CASE STUDY

SECURITY AUDIT OF AN INSURANCE MOBILE APPLICATION

Client Background

Our client is a non-profit company that serves millions of health plan members and tens of thousands of physicians. The company focuses on collaborating with doctors and hospitals to help them deliver more efficient, cost-effective care for their members. Additionally, they predict and prescript health issues, which will help decrease the cost of medical insurance. The company builds tools for both insurance members and physicians to help them effectively communicate.

softserve

Business Challenge

The client developed a new mobile insurance application for their customers. According to the internal software development lifecycle (SDLC) rules, the newly created application needed to pass an independent third-party security audit before it could go into production. The new mobile application—developed with a Kony hybrid mobile framework—required a security tool for automated security verification.

The company partnered with SoftServe to provide application security verification with a focus on the following potential threats and associated business risks:

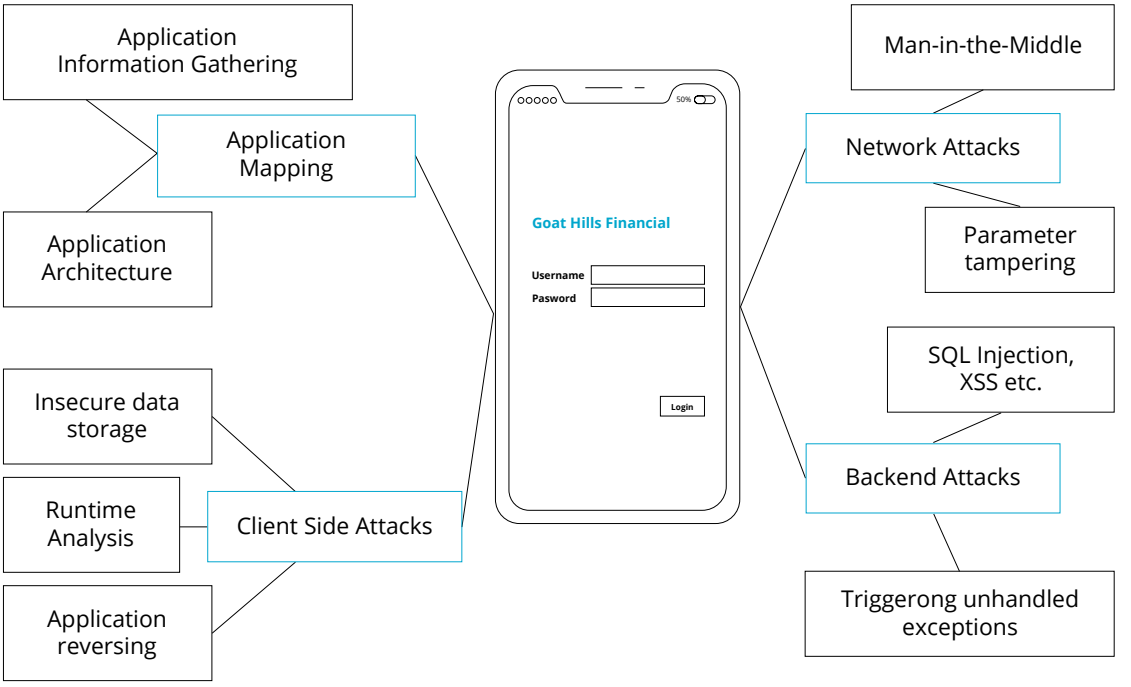
- Unauthorized access to backend, sensitive client data
- Potential chance of password brute forcing
- Hardcoded values that lead to application research by hackers

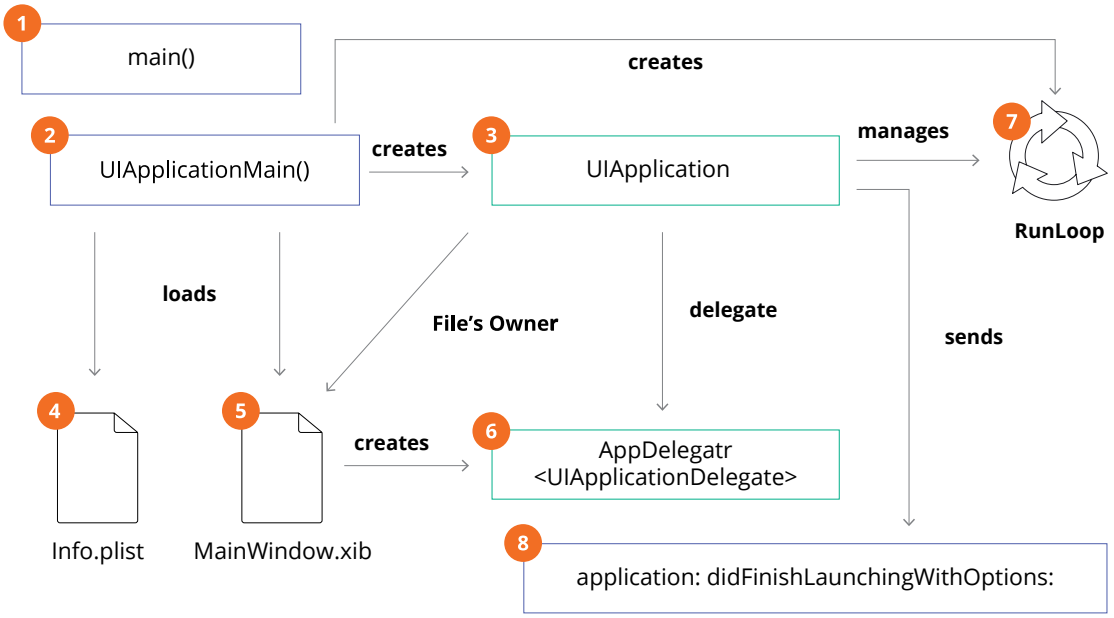
Project Description

The teams collaborated to perform a white-box application security assessment. SoftServe's security audit team included two certified ethical hackers and two software security architects. They performed a dynamic application analysis on Android and iOS as well as a static code review and found a number of security issues that needed to be addressed:

- Limited Cryptography
- Hardcoded test values and credentials
- Backend security
- Password brute-forcing
- Weak change user password mechanism
- Sensitive file artifacts and data

At the final stage of the security audit, SoftServe provided the client's development team with detailed technical recommendations on how to correct the identified security issues, which allowed them to remain on schedule and release the new application into production on time.





Value Delivered

The security audit, which took one week, allowed the client to:

- Quickly detect, analyze, and correct identified security defects
- Release its new mobile application as planned
- Protect the company brand and ensure sensitive client information was safe
- Prevent HIPAA penalties for data breaches—known as HIPAA Omnibus rule, which was enacted March 23, 2013. Penalties could cost up to $1.5 million per incident

ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation—from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience are built on a foundation of empathetic, human-focused design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy—No matter where you are in your journey.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.

NORTH AMERICAN HQ

Tel: +1 866 687 3588 (USA)
Tel: +1 647 948 7638 (Canada)

EUROPEAN HQ

Tel: +44 (0) 800 302 943

info@softserveinc.com
www.softserveinc.com

softserve