(K)ERIS: A Novel Approach for API Security Testing, Applied to the System Call Interface of the Linux kernel

Dimitris E. Simos, Bernhard Garn

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research
MATRIS

Combinatorial Designs meet Software Testing and Information Security

Motivation

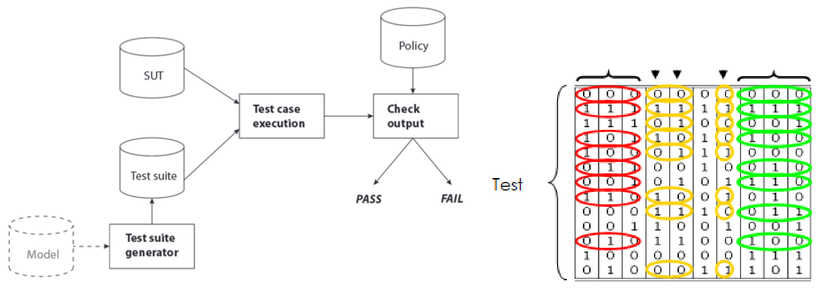
- We cannot test everything.
- Exhaustive search of problem space increases time needed exponentially.
- Automated detection of security vulnerabilities.

Combinatorial Security Testing (CST)

- Parameters and values provide abstract models of attacks.
- Generated test sets provide 100% coverage of t-way parameter value combinations.
- Automated test set generation, execution and evaluation via dedicated test oracle.

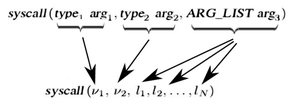
Technical Challenges

- Generation of minimal t-way test sets is a hard combinatorial optimization problem.
- Modelling of parameters, values and constraints is domain-specific.
- Deploy CST to all application layers of information security.



Combinatorial API Testing

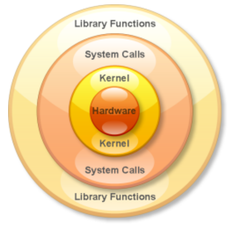
- **Focus:** Test APIs function calls of software / libraries.
- **Modeling:** Combinatorial models:
  - IPM via equivalence- and category partitioning
  - IPM via novel flattening methodology
- **ERIS:** Highly configurable testing framework encompassing CT, execution environment, logging and database infrastructure.



Abstr. Parameter	Parameter values
ARG_CPU	1, 2, 3, 4, ..., 8
ARG_MODE_T	1, 2, 3, 4, …, 4095, 4096
ARG_PID	-3, -1, $pid_cron, $pid_w3m, 999999999
ARG_ADDRESS	null, $kernel_address, $page_zeros, $page_0xff, $page_allocs, …
ARG_FD	fd_1, fd_2, fd_3, ..., fd_{15}
ARG_PATHNAME	$pathname_1$, $pathname_2$, $pathname_3$, ..., $pathname_{15}$

ERIS: Combinatorial Kernel Testing

- **Focus:** Reliability and quality assurance of kernel software.
- **Motivation:** Kernel is the central authority to ensure security.
- **SUTs:** System calls of every git-commit of any (variant of) Linux.
- **Evaluation**: Various kernel crashes for RCs and distribution kernels.



Large-Scale Kernel Testing

Case Study

- Total of 3082 systems-under-test:
  - 23 different system calls
  - 134 kernel versions
- Kernel versions tested in the range of v4.0 up to v4.6:
  - The final releases
  - All release candidates
  - A selection of stable releases
- 102h execution time.

Evaluation via Differential Testing

- Compare number of accepted vs rejected system calls between versions.
- Mostly stable behaviour between versions.
- Largest deviations in the **settimeofday** system call:

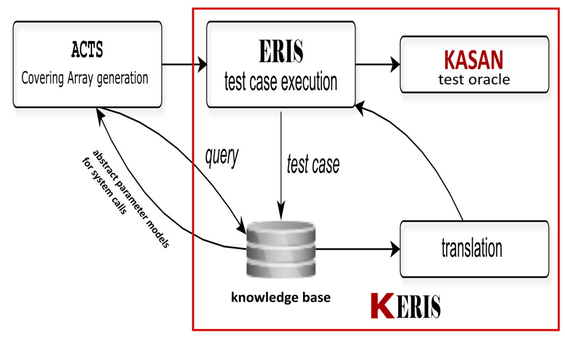
Count kernel versions	# of test cases	# of accepted	# of rejected
72	100	0	100
43	100	45	55
15	100	30	70
1	100	34	66

Evaluation via Kernel Address Sanitizer (KASAN)

- Test oracle uses internal dynamic memory error detector of Linux.
- Fine-tuned combinatorial model of a network configuration setup.
- Demonstrated reproducibility of vulnerability in the **sendto** system call.

Automated Test Execution Framework

- **Ease of use:** Only high-level parameters needed, everything else handled by the system.
- **Test-runs:** Each invocation runs in a dedicated virtual machine.
- **Logging:** Extensive information is captured:
  - Adjustable to user demands / needs
- **Database:** Allows sophisticated post-processing queries.



Vision

- **Goal:** Extend approach.
- **Modeling**: Optimization and automation of testing.
- **Automated t-way testing** and translation layers.
- Testing of **security patches** to ensure attack-free environments.
- **Continuous integration** tests of kernel versions.
- Web **monitoring platform**.

S	W	Name ↓	Last Success	Last Failure	Last Duration
		Project F cubicCoins	20 hr - #106	27 days - #71	9.2 sec
		Project I Entrepreneur Sim	26 days - #30	26 days - #29	10 sec
		Project J Sports	8 hr 7 min - #98	15 days - #81	1 min 7 sec
		Project Team C Gamers	21 hr - #93	17 days - #72	48 sec
		Project Team D Gamers	1 hr 10 min - #68	N/A	1.2 sec
		Project X thefailedandthefurious	5 days 20 hr - #113	20 hr - #123	39 sec

B. Garn and D.E. Simos. Eris: A Tool for Combinatorial Testing of the Linux System Call Interface. In *Software Testing, Verification and Validation Workshops (ICSTW), 2014 IEEE Seventh International Conference on*, pages 58–67, March 2014.
Bernhard Garn, Fabian Würfl, and Dimitris E. Simos. Keris: A ct tool of the linux kernel with dynamic memory analysis capabilities. In Ofer Strichman and Rachel Tzoref-Brill, editors, *Hardware and Software: Verification and Testing*, pages 225–228, Cham, 2017. Springer International Publishing.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.