## Feature List

### Core features

- Automated security testing
- Fuzzing – systematically generates security-relevant test vectors by manipulating correct input
- Different message format support – XML, ASN.1 DER, text, custom binary
- Reactively iterating test algorithms – Observe the previous reactions of the ToE
- Generic test plug-ins – reusable test algorithms for typical bugs
- Cryptographic & encoding support – encryption, digital signatures, and compression methods
- Protocol state machine – based on UML statecharts
- Automatic test report generation – easy-to-navigate HTML output

### Modes of operation

- Man-in-the-middle black-box testing
- Source-code-based testing with fault injection

### Typical security-relevant bugs

- Buffer overflow
- Integer overflow
- Signedness bug
- Widthness bug
- Encoding bugs
- Inappropriate certificate handling

### Supported platforms

- Windows, Linux, Symbian
- x86, ARM
- Various network and security protocols

Flinder

*We make your software secure*

SEARCH

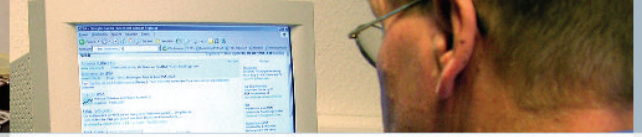
SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

FLINDER
www.flinder.hu
info@flinder.hu

phone/fax: +36-1-205-3098
Infopark 1. Budapest 1117, Hungary

Flinder





Security Testing

## What is Flinder?

Flinder is an automated security testing tool that discovers typical security-relevant programming bugs. Flinder can detect potential vulnerabilities of the evaluated product by generating and executing a vast number of special test vectors.

## High danger of security bugs

- Exploitable security vulnerabilities
- Virus spreading
- Spamming and phishing
- Credit card fraud

## Benefits of Flinder

- Greater test coverage
- Better customer satisfaction through improved security
- Risk mitigation due to the eliminated security flaws
- Increased overall dependability and quality of software components

## Application areas

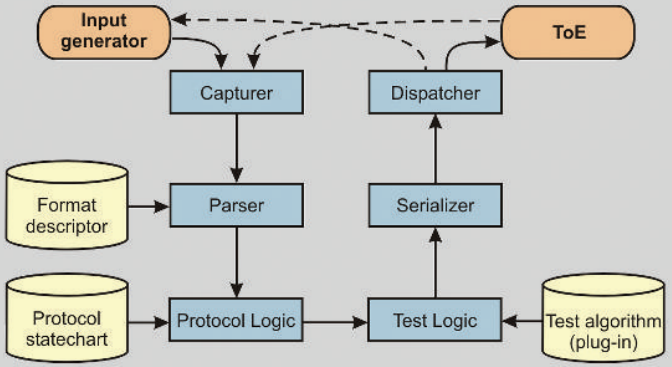
- Web applications
- Security protocols
- Operating systems
- Network protocols
- Embedded systems
- Critical infrastructures

## All your security testing needs

- We offer complete audit and security testing services

## Black-box security testing

Flinder operates as a man-in-the-middle between the Target of Evaluation (ToE) and the Input Generator. Flinder intercepts and modifies the messages of the communication flow. The reactively iterating test algorithms observe the ToE's reaction to the altered messages and generate the next test vectors accordingly.




## Fuzzing with Flinder

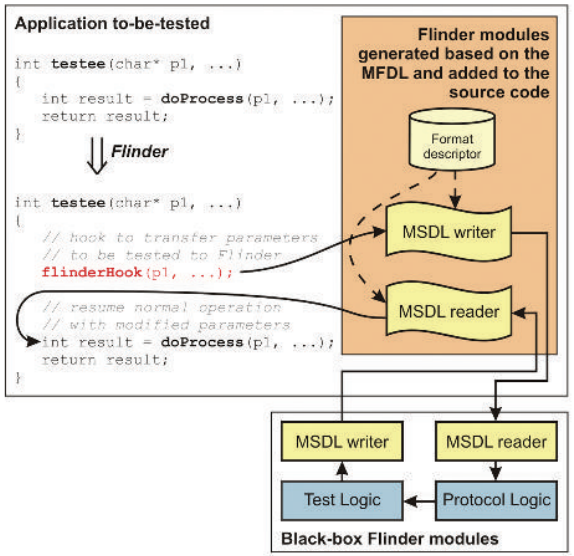
1. Input Generator sends a correct input message towards the ToE
2. Capturer intercepts the binary message
3. Parser translates the binary data into a generic internal structure (MSDL) using a customizable message format description (MFDL)
4. Protocol Logic executes a UML statechart-defined state machine that follows the state transitions of the network protocol
5. Test Logic supports generic, plug-in test algorithms which can generate test vectors by altering the interpreted MSDL message structures
6. Serializer transforms the internal MSDL back to the protocol specific binary representation
7. Dispatcher delivers the binary test vector to the ToE and observes the reaction of it (normal response, timeout, overload, crash, etc.) to detect signs of security weaknesses

## Source-code-based testing

Flinder can also execute a more effective fault injection based security testing when source code is available. In this mode Flinder can apply its fuzzing algorithms not just to input messages, but to parameters of internal function calls or even to internal memory structures, resulting in a deeper and more effective function-level security testing.

## Fault injection with Flinder

1. Structures and functions to be tested are annotated in the ToE's source-code
2. Flinder semi-automatically generates the message format descriptions (MFDL) for the given data structures and function parameters
3. Special hooks are injected into the source code, with which Flinder is able to access and modify the internal data structures
4. Flinder starts the ToE and injects test vectors via the hooks during execution.
5. Unintended behavior potentially leading to security weaknesses is detected and reported




System Overview