Issue # 9 Volume #15 September 2014

AaSys Solutions

Solutions are our Business

Can You Get Hacked 30,000 Feet in the Air?

For majority of people, traveling by air, whether for business or leisure, has become the norm. Many spend hours in airports or on planes. In 2013, Atlanta's Hartfield International Airport reported over 94.4 million passengers flew into or out of their airport. Traveling has become more convenient by having access to Wi-Fi. You can be connected anywhere, anytime, even at 30,000 feet in the air. But new findings show being connected while flying may be riskier than we think. The possibility of being hacked at 30,000 feet in the air has many taking a good look at the situation.

Wi-Fi security on planes has been a major concern since 2001. In 2010, the Atlanta Journal-Constitution out of Atlanta, GA claimed allowing passengers to have internet access would be like opening a Pandora's Box. Fast forward four years, and here we are again with new security concerns. Ruben Santamaria, one of the most respected cyber security researchers, found a loop hole and has figured out how to hack the satellite communications equipment on airlines through their Wi-Fi and inflight entertainment systems. The researcher said he discovered the vulnerabilities by 'reverse engineering' - or decoding - highly specialized software known as firmware, used to operate communications equipment. In theory, a hacker could use a plane's onboard Wi-Fi signal or inflight entertainment system to hack into its avionics equipment, potentially disrupting or modifying satellite communications. This could interfere with the aircraft's navigation and safety systems, Santamaria said. He has made it clear his findings were tested in a very controlled environment, but Santamaria also stated that it may not be difficult to replicate his findings in a real situation. Santamaria wants manufacturers to take a really good look at the vulnerabilities he found and to fix the issues. Aviation experts like Marisa Garcia has debunked Santamaria's findings, advising that hacking into an airplane's Wi-Fi is "virtually impossible." She states that airplanes are not networked like computers and confirms that as digital usage slowly enters the skies, it has done so with only the highest scrutiny to ensure safety.

So can you get hacked 30,000 feet in the air? Some will argue yes and others will argue it's impossible. But one thing is for sure; as we see how technology has grown in online banking, smart phones and even the newer model cars, security always remains a top priority. Until Santamaria's research can be proved, you can go back to worrying about whether you got a window or an aisle seat. If he's correct, though, there would need to be a serious investigation into the safety of these satellite systems.

Source: Fickle, Jim "Hackers says to show passenger jets at risk of cyber attacks" August 4, 2014 http://www.reuters.com/article/2014/08/04/us-cybersecurity-hackers-airplanes-idUSKBN0G40WQ20140804

Are there subjects that you would like to have covered in future newsletters? We are always looking for topics of interest and we welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please send an email to newsletter@aasysgroup.com

11301 N. US Highway 301,
Suite 106
Thonotosassa, FL 33592
(800) 799-8699
www.aasysgroup.com

Inside this issue:

Do You Know Where Your Data Is and Is It Safe??

The highest level of scrutiny has been placed on financial intuitions to ensure their data is safe and that their customers and organizations are protected. But this task has proved to be more difficult to put into action than in theory. Many banks have implemented the “big data” mentality and have used it to assist with anticipation and planning of real time events. This tactic is great, but the banking infrastructure has always been a complex entity and as the landscape for technology changes so quickly, it makes it hard to stay one step ahead. ***So the question is: do you know where your data is and is it safe?*** That is the challenge not only for banks but for all businesses. Many experts believe data centralization is the name of the game. Although there have been sceptics that disagree and believe that housing all information in one location is literally Disney World for hackers, it has gained enormous support throughout the IT community.

Here is how the experts explain their thinking. They believe that by breaking down the mine of fixed data that an organization does not regularly use in its day-to-day operation and then centralizing the data, it is more likely to increase visibility across an organization, thus allowing it to stay in a real time environment. This has shown to be beneficial when making long and short term business decisions. Centralizing the data also allows an organization to view data coming in and out that can be regulated by device, user and location. What is equally important as having all data in one location is also having the information encrypted.

Encryption has been an indispensable tool in technology and many are calling for the federal government to step in and make it mandatory to use encryption for all organizations that have any digital information. Some believe that is a bit extreme and heavy handed, but with many recent security attacks on large companies, it seems to now be a necessity. Failure to inadequately encrypt sensitive information can lead not only to hacker’s infiltrating the data, but also to regulators publicly bringing down the hammer on those who find themselves in a security breach kerfuffle.

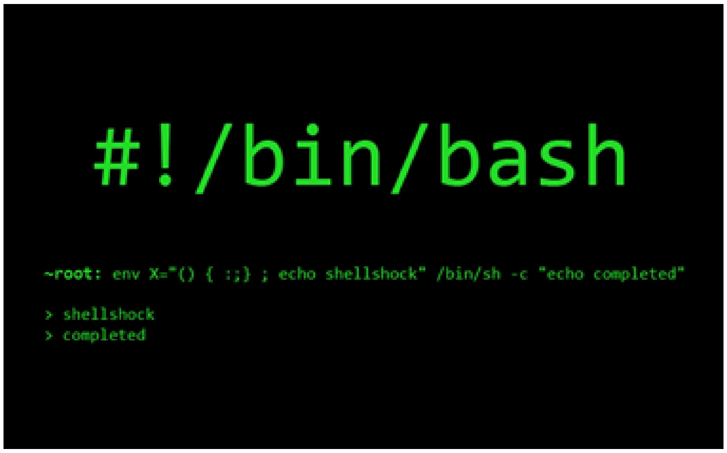
The public is also becoming more tech savvy and paying close attention to how financial intuitions and other companies handle the data they store. And with social media, it makes it very convenient for dissatisfied customers to voice their concerns and request change with 140 characters or less.

The good news is there are several resources and software programs that fit the need of every budget and size company. And there are new ways to keep the data encrypted while it is in use allowing the information to never be decrypted on the server and remaining in the hands of the owner of the data.

Having complete control of data is crucially important, especially to those in the financial sector who have compliance and regulations they must observe. Most consumers don’t understand the logistics or technical terms about storing or encrypting data. What they want to know is that their information is safe. So coming up with the best plan for storing data and ensuring it is secure should always be top of the priority list.

In the News: New Bug May Pose Bigger Risk Than “Heartbleed”

On September 24th, The Department of Homeland Security's United States Computer Emergency Readiness Team, issued an alert warning that there is a new vulnerability in Linux software known as “Bash.” **The bug is affecting Unix-based operating systems, including Linux and Apple Ink's <AAPL.O> Mac OS Xexperts**.” Experts believe this bug could be worse than “HeartBleed.” Unlike “Heartbleed,” this new bug actually allows the perpetrator to gain control of the victim’s computer, allowing them access to confidential information and the ability to make changes. Officials are rating this bug at a 10 (high risk) and are asking anyone who uses “Bash” to deploy patches **immediately.** All though Microsoft Windows will not be directly impacted by this bug there will be other network equipment that could be affected. AaSys will continue to monitor this vulnerability and notify its clients as more information becomes available.



```
#!/bin/bash

~root: env X="() { :;} ; echo shellshock" /bin/sh -c "echo completed"

> shellshock
> completed
```

Fall is in the Air

The first day of fall was on September 22. For many who don’t have the luxury of living in the warmer parts of the United States, Fall symbolizes the coming of a cold winter. But here is a little science trivia for you. This year the Autumnal Equinox occurred on September 22 which means the sun crosses the celestial equator – the imaginary line in the sky above the Earth’s equator – from north to south. This happens either on September 22, 23, or 24 every year. It’s one of only two days in the year when day and night are of equal length!