eclypses

WHITE PAPER

How Vulnerable are Your Systems to a Brute Force Attack?

Authors: Tim Reynolds, Eclypses Chief Technology Officer and David Schoenberger, Eclypses Chief Innovation Officer

November 11, 2021

Document ID: ECLYPSES – 1532395320-209

Contents

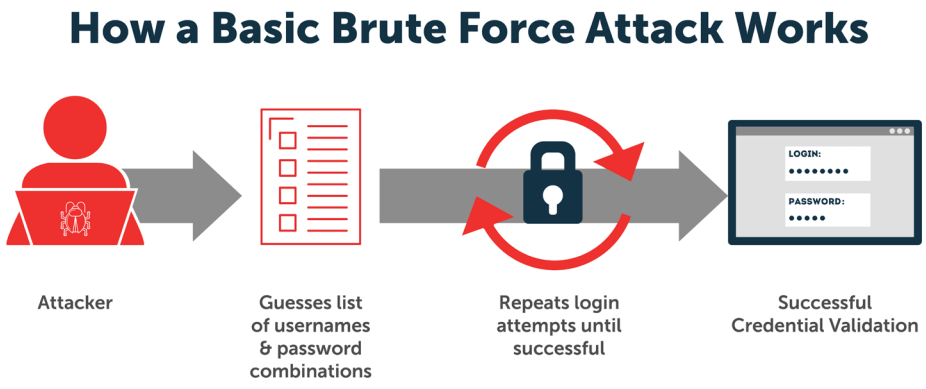
Introduction

Brute force attacks are when a hacker attempts to capture and reveal information by repeating encryption keys a multitude of times until they are able to gain access to the data. It is called a “Brute Force” attack because it requires the bad actor to continuously attempt to force their way through a mobile or web application’s security until they succeed. This type of attack may seem simple, but it has been effective for a long time.

The Problem & Outcomes

The information transferred between applications and consumer endpoints is transmitted across networks, many of which are public. At any point, this information is susceptible to interception by various means and if the data is highly sensitive or confidential, it must be protected. According to *Verizon’s Data Breach Investigation Report*, 80% of breaches involved the use of brute force, meaning utilizing stolen or brute-forced credentials.[4]

TLS (Transport Layer Security) uses a certificate exchange to encrypt and decrypt the data in transit, however, it uses a fixed key to manage its secret.[1] If an attacker intercepted this data, they could use high powered computing devices to try a multitude of different decryption keys until they reveal the sensitive payload. With today’s computing power, a state actor would apply millions of combinations of keys until they reach success. In fact, recent news indicates that state actors have developed much faster computing resources that could certainly render basic encryption (even 256 bit) an unsecure alternative.[5] The attacker would then be able to reveal the data that is in transit and gain access to the sensitive information. The process of repeatedly trying to determine the key is known as a brute force attack.[2]



These are considered man-in-the-middle (MITM) attacks, where cyber criminals lure victims into launching a website under their control to access a cross-origin HTTPS request with a specially crafted HTTP payload. This request is then redirected to an HTTP server that uses a certificate that is compatible with that of the website, therefore spawning a valid TLS session.

TLS is a protocol that requires ongoing update and maintenance and cannot be left in applications without programming for the ability to update actively.

As recently as July 1, 2021, NSA and Central Security Service partnered with CISA to release an advisory on a Russian brute force global campaign.[3] They reported that this campaign has already targeted hundreds of U.S. and foreign organizations worldwide, including U.S. government and Department of Defense entities. While the sum of the targeting is global in nature, the capability has predominantly focused on entities in the U.S. and Europe. Types of targeted organizations include:

- Government and military organizations
- Political consultants and party organizations
- Defense contractors
- Energy companies
- Logistics companies
- Think tanks
- Higher education
- Institutions
- Law firms
- Media companies

MTE Technology Solution

Using MTE technology ensures that the information is always uniquely protected regardless of the transport mechanism. For small pieces of data, such as location coordinates or financial balances, MTE technology does not use any type of encryption, so attempting to determine a key has no value. A highly sensitive piece of information can now be protected against pattern recognition, inference of a value based on size, replays of data, and “catch and release” attacks.

Since MTE technology protects data at the application layer, vulnerabilities seen in TLS such as negotiating down to the least common denominator (which exposes compromised specifications of the TLS protocol) are not a threat. With the new MTE 2.0, this is even more true as data is obfuscated with a one-time pad before it is even processed with MTE. This means that even if a bad actor was able to determine a key and break it, the data would still be useless to them, even before any kind of encryption.

Furthermore, when using the Managed Key Encryption (MKE) add on, each transmission within a larger digital conversation is protected with a different, randomly generated key that is never exchanged between the endpoints and is not derived from any certificate, which is susceptible to hijacking.

In either case, because only uniquely paired endpoints can conceal / reveal the information, hijacking of a session is impossible.

In standard encryption (or TLS), the following takes place:

- An exchange of certificates generates an encryption scheme
- Information is encrypted
- Information is transmitted
- The information can be intercepted, and an attacker can apply their brute-force until they have successfully revealed the information.

Using MTE technology, the following takes place:

- Information is protected (encoded) by the sending endpoint
- Information is transmitted
- The information can be intercepted, however since it was NOT encrypted, no amount of attempting to determine a key is possible
- Each time the information is transmitted, (even identical information), it is different, and if the same protected information is transmitted (replayed), it is recognized as a replay and is discarded

Using MKE technology (Managed Key Encryption), the following takes place:

- The standard MTE technology generates an encryption key (no certificate exchange is required)
- The information is encrypted
- The information is transmitted

- The information can be intercepted, and a brute force technique could be attempted against the single transmission, however, each transmission would have to be separately attacked since the MTE Technology generates a new encryption key for each exchange of information. Each new key is in no way related to a previous key and no information is transmitted to allow an attacker to re-create the key.

Using segmented MKE, the following takes place:

- The information is broken into segments of a pre-determined size
- Each segment is individually protected with MKE and then glued back together into an overall package of information
- The re-constructed package of information is then transmitted
- The information can be intercepted; however, each segment would have to be individually brute force attacked in order to put the original package of information back together and revealed. Since the amount of time and computing resources to determine even a single key using brute force techniques is quite large, the attacker would have to expend that amount of effort for each segment. That coupled with the fact that the attacker does not know the size of a segment, they would have to brute force multiple combinations of segment sizes, and then repeat the attack on each segment. For example, if the amount of information being transmitted is 3 megabytes, and the segment size was 512 bytes, the attacker would have to attack 6144 segments, and if they did not know the segment size and started with 64 and then increment by one, they would have to attempt over 2.7 million attacks before they reached success.

Conclusion

In conclusion, if you have highly sensitive, or confidential information to transmit over a network, using MTE technology completely thwarts any kind of capture and brute force attack. The attacker could try every combination of values to decrypt the information only to be stymied, since the information is protected with MTE and not encrypted.

If your information is large and you do not wish to incur any overhead in payload size, using MKE would require the attacker to repeat their process for *each and every* transmission (rather than once per session) to be able to eaves-drop on your digital conversation. If that is still too much of a risk, the use of the segmented MKE renders the likelihood of success to nearly zero.

Sources:

1. Lakshmanan, R. (2021, January 9). New TLS Attack Lets Attackers Launch Cross-Protocol Attacks Against Secure Sites. The Hacker News. https://thehackernews.com/2021/06/new-tls-attack-lets-attackers-launch.html

2. O'Donnell, L. (2021, January 6). NSA Urges SysAdmins to Replace Obsolete TLS Protocols. ThreatPost. https://threatpost.com/nsa-urges-sysadmins-to-replace-obsolete-tls-protocols/162814/

3. Security Agency/Central Security Service. (2021, July 1). NSA, Partners Release Cybersecurity Advisory on Brute Force Global Cyber Campaign. Retrieved October 15, 2021, from https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2677750/nsa-partners-release-cybersecurity-advisory-on-brute-force-global-cyber-campaign/

4. Verizon. (2020, January 1). 2020 Data Breach Investigations Report. Https://Enterprise.Verizon.Com/. https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

5. Chen, S. (2021, October 28). China launches world's fastest programmable quantum computers. South China Morning Post. Retrieved November 1, 2021, from https://www.scmp.com/news/china/science/article/3153727/china-launches-worlds-fastest-programmable-quantum-computers

ABOUT ECLYPSES

Eclypses has a disrupting cyber technology, offering organizations with an advanced data security solution not seen in today's environments, called MTE®.

Founded in 2017, Eclypses originated as a subsidiary of Secure Cloud Systems, Inc. with the primary focus of developing the MTE cyber technology to be the most innovative and disruptive data security solution for all mobile application technologies and websites. The development of this technology led to the MTE toolkit, as we know it today.

Eclypses' patented MTE technology was developed through their technical team in Colorado Springs, CO, where they continue to innovate and expand on this cutting-edge security technology. The MTE technology generates a random string of values that is used to replace any form of structured or unstructured data. This replacement string of values is referred to as MTE, which provides innovative security against man-in-the-middle cyber-attacks.

With a focus in the mobile sector, this technology allows for a higher level of security to protect against man-in-the-middle cyber-attacks in products and applications that may have limited resources, such as battery life, processor, or throughput.

CONTACT US

contact@eclypses.com
www.eclypses.com
(719) 323-6680