# PEACH FUZZER™

# DISCOVERING UNKNOWN VULNERABILITIES IN EMV TERMINALS

## Peach Fuzzer Helps EMV Terminal Manufacturers Close Security Loopholes

Chip-enabled (EMV) credit cards are touted as the way to end credit card fraud and brand damaging attacks like those of the Target, Home Depot, and Wendy's incidents.[1,2,3] The EMV-ready terminals aim to provide enhanced security to card transactions. This paper provides a testing platform to examine these claims.

EMV cards store payment information on a chip containing a microprocessor rather than on a magnetic stripe. To successfully complete a chip-enabled transaction, a series of sophisticated cryptographic transactions takes place between the card, terminal, and back end. This ensures the authenticity of both card and cardholder.

In October 2015, a liability shift occurred in the U.S., making point-of-sale (POS) and ATM merchants liable for fraud that occurred when they didn't provide EMV-ready terminals to their customers.[4] Preceding this shift, banks and merchants began updating their infrastructure to support EMV cards and terminals. By the end of 2015, over 400 million EMV credit cards were in circulation in the U.S., accepted at roughly 17% (675,000) of credit card terminals.[5,6] Billions of dollars in brand equity rely on secure credit card transactions.

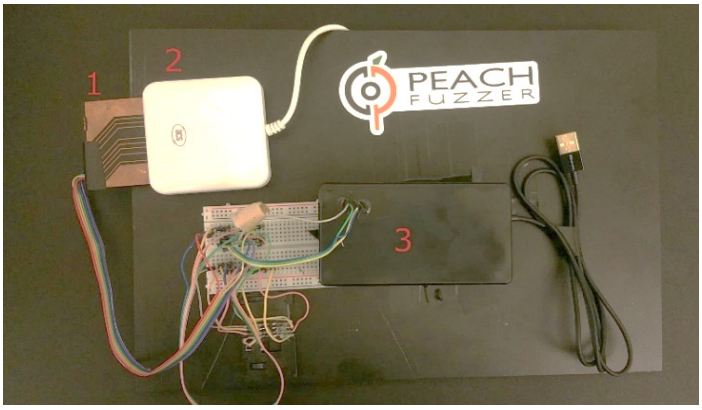
Our experience is that industry leaders – issuers of credit cards, POS terminal manufacturers, and merchants relying on POS transactions – are keen to protect their company's brand equity by ensuring their data is secure. Recognizing the breadth and complexity of the EMV system at large, these leaders require solutions that are economically feasible and scalable in order to identify vulnerabilities before hackers do.

## Peach Fuzzer's Testing Solution

Testing the security of EMV solutions is business critical for many organizations. Researchers, using Peach Fuzzer, were able to find multiple cases in which malicious credit cards were able to compromise EMV terminals. Discovering these exploitable vulnerabilities enabled solution providers to mitigate their vulnerabilities quickly and cheaply, before they became a hacker's attack vector.

Peach Fuzzer is a scalable security testing platform which discovers unknown vulnerabilities in the hardware and software systems across a wide range of industries. Organizations leverage Peach Fuzzer to produce secure, high-quality solutions, and test the quality of third-party products. Peach Fuzzer was used for this effort for its ability to test custom protocols and its robust monitoring features. It helped researchers efficiently find vulnerabilities in EMV terminals.

Researchers used two different setups during their testing. First, they tested physical terminal hardware using the setup pictured to the right. Second, they tested software using multiple EMV terminal emulators.




1. Malicious Credit Card
2. EMV Payment Card or Smart Card Reader
3. FPGA Simulating EMV Protocol Bridges to Peach

1 http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/
2 http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282
3 http://time.com/money/4196058/wendys-hack-fraudulent-charges/
4 http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf
5 http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264/
6 http://www.emv-connection.com/emv-faq/



1-844-55-PEACH | sales@peach.tech
www.peach.tech

Peach Fuzzer was effective at finding vulnerabilities in EMV solutions due to four key Peach features:

- **Advanced state machine modelling** – leveraged to find complex issues in state logic
- **Test case automation** – enabled teams to run hundreds of thousands of test cases quickly
- **Extensibility of custom monitoring** – used to capture valuable data about vulnerabilities
- **Integration with Jenkins/Jira** – utilized by developer teams to integrate with build systems

## Advanced State Machine Modeling

Peach Fuzzer's advanced state machine modelling ability allowed it to behave like an authentic credit card, which tricked the EMV terminals into allowing access to their systems. At this point, Peach was free to launch hundreds of thousands of test cases in which malformed data was sent at the terminal. This fuzzed data caused several potentially exploitable crashes. Advanced modelling of the EMV protocol enabled researchers to attack the terminals at a level other security tools could not, allowing manufacturers to create more secure systems.

## Test Case Automation

Fuzz testing the EMV terminals through a physical terminal established that malicious cards could be used to exploit vulnerabilities. Peach Fuzzer's unique value was its ability to automate test cases. Researchers modelled the custom EMV protocol, enabling them to run multiple terminal emulators concurrently. Testers avoided the capital and time-intensive process of manually testing the setup, allowing for more test cases over a condensed testing period. Our analysis shows that Peach automation allowed the research team to run more an order of magnitude on more test cases when compared to manual assessments.

## Extensibility of Custom Monitoring

The custom monitoring features which come with the Peach Fuzzer platform allowed security testers to create monitors specific to the EMV terminal. Peach's advanced monitoring captured valuable crash data and enabled device manufacturers to quickly locate and fix bugs in their products. Other fuzz testing tools would have only indicated that the terminal had failed.

## Integration with Jenkins and Jira

Security testers utilized Peach Fuzzer's ability to integrate with Jenkins and Jira build systems throughout their research. Testers configured Jenkins to run a new Peach Fuzzer session every time the EMV terminal's code base was updated. This enabled the team to build and test their software continuously, ensuring each build was as secure as the last. Peach Fuzzer also integrated with Jira, creating and logically grouping tickets for engineers when new bugs were found.

## Findings

Throughout testing of the EMV terminals, Peach Fuzzer found that malicious credit cards could be used to compromise EMV terminals. Three major categories of vulnerabilities were discovered:

- **Memory Corruption** – Allows attackers to read and write memory and crash the reader
- **Denial of Service** – Renders the unit unusable to POS vendors or their customers
- **Arbitrary Code Execution** – Enables attackers to define and run their own code on the terminals

---

*"Peach found crashes that would cause the readers to be directly compromised if given a malicious credit card."*

– Adam Cecchetti, Lead Researcher

---

In one test case, a spoofed card was created to match all of the physical specifications of an EMV card. This card was put into an EMV terminal, connected to a field programmable gate array (FPGA) which simulated the EMV protocol, and then connected to Peach. This allowed Peach Fuzzer to trick the terminal into thinking a real card was being used, granting access to its systems.

Compared to alternate methods of security assessment, Peach Fuzzer had three primary advantages:

- **Speed and Coverage** – Over half a million test cases run quickly, which would take months using manual testing
- **Complexity of Findings** – Custom monitors allowed for valuable data capture
- **Repeatability** – Scalability of testing and integration with Jenkins enabled testing of each new software build

# Conclusion

The security of EMV transactions are crucial to many solutions' viability, reputation, and competiveness. This project successfully demonstrated the flexibility and effectiveness of Peach Fuzzer as a security testing platform for EMV solutions. The Peach Fuzzer platform can help solution providers ship secure EMV solutions.