PSI 2001

Perspectives of Systems Informatics

TECHNISCHE UNIVERSITÄT MÜNCHEN

Specification-Based Testing of Firewalls

Guido Wimmel
Software & Systems Engineering
Technische Universität München

(with Jan Jürjens, University of Oxford)

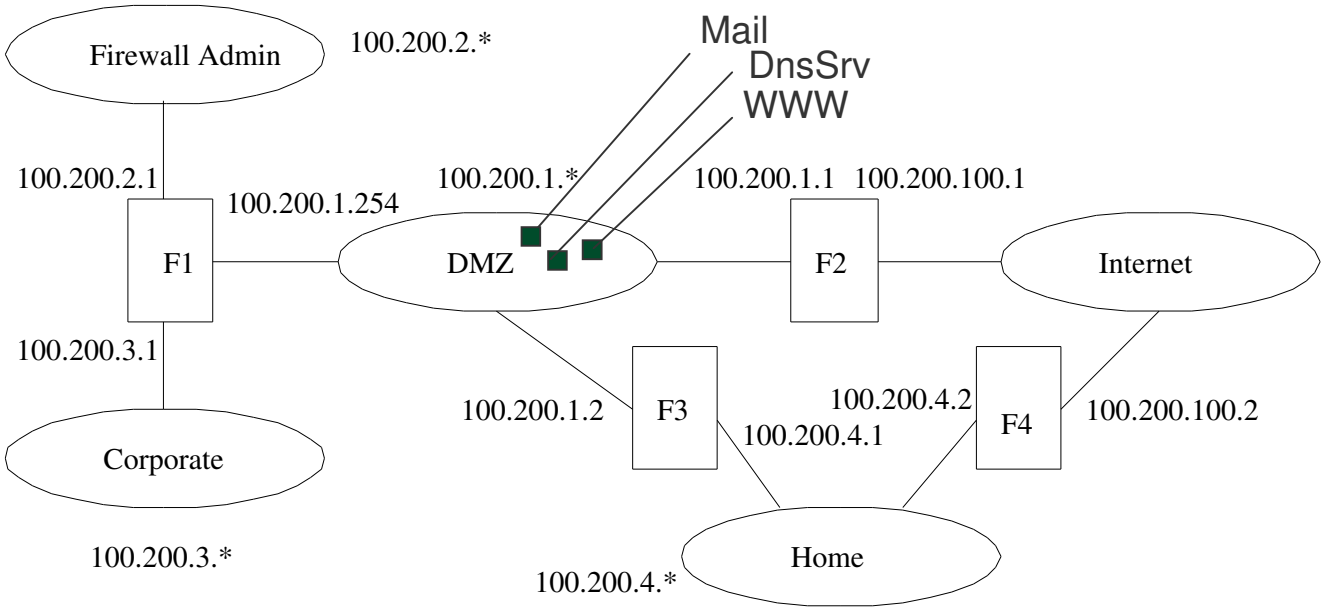
Overview

- Security and Firewalls
- AutoFocus
- Formal Model of Firewall System
- Specification Based Testing
- Test Cases for Firewall System
- Conclusion / Further Work

Security and Firewalls

- Increasing connection of businesses via the Internet facilitate attacks on vulnerabilities of internal hosts
- $\Rightarrow$ Firewalls for protection of the network
- Correctness of the security measures is crucial
  - A single weakness can compromise the whole system
  - Very high potential damage
  - However, few systematic approaches to ensure correctness
- Approach
  - General formal model of the network and firewall system using a CASE tool
  - Systematic, specification-based testing to provide confidence

Network with Firewalls

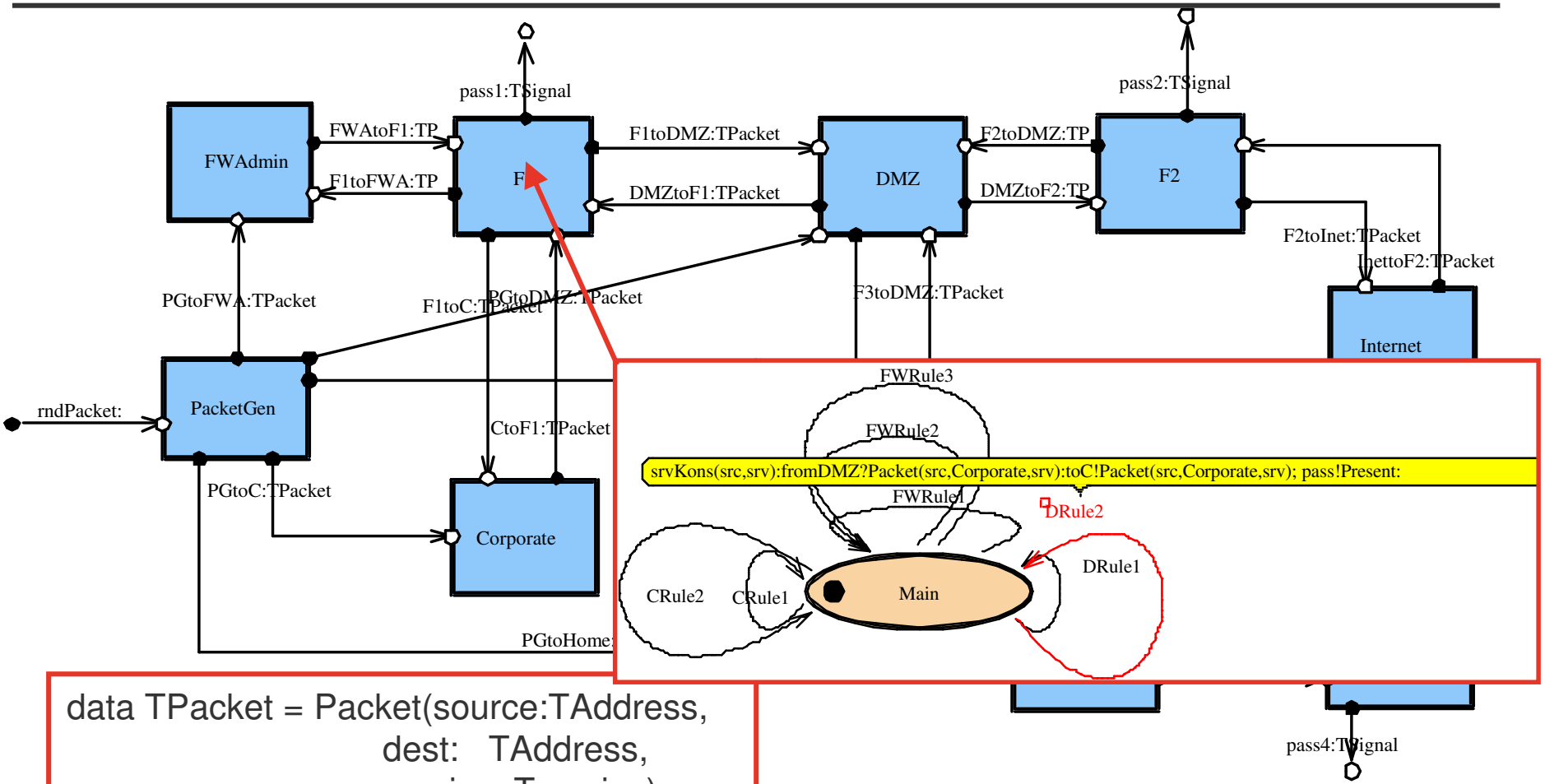


- Firewalls implement security policy by enforcing local packet filtering rules
- E.g., allow traffic between Internet/Corporate/Home and Mail-Server only for smtp-Packets

Modelling Systems with AutoFocus

- CASE tool, based on formal background (FOCUS)
- Graphical, view oriented modelling
  - System Structure Diagrams
  - State Transition Diagrams
  - Message Sequence Charts
  - Data Type Definitions
- Views related to UML-RT, support hierarchy
- Features:
  - Simulation
  - Code Generation (e.g. Java, C)
  - Validation (Consistency, Testing, Model Checking)

Firewall System in AutoFocus




```
data TPacket = Packet(source:TAddress,
                      dest:   TAddress,
                      service: Tservice);
```

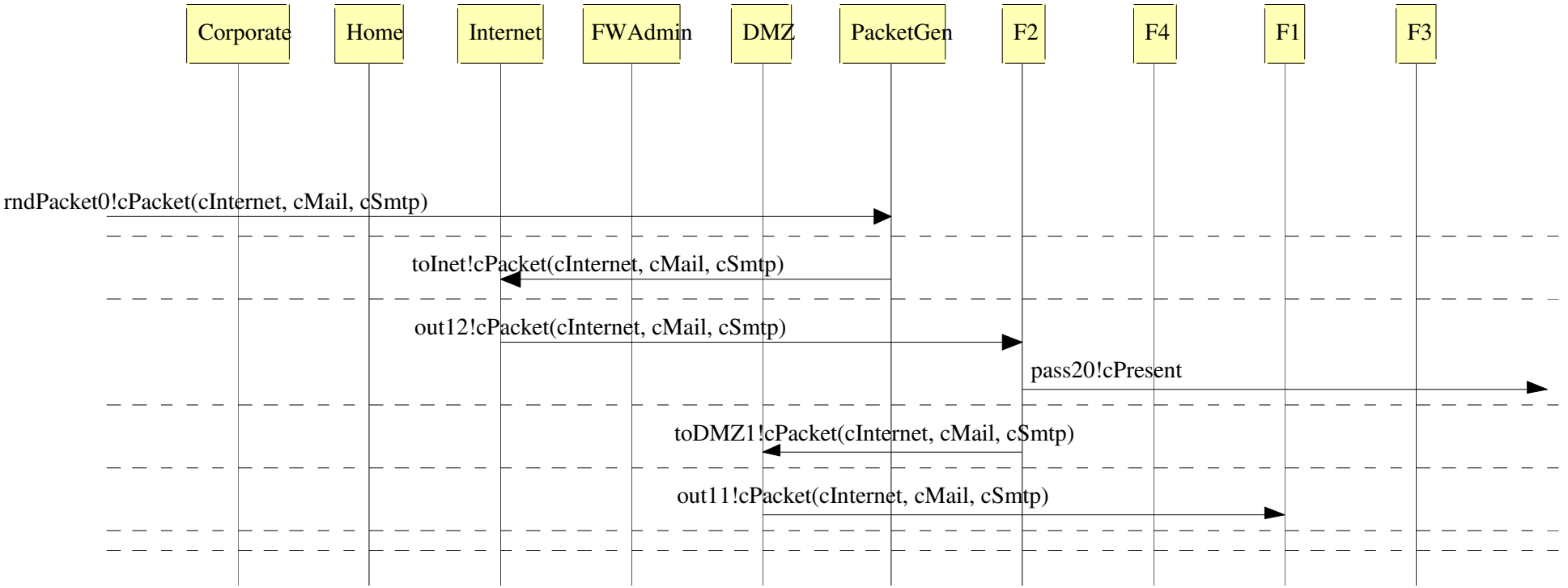
Specification Based Testing

- Test case specification:
  - Characterizes system behaviour to be tested
  - In our case: conditions on paths of packets and behaviour of firewalls: arrival at a component, drop at firewall F1 etc.
- Test sequence generation:
  - From the system model, generate execution sequence fulfilling the test case specification
  - Use execution sequence to test implementation
  - Computed by translating system model and test case specification to constraint logic program
  - Similar to bounded model checking

Test Cases for Firewall System

- Stress test
  - Test case specification: network behaviour so that a packet will be dropped at firewall Fn
  - $\Rightarrow$ systematic „flooding“ of implemented firewalls with security critical packets
- Spoofing
  - Test behaviour for packets with forged source addresses
- Policy Violations
  - Test executions for fulfillment / violation of security policy („was-in – reaches“
- Systematic Selection
  - E.g., bound to length of sequence; cover all possibilities for source address (destination address / service respectively), ...

Example Test Sequence



- Result of Specification for
  - Stress test (drop at F1)
  - Policy violation (packet from Internet to Mail must not be relayed to Corporate or FWAdmin subnets)

Conclusion

- General formal framework for specification-based testing of firewall systems in AutoFocus
- Automatic generation of test sequences for security relevant scenarios
- Performance: approx .1s per test sequence
- Further work:
  - Advanced firewall designs (e.g. using cryptography)
  - Higher level specification language
  - Automatic testing of actual implementation