Virtel Security Features

The following is an inventory of Virtel default and optional security features.

User Authentication

By default - Virtel calls RACF (optionally ACF2 or TSS) at logon with the user's identifier and password to authenticate the user. Virtel converts the RACF response into an application selection menu which it serves to the authenticated user: authorized applications are listed in this menu, whereas unauthorized applications are not. Besides leveraging existing RACF rules to authorize accessing the host from a web-enabled device, this allows confining each user to the applications that he/she is authorized to access. Combined with the multi-windows capability of web browsers, this application selection menu serves as a simple session manager, i.e. users can access several authorized applications concurrently.

Optionally – Virtually any other user authentication techniques can be deployed given proper Virtel configuration. Here are a few examples:

- Multi-factor authentication - Asking users to answer personal questions to double-check their identify (name of first pet, city of birth, name of high school, etc).
- PROXY – Authenticating users via a PROXY server.
- SSO – Authenticating users via a Single-Sign-On system.
- PassTicket – One-time temporary RACF credential.
- Biometrics – Authenticating users via a biometrics application (voice, finger prints, eye iris, etc).

Virtel can interface with ancillary user authentication systems hosted on clients, servers, or host.

Device Authentication

By default – Virtel uses a proprietary session control technique that relies upon dynamically-generated exchange-specific tokens and user IP addresses to mitigate the risk of "man-in-the-middle" attacks:

- Virtel dynamically generates and sends a new and unique security token to the user's web browser with each outgoing call. The token must be returned in the next incoming call to maintain the session integrity.
- For non-mobile devices, Virtel memorizes the user's IP address at logon and expects it to remain unchanged in subsequent incoming calls to maintain the session integrity. This technique doesn't work with mobile devices because their IP address changes from exchange to exchange even when the devices are not on the move.

Optionally - Virtually any other device authentication techniques can be deployed given proper Virtel configuration. Here are a few examples:

- Device type control - Filters can be added to restrict host or application access to authorized device types: e.g. iPad and Android tablets but no Smartphones, etc.

- Terminal/printer control – Because it is a VTAM solution, Virtel supports terminal control through a proprietary technology referred to as "LU nailing". It is used with police departments, court systems, and payroll departments for example, to restrict access to highly sensitive transactions to specific terminals in specific rooms. The same technology can be used to associate a printer to a web client. Because IBM connectors (such as HOD, CTG, CWS, or IMS connect) and many ISV's connectors are non-VTAM solutions, they have lost the concept of terminal and cannot support terminal or printer control.
- One-time token or password – At logon, Virtel can send to the user an email with a one-time security token or password that must be returned by the user to complete the logon process and initiate the session. The token or password may be stored in a cookie to accelerate future logons.
- Workstation Name Control – As an example of customized device authentication, Virtel has been configured to match at logon the name of client workstations to corresponding VTAM terminal definitions, on a customer site where applications can match those names to user identifiers.

Client Security

By default – Being thin-client provides “natural” client security, especially with mobile devices:

- App-less clients - Mobile device attacks cannot modify, jail brake, or root the web access app because there is no Virtel app on client devices: the Virtel app runs on the host. It is particularly important with mobile devices which are more exposed to such attacks.
- Data-less clients –Virtel doesn't store data on clients, which avoids exposing data when a client is lost or stolen. It is particularly important with mobile devices which are more exposed to loss or theft.

Transport Security

By default – Virtel’s HTTP/S connections are intrinsically safer than TN3270 connections because:

- TN3270 connections work in synchronous connected mode, which means that they are constantly open (i.e. subject to hacking) even when inactive (most of the duration of a session): this is sometimes referred to as the “TN3270 tunnel”.
- HTTP/S connections work in asynchronous disconnected mode, which means that they are open only for the very brief duration of an exchange (incoming or outgoing call) and closed (i.e. cannot be hacked) between exchanges (most of the duration of a session).

This is in part why TN3270 connections must be protected with a VPN whereas Virtel connections do not require VPN (Virtual Private Network) protection, although they are compatible with VPNs.

Virtel's integrated HTTPS server uses the AT-TLS (Application Transparent – Transport Layer Security) of z/OS Communication Server to provide SSL (Secure Socket Layer) encryption.

As discussed in “Device Authentication” above, Virtel uses a proprietary session control technique that relies upon dynamically-generated exchange-specific tokens and user’s IP addresses to mitigate the risk of “man-in-the-middle” attacks.

Optionally - Virtel can be configured to support selective encryption (e.g. encryption of non-display fields only: password, SSN, credit card number, etc).