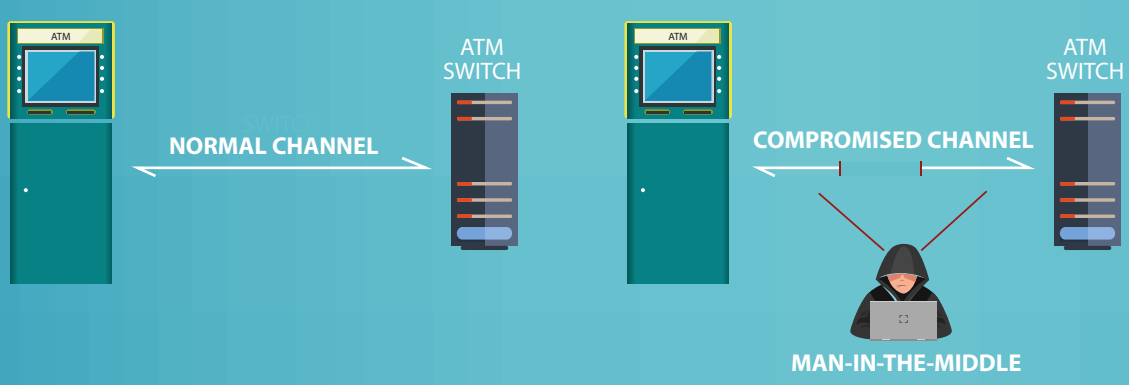
vortex™
Helping banks reach out

Protect Your ATMs against Man-in-the-middle attack (MITM)

As the world witnessed a meteoric rise in connected devices, criminals are always on the lookout for loopholes in a connected environment to exploit vulnerabilities and destabilize the ecosystem. The deployers must protect the ATMs against multifarious attacks, executed to compromise the security of the devices.

Attack Methodology

The ATMs are driven by the financial switch to which they are connected. Every transaction in the ATM is executed based on the requests and responses that flow between the ATM and the switch, which is the host. The MITM attack is executed when a program intercepts the communication and impersonates the switch. Post successful execution, the MITM will act as the proxy switch and will falsify the communications between the ATM and the Switch by sending a proxy switch to the ATM to dispense cash without debiting from the customer's account. The intruder can prevent the customer from using the service by declining every transaction request that flows between the ATM and the host resulting in a "Denial of Service (DoS)" attack. Any of these actions will result in either financial loss to the bank or customer dissatisfaction.



Protection against MITM attack

The best method to prevent MITM attacks is to ensure that the communication between the ATM and the host is secured and follows strict security protocols. Ecoteller® ATMs are equipped with security features that offer the best protection against such attacks.

Secure communication between the ATM and the host

Ecoteller® ATMs support TLS 1.2 communication protocol between the machine and the host which offers protection to the message flow and also prevents any rogue agent to interfere in the communication.

Firewall

Ecoteller® ATMs are equipped with robust firewalls that prevent any malicious program that can interfere with the communication between the ATM and the host. Firewall rules are enabled to lock down the communication port so that no rogue channels of communication can be established to the ATM.

Network communication

Sensitive messages that are exchanged between the ATM and the host are protected through network communication protocol encryption with TLS socket.

Mandatory Access Control

Ecoteller® ATMs support MAC protocols to ensure message integrity and tamper detection thus protecting against rogue interventions.

CONNECT WITH US TODAY FOR A SECURE BANKING TOMORROW

Email: info@vortexindia.co.in