PAYWALL - SYMPTOMS OF A BADLY IMPLEMENTED SYSTEM

Lets first get some things out the way, for starters a paywall is defined as;

> *"A feature of a website that only allows access to certain pages or data to paid up subscribers"*

And secondly I am not saying all of these systems are poorly implemented, but the one I am going to talk about was. You see I was traveling recently, and like most geeks, I miss my connectivity when I do not have it. Now this hotel was supposed to have free wifi, but it turns out that there was a usage fee of a non-trivial amount per day. Now the hotel and myself managed to realign our expectations and sort things out, but it still left me feeling peeved. So I indulged in some thought experiments, what if I did not want to pay?

First thing I did was take a look at how the system is supposed to work. It was a unsecured wifi network, and when you tried to browse somewhere, up popped the page to pay. Simple enough, so lets see what it is looking for? I took a look at the source code of the pages and saw it was looking for a cookie of some type. Boy, how secure. So while I am thinking about things I hit the refresh button on my browser a couple of times, and what do I see happen? The page errors out... badly. It prints out the source code of all the background code and javascript - without me doing anything fancy. Interesting...

Ok, so I figure I could forge a cookie and happily browse away, but me being me, I wondered if there was an easier way? Hmmm...

So lets connect to the wireless and fire up yea-old wireshark. Let it run while I get some coffee and then lets take a look. First thing I see is other peoples traffic. Not just broadcast traffic but actual point to point ip traffic - like web traffic. So I can see what people are browsing and getting without any authentication. Boy, I just feel more and more secure. But ignoring all that, lets see if my ideas about the cookie authentication is valid, maybe it is easier to just grab one out of the air?

So I sit a bit and watch traffic scroll by, just regular fun right? I see someone hit the paywall, bingo. So I go looking for the cookie. But wait... What is this? I see this same client now browsing the web, but as they change websites, the authentication mechanism is not rechecked? Can it be? After much watching and looking, I deduced that the cookie is only checked if you send no traffic for a long time (upwards of an hour seemed to be the magic time), but as long as you had traffic flowing, the cookie was never checked. The only time this check is forced is each day at midnight, obviously to stop those people who only paid for a day's access.

So lets recap;

- the authentication mechanism is a cookie
- this cookie is only checked after longs periods of inactivity or at end of day
- the medium of connection wireless
- the wireless is unsecured
- any wireless client seems able to see any traffic

So here we sit, what is the easiest way to browse the web without paying? I figured spoofing the cookie? possible. Grabbing someone else's cookie? possible. But I reckon the easier way is to just be the someone else. You wait for someone to connect to paywall and get access. Once you see them browsing, grab their mac address, change yours to that, dhcp request and away you should go. And just to keep "alive" do a constant ping to somewhere so the cookie is never checked. Rinse and repeat daily.

Way to show off my mad leet skillz hey? Yeah right. Nothing here required technical magic or private exploits or such like. It just required the hotel to fail badly with their systems and someone to look at the traffic. Simple really. Anyone could do this. But me working through being peeved besides, what can we draw from this?

- Do I think this "secure" implementation is unique? No.

- Do you think the other people -business people- staying at this hotel knew anyone could access their traffic and it's contents? No.
- Do you think they would be happy if that happened? I wold like to think not.
- Do you know other attacks which could have been fun? Why yes, my own dhcp server using my dns, metasploit main in the middle, that would be fun.
- Do you know of other attacks? Yes.
- Do you think the hotel cared? No.
- Do I think some simple things would have helped? Yes. Using encryption, using a switch, using automated vlanning, many things.

I wish businesses would care about putting in secure systems, if for no other reason but to respect their clients. But this is the reality we face, the lowest bid, with the most ceo-relatives and the most CYA factor, that is what wins. I wish it was different. In the film '*Armageddon*', the characters are sitting in a space shuttle waiting to take off, and Rockhound says;

"You know we're sitting on four million pounds of fuel, one nuclear weapon and a thing that has 270,000 moving parts built by the lowest bidder. Makes you feel good, doesn't it? "

Sometimes I feel like that.