Mike Galler

Basic Recommendations for HVAC Cybersecurity

The Problem With Passwords

BY MIKE GALLER, MEMBER ASHRAE

Cybersecurity has been a topic of increasing importance for several years. While fully securing a large and complex system can be very complicated, some basic precautions can easily be applied to any system, and some basic precautions can be implemented by the users of any system. This column will briefly explore an important aspect of identification and authentication: passwords. Other forms of authentication, such as ID badges, cryptographic keys and biometrics are also important, but are not discussed here.

In 2021 61% of breaches involved compromised credentials. Credentials are one of the most sought-after data types and are a target in 58% of breaches.[1] A strong password policy and good passwords are essential to securing any system. Password selection is one of the few areas where the actions of each user can affect the security of the entire BAS. A compromised credential may allow malware access to every other system on the company network. The methods to select a strong password on a BAS are identical to the methods used on an IT system.

Password Policy

- Ensure that administrator accounts have strong and unique passwords.
- No account of any type should use the same password as another account.
- Do not reuse passwords across different services or devices.
- **Never** leave default passwords in use, on any device. Many attacks rely on using default passwords.
- Avoid use of generic accounts for all users—assign unique account credentials to each user and remove them when that user no longer requires access.

Password Strength

The strength of a password is determined by its length and diversity. The strength of a password should reflect the importance of what it protects. Password strength is often increased by enforcing a minimum length. Some systems require a password of at least eight characters; this length provides a bare minimum of protection and can be cracked quickly, regardless of relative complexity.[2] Your BAS deserves better. NIST recommends manufacturers allow passwords at least 64 characters long,[3]

Mike Galler is an engineer at the National Institute of Standards and Technology in Gaithersburg, Md. He is the chair of ASHRAE's Cybersecurity for HVAC Systems and Related Infrastructure Multidisciplinary Task Group.

which allows users plenty of room to make a secure password. *Adding length makes a stronger password than increasing diversity.* A password may be made more diverse by using symbols, numbers and varying case on letters. A strong password may be easy to make and remember by basing it on a short phrase or a few random words, and then interspersing symbols, numbers and capital letters. A strong password may also be created by a password generator, but it will probably be very difficult to remember.

Table 1 shows basic guidance on how to construct a password based on three words, as scored by an online password checker. The score is calculated by length and diversity of the password. The score will be decreased for lack of diversity or for repeating, consecutive or sequential letters, numbers or symbols. Different words should be used in actual passwords. Avoid company and industry related words, and any other words that would be predictable to an attacker. Password strength could be increased by modifying the text of the words used so they don't match any words that would be found in a dictionary. Example techniques are found in Test ID 9 and 10.

This column is intended to be a basic introduction to safe selection and use of passwords. A deeper understanding of relevant cybersecurity topics is necessary to ensure your network is secure. A good cybersecurity plan addresses not only the physical components of the facility, but also the personnel, policies, legal, liability and education requirements. There is no "one-size-fits-all" when it comes to protecting a facility from attacks. Knowing your levels of risk[4] and cybersecurity awareness, likely threat vectors, technical abilities and your budget will help create a workable plan. For more information about cybersecurity, see *2019 ASHRAE Handbook—HVAC Applications*, Chapter 41, Computer Applications, Section 5. In addition, ASHRAE Guideline 13-2015, *Specifying Building Automation Systems*, has a new section specifically addressing cybersecurity requirements. There are also multiple sources of information available on the internet, including more detailed recommendations and references to applicable standards.

TABLE 1 It's possible to have a very strong password that isn't difficult to remember.

TEST ID	TEST PASSWORD	LENGTH	RESULT	SCORE
1	threephasepassword	18	Failure	18
2	threephasepassword!!	20	Warning	57
3	ThreePhasePassword	18	Sufficient	64
4	threephasepassword!9	20	Sufficient	69
5	three!phase9password	20	Sufficient	75
6	ThreePhasePassword42	20	Exceptional	115
7	ThreePhasePassword!!	20	Exceptional	115
8	Three!Phase9Password	20	Exceptional	123
9	Thre!ePhas9ePaswsord	20	Exceptional	127
10	ThRe#!PhAsE9PaSsWoRd	20	Exceptional	147

Result Key—Exceptional: Exceeds minimum. Sufficient: Meets minimum. Warning: Advised against. Failure: Does not meet minimum.

References

1. Verizon. 2021. "2021 Data Breach Investigations Report." https://verizon.com/dbir

2. Kast, B. 2020. "How Long Should Your Password Be? The Data Behind A Safe Password Length Policy." LMG Security. https://tinyurl.com/4esz3ss2

3. Grassi, P., et al. 2020. "Digital Identity Guidelines Authentication and Lifecycle Management." NIST Special Publication 800-63B.

4. NIST. 2012. "Special Publication 800-30, Revision 1. Guide for Conducting Risk Assessments." National Institute of Standards and Technology. ■