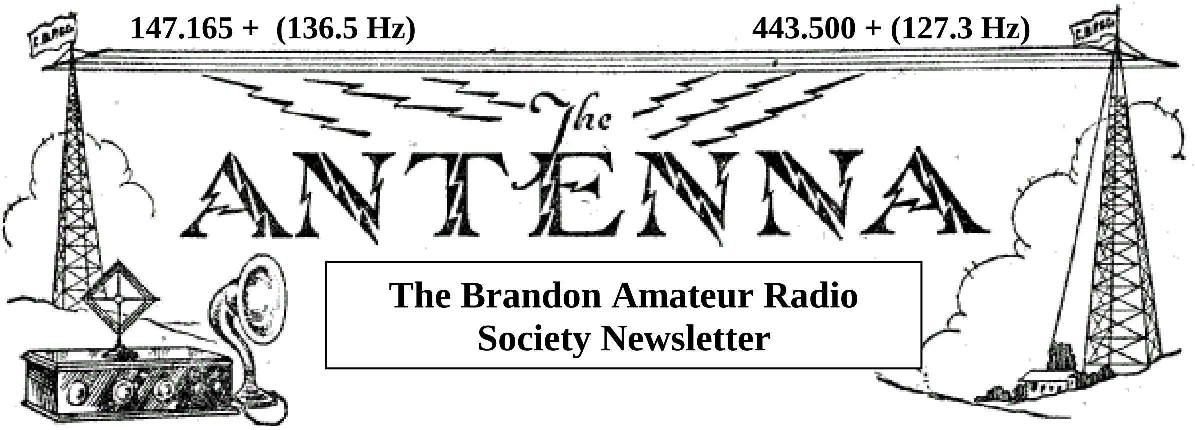
147.165 + (136.5 Hz) 443.500 + (127.3 Hz)



The ANTENNA

The Brandon Amateur Radio
Society Newsletter

OVER 39 YEARS OF PUBLIC SERVICE TO THE BRANDON AREA
BRANDON, FLORIDA, USA
VOL XLIII, NUMBER 11 NOVEMBER 2016

Come to the Club Meeting Thursday November 17th

Our meeting this month is in the Large Modular at Brandon Assembly of God 710 South Kings Avenue in the Annex. There is another activity scheduled for the Annex. Things get underway at 7:30 p.m. when Doris WB9VDT bangs the gavel to start things off.

-30-

November Program: Schematic Program Editor

The program is a video describing and demonstrating a schematic editor and circuit emulator called Micro-Cap Version 11. This program runs on Windows and there is a free evaluation version that can be downloaded via the internet. After entering a schematic using a graphic editor with a selection of standard components one can select several analytical tools to show the 1. Transient (or time) behavior, the AC or swept frequency response, or 3. the DC operating points of the circuit. This is a great tool if you're building a DIY project to help you understand and perhaps modify a circuit to solve a Ham Radio problem.

-30-

SKYWARN Recognition Day 2016

Friday 2 December 6 to 10 pm and Saturday 3 December 9am to 5 pm

Richard Rude KE4EXL

The Tampa Bay National Weather Service office in Ruskin will be participating in SKYWARN Recognition Day this year. We will be operating Friday evening, December 2nd and again during Saturday December 3rd

SKYWARN Recognition Day was developed in 1999 by the National Weather Service and the American Radio Relay League to celebrate the contributions that volunteer SKYWARN radio operators make to the NWS mission, the protection of life and property. During the event SKYWARN operators visit NWS office and contact other stations across the nation and world.

All amateur radio operators are invited to drop in and help us made contact with as many other stations as possible. If you have any question please contact Rudy/KE4EXL at richard.rude@noaa.gov or 813 645-2323 X329.
Links with additional information: http://hamradio.noaa.gov. http://www.weather.gov/tbw/wx4tor http://www.arrl.org/skywarn-recognition-day
Our address:
National Weather Service Tampa Bay Area, FL 2525 14th Ave. SE Ruskin, FL 33570 (813) 645-2323

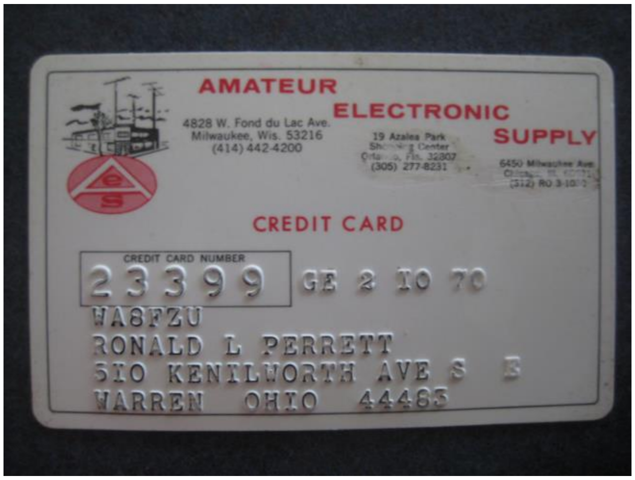
-30-

Credit Card Technology

Ron Perrett K4FZU

According to one industry forecast, online transaction fraud is expected to double over the next three years. Here is some information to aid you in being better informed about the technology in play, and NOT becoming a victim. Let’s drop back a bit and take a look at the background to credit card technology. Initially we had the “charge card” which was credit at local vendor (on-account at the store). The next evolution was the credit card at the store or at that chain of stores with a numbered account. With the growth of electronic banking the local, store specific card gave way to a general use card with a magnetic stripe. We will go into detail on that later. The newest developments are cards with radio frequency identification (RFID) technology and credit cards with EMV (Europay, Mastercard, and Visa) technology. Let’s look at all of these in detail.

Magnetic Stripe:



Magnetic strips on credit cards have 3 data tracks.
- Track one and track three usually contain 210 bits per inch
- Track two contains about 75 bits per inch

Data stored on these magnetic stripes are often unencrypted and data in plain text format is easily read and counterfeited by skimming devices

Some Nice-to-know: The process of attaching the magstripe to the plastic card was invented by IBM in 1960 under a contract with the US government for a security system. Forrest Parry, an IBM engineer, had the idea of securing a piece of magnetic tape to a plastic card. Jerome Svigals was the IBM worker to invented the process steps that were used to successfully attach the strip - circa 1966 to 1975.

Enter RFID: RFID technology came to life around 1970. At first RFIDs were created to track cows, railroad cars, and airline luggage. The original tags were called Inductively Coupled RFID Tags and were systems of metal coils, antennas, and glass. Capacitively coupled "tags" were invented next to try and lower technology cost. They were supposed to be disposable tags that could be applied to less expensive merchandise. They also used conductive carbon ink instead of metal coils to transmit data. The conductive ink was printed on paper labels. These RFIDs only stored up to 96 bits of information. Today's RFIds are known as active, semi-active and passive RFID tags. They can hold up to 2 kilobytes of information and are made of a microchip, antenna, and sometimes a battery.

RFID type Credit Cards: When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna's transmitter. That "wakes up" the RFID chip, and it transmits the information on its microchip, to be picked up by the scanning antenna and receiver. Think mostly passive devices here, where the chip must pick up enough signal to power the tag device. Presto, no more kur-chunking credit card carbonless paper machines or time consuming clerk-written transaction processing. Another practical application of this technology might be an anti-theft sensor, at entrance/exit doors of a business - Hidden or embedded security tag devices ring their data at a prescribed frequency, alerting everyone as an nonpaying customer passes between the antenna structures. For credit cards, typical distance parameters may extend convenience to 24 inches. But, with specialized equipment this scenario could extend to much greater distances. Consider the possibility of an "Open-Road" trolling system that can pick up passing tags from many feet away. This exact concept is the heart of the I-Pass and EZ-Pass toll-road system.

More than just RFID... Enter the latest technology, "The EMV Chip":
EMV stands for the three companies that came up with the standard: Europay, MasterCard, and Visa. The claimed truth(?) "The computer chips in EMV cards don�t send out radio frequency signals at all." Well, say what? It's still a peer-to-peer communication structured environment. But, they don't call it "Radio" broadcasting, they call it contactless inductive coupling i.e.) Near Field Communication (NFC), as in physical separations of only up to 4 or 5 centimeters. NFC technology exists as four different types of "Tags", three different signaling technologies, and four modes of operation that engineered NFC compatible devices can undertake. Radio frequency, amplitude modulation, modified Miller and Manchester coding schemes all seems like radio to me.

You can get an NFC Technology Primer here:
http://arstechnica.com/gadgets/2011/02/near-field-communications-a-technology-primer/2/

Oh, and on your next drive up FL-Route-60 and a stealthy trip to the department store, include your HF rig and a battery in your back pack, (don't forget a nice large set of privacy headphones) and listen on 13.56 MHz. Wow, 20/S9 100 feet from the donut place. Then, many slightly beating signals come, peak, and go as you pass by several big-box stores. Finally to the parking lot - louder! Yikes, carriers from all directions - sounds like a DX pile-up down there on Isles #3-4-5. Such carrier-ings on, them "near fields" are "farther" than I thought! On second consideration, your Whip antenna and commando get-up would probably attract way too much unwanted attention.

The advertised security feature is that you can’t close a transaction with an EMV chip card unless you actually dip it into a card reader (Pun intended I think... as in Chip-n-dip). However... It’s true that some banks offering EMV cards, additionally equip these cards with contactless RFID technology as well.

Chip-n-pin vs. chip-n-signature Europe, and a growing number of other world areas, require you to insert your chip card and then additionally enter a verification PIN for security. Here in the U.S.A. it was decided to only require a verification signature - some vendors only ask for the signature above a certain transaction value. This processing difference, of course, causes much frustration for international travelers (no PIN) and denial of use, including blocked accounts. Oh, and a CAUTION: Spray Paint purchases may additionally require strip-search, blood sample, and finger printing as a deterrent to graffiti. "Maybe(!)" even a 3-day waiting period is legislatively being proposed, including an executive-order background check and painting license registration requirement. (sorry!)

Starting in October 2015, the liability for fraudulent credit card transactions shifted from the credit card issuer to whichever party (the credit card issuer or the merchant) is using the least secure technology. Gas stations and ATMs have until October of 2017 to become compliant. Just FYI: Chip equipped cards cost upwards of ~$3.50 to manufacture and deliver to a consumer. Oh, and for every signature-authorized transaction, vendors must pay Visa five cents more than it does on a PIN-authorized transaction.

PATIENCE:

WHAT YOU HAVE WHEN THERE ARE TOO MANY WITNESSES.

@ REBEL CIRCUS

A vendor's reader communicates with the chip inside your card using dynamically changing cryptographic algorithms, unique to each transaction, to authenticate the card. The benefit is that because the data is housed on the chip tag, it will be much harder for thieves to replicate than it was when it was stored on the magnetic stripe. The reader and networking interface use strong encryption, 128-bit, and Triple-DES (Data Encryption Standard), to protect information. When a transaction is initiated, the chip and the terminal work together to create a unique transaction session and to secure the data. The hope is that in the event that the data is illegally intercepted electronically, it will be almost impossible to decode in a timely or economically feasible way. i.e.) crooks are inherently lazy! So, what's 10 years among friends if you have a super computer?

There is, however, the underlying vulnerable to this new technology that can facilitate the stealing of your credit card information, without even touching you. Your card can be read surreptitiously. An unidentified technology-enabled crafty thief boldly claimed that many of the supposedly encrypted cards actually easily transmitted card numbers, expiration dates and cardholder names in plain text -- which could be read through the envelopes the cards were mailed in. i.e.) radio "Skimming"

in current versions of the cards, the user’s name, PIN and the three-digit CVV on the back of the card aren’t included in the data exchange. Now, along with the card’s 16-digit number and expiration date, the cards are set to offer up, via transaction processing, a one-time CVV code with every scan. Those codes are sequenced and tracked, so can only be used for one transaction. The merchant's reader utilizes "Near Field" technology (signals within one wavelength). You will also see the NFC term applied as a set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, and personal computers. Think it's top secret? think again. If you'd like to assume a developer's role, the NFC Forum affords you complete technical specifications.

http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/

Ah, but wait... Now even smartphone manufacturers, including Apple, Samsung, Nokia, Motorola, LG and HTC are releasing phones that are "NFC" enabled. Just "wave-n-pay". With a firmware modification and a free open source application that can easily be found on the internet, the average person can turn their NFC enabled smartphone into a credit card stealing machine and then use the smartphone as that stolen credit card. Well assuming they have the where-with-all to program and implement a functional app.

Personal protection (electronic) - Guard Bunny by Paget's: RF shielding card sleeve, senses an RF signal attempt and beeps, as well as lights-up Mr. Bunny's eyes, then reflects back the signal it received, with its own chip structure - intending to jam the offending reader's attempt. Cute!

Oh, and did I mention that the New Passport structures incorporate this technology too? Well, now that you know, ya'll be careful out there!

-30-

That wraps it up for this month. Have FUN with radio!
After all, if it is not FUN, why do it?

Keep in Mind Our Weekly Nets and Bulletins

Monday 8 p.m. The Two Meter Net 147.765 - 147.165 MHz Hosted by Doris Haskell WB9VDT

Tuesday 7 p.m. 6-meter Roundtable 50.200 MHz USB followed at 8 p.m. with the 10 Meter Roundtable 28.365 MHz USB

Send us your articles AND PICTURES! We do much more in the digital format! I would like to have pictures of BARS members and their ham shacks!

Remember to check out the BARS website:
brandonhamradio.org