5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection

Zujany Salazar, Huu Nghia Nguyen, Wissam Mallouli, Ana R. Cavalli, Edgardo Montes De Oca

Montimage, France

August 2021

Outline

1. Introduction
2. Background
3. Architecture
4. Experimental Evaluation
   - Malformed packets against open-source 5G cores in real-time
   - NAS-5G SMC Replay attack
   - High-bandwidth traffic generation
5. Conclusion
   - Future works

Introduction: 5G key enabling technologies

1. Software defined networks (SDN)
2. Network functions virtualization (NFV)
3. Mobile Edge computing (MEC)
4. Network Slicing (NS)

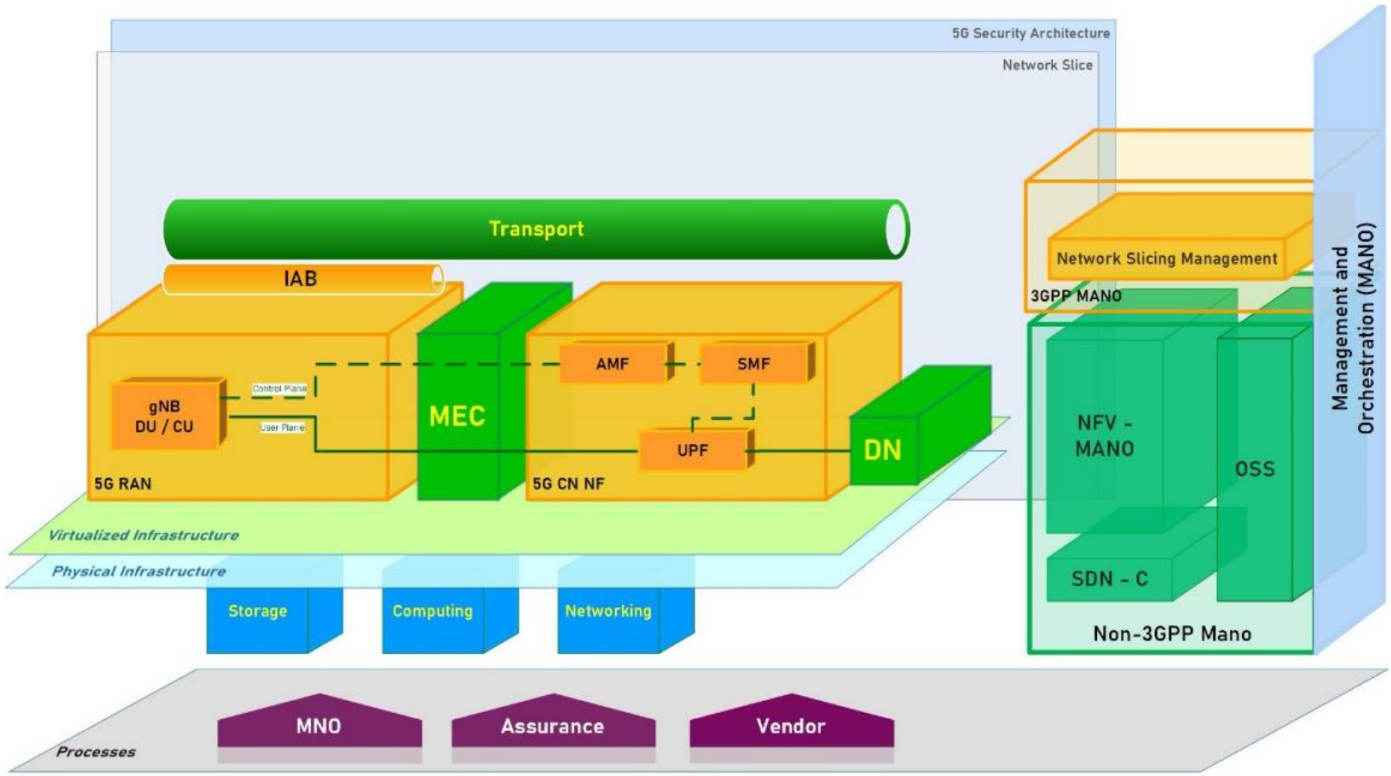


Figure 1: 5G Architecture by ENISA [5]

Introduction: 5G Security Challenges

- 5G new technologies require to be **tested** from a **functional** and **non-functional**

Introduction: 5G Security Challenges

- 5G new technologies require to be **tested** from a **functional** and **non-functional**
- **New** cybersecurity threats

Introduction: 5G Security Challenges

- 5G new technologies require to be **tested** from a **functional** and **non-functional**
- **New** cybersecurity threats
- Previously adopted security and privacy **mechanisms** become **ineffective**[3]

Introduction: 5G Security Challenges

- 5G new technologies require to be **tested** from a **functional** and **non-functional**
- **New** cybersecurity threats
- Previously adopted security and privacy **mechanisms** become **ineffective**[3]

This requires...

The creation of **new sets of security test cases** and **tools** specifically targeting 5G security concerns

SoA: Testing the 5G

<table>
<tr><th>Threat and vulnerability reports</th><th>Security test cases</th><th>Application</th></tr>
<tr><td>ENISA [5]</td><td rowspan="2">3GPP Catalogue of General Security assurance requirements [1]</td><td>Python Scapy</td></tr>
<tr><td>3GPP [1]</td><td>Tcpreplay</td></tr>
<tr><td>Academic research [3, 4]</td><td rowspan="2">3GPP 5G Security Assurance Specification of the AMF [2]</td><td rowspan="2">5Greplay</td></tr>
<tr><td>Industrial reports [7, 6]</td></tr>
</table>

Table 1: Testing in 5G previous works

Challenge: The testing of 5G network components and IDSs

5Greplay

An **open-source** solution to perform **fuzz testing of 5G networks**, allowing to forward network packets from one NIC to another with or without modifications.

http://5greplay.org

Outline

1. Introduction
2. Background
3. Architecture
4. Experimental Evaluation
   - Malformed packets against open-source 5G cores in real-time
   - NAS-5G SMC Replay attack
   - High-bandwidth traffic generation
5. Conclusion
   - Future works

5Greplay atomic operators

Definition

Let **P** denote a **5G network packet** in a PCAP file or a specific real-time flow of network packets. **5Greplay** performs **fuzz testing** in 5G VNFs, IDSs, apps, etc, relying in the following operators...

Atomic operator	Description
DEL_PKT(*P*)	Delete a packet
CH_ATTR(*P*)	Change a specific attribute of a message header
ORD(*P1, P2*)*	Exchange the order of two consecutive packets
DUP_PKT(*P*)	Duplicate packet

Table 2: 5Greplay atomic operators. *Currently not implemented

Outline

1. Introduction
2. Background
3. Architecture
4. Experimental Evaluation
   - Malformed packets against open-source 5G cores in real-time
   - NAS-5G SMC Replay attack
   - High-bandwidth traffic generation
5. Conclusion
   - Future works

General Architecture

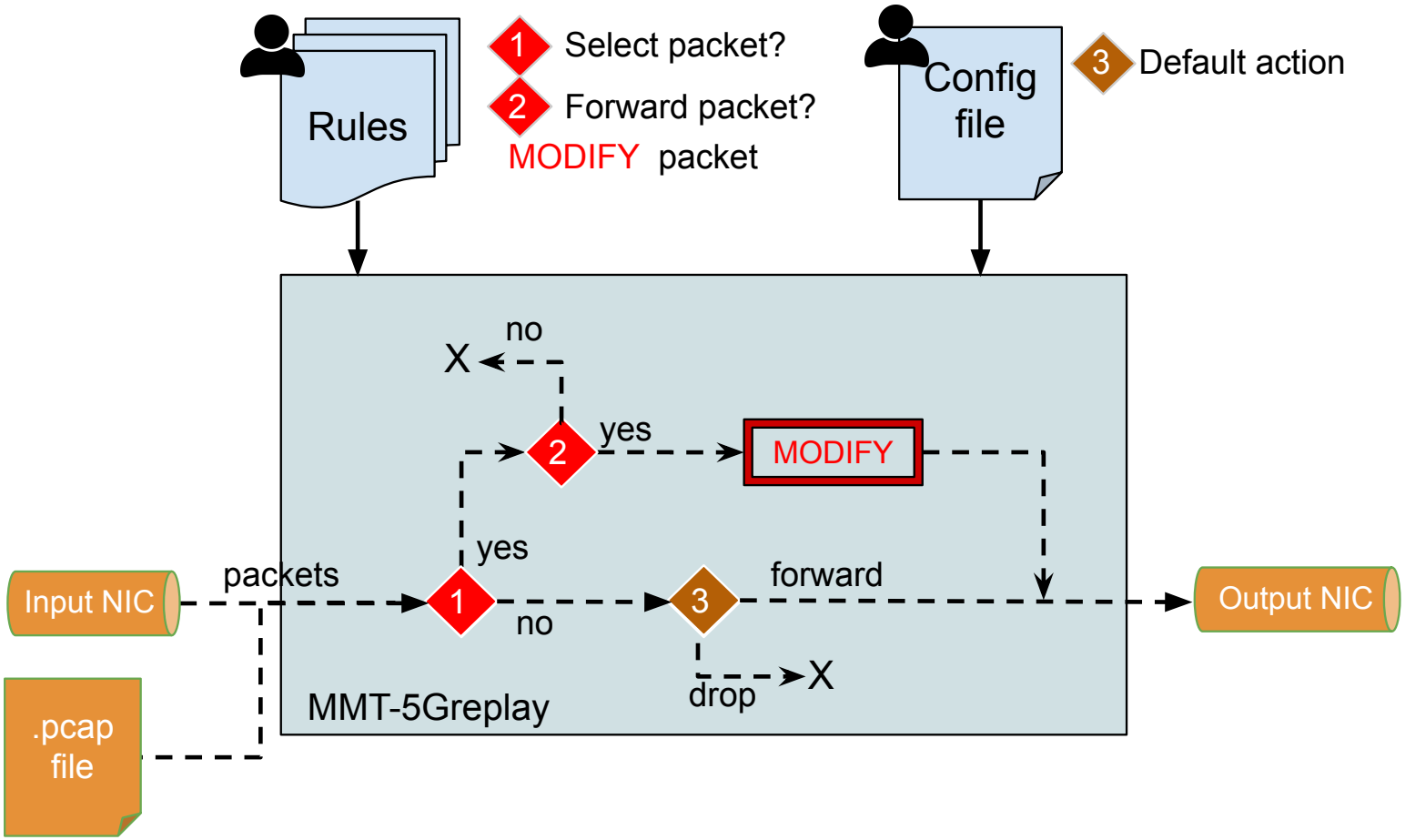


Figure 2: 5Greplay main process. Incoming network packets are filtered according to predefined rules that determine which packets will be modified, forwarded, or dropped before being sent to the output NIC

Outline

1. Introduction
2. Background
3. Architecture
4. Experimental Evaluation
   - Malformed packets against open-source 5G cores in real-time
   - NAS-5G SMC Replay attack
   - High-bandwidth traffic generation
5. Conclusion
   - Future works

Scenario 1: Sending malformed packets against open-source 5G cores in real-time

Objective

Create and **send malformed packets** to a 5G core network, to evaluate robustness against unexpected entries at run-time.

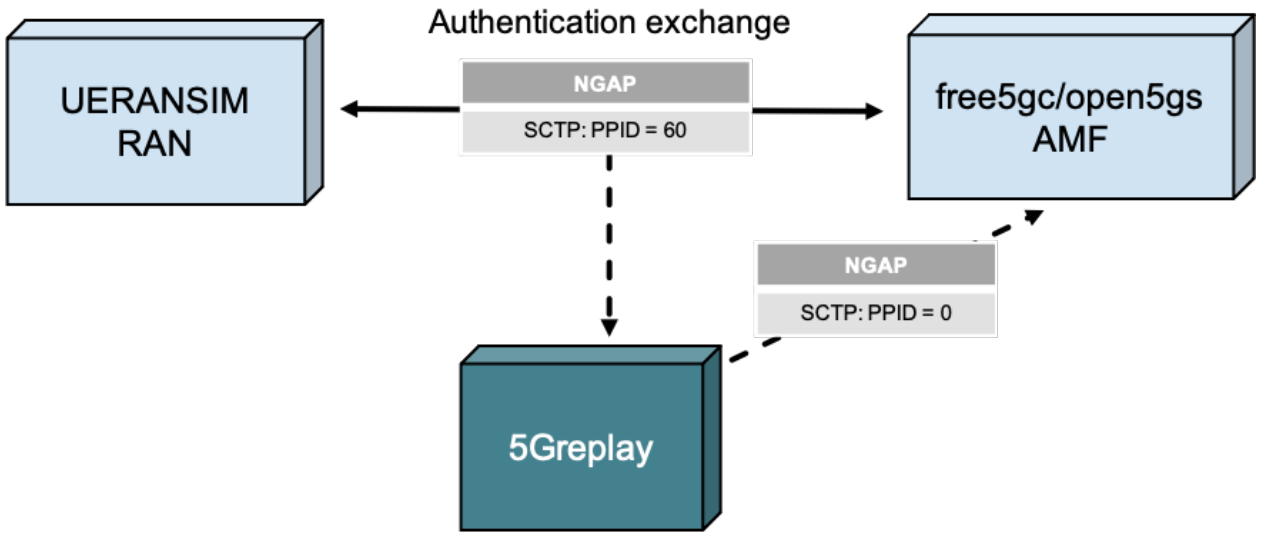


Figure 3: Sending malformed NGAP packets against free5GC

Scenario 1: Sending malformed packets against open-source 5G cores in real-time

Evaluation of 5G core simulators

- **free5GC** show an AMF warning, but the simulator keep running and allowed new UE connections
- **Open5GS** was not able to handle this packet and the simulator crashed

```
05/12 17:23:47.069: [gmm] INFO: [suci-0-901-70-0000-0-0-0000000001]    SUCI (../src/amf/gmm-handler.c:72)
05/12 17:23:47.069: [amf] WARNING: GUTI has already been allocated (../src/amf/context.c:1045)
05/12 17:23:47.070: [gmm] ERROR: Invalid service name [nudm-sdm] (../src/amf/gmm-sm.c:625)
05/12 17:23:47.070: [gmm] WARNING: gmm_state_authentication: should not be reached. (../src/amf/gmm-sm.c:626)
05/12 17:23:47.070: [core] FATAL: backtrace() returned 9 addresses (../lib/core/ogs-abort.c:37)
/usr/bin/open5gs-amfd(+0x17418) [0x55f750b1d418]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x16) [0x7ff86bb4ec76]
/usr/bin/open5gs-amfd(+0x1bb4e) [0x55f750b21b4e]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x16) [0x7ff86bb4ec76]
/usr/bin/open5gs-amfd(+0x5ec6) [0x55f750b0bec6]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(+0xd718) [0x7ff86bb46718]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x76db) [0x7ff869f416db]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x3f) [0x7ff869c6aa3f]
Open5GS daemon v2.2.7
```

Figure 4: open5GS AMF log when receiving a malformed NGAP packet

Scenario 1: Sending malformed packets against open-source 5G cores in real-time

Evaluation of 5Greplay

Replay and **modify** 5G network packets in a **online way** by using the fuzz operator CH_ATTR(P).

Scenario 2: NAS-5G SMC Replay attack

Objective

Perform **security tests** by modifying and injecting network traffic into a specif target. Test proposed in the **3GPP TS33.512** [2].

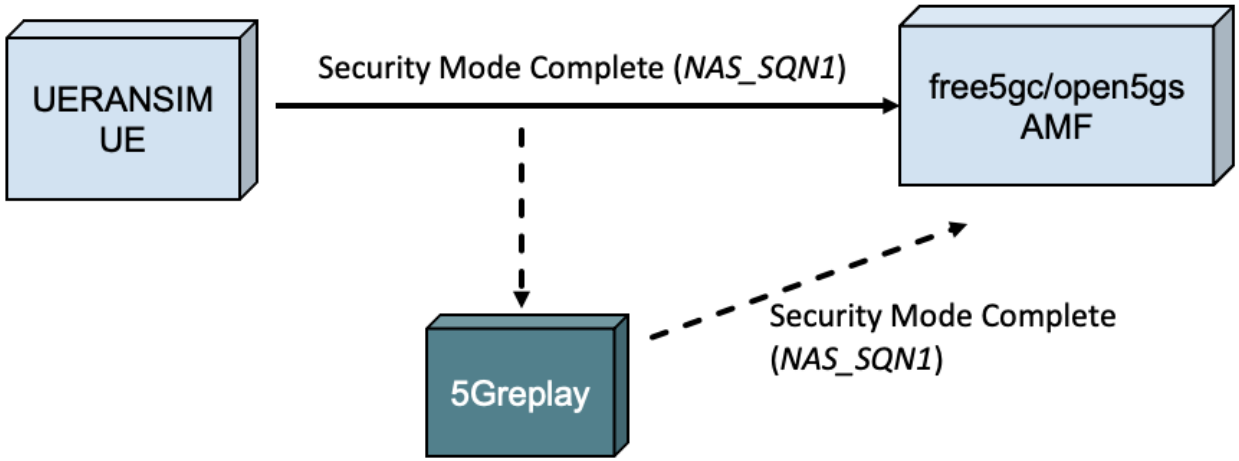


Figure 5: Sending malformed NGAP packets against free5GC

Scenario 2: NAS-5G SMC Replay attack

Evaluation of free5Gc

The AMF identified the replayed packets as not belonging to the same NGAP security context. **free5Gc** AMF **passed** the test.


```
2021-05-19T08:40:28-07:00 [INFO][AMF][GMM][AMF_UE_NGAP_ID:7][SUPI:imsi-208930000000003] Send Security Mode Command
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4:35118][AMF_UE_NGAP_ID:7] Send Downlink Nas Transport
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4:35118] Handle Uplink Nas Transport
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4:35118][AMF_UE_NGAP_ID:7] Uplink NAS Transport (RAN UE NGAP ID: 2)
2021-05-19T08:40:28-07:00 [INFO][AMF][GMM][AMF_UE_NGAP_ID:7][SUPI:imsi-208930000000003] Handle Security Mode Complete
2021-05-19T08:40:28-07:00 [INFO][AMF][GMM][AMF_UE_NGAP_ID:7][SUPI:imsi-208930000000003] Handle InitialRegistration
2021-05-19T08:40:28-07:00 [INFO][NRF][DSCV] Handle NFDiscoveryRequest
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP] Create a new NG connection for: 192.168.49.4/172.16.151.12/10.45.0.1:49183
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] Handle Uplink Nas Transport
2021-05-19T08:40:28-07:00 [ERRO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] No UE Context[RanUeNgapID: 2]
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] Handle Uplink Nas Transport
2021-05-19T08:40:28-07:00 [ERRO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] No UE Context[RanUeNgapID: 2]
```

Figure 6: Free5Gc AMF log when replaying Security Mode Complete messages (SMC)

Scenario 2: NAS-5G SMC Replay attack

Evaluation of 5Greplay

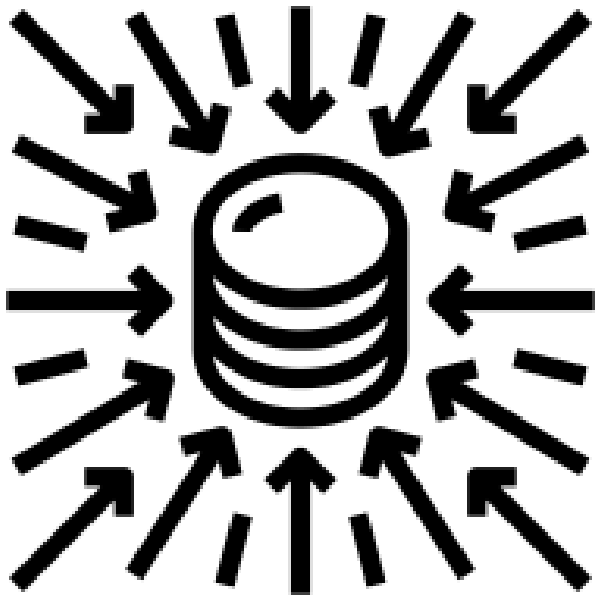
We tested the utility of 5Greplay to perform standardized security tests by using the fuzz operator CH_ATTR(P).

Scenario 3: High-bandwidth traffic generation

Objective

Scalability of 5Greplay[a]. **DoS attacks or stress tests** on open5GS and free5GC.

[a] while using only one thread on a Intel Ethernet Network Adapter X710



Scenario 3: High-bandwidth traffic generation

Evaluation of 5G core simulators

	#packet copies	Avg. packets/s	Avg. kbit/s
open5Gs	1780	509.5	834
free5GC	3000	594.9	974

Table 3: Endurance of 5G AMF services against traffic replaying

Scenario 3: High-bandwidth traffic generation

Evaluation of 5Greplay

5Greplay can be used to test the robustness of 5G core services by using in the fuzz operator DUP_PKT(P).

Outline

1. Introduction
2. Background
3. Architecture
4. Experimental Evaluation
   - Malformed packets against open-source 5G cores in real-time
   - NAS-5G SMC Replay attack
   - High-bandwidth traffic generation
5. Conclusion
   - Future works

Conclusion

The tool is capable to...

- Receive online and offline entries
- Systematically create and send malformed packets that are accepted by 5G simulators
- Evaluate the robustness against unexpected entries of a target
- Perform 5G security test cases
- Stress testing a target

Future works

- Defining new 5G attacks that can be performed by the tool
- Techniques to manage encrypted traffic
- Implement and test new ways to alter packets, such as changing the order of two packets
- Experimental evaluation will be performed on other 5G interfaces

Acknowledgments

This research is supported by the H2020 projects SANCUS N° 952672, INSPIRE-5Gplus N° 871808.

Thanks
Q&A

References

T. 3rd Generation Partnership Project (3GPP).

3gpp ts 33.117 – catalogue of general security assurance requirements, 2020.

T. 3rd Generation Partnership Project (3GPP).

3gpp ts 33.512 – 5g security assurance specification (scas); access and mobility management function (amf), 2021.

I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov.

Overview of 5g security challenges and solutions.
IEEE Communications Standards Magazine, 2(1):36–43, 2018.

D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler.

A formal analysis of 5g authentication.
In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1383–1396, New York, NY, USA, 2018. Association for Computing Machinery.

ENISA.

Enisa threat landscape for 5g networks, Feb 2021.

Ericsson.

A guide to 5g network security. conceptualizing security in mobile communication networks – how does 5g fit in?, 2018.

S. Valenti, D. Rossi, A. Dainotti, A. Pescapè, A. Finamore, and M. Mellia.

Reviewing Traffic Classification, pages 123–147.
Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.