OTP AND RADIUS

InkBridge Networks

We authenticate the Internet

THINGS TO KNOW ABOUT ONE-TIME PASSWORDS

There are a number of issues with using different authentication methods. These issues include security vulnerabilities, along with limitations of the underlying protocols.

PAP

RADIUS provides for PAP authentication, in which the RADIUS client sends a clear-text password to the RADIUS server. This clear-text password is encrypted in transit. Despite nearly three (3) decades of analysis, there have been no vulnerabilities found with this encryption.

The benefit of PAP authentication is that the clear-text password is compatible with all databases and other back-ends. The RADIUS server effectively pretends to be the user in order to login. If the login is successful, the RADIUS server returns “accept”, otherwise it returns “reject”.

The only security issue with PAP is that the RADIUS server sees this password. If the RADIUS server is compromised, then the passwords may “leak”. However, if the RADIUS server is compromised, then leaking passwords is only a small proportion of bad things which can happen.

Multi-Factor Authentication (MFA) is possible with PAP authentication via two methods. The simplest is use a token such as Google Authenticator, and then have the user put the token and password into the login field. e.g. “`123456mypassword`”. the RADIUS server receives the password as “`123456mypassword`”, and splits the field into two values. The token part “`123456`” is verified against the OTP token server. The password part “`mypassword`” is verified against the user directory such as LDAP or Active Directory. If either check fails, the user is rejected. If both checks pass, the user is authenticated.

The second way to implement MFA via PAP is via RADIUS challenge-response packets. In this method, the user enters a password such as “`mypassword`”. The RADIUS server verifies the password against the user directory. If the password is correct, the RADIUS server returns a RADIUS Access-Challenge packet, containing test such as “`Please enter the token:`”. The RADIUS client displays this token to the user, who enters the token, e.g. “`123456`”. This token is then passed to the RADIUS server, which verifies it against the OTP token server.

In general we recommend using PAP as much as possible. It is secure, and compatible with everything.

CHAP

RADIUS also supports CHAP authentication. In this authentication method, the RADIUS client calculates a MD5 hash of a random challenge, and the users password. Both the challenge and password are sent to the RADIUS server.

The RADIUS server then obtains the users clear-text password from a database. The server then performs the same MD5 hash of the random challenge and the clear-text password. If the two hashes are identical, then the password entered by the user is correct, and the RADIUS server returns “accept”.

The security issues with CHAP are largely the same as with PAP. The passwords are “encrypted” on the wire, and the RADIUS server has access to the users clear-text password. Despite nearly three (3) decades of analysis, there have been no vulnerabilities found with this encryption.

The downside to CHAP authentication is that the RADIUS server mush obtain the users clear-text password from a database. If that password is not available (e.g. as with Active Directory), then the RADIUS server cannot perform the CHAP calculations necessary to authenticate the user.

MS-CHAP / MS-CHAPv2

MS-CHAP authentication is similar in some respects to CHAP, except that the calculations are done with MD4 and DES instead of MD5. MS-CHAPv2 is slightly different from MS-CHAPv1, but the underlying design principles are the same.

The problem with MS-CHAP is that the underlying design is fundamentally flawed. Both MD4 and DES have been cracked since the protocol was designed. In addition, the way MS-CHAP uses DES makes it almost trivial to reverse engineer the DES keys used. Microsoft has acknowledged this weakness in their web site at the following page:

https://msrc-blog.microsoft.com/2012/08/20/weaknesses-in-ms-chapv2-authentication/

Anyone who can observe the MS-CHAP exchange can run easily available "cracking" tools, such as this one on GitHub:

https://github.com/moxie0/chapcrack

As of 2012, the authors of the above tool were offering to crack any MS-CHAPv2 exchange for $20, and obtain the users password:

https://boingboing.net/2012/09/24/exhaust-all-of-des-and-crack-a.html

We can only assume that the cost of cracking MS-CHAPv2 has dropped significantly since then.

Due to the above issues, we recommend using MS-CHAPv2 only when no other alternatives are available. We also recommend that all RADIUS traffic carrying MS-CHAPv2 be sent over secure, management networks.

EAP-MSCHAPv2

EAP-MSCHAPv2 is essentially MS-CHAPv2 carried over the EAP protocol. EAP is an authentication protocol which is little more than a framework for carrying other authentication protocols. It consists of a four (4) byte header which contains a 1-byte identifier that tracks requests and responses, a 1-byte field which identifies the EAP type being carried, and finally 2 bytes which describe the length of the data being carried.

For EAP-MSCHAPv2, the data being carried in EAP is just MS-CHAPv2.

The underlying EAP protocol requires additional packet exchanges over normal MS-CHAPv2. As such, it is more complex to implement.

In the end, EAP-MSCHAPv2 is essentially MS-CHAPv2, but is more complex. EAP-MSCHAPv2 adds no additional security or integrity checks over MS-CHAPv2.

Microsoft Azure MFA Server

The Microsoft MFA server has limited capabilities, as documented on the following Microsoft page:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-dir-radius

It supports PAP and MS-CHAPv2. It does not support EAP, or EAP-MSCHAPv2. The MFA authentication server supports MFA only with PAP, and RADIUS Access-Challenge packets as described above.

Recommendations

Our recommendation is to use PAP whenever possible. It is compatible with all known back-end databases, and it has no known security issues. The Microsoft MFA server supports MFA with PAP. FreeRADIUS can do OTP with PAP and Active Directory.

Further, we recommend using passwords where the users password is appended to the OTP token, e.g. "`123456mypassword`". That form is simple to use for both users and administrators.

If MS-CHAPv2 is required for operational or inter-operability reasons, we recommend running it over a secure management network. The Microsoft MFA server does not support MFA with MS-CHAPv2.

We do not recommend using EAP-MSCHAPv2, as it offers no benefits over MS-CHAPv2, and it is more complex to implement.

CONTACT INFORMATION

InkBridge Networks
26 rue Colonel Dumont
38000 Grenoble
FRANCE

T +33 4 85 88 22 67
F +33 4 56 80 95 75
W inkbridgenetworks.com
E sales@inkbridgenetworks.com

InkBridge Networks (Canada)
100 Centrepointe Drive, Suite 200
Ottawa, ON, K2G 6B1
Canada

T +1 613 454 5037
F +1 613 280 1542

InkBridge Networks (Greece)
Kostas Kalevras
Heroon Polytechniou 9, 15780 Zagrofou
Athens, Greece

T +30 2107 724 057
F +1 (408) 465-7393
E greece@inkbridgenetworks.com