to replay the same conference-and-ham project in years to come, particularly if the HF antenna could be erected to a better (and higher) position, such as to a terrace above the neighboring room to the left side (where ladders are seen in Fig. 20). It might also happen that some good food will help us who participated in this event, having in mind that the famous brand of some food ingredients was probably named after yours truly … Misko YT7MPB … (Fig. 21)

Fig. 22

Fig. 23

Let us hope that pandemic will decrease in times to come, so that West Mountain Radio and its RIGblasters will continue to be introduced, displayed and promoted as quality instruments for 'digital hams'.

Remote Monitoring

By Mark Siegesmund

The CBA is a great tool for testing batteries. For a proper test it can take a long time to run a test. Consider a 80AH car sized Lead Acid battery. To get the same results as is stamped on the battery you need to do a 4A test for around 20 hours. If you do the test at home you may want to check in on it from work or vice-versa.

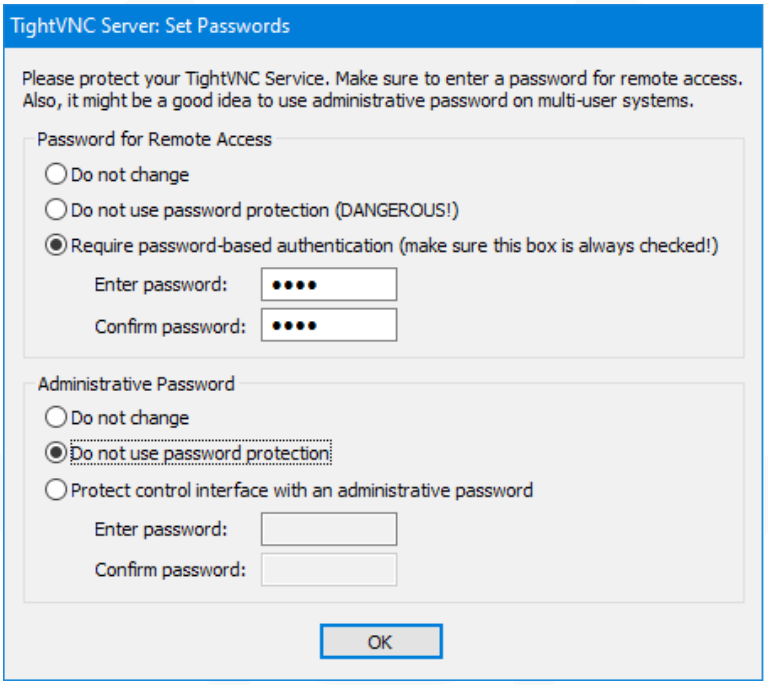
This article describes how you can check in on the test from a remote location. The technology is called VNC (Virtual Network Computing). What this allows you to do is connect to your PC from a remote location and work at the PC (monitor, keyboard and mouse) as if you were there. You may have experienced this when calling tech support for some computer problems. In that case you need to be at the target computer and give permission for access. For our situation that would not be practical.

There are a number of programs available to implement a VNC system. For the examples in this article I will use TightVNC. It is a free program that is easy to use and performs well. It does not currently have encryption as most paid programs will have. This means someone else could snoop in on what you are doing.

The computer you want to monitor/control remotely is referred to as the server. The other computer you want to connect to the server is referred to as the client or viewer. Here are the steps to set everything up:

1. Download TightVNC. The link as of this article is:
   https://www.tightvnc.com/download.php

2. On the server install the server, when asked select the CUSTOM option and select just the server software, no need for the viewer software.
3. You will need to enter a password to be used for remote access.



4. Maybe the most difficult task is to make sure requests from the outside world can get to the server software. Usually you need to set up your router to always give your server PC the same IP address. You then need to tell the router that whenever a request comes in for port 5800 or 5900 (the TightVNC ports) the request should be routed to that static IP address.

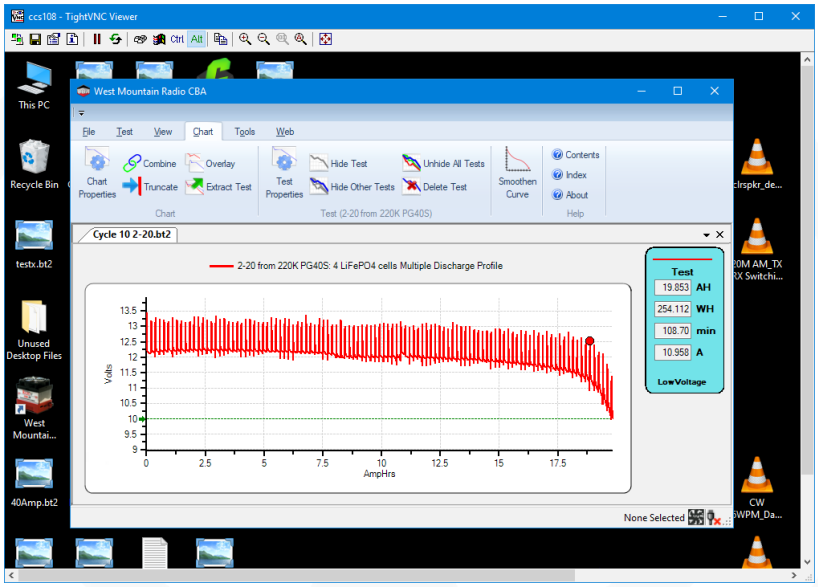
You can get some specific help using your router model and a Google search like this: “open port on MYROUTER 1234”

You can also get help at: https://www.portforward.com/

5. On the server PC open a web browser, go to Google and type the question:
“What is my IP address?”
Write down the four numbers separated by periods that come up. That is the address of your router to the outside world.

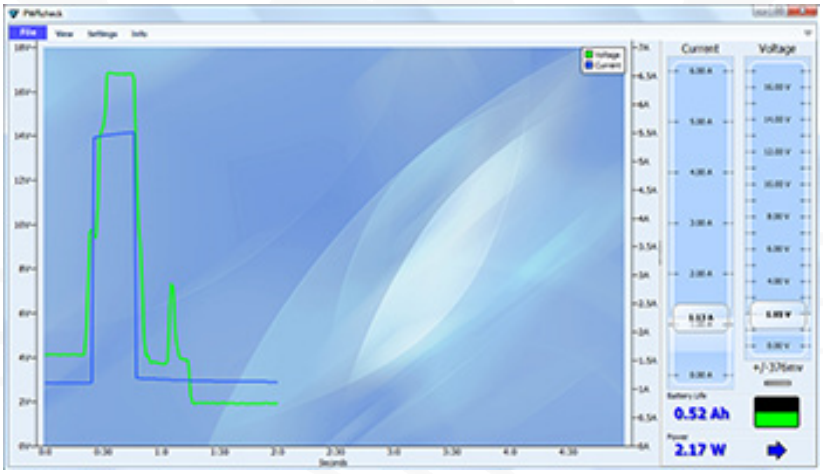
6. On the client PC install the TightVNC software and install just the viewer software.

7. Run TightVNC on the client PC and then enter the IP address you wrote down and click CONNECT. You will be prompted for a password and with some luck you will see:



For the best resolution click on the full screen icon (far right on toolbar).

Consider remote monitoring the PWRcheck+



Or maybe the Epic PWRgate:

```
Charging PS=14.05V Batt=12.47V,  9.6A Sol=0.00V Min=14
Charging PS=14.05V Batt=12.47V,  9.5A Sol=0.00V Min=14
Charging PS=14.05V Batt=12.48V,  9.6A Sol=0.00V Min=14
Charging PS=14.05V Batt=12.48V,  9.6A Sol=0.00V Min=15
```

The USB port on the PWRguard+, RIGrunner4010S+ and RIGrunner4007U all have the ability to turn the power on and off over the USB port. With a VNC you can now do that from a remote computer.

It should also be pointed out the RIGrunner4005i and RIGrunner10010i are internet ready and you have remote monitoring (voltage, current, fuse reset...) from any web browser.

Signature Headaches

By Mark Siegesmund

Back in 1995 the most popular web browser company in the world, Netscape, decided to use asymmetric encryption to allow people to safely enter credit card numbers in the web browser. Mathematicians started talking about asymmetric encryption in the late 70's. There are two keys, one to encrypt and a different one to decrypt. It is very difficult to figure out one key unless one has the other. This way a website can send an encrypt key to the browser and the browser can encrypt the data to be sent. Even if someone is able to see the encrypted data and the encrypt key, the data can not be decrypted without the decrypt key. Part of the magic involves very large prime numbers and complex equations.

That is not all the browser did for SSL (Secure Socket Layer, AKA https). This also created the idea where each SSL website would have a certificate issued by a trusted authority. That certificate indicates the web site domain is encrypted by the authority. The browser can decrypt the certificate to learn the verified name of the company that is running the web site. In this case, it is the encrypt key that remains secret. The idea was to prevent a user from being spoofed into entering their credit card on a web site that appears to be a well known site, but is not.

It is that second use that caught the eye of Microsoft in the XP days. They decided to use the certificate concept to add a signature to executable files loaded by Windows. It works like this: A software publisher gets a certificate from a trusted authority, the same people doing web site certificates. Using a tool from Microsoft, a signature using the certificate with the company name and a CRC of the executable file is appended to the file. When the OS loads the file, it can decrypt the signature, verify the CRC and decide how trusted the file is. For example if a message like "This program was published by CCS, Inc; if you trust that company press continue."

The only encryption algorithm used up to 2001 was called SHA1. In 2001 a new algorithm called SHA2 (AKA SHA256) came out that was considered harder to break with the newest fast computers. XP SP3 would accept either encryption but the older XP versions would only take SHA1. One could sign a file with two signatures, SHA1 and SHA256 and it would all work, so this became the norm.

Starting with 64 bit Windows 7 Microsoft began requiring all drivers be signed with a certificate traceable to an authority they approved of. The way these certificates work is company A can issue a certificate to you and they have a certificate issued by company B and they have one issued by company C. This chain of certificates is all part of the signature. Microsoft maintains a list of the large handful of top level certificate issuers it trusts. Drivers were considered sensitive because they often operate in kernel mode where they can access any memory in the PC.

With all the websites in the world a lot of companies were issuing a lot of certificates and some of these authorities were not doing much to check for who they were issuing them to. The concept of an Extended Validation certificate (EV) was created where it requires a great deal of verification to ensure the certificate holder is who they say they are. Microsoft uses this in their SmartScreen web browser download checker. It flags any software without a EV certificate as suspicious.

This was all well and good until the release of Windows 10 that first was sent out October of 2020. Microsoft decided drivers loaded into Windows would only be accepted if they were signed by

Microsoft. The way this worked is the software publisher would first sign the driver with an EV certificate, then send it to Microsoft. If approved, the publisher signature was stripped and a Microsoft signature applied. They would then send the package back to the publisher. So the whole world did not grind to a halt, they have exceptions as a part of a roll out plan. In general, right now anything signed in 2021 needs a Microsoft signature and most older files are accepted.

So here come the headaches for CCS. First I should point out even though we have a yearly developer subscription with Microsoft we did not get the memo about this new rule. In the old days Microsoft published a newspaper sent via snail mail to all developers. The last one we got was October of 2000. For a while we got news by CD and then that was replaced with a slew of online blogs.

Microsoft does not update all machines at the same time, so early this year we started getting some calls of trouble but not enough to be very concerned. There seemed to be work-arounds that got people going. Only new drivers had a problem and only on machines that did not have the driver previously installed. The error did not say “Sorry this driver must be signed by Microsoft”, it did say “Invalid signature hash.”

We put in a support ticket with Microsoft in May and were then told about the new rules. Our first step was getting an EV certificate. We had been using the ordinary certificates (OV) since the beginning but never bothered with the EV. It then took over two months and a pile of tickets in attempts to log into the Microsoft driver signing website. The problem turned out to be another account with the same company name was taken out 10 years ago and not used since. The error was not “Company name already used”, it was “Something went wrong, try again later.” The next problem was our files were not being accepted. Another dozen tickets and we found out the reason our certificate was not working was the authorities started issuing SHA3 certificates and the Microsoft website could not handle those yet. Windows is OK with SHA3 but not the website that accepts the driver submittals. After making a special request for an SHA2 certificate and another couple of weeks to figure out what the special website wanted, we started getting Microsoft signed drivers.

So far we have not been able to figure out how to append additional signatures on to the files so it seems we need to have new and old style drivers depending on the OS.

Many of our customers are using USB CDC drivers to talk to the PIC® MCU. This creates a COM port in Windows that can use the normal serial API functions. The driver for a CDC device is just a .inf file with VID, PID and company information, plus the .cat file with the signature. In Windows 10 no driver is required for CDC devices. You do need it for older versions of Windows. If you do want to use a .inf for a CDC device in Windows 10 then it does need the Microsoft signature even though the driver file is optional.

It is possible to load a driver into Windows that has a bad or wrong signature. This link details the procedure:
https://www.howtogeek.com/167723/how-to-disable-driver-signature-verification-on-64-bit-windows-8.1-so-that-you-can-install-unsigned-drivers/

The procedure will not work if you have secure boot enabled and on some PC's you need a password to disable secure boot. This also will not work on PC's that are in S-Mode. Only software products in the Microsoft store can be installed in S-Mode. This might be a hint that new rules for normal executable are coming.

Microsoft is evolving with encrypted certificates as are web browsers. If you ever try powering up a old PC you may find it can no longer browse the web because it uses an older encryption method and most websites are now the newest https. Asymmetric encryption technology can be used to send encrypted data to anyone you have not previously made secure contact with. It is finding use in a large variety of applications. One big use, that would not otherwise be possible, is cryptocurrency.

We are sorry for the inconvenience to customers who were trying to use our products during this adventure (nightmare). Many customers were able to use the above workaround and others returned product out of fear of damaging their system. We are now back to normal and everyone should be able to install our drivers.

CBA V

Computerized Battery Analyzer

- Improved cooling system allowing higher continuous loads for testing
- New remote voltage sensing for higher accuracy
- Fuse blown LED and easy to change fuses
- More detailed LED status indication

RIGblaster DXpro

A RIGblaster is the easiest way to properly connect your radio to a computer so that you may operate using over 100 existing and future ham radio sound card software programs. You will be able to operate any sound-card based digital mode that your radio could not otherwise operate.

WE WANT TO HEAR FROM YOU!

If you would like to submit an article for consideration in future newsletters please contact marketing@westmountainradio.com

Bulletin Board

Visit Our Booth!

MRC Swapfest
November 6

Fort Wayne Hamfest
November 13 - 14

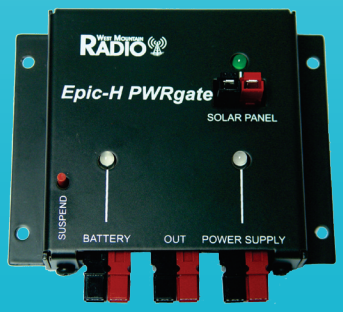
Due to COVID-19, production has been delayed. West Mountain Radio encourages all the hams to keep communication going through these hard times over radio! Stay healthy!

Epic PWRgate

DC Power Management Device
12V Backup Power System

Features:

- USB Port Access to Monitor system
- Program for specific battery types
- Supports either Lead Acid or Li-Ion Battery Charging
- Optional direct solar panel input for MPPT battery charging



Horizonal Version Available

Interested in microcontrollers?
Click here for more info:
www.westmountainradio.com/pic_resources

Want to Learn C programming for microcontrollers?
Click here for details of a NEW book that includes a FREE C compiler:
www.ccsinfo.com/e3book

West Mountain Radio
1020 Spring City Dr. Waukesha, WI 53186
www.westmountainradio.com

WEST MOUNTAIN RADIO

Follow Us!