CITIZEN'S DISPATCH

GOLDEN TRIANGLE TRI AGENCY CPAAA

This months guest speaker

CHARLES TEEL , MBA

SR2 SOLUTIONS

CYBER SECURITY

NEXT MEETING
OCTOBER 17TH
7;00 PM

VOLUME 7 ISSUE 10

POINTS OF INTEREST

WHAT IS CYBER SECURITY

COPS AND KIDS

LT KY BROWN FUNDRAISER

ITS ALMOST TIME FOR COPS N KIDS

COPS AND KIDS

SATURDAY OCTOBER 28TH 2017

BEAUMONT CIVIC CENTER

Computer security

Computer security, also known as **cyber security** or **IT security**, is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.[1]

Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection.[2] Also, due to malpractice by operators, whether intentional, accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods.[3]

The field is of growing importance due to the increasing reliance on computer systems and the Internet,[4] wireless networks such as Bluetooth and Wi-Fi, and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things.

Vulnerabilities and attacks

A vulnerability is a weakness in design, implementation, operation or internal control. As they are discovered many vulnerabilities are documented in the Common Vulnerabilities and Exposures (CVE) database.

An *exploitable* vulnerability is one for which at least one working attack or "exploit" exists.[5] Vulnerabilities are often hunted or exploited with the aid of automated tools.

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

Backdoor

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.[6] Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding

Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice.[7] Even when the system is protected by standard security measures, these may be able to be by-passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

Spoofing

Spoofing is the act of masquerading as a valid entity through falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain[8][9]. This can be done in tandem with phishing, and can lead to privilege escalation. There are several types of spoofing, including but not limited to:

- Email spoofing, where an attacker forges the sending (*From*, or source) address of an email.
- IP address spoofing, where an attacker alters the source or destination IP address contained within a network packet.
- MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of a network interface over which they have control to pose as a valid user on a network.
- Biometric spoofing, where an attacker produces a biometric sample that matches to a user other than himself or herself.[10]

Tampering

Tampering describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers[11] are examples.

a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points — and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users.[12] Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trust, phishing can be classified as a form of social engineering.

Clickjacking

Clickjacking, also known as "UI redress attack" or "User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

Social engineering

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.[13]

A common scam involves fake CEO emails sent to accounting and finance departments. In early 2016, the FBI reported that the scam has cost US businesses more than $2bn in about two years.[14]

In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.[15]
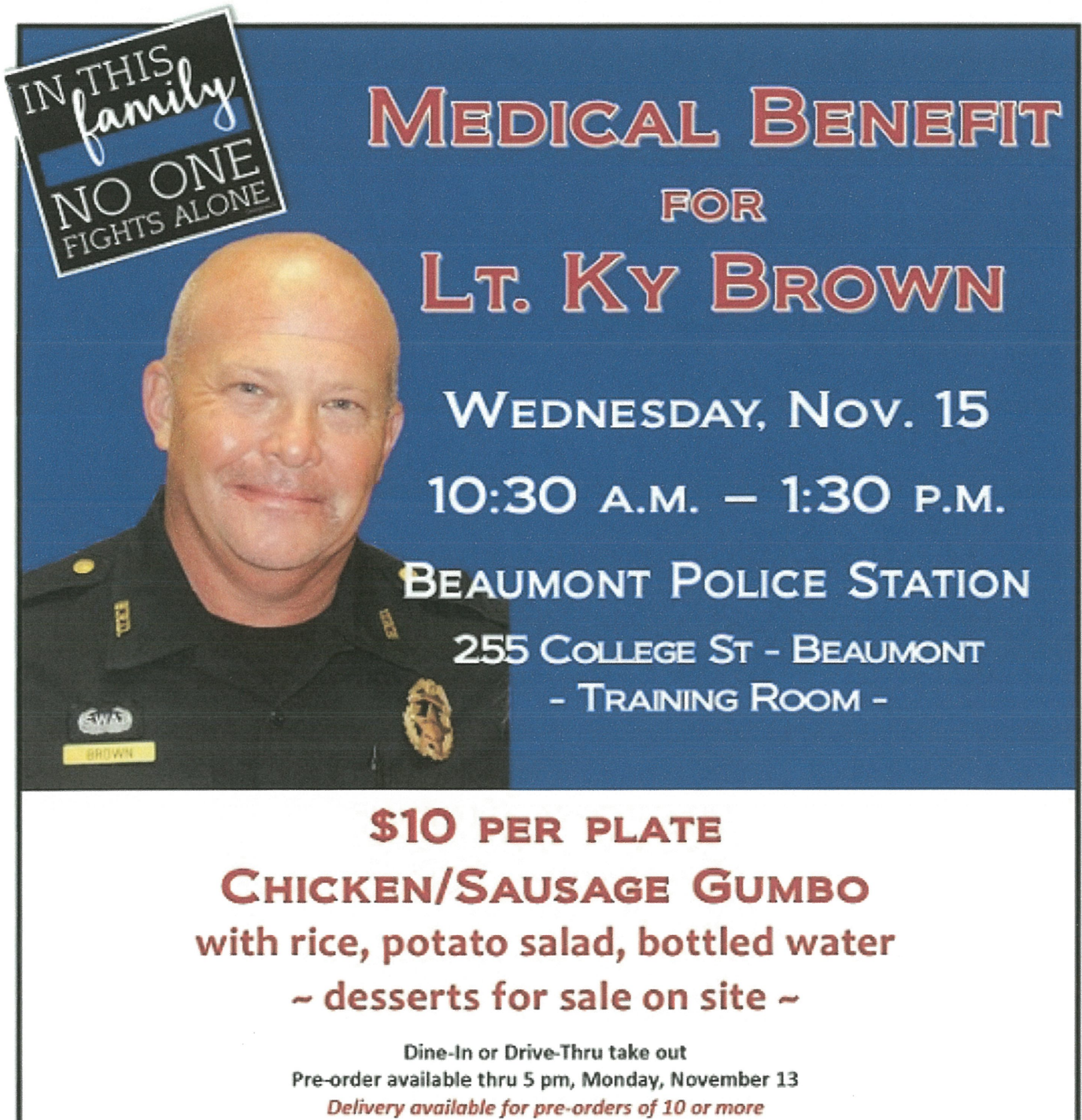
Information security culture

Lieutenant Ky Brown has been a hero and a friend to many through his profession and in his personal life.

He's been there for us - let's be there for him...because in this family **NO ONE FIGHTS ALONE!**

Mark your calendars now!

MEDICAL BENEFIT
FOR
LT. KY BROWN

WEDNESDAY, NOV. 15

10:30 A.M. – 1:30 P.M.

BEAUMONT POLICE STATION

255 COLLEGE ST - BEAUMONT
- TRAINING ROOM -

$10 PER PLATE
CHICKEN/SAUSAGE GUMBO
with rice, potato salad, bottled water
~ desserts for sale on site ~

Dine-In or Drive-Thru take out
Pre-order available thru 5 pm, Monday, November 13
Delivery available for pre-orders of 10 or more

2017 OFFICERS

President
Roy McGrath

roymcgrath@sbcglobal.net

Vice Pres.
John Theriot

Vice Pres.
Rita Foster

Treasurer
Sheri Baden

Secretary
Gayle Hollar

PRESIDENTS MESSAGE

WELL HERE WE ARE AND ITS ALREADY OCTOBER

AS YOU KNOW BY NOW COPS N KIDS HAS BEEN COMBINED WITH TRUNK OR TREAT THIS YEAR .ITS OCTOBER 28TH AT THE CIVIC CENTER IN BEAUMONT . MOST OF US ALREADY SIGNED UP AT THE AUGUST MEETING , BUT WE WILL HAVE A NEW SIGN UP SHEET AT THIS MONTHS MEETING SO IT CAN BE UPDATED .

THE UNIFORM OF THE DAY WILL BE THE GOLD CPAAA T-SHIRTS

SOME UNIFORM CIA WILL BE NEEDED AS WELL

THERE WILL BE A LOST KIDS BOOTH AS WELL AS A LOST AND FOUND AND SOME CIA WILL BE POSTED AT THE EXITS

IT IS ELECTION TIME FOR 2108 CPAAA OFFICERS

THE FIRST ORDER OF BUISINESS WILL BE TO CONDUCT THE ELECTION. WE WILL OPEN THE FLOOR FOR AND ADDITIONAL NOMINATIONS , AND THEN A PRINTED BALLOTT WILL BE PASSED OUT TO THE MEMBERSHIP .RONNIE DILLON WILL BE IN CHARGE OF THE ELECTION AGAIN THIS YEAR .

DONT FORGET TO PROMOTE OUR 2017 RAFFLE

THERE ARE SOME REALLY GOOD ITEMS THIS YEAR

I UNDERSTAND THAT ALL OF US WERE AFFECTED BY THE RECENT STORM IN ONE WAY OR ANOTHER

RAFFLE TICKET PROCEEDS GO TO FUND SCHOLARSHIPS

THEY WILL PAY DIVIDENDS IN THE FUTURE BY ALLOWING SOMEONE WHO MAYBE WOULD NOT HAVE BEEN ABLE TO GO TO ATTEND THE REGIONAL POLICE ACADEMY AND THAT BENEFITS US ALL

PLEASE KEEP ALL OF OUR OFFICERS AND THEIR FAMILIES AND MEMBERS OF OUR GROUP THAT WERE IMPACTED BY THE STORM IN YOUR THOUGHTS AND PRAYERS

SEE YOU AT THE MEETING

ROY MC GRATH

PRESIDENT CPAAA

Sent from my Verizon, Samsung Galaxy smartphone

TRI-AGENCY CITIZENS POLICE ALUMNI ASSOCIATION RAFFLE

2017

- *1ST place: 4 Southwest Airline Tickets $800.00*
- *2nd place: Smith & Weston AR 15 $600.00*
- *3rd place: Overnight and dinner for two @ Isle of Capri $300.00*
- *4th place: Overnight and dinner for two @ Delta Downs $300.00*
- *Donation: $5.00 ticket or 5 for $20.00*
- *Starts Aug 15, 2017 and ends Dec. 16, 2017*
- *Drawing to be held December 19, 2017*
- *Winners need not be present to win*
- *Winner will go through Mark Godley FFL to pick up*

FOR TICKETS CALL

Roy M - 659-2870

John T – 720-7931

Ronnie D – 790-1616

We use the funds to help pay for a student scholarship attending LIT Lamar Police Academy, we are a 501 (c) (3) club.

Auction items

- 4 Southwest Airlines Tickets $800.00
- Harley Speakers Audio Edge $399.00
- 12 Refills Propane Coastal Welding $168.00
- Drone $100.00

Give away

- 5 free Oil Change $100.00

- Hunter Knife set $100.00
- 2 TexJoy Coffee gift Sets $60.00
- Coushatta Overnight stay

2017 list of new Sponsors

- **Southwest Airlines**
- **Delta Downs Casino**
- **Isle of Capri Casino**
- **Coushatta Casino**
- **Ritter Lumber**
- **Coastal Welding**
- **Firestone Auto**
- **Audio Edge**
- **TexJoy Coffee**