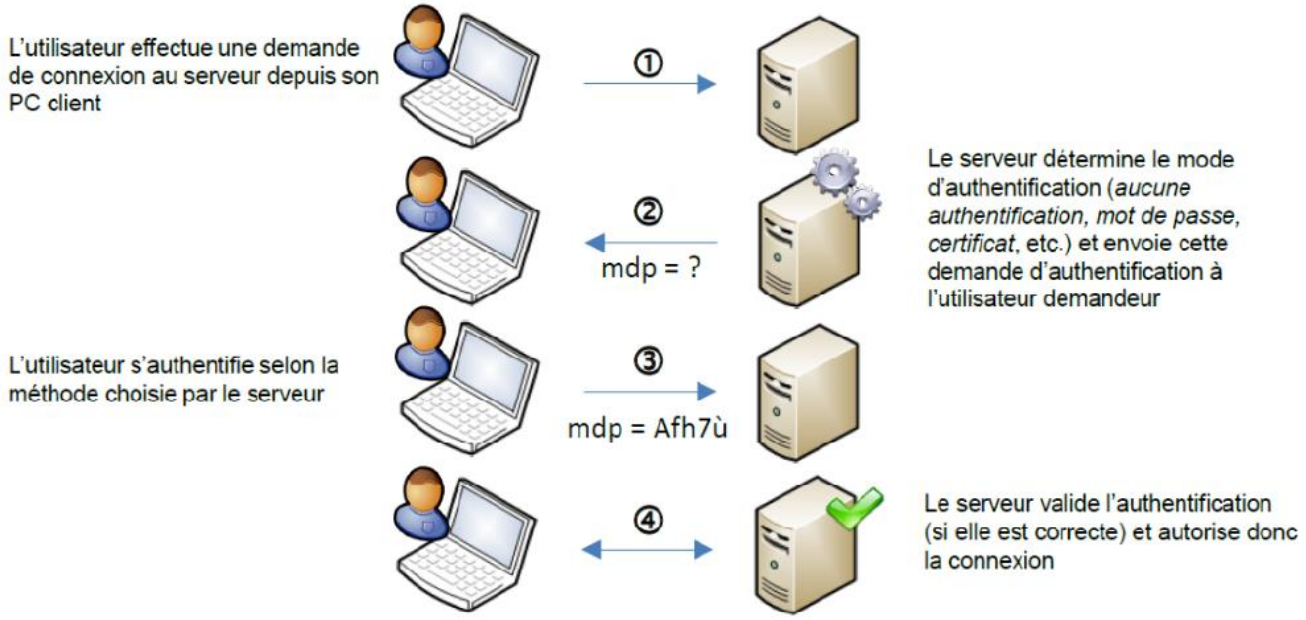
Fiche 2
Contournement authentification à un serveur VNC

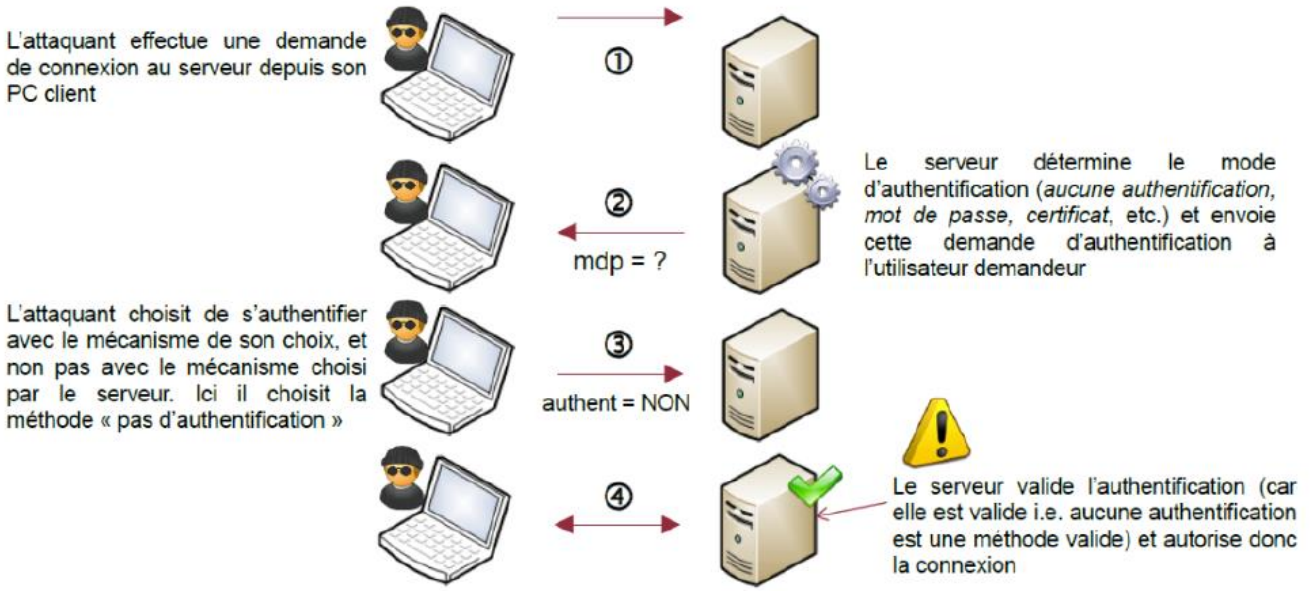
La vulnérabilité décrite ci-après est corrigée depuis de nombreuses années.

1 – Fonctionnement « normal » de l'application

L'application permet à un utilisateur de se connecter à distance sur une machine et ainsi disposer d'un « bureau à distance ». En 2006, il est découvert que cette application - utilisée partout dans le monde depuis de nombreuses années - présente une vulnérabilité critique : il est possible de se connecter à distance sans avoir besoin de s'authentifier (tout utilisateur sur internet peut se connecter à distance sur les systèmes en question).
La vulnérabilité porte la référence **CVE-2006-2369**.



2 – Exploitation de la vulnérabilité



Le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte).