Arrowhead Bank Cyber-Tips Newsletter

Virtual Conferencing Platform Tips

With the recent move for many to working from home, there are a lot of questions around virtual conferencing platforms. Much of the attention has focused on the security of some platforms compared to others. However, the majority of the security issues actually have a lot to do with the users' familiarity with these platforms and their proper usage.

The first thing to remember is this: If you are going to download a virtual conferencing application, be certain the download is from a reputable source. Most often the company will host the download themselves or have a link to the download on their website. It is advisable not to trust a download from third-party if you were not directed there by the official website.

Security concerns regarding virtual conferencing

1. Encryption may not be adequate to secure sensitive information or to protect the privacy of individuals.

- End-to-end encryption is not an easy task for real-time audio or video connections. In most use cases it takes special hardware or software. It is very important to remember that some topics should not be discussed over a virtual conference. This is especially true regarding sensitive data, personally identifiable information (PII), and regulated data such as the Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Rule (COPPA), and Federal Tax Information (FTI).
- Consider where encryption key distribution servers are located when evaluating a company's offerings. Researchers have found that some companies' encryption key distribution servers for U.S.-based meeting sessions were located in Beijing, China. In such situations, companies may be obligated to disclose meeting encryption keys to the Chinese government.
- Just because a company advertises encryption, doesn't mean that the best version of encryption being utilized.

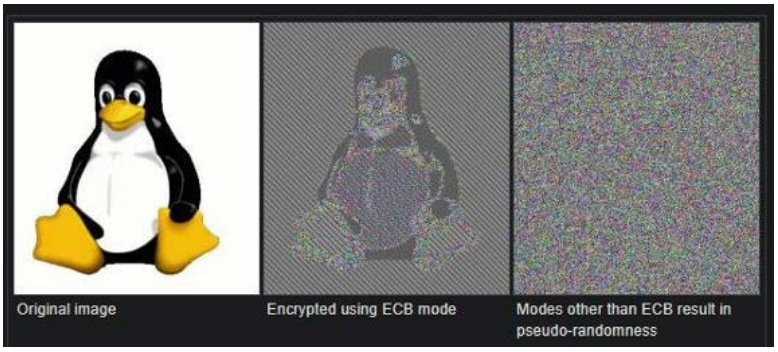

Figure 1: Tux the Penguin Encrypted in ECB vs Pseudo-Random Encryption: Source GitHub picoctf-2019-solutions/Cryptography/aes-abc/readme.md

2. Virtual conferencing applications are vulnerable to multiple attacks

- Malicious actors are creating fake installation files for multiple meeting platforms including Zoom Meetings, MS Teams, and Google Classroom.
- Some conferencing platforms have been “conference bombed.” This is when an uninvited guest gains access with the intention to disrupt or eavesdrop on the meeting.
- Virtual conference meeting users have been targeted to capture potentially sensitive data disclosed during meetings. As well, recorded meetings may not be stored by their meeting host in a secure manner. Attackers have accessed Zoom Meetings files stored on a computers and unsecured public cloud environments.

Guidelines for Virtual Conferencing

Below are some helpful recommendations to improve the privacy and security of web based virtual meetings:

a. If possible, NEVER share sensitive or regulated data during virtual conference meetings.
b. Become familiar with who may record your meeting. Be aware that individuals may choose to record a meeting using audio or video recording tools outside of the meeting software.
c. Download virtual conferencing clients directly from the manufacturer or your service provider.
d. Always run the newest version of the conferencing client (if required to download and install a client).
e. Password protect each meeting with a unique and complex password using letters, numbers and special characters.
f. Password protect recordings of meetings with a unique and complex password using letters, numbers and special characters.
g. Do not share your meeting link in public forums or on social media. In the event you must advertise your meeting publicly, remove the password embedded in the link and ask attendees to contact the organizer for the password.
h. Use a meeting ID rather than the personal ID associated with a virtual conferencing account. This way the meeting ID should change for each meeting.
i. Disable sharing for all attendees except for the meeting host.
j. Use the waiting room/lobby feature when it is available. This requires the organizers to admit people singly (for small meetings) or all at once (for larger meetings). If an attendee seems suspicious, the waiting room feature allows organizers to prevent them from joining the meeting.
k. Remove and block anyone from meeting rooms with an unrecognizable or unverifiable identity. Once removed, the person or people cannot come back in.

Taking the above steps will help ensure your organization's virtual meetings will remain secure while employees connect and collaborate through these platforms.