Comments on “An Initial Security Analysis of the IEEE 802.1X Standard” [Professor William Arbaugh and Arunesh Mishra, University of Maryland; http://www.cs.umd.edu/~waa/1x.pdf]

Since the advent of 802.11 wireless connectivity, several serious attacks have been discovered against the security of such systems. This is not one of them.

The previously discovered attacks have been against the WEP encryption used between the user’s mobile station and an access point. This paper, on the other hand, concerns itself with the 802.1X security standard for authentication between mobile station and access point.

The 802.1X standard describes how the EAP authentication protocol is used to authenticate the user via a RADIUS authentication backend. EAP traffic flows between the user’s machine and the RADIUS server, with the access point as conduit. Once authentication is successful, the RADIUS server informs the access point, which then bridges the user onto the network.

This paper basically boils down to the following points:

1. 802.1X is an asymmetric protocol, allowing the network to authenticate the user, but not allowing the user to authenticate the network. Therefore, an attacker can easily fool the mobile station into connecting with it rather than with a legitimate access point. The attacker can then play “man-in-the-middle”, passing data between the mobile station and the legitimate access point, and eavesdropping all the while.

2. Because the low-level signaling between access point and mobile station is not secured, an attacker can pose as the access point to the mobile station, and pose as the mobile station to the access point. First, it fakes a packet to the mobile station as if it came from the access point, telling the mobile station to “disassociate”, or drop its connection. Then, the attacker “hijacks” that connection, using the mobile station’s MAC address to fool the access point into exchanging data with it.

3. There are a variety of denial of service attacks, described in the paper’s appendix, that can cause legitimate connections to suddenly disconnect, and that can swamp network equipment to the point at which providing service becomes difficult.

Response to point 1

Yes, 802.1X was conceived of as asymmetric, but there are a number of protocols that are now being used or about to be used that change all of that. EAP-TLS, EAP-TTLS, and EAP-PEAP are examples of such protocols. These provide for strong mutual authentication between mobile station and access point.
And, most importantly, they result in master keys on both station and access point for encrypting data between the two. The master keys are intimately bound to the authentication that preceded them. This eliminates the man-in-the-middle threat. Because the attacker was not authenticated to either party, it has no master key and can't get one. Therefore, even if it were able to pass data between mobile station and access point, it would not be able to decipher that data.

The authors are dismissive of the new EAP mutual authentication protocols, stating that the 802.1X state machines call for an “EAP-Success” message to immediately throw the mobile station into a connected state. This is a bit disingenuous. Yes, if authentication were one-way, that’s what you’d do. But when authentication is mutual, it’s quite obvious that a mobile station should condition its opening of the connection on a satisfactory authentication. This is but a nit in the spec, not an architectural problem.

Response to point 2

When strong mutual authentication is used with master keys bound to that authentication, the attack that is described is not possible. Yes, the attacker could forge a “disassociate” packet to disconnect the mobile station, but it could not hijack its connection. To hijack the connection it would need the correct master keys; to get those it would need to have been authenticated.

Response to point 3

We agree with the authors that denial of service attacks are quite possible. In fact, denial of service attacks are quite feasible in many areas of networking.

In a denial of service attack, the attacker uses techniques like forged packets or large quantities of packets to interrupt the normal workings of the network.

But denial of service attacks don’t make people not want to network. Why? Because, first, they don’t compromise sensitive information. Second, because you know when it’s happening and can take countermeasures (unlike a successful eavesdropping attack which could go on for years without anyone knowing). Third – in the case of 802.11b – because the area of coverage of an access point is small enough that an attacker would have a substantial risk of discovery.

Conclusion

The authors really provide no new insight into wireless LAN authentication issues. Indeed, the issues they bring up are exactly the ones that have been understood for months and have motivated work on the EAP mutual authentication protocols that are now coming to market. Using such protocols, the security attacks described by the authors are not possible.