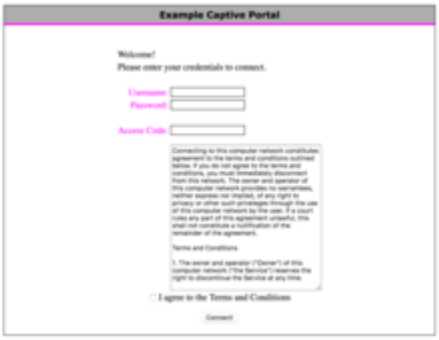
WIKIPEDIA

Captive portal

A **captive portal** is a web page which is displyed to newly connected users before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of EULA/accepted use policies, or other valid credentials that both the host and user agree to adhere by. Captive portals are used for a broad range of mobile and pedestrian broadband services - including cable and commercially provided Wi-Fi and home hotspots. A captive portal can also be used to provide access to enterprise or residential wired networks, such as apartment houses, hotel rooms, and business centers.



Welcome!
Please enter your credentials to connect.

Connecting to this computer network constitutes agreement to the terms and conditions outlined below. If you do not agree to the terms and conditions, you must immediately disconnect from this network. The owner and operator of this computer network provides no warranties, neither express nor implied, of any right to privacy or other such privileges through the use of this computer network by the user. If a court rules any part of this agreement unlawful, this shall not constitute a nullification of the remainder of the agreement.

Terms and Conditions

1. The owner and operator ("Owner") of this computer network ("the Service") reserves the right to discontinue the Service at any time.

□ I agree to the Terms and Conditions

An example of a captive web portal used to log onto a restricted network.

The captive portal is presented to the client and is stored either at the gateway or on a web server hosting that page. Depending on the feature set of the gateway, websites or TCP ports can be white-listed so that the user would not have to interact with the captive portal in order to use them. The MAC address of attached clients can also be used to bypass the login process for specified devices.

Contents

Uses
Implementation
HTTP redirect
ICMP redirect
Redirect by DNS
Circumvention of captive portals
Limitations
See also
References
External links

Uses

Captive portals are primarily used in open wireless networks where the users are shown a welcome message informing them of the conditions of access (allowed ports, liability, etc.). Administrators tend to do this so that their own users take responsibility for their actions and to avoid any major problems. It is discussed whether this delegation of responsibility is legally valid. [1][2]

Often captive portals are used for marketing and commercial communication purposes. Access to the Internet over open Wi-Fi is prohibited until the user exchanges personal data by filling out a registration form. The online form either automatically opens in a device's browser, or appears when the user opens their browser and tries to visit any webpage. In other words, the user is "captive" - unable to browse freely until they accept the terms and conditions. This allows the provider of this service to display or send advertisements to users who connect to the WiFi access point. This type of service is also sometimes known as social WiFi, as they may ask for a social network account to login (such as Facebook).

The user can find many types of content in the captive portal, and it's frequent to allow access to the Internet in exchange for viewing content or performing a certain action (generally providing personal data to enable commercial contact); thus, the marketing use of the captive portal is a tool for lead generation (business contacts or potential clients).

Implementation

There is more than one way to implement a captive portal.

HTTP redirect

A common method is to direct all web traffic to a web server, which returns an HTTP redirect to a captive portal.[3] When a modern, internet-enabled device first connects to a network, it sends out an HTTP request and expects an HTTP status code of 204. If the device receives a HTTP 204 status code, it assumes it has unlimited internet access. Captive portal prompts are displayed when you are able to manipulate this first HTTP message to return a HTTP status code of 302 (redirect) to the captive portal of your choice.[4][5]

ICMP redirect

Client traffic can also be redirected using ICMP redirect on the layer 3 level.

Redirect by DNS

When a client requests a website, DNS is queried by the browser. In a captive portal, the firewall will make sure that only the DNS server(s) provided by the network's DHCP can be used by unauthenticated clients (or, alternatively, it will forward all DNS requests by unauthenticated clients to that DNS server). This DNS server will return the IP address of the captive portal page as a result of all DNS lookups.

In order to perform redirection by DNS the captive portal uses DNS hijacking to perform an action similar to a man-in-the-middle attack. To limit the impact of DNS poisoning typically a TTL of 0 is used.

Circumvention of captive portals

Captive portals have been known to have incomplete firewall rule sets.[6] In some deployments the rule set will route DNS requests from clients to the Internet, or the provided DNS server will fulfill arbitrary DNS requests from the client. This allows a client to bypass the captive portal and access the open Internet by tunneling arbitrary traffic within DNS packets.

Some captive portals may be configured to allow appropriately equipped user agents to detect the captive portal and automatically authenticate. User agents and supplemental applications such as Apple's Captive Portal Assistant can sometimes transparently bypass the display of captive portal content against the wishes of the service operator as long as they have access to correct credentials, or they may attempt to authenticate with incorrect or obsolete credentials, resulting in unintentional consequences such as accidental account locking.

A captive portal that uses MAC addresses to track connected devices can sometimes be circumvented by connecting a router that allows setting of the router MAC address. Router firmware often calls this MAC cloning. Once a computer or tablet has been authenticated to the captive portal using a valid username and valid password, the MAC address of that computer or tablet can be entered into the router which will often continue to be connected through the captive portal as it shows to have the same MAC address as the computer or tablet that was previously connected.

Limitations

Some of these implementations merely require users to pass an SSL encrypted login page, after which their IP and MAC address are allowed to pass through the gateway. This has been shown to be exploitable with a simple packet sniffer. Once the IP and MAC addresses of other connecting computers are found to be authenticated, any machine can spoof the MAC address and IP of the authenticated target, and be allowed a route through the gateway. For this reason some captive portal solutions created extended authentication mechanisms to limit the risk for usurpation.

Captive portals require the use of a browser; this is usually the first application that users start, but users who first use an email client or other application may find the connection not working without explanation, and will then need to open a browser to validate. It is however sometimes possible to use email and other facilities that do not rely on DNS (e.g. if the application specifies the connection IP rather than the web address). A similar problem can occur if the client uses AJAX or joins the network with pages already loaded into its browser, causing undefined behavior when such a page tries HTTP requests to its origin server.

Platforms that have Wi-Fi and a TCP/IP stack but do not have a web browser that supports HTTPS cannot use many captive portals. Such platforms include the Nintendo DS running a game that uses Nintendo Wi-Fi Connection. Non-browser authentication is possible using WISPr, an XML-based authentication protocol for this purpose, or MAC-based authentication or authentications based on other protocols.

It is also possible for a platform vendor to enter into a service contract with the operator of a large number of captive portal hotspots to allow free or discounted access to the platform vendor's servers via the hotspot's walled garden. One such example is the 2005 deal between Nintendo and Wayport to provide free WiFi access to Nintendo DS users at certain McDonald's restaurants.[7] Also, VoIP SIP ports could be allowed to bypass the gateway to allow phones to work.

See also

- HTTP proxy

References

1. "Wi-Fi Hotspots and Liability Concerns - Maiello Brungo & Maiello" (http://www.mbm-law.net/newsletter-articles/wi-fi-hotspots-and-liability-concerns/1229/). *Maiello Brungo & Maiello*. 2007-04-09. Retrieved 2017-05-18.
2. "Myths and Facts: Running Open Wireless and liability for what others do" (https://openwireless.org/myths-legal.html). *Open Wireless Movement*. 2012-08-07. Retrieved 2017-05-18.
3. Wippler, Andrew J. (2017-04-07). "Captive Portal Overview" (https://andrewwippler.com/2017/04/07/captive-portal-overview/). *Andrew Wippler's Sketchpad*. Retrieved 2017-05-18.
4. Wippler, Andrew J. (2016-03-11). "WiFi Captive Portal" (https://andrewwippler.com/2016/03/11/wifi-captive-portal/). *Andrew Wippler's Sketchpad*. Retrieved 2017-05-18.
5. "Network Portal Detection - The Chromium Projects" (https://www.chromium.org/chromium-os/chromiumos-design-docs/network-portal-detection). *www.chromium.org*. Retrieved 2017-05-18.
6. "Lessons from DEFCON 2016 – Bypassing Captive Portals" (https://www.secplicity.org/2016/08/26/lessons-defcon-2016-bypassing-captive-portals/). *Secplicity - Security Simplified*. 2016-08-26. Retrieved 2017-05-18.
7. "Nintendo And Wayport Join Forces To Bring Free U.S. Wi-Fi Access To Nintendo DS Users" (http://www.gamesindustry.biz/articles/nintendo-and-wayport-join-forces-to-bring-free-us-wi-fi-access-to-nintendo-ds-users). *gamesindustry.biz*. Retrieved 24 November 2015.

External links

- Android Captive Portal Setup (http://developer.android.com/reference/android/net/CaptivePortal.html)
- RFC 7710 (https://tools.ietf.org/html/rfc7710) Captive-Portal Identification Using DHCP or Router Advertisements (RAs)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Captive_portal&oldid=816996161"

This page was last edited on 25 December 2017, at 08:43.