Case study

Park and Fly

Parkeon steers its applications to a secure spot

Industry
Travel and leisure

Objective
Improve security level for electronic payment processing systems, and ensure PCI-DSS compliance

Approach
Chose HP Fortify Software Security Center as application security partner, to analyze source code and provide real-time monitoring and protection for deployed applications

IT matters
- Makes application security an integral part of Parkeon's IT operations
- Finds and assesses potential vulnerabilities during Parkeon's software development processes
- Secures all applications throughout the entire software development lifecycle

Business matters
- Fosters an awareness of security risks and the need for remediation by educating Parkeon developers
- Supports creation of new security features and continues methods of locating vulnerabilities in Parkeon's production applications
- Delivers cost savings to Parkeon by finding vulnerabilities earlier

PARKEON

"Parkeon has clients all around the world who currently use our products to make and receive payments. The security of these electronic transactions is of paramount importance to us."

– Luc Porchon, Banking Applications Project Manager, Parkeon

Parkeon, one of the world's largest parking and transport management companies, provides end-to-end electronic payment solutions for its customers. While designing its latest electronic ticketing and transaction product, *ArchiPEL*, the company chose HP Fortify to assess potential vulnerabilities during the software development process and throughout the product lifecycle. With HP Fortify, application security is now an integral part of Parkeon's IT operations.

Parkeon is one of the world's largest parking and transport management solution providers. Headquartered in France, the company has operations in 40 countries, including the U.K., U.S., Australia, Belgium, Germany, Italy, and Spain. Its unique range of services and solutions, together with its constant ability to innovate over the last 35 years, has made Parkeon a leading player within its market. To date, it has developed over 150 software systems and processes 550,000 payment transactions per month while centrally monitoring 21,000 terminals.

Parkeon provides end-to-end electronic payment solutions from transaction processing at the point of sale (POS) through vendor payment by their customers' financial institutions. Parkeon's offerings are complemented by a full range of payment methods, including credit and debit cards, mobile phone accounts, and prepaid cards. These solutions are deployed on Parkeon's own POS terminals, such as parking meters at curbside and "pay and display" and "pay on foot" car parks.

Secure Payment Processing Integral to Parkeon

As a payment processor, Parkeon is very concerned about payment security. The recent annual Data Breach Investigation Report by U.S. mobile network provider Verizon revealed that 285 million records were compromised during 2008—a major increase from 230 million during each of the previous four years. These figures provided the motivation for Parkeon to raise its application security level system-wide, regardless of the diversity of its customers' geographic locations or the lack of adoption of payment security standards within some countries in which Parkeon operates.

Luc Porchon, banking applications project manager of Parkeon, explains further: "Parkeon has clients all around the world who currently use our products to make and receive payments. The security of these electronic transactions is of paramount importance to us, and therefore we closely monitor our payment systems to ensure a proven level of security. Our payment processing validates the integrity while maintaining the confidentiality of each user's personal data."

Parkeon Subject to PCI Security Standards

To protect the flow of sensitive customer data, the major global credit card issuers have come together in the Payment Card Industry Security Standards Council (PCI-SSC), an open and global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for card account data protection. Its mission is to enhance payment account data security by driving education and awareness of the PCI Data Security Standard (PCI-DSS).

PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. PA-DSS is the program to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2, or PIN data. PCI-DSS compliance is an industry-driven, not government, mandate. Only payment applications that are sold, distributed, or licensed are subject to the PA-DSS requirements. In-house payment applications developed but not resold to a third party are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI-DSS. As Parkeon provides a complete payment solution, it is subject to both PA-DSS and PCI-DSS certification of its software architecture.

Cutting Edge Technology – Guaranteed Flawless

When designing its latest state-of-the-art electronic ticketing and transaction product, ***ArchiPEL***, Parkeon knew it was essential that its developers build secure software from the earliest stages of the lifecycle. Thus these stringent processes ensured that *ArchiPEL*'s flawless code was free of known vulnerabilities, preventing hacking incidents or breaches.

"Security should not be seen as the icing on the cake, being added at the last minute to make an application attractive, but instead as the basic vital ingredient needed to ensure the success of the recipe and therefore incorporated right at the beginning," Mr. Porchon says. "HP Fortify's expertise

was engaged in May 2009, very early in our development process. They were the natural choice, being the application security and testing provider chosen by the U.S. government, the U.S. armed forces, many of the major banks such as ABN-AMRO and JP Morgan, and numerous Fortune 500 companies."

HP Fortify products protect companies from today's greatest security risk: the software applications that run their businesses. Any organization storing or processing credit card information must comply with the PCI-DSS or face the risk of losing card processing privileges with the major issuing brands. Specifically, HP Fortify software focuses on helping customers pass compliance audits of Section 6 of the standard, the critical set of requirements dealing directly with application security.

Parkeon selected HP Fortify Software Security Center, which enables an organization to conduct static analysis of an application's source code, dynamic analysis of a running application, and real-time monitoring and protection for a deployed application. No other vendor offers all three of these solutions in one integrated platform. For a company such as Parkeon trying to pass PCI-DSS compliance, HP Fortify offers dynamic security tests, code reviews, and an application layer firewall. HP Fortify's application security experts are at the cutting edge of software vulnerability research, tool development, and deployment practices.

Parkeon selected HP Fortify as its primary application security partner based on the company's ability to reduce risk by employing analysis and remediation solutions that can:

1. Specify the vulnerabilities within the software so the development organization can eliminate them prior to deploying the application into production.

2. Implement a continuous review by testing and verifying the code for security vulnerabilities introduced during development. Mr. Porchon notes, "The specialists at HP Fortify helped us establish development best practices based on the analysis of our architecture and code base. Then we set up the production environment and ongoing verification processes."

3. Incorporate security into Parkeon's preferred integrated development environment.

4. Build in security gates to prevent applications with vulnerabilities from ever going into production. This requires finding and addressing vulnerabilities, as they are located.

5. Track metrics to gauge the success of the security plan so that the organization can continually improve the process.

For three months, HP Fortify provided professional services to Parkeon to ensure its success with HP Fortify Software Security Center, checking and scrutinizing its *ArchiPEL* software to ensure that it passed the stringent requirements expected from the latest PCI-DSS and PA-DSS standards. HP Fortify Static Code Analyzer (SCA) software quickly and easily checked all source code, testing and revealing critical, potentially hazardous vulnerabilities. HP Fortify trained Parkeon's development team to prioritize their work and helped to seal those vulnerabilities that hackers most commonly target.

> "This partnership has been essential in getting our product to market on time while ensuring it meets stringent compliance standards such as PCI-DSS and PA-DSS."
>
> —Luc Porchon, Banking Applications Project Manager, Parkeon

"Using HP Fortify's expertise to test our software at the code development stage and again at various stages in its deployment, we uncovered flaws and then successfully removed them. This partnership has been essential in getting our product to market on time while ensuring it meets stringent compliance standards such as PCI-DSS and PA-DSS," summarized Mr. Porchon. "HP Fortify has helped us to establish secure development best practices based on its analysis of our software security architecture and application code. We will continue to use HP Fortify software to test all our software throughout its lifecycle to ensure it is secure at all times."

Parkeon is on target to move quickly through the next PCI-DSS audit process, which will test that their latest innovative and cutting edge payment systems are secure for the customers waiting to use them. In partnership

with HP Fortify, Mr. Porchon remains confident that future secure payment applications will go to market on time and on budget.

Mr. Porchon believes that managing software security risk is a cost of doing business. "A quick estimate of the costs incurred by one instance of compromised data, coupled with the interests of an attacker, provides a sobering quantification of risk. Indeed, the risk is mainly financial, including repair to a compromised image or brand plus any penalties imposed by the PCI governing body offending bank plus any recovery of damages to other players such as the carrier and issuing banks."

About Parkeon

Parkeon is one of the world's largest parking and transport management solution providers. Headquartered in France, the company has operations in 40 countries. Parkeon provides end-to-end electronic payment solutions from transaction processing at the point of sale through vendor payment by the customers' financial institutions.

About HP Enterprise Security:

HP is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats. Visit HP Enterprise Security at: hpenterprisesecurity.com.

Customer at a glance:

Applications
Solutions for parking and transport management

Software
- HP Fortify Software Security Center
- HP Fortify Static Code Analyzer

HP Services
- Ongoing technical support

4AA3-7467ENW, October 2013, Rev. 1