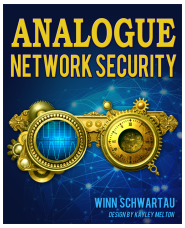

Winn Schwartau
545 Westport Dr.
Old Hickory, TN 37138
+1.727.393.6600
Winn@TheSecurityAwarenessCompany.Com
www.WinnSchwartau.com

17 May 2015

FLY – S.A.F.E.

Security for AirFrame Entertainment

STOP Inflight Entertainment in the interest of Public Safety

I and many of my security professional colleagues are not so sure that it's safe to fly anymore. I know I cannot, without any level of confidence, say whether inflight onboard networks are secure, or whether they present a clear and present danger to the flying public.

I am saying, let's take a pause.

In light of the myriad cyber-security questions about the differing current implementations of onboard entertainment on commercial aircraft, I ask that, in the name of Passenger Safety First, airlines voluntarily shut off their aircraft WiFi and entertainment systems until proper open-source security reviews can establish their safety for the flying public. The evolution of Passenger Comfort and Profit via onboard electronic systems raises questions about the potential for miscreant and cyber-terrorist actions.

Defensive protestations about *'no known vulnerabilities'* invokes a level of arrogance that cyber-history has proven to be profoundly wrong and a guaranteed recipe for Failure. Political and profit-driven hubris must not be permitted to dominate while thousands of planes hurtle millions of passengers around the world at 530mph.

I do not question the need for inflight distraction or the profit incentive of for-pay entertainment. I, for myself, read a book. I merely believe that it is incumbent upon the cyber-security industry in association with appropriate air-industry legislative and regulatory bodies to create and enforce tougher criteria for onboard commercial aircraft networks, where the cost of failure is unacceptable. The vendors cannot and should not self-certify any cyber-security criteria for commercial aircraft. There is just too much room for self-serving agendas.

My thoughts:

1. Shut down all inflight entertainment and WiFi capabilities immediately until proper open-source evaluations are conducted. Yes, that means turning off Skype, Facebook, eMail and streaming in the air while a secure workable method is designed.
    a. Stringent security guidelines and minimum specifications are necessary for the Public Safety.
    b. Security by obscurity will not be tolerated. It has been suggested that onboard systems cannot be disclosed for security reasons. There are only two possible concerns here.

        i. The entertainment and avionics systems are in fact connected, and fear of flaw and exposure hinders open source security efforts.
        ii. The entertainment/internet system is indeed isolated, but for fear of loss of profits, refuses to discuss security controls.
        iii. Either approach, when it comes to Public Safety First is unacceptable. Security controls should be a Public Relation Benefit. A plus. A big positive. These guys have a lot to learn.
2. Avionics, airplane communications and other onboard systems must be isolated from any customer or internet facing services.
    a. Public networks may not be physically connected nor connected by any wireless means to any other onboard aircraft navigation or control systems.
    b. Separate physical wiring shall be used for each system
    c. Air-to-ground communications and those from the aircraft to public systems shall be electronically isolated from aircraft communications, via separate channels and through acceptable cryptographic isolation where physical isolation is not possible.
    d. Both solutions will be subject to the same level of assurance verification.
3. Validation of the cyber-security of onboard systems shall be performed on a periodic basis, and prior to any onboard upgrades of either public or internal systems.
    a. At least two third parties, non-affiliated with any aircraft manufacturing concerns, will 'red-team' a benign environment, fully functional aircraft, to assess vulnerabilities prior to deployment.
    b. Aircraft manufacturers and their suppliers will be required to 'open source' their security protocols, for peer review, just as cryptographic algorithms do.
    c. All systems should be subject to a Common Criteria evaluation and certification, in addition to Red Teaming, for each revision and deployment.
4. Reporting of any aircraft network system vulnerability shall not be considered a crime, until specific intent of harm is implicit.
5. We will aggressively attempt to assemble the Pen Teams to verify the security of targeted aircraft and systems.
    a. All activities will be documented
    b. All activities will be made public
    c. Aircraft suppliers will cooperate in any way requested in the interest of public safety.

I believe I have the moral imperative, and offer an effective zero-cost method to solve a problem and restore public confidence before it becomes deadly. Would someone give me the mathematics of human life for the bullshit mantra, "It hasn't happened yet, so why should I worry?"

Been there. Done that. We know that doesn't work.

With aircraft, 'hacking' the electronics is only one vector of concern. In the mid-1990s, long discussions were held about the influence of EMI, accidental or incidental electromagnetic interference caused by portable electronics on the plane's electronic integrity. Today, we are permitted to use certain devices throughout a flight. EMI breeds the potential for intentional electronic disruption of flight systems through the intentional introduction of EMI using a variety of high power discharge technologies.

Additionally, an open source investigation into the security of GPS and communications systems, using a Red Team approach is in the best interest of the flying public, and should occur in tandem with the onboard systems security review. While these two vectors may be of low probability, any discussion about cyber-security and air safety belongs in the public view.

Please get this or a similar message of your preference to:

- The FAA http://www.faa.gov/contact/
- The NTSB http://app.ntsb.gov/pubmail/pubmail.aspx
- Your Airline(s)
- Facebook/LinkedIn
- Your Congresspeople http://www.contactingthecongress.org/
- Air Safety Groups
- http://en.wikipedia.org/wiki/List_of_civil_aviation_authorities
- http://en.wikipedia.org/wiki/List_of_airlines

Please spend 1 hour in the next week making some noise. I really don't want to see the headlines.

Let me know your thoughts!

Winn Schwartau
CEO, The Security Awareness Company