itransition

ADVANCED NETWORK ACCESS CONTROL

One of the largest network security services providers in the US collaborates with Itransition on the development of a next gen system for corporate network access control.

PROBLEM

Our Customer, ForeScout Technologies, Inc., is one of the largest network security companies in the US, providing continuous monitoring and mitigation services to enterprises and government agencies in over 60 countries worldwide. With headquarters in Campbell, California, the company offers its solutions through a global network of authorized partners.

Understanding the ever-growing trend of bring your own device (BYOD) initiatives being adopted and the risks it entails, our Customer aimed to launch a robust system that would help enterprises enforce their network security. The system was to bring real-time visibility and control over corporate networks and devices connected to them, allowing both corporate and guest users access secure networks from their personal devices.

Itransition had cultivated a trusted and productive relationship with ForeScout Technologies through a number of successful engagements over the last years, and so was a partner of choice to deliver network security services for the new project as well. This time our team was tasked with the development and testing of a dynamically loaded library for Windows as a part of the core system, and an enterprise mobile application for Android.

The core system, named ForeScout CounterACT™, was developed by Customer's in-house team.

SOLUTION

FUNCTIONALITY

Consisting of two functional parts — mobile client applications (for Android, iOS, Windows Phone, as well as BlackBerry and Nokia Symbian) and a server backend — ForeScout CounterACTTM is aimed at providing secure access to corporate networks and allows for automating the following processes:

1. Preparation and acquisition of certificates for Wi-Fi connection setup;
2. Creation and configuration of secure Wi-Fi connections via the certificates received.

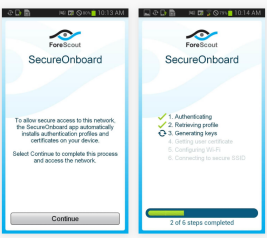
To get access to a secure network, users have to install the ForeScout SecureOnboard mobile application on their personal devices. The level of access for each user group, whether employees or outside users, can be set on the server side by system administrators.

MOBILE APPLICATION

Itransition team has supplemented ForeScout CounterACTTM with a convenient mobile application for Android operating system. The way the app works is simple and clear: it verifies user's login and then automatically downloads and installs necessary certificates on a device (either a personal computer or a smartphone), enrolling it in the secure network. After this one-time enrollment, users are able to access the network at any time with no further authorization.

When developing the required mobile application, one of the main aspects for our technical experts to consider was ensuring the app would be compatible with different versions of Android OS (starting from 4.0) and would run smoothly on any Android device. The core system built by our Client's team was supplied with the mechanisms needed to allow complete automation of authentication process on the latest Android versions, whereas the earlier versions either didn't provide the necessary functionality at all or were limited in capabilities.

After discussing the issue with the Client, we agreed on implementation of additional functionality that would enable users of earlier versions to access the secure network by conducting a number of operations manually.



DYNAMICALLY LOADED LIBRARY

Working concurrently with ForeScout's in-house team, Itransition experts also delivered a dynamically loaded library for Windows, which was later on integrated to the core system.

Itransition team provided the Customer with a comprehensive mobile application for managing access to secure networks, as well as took part in the core system development, having built a dynamically loaded Windows library. Delivered just on budget, the ForeScout CounterACTTM application was successfully launched and is now available on Google Play.

While implementing network security services on this the project, our team had the opportunity to dive in and explore new technologies and techniques, which will definitely be utilized by us in the future. The Customer evaluated highly the work we had done and expressed his willingness to continue collaborating with Itransition. And as for now, our team is already working on the development of a new ForeScout desktop client application for macOS.

PROCESS

PROJECT DELIVERY

Itransition's project team comprised three specialists, supervised by an experienced project manager. A C++ developer was responsible for the implementation of dynamically loaded library for Windows, whilst an Android developer delivered the Android mobile application. Within the project's framework, our specialists had to develop seamless mechanisms for certificate generation and signing, client device configuration, as well as certificate acquisition for authentication, which would allow accessing to secure networks.

To make sure the solution works without a hitch, a dedicated QA-engineer was also engaged into the project and collaborated with the Client's in-house team on system testing, including:

- Full testing on two devices, which were chosen based on usage statistics;
- MAT testing on other four devices;
- Regression testing on all the devices.

Thanks to the conducted testing, Itransition team managed to significantly increase the quality and performance of the final solution.

TECHNOLOGY OVERVIEW

Working on the project development, our team managed to endow the solution with a number of notable technological features that allowed enhancing the security of data transfer within the system. These features are as follows:

- Support of PKCS7 and PKCS10 certificate standards for certificate enrollment;
- Integration with SCEP-server;
- Configuration of Wi-Fi connection via X.509 certificates.

The dynamically loaded library for Windows is built on SCEP protocol:

The Android mobile application is based on the client-server architecture with SCEP integration. As for the ready-made solutions leveraged for the mobile application development, our experts utilized the following:

- Dd-plist parser of XML plist structures;
- Spongy Castle package for processing PKCS requests and SCEP;
- jSCEP open-source Java implementation of SCEP for integration with SCEP-server.

Tags: Application Development, Business Process Management, Mobility, IoV