ICAO BANGKOK UNITING AVIATION

Cyber security

Peter Dunda

Regional Officer, Aeronautical Meteorology
International Civil Aviation Organization

Webinar on the implementation of the ICAO Meteorological Information Exchange Model (IWXXM), 27 to 29 October 2020

Cyber Security

GUIDELINES FOR THE IMPLEMENTATION OF OPMET DATA EXCHANGE USING IWXXM

- Appropriate AFS security elements should be defined by the ICAO groups in charge of information management / networks in order to introduce the operational exchange of IWXXM data via extended AMHS.
- It is recommended that appropriate malware and anti-virus precautions are exercised as a bare minimum when dealing with FTBP messages.

IWXXM and AMHS

- AMHS provides a mechanism for exchange of IWXXM information as an attachment to AMHS message refers to as File Transfer Body Part (FTBP)
- The FTBP exposes virus or malware attacks. Therefore, MET user and RODBs are recommended to make arrangements to scan, screen or filter those FTBP attachments

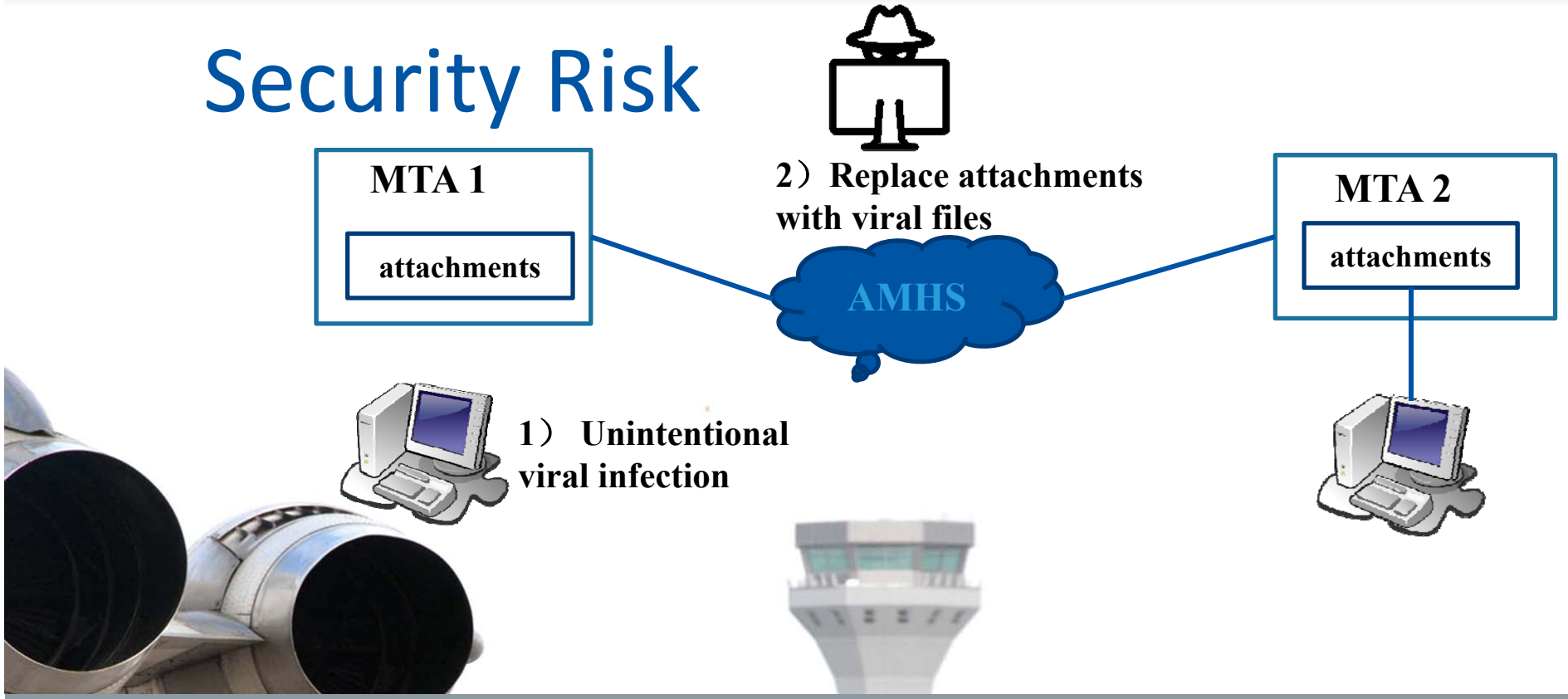
IWXXM Security Issue

Two options were identified to prevent the virus/malware infection:

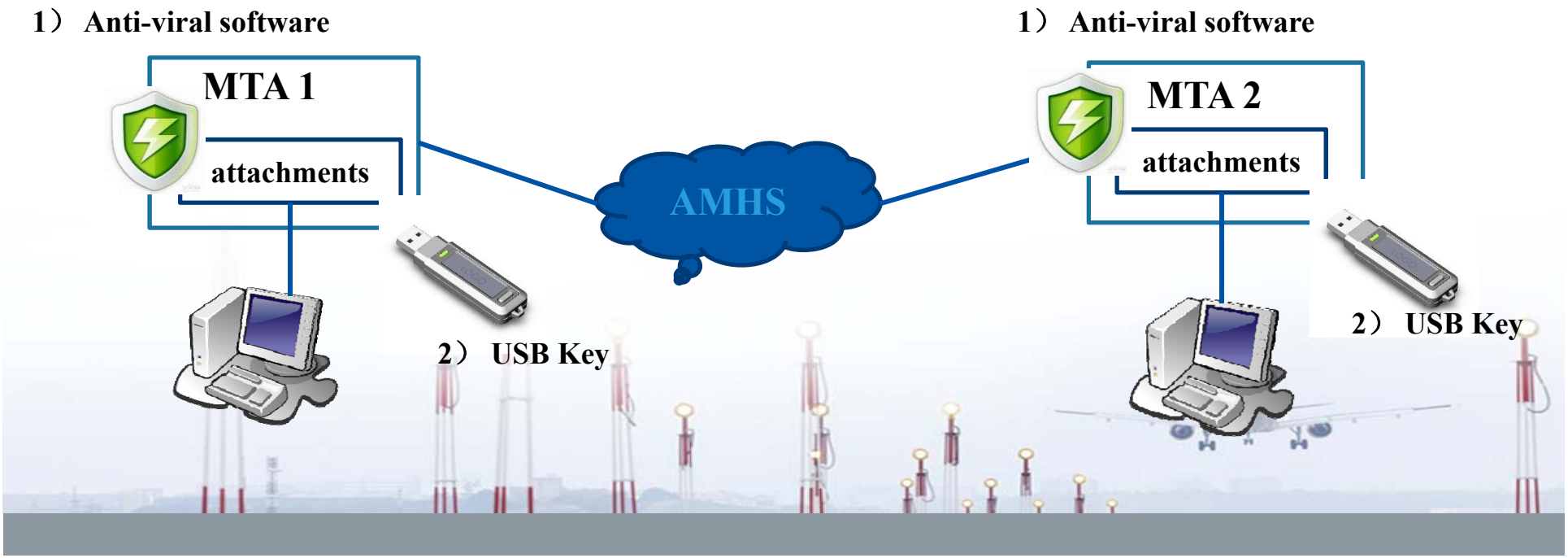
1. scan all attachments at Message Transfer Agent (MTA) and isolate/remove infected files before distribute to its end users; and/or
2. scan at user terminals

install antivirus functions and scan at MTA would delay processing by 10-20% while install antivirus at user terminals might have the infected files to be spread into the user's network.

Security Risk



Preventive consideration



Preventive Solutions

- Anti-virus:
  - Anti-virus software is deployed at the **sending end** to ensure that the virus or malware is not unintentionally transmitted
  - Anti-virus software is deployed at the **receiving end** to protect the system in use from virus or malware infection

More consideration on solutions

- Anti “man-in-the-middle” attack:
  - The sender hashes the attachment and signs it with its own private key.
  - MTA 1 send the package to MTA2.
  - The receiver verifies the signature of the attachment with the sender’s public key to ensure that the attachment actually comes from the right sender.
  - The receiver compares the HASH value of the attachment to ensure that the attachment is not tampered.

ICAO


North American Central American and Caribbean (NACC) Office Mexico City
South American (SAM) Office Lima
ICAO Headquarters Montréal
Western and Central African (WACAF) Office Dakar
European and North Atlantic (EUR/NAT) Office Paris
Middle East (MID) Office Cairo
Eastern and Southern African (ESAF) Office Nairobi
Asia and Pacific (APAC) Sub-office Beijing
Asia and Pacific (APAC) Office Bangkok
THANK YOU