Specification-based testing of IPsec

Institute for system Programming
Russian Academy of Sciences

Nickolay Pakoulin npak@ispras.ru

Agenda

- **Work Background**
- Specification based testing in IPsec
- Discussion
- Future work

The work background

- RFBR Grant on Research in IP security and mobility
- Currently we are working on IPsec
  - IPsec formalization
    - AH and ESP
    - Inbound / Outbound processing
    - IKE v1
    - Focus on IPsec over IPv6
  - Implementations evaluation
    - Free BSD 5.2.1
    - OpenBSD 3.6

Project info

- Funded by the Russian Foundation for Basic Research
- Test suites would be available for free from http://ipv6.ispras.ru/
- The CTesK toolkit is available for free from http://www.unitesk.com/
- Open for international collaboration in the field of IPsec R&D

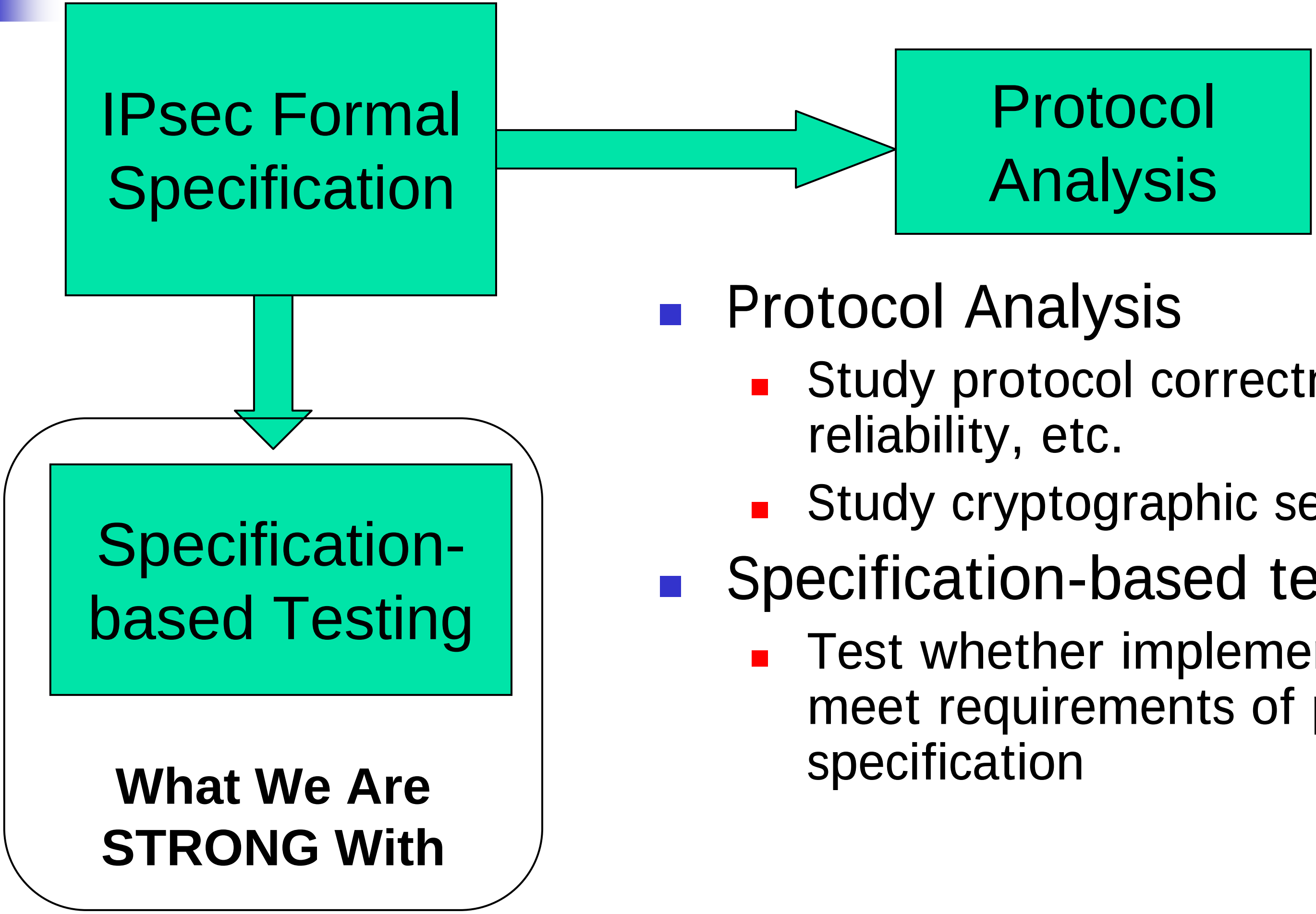
IPsec research project : what it is NOT

- NOT Cryptanalysis of ciphers / message digest
  - This goes beyond IPsec study anyway
- NOT Formal study of IPsec features, such as
  - Protocol validation
  - Attacks discovery for IPsec security features

IPsec research project: what it is

- Conformance test suite development
  - Trial whether implementations really meet requirements
  - Interoperability by conformance
  - Reliability testing
- Formal specification of IPsec
  - Formal specification of basic IPsec features
    - Inbound / Outbound processing
    - IKE v1
  - RFC as reference standard

How to use formal specs



IPsec Formal Specification

Protocol Analysis

Specification-based Testing

What We Are STRONG With

- Protocol Analysis
  - Study protocol correctness, reliability, etc.
  - Study cryptographic services, etc.
- Specification-based testing
  - Test whether implementations meet requirements of protocol specification

Agenda

- Work Background
- **Specification based testing in IPsec**
- Discussion
- Future work

Need for IPsec conformance testing

- Interoperability is crucial for IPsec deployment
- Interoperability by conformance
  - IPsec is a solid protocol, two conforming implementations are expected to interoperate
- Reliability of implementations
  - IPsec is a complex protocol

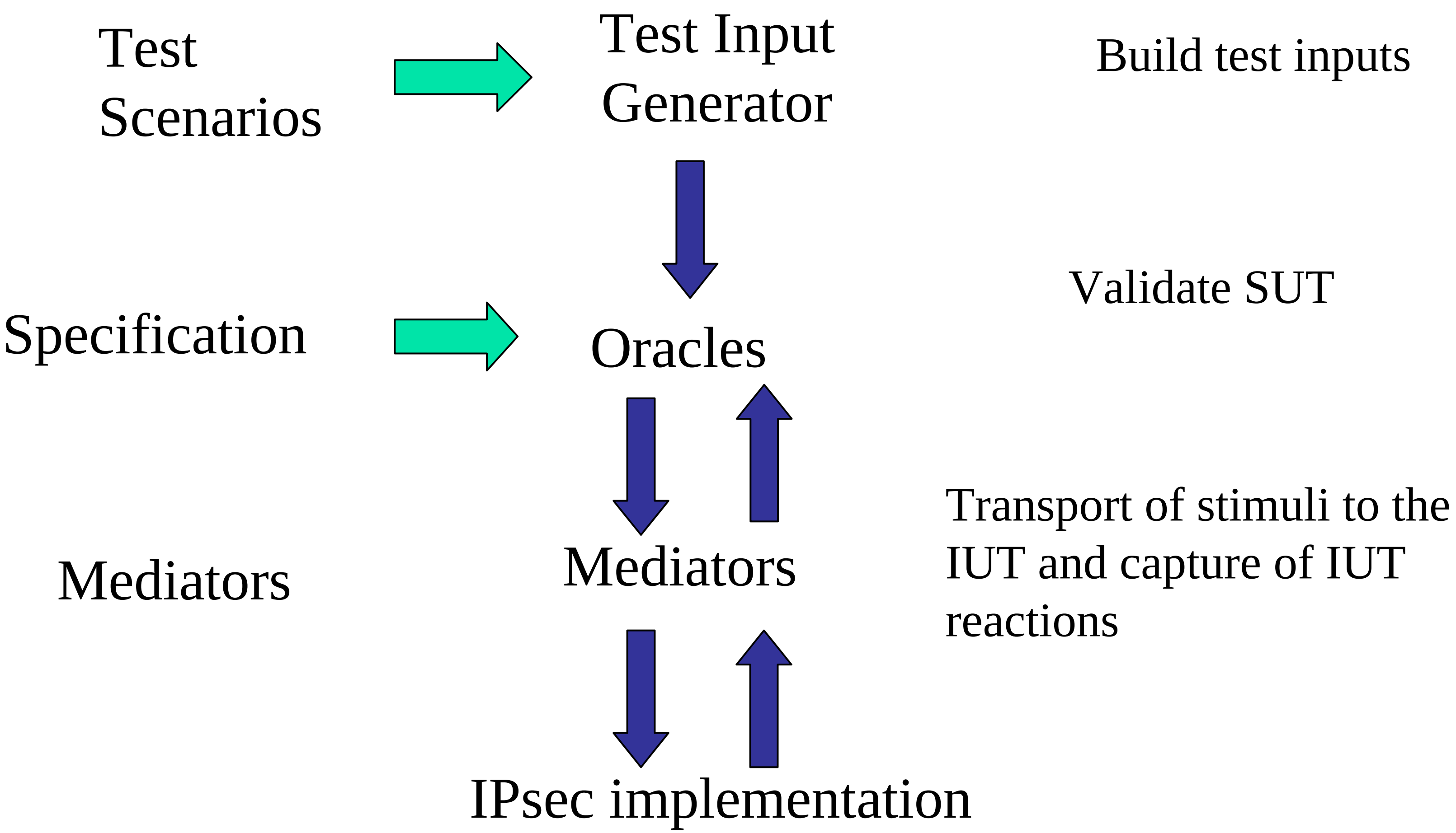
IPsec specification-Based Testing

- Based on UniTesK technology http://www.unitesk.com/
- Using CTesK toolkit
  - Implementation of UniTesK for C programming languages

UniTesK specification-based testing technology

- Verdict is assigned by an oracle
  - Oracle is generated from the formal specification
- Adaptive generation of test inputs
  - Test inputs are generated from FSM-based test scenarios
- There is an adapter between “abstract” specification model and implementation
  - Mediator

Test Suite Architecture



Test Scenarios

Test Input Generator

Build test inputs

Specification

Oracles

Validate SUT

Mediators

Mediators

Transport of stimuli to the IUT and capture of IUT reactions

IPsec implementation

Test suite: underlying technology

- Specification is developed in SeC ([sek])
  - Specification extension of C language
- Test scenarios – SeC
- Mediators – SeC and C + RPC

Test suite: technology support

- SeC development is supported by CTesK toolkit
  - Requires Java and C compiler – GCC or MS VC
  - Windows, Linux, FreeBSD, Solaris
  - Stable release is available for free
- Test report generator and test run visualization
  - Requires Java
  - Windows, Linux, FreeBSD, Solaris
  - Stable release is available for free

Specification development

- Specification is based upon regulating documentation
  - RFC 2401 (IPsec Architecture) and others
- Specification is implicit
  - Specification imposes constraints on the properties of protocol implementation
  - Pre- and post- conditions
  - Constraints are written using specification extension of C language

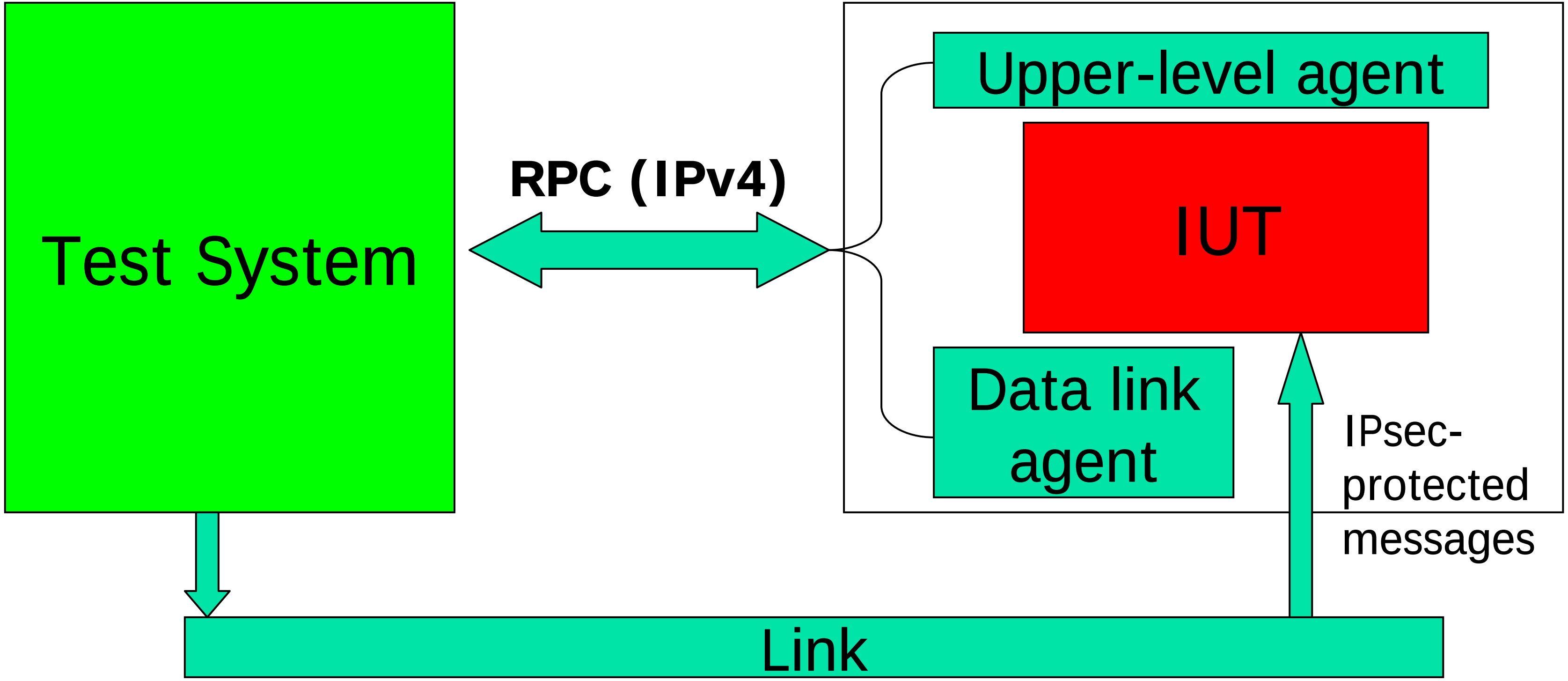
Specification and coverage criteria

- Coverage
  - Define criteria to split the space of inputs into equivalence classes
  - More then one criteria can be defined
- Source of coverage criteria
  - RFC define conditions that govern rules of processing
  - Coverage is formal representation of those conditions

Example

```
specification void receive_AHHeader( AHHeader * ah_hdr )
{
  pre { /* Precondition */ }
  coverage SecAssoc {
    if ( NULL == find_SA(receiver_SAD, ah_hdr)) {
      return { ah_no_sa, "No SA" };
    } else {
      return { ah_sa_exists, "SA found" };
    }
  }
  post {
    SA * sa = find_SA (receiver_SAD, ah_hdr);
    if ( sa == NULL ) {
      return isDiscarded_Header( ah_hdr )
          && contains_Log(/* Discard event */) )
          && equals( @receiver_SAD, receiver_SAD )
          && equals( @receiver_SPD, receiver_SPD );
    }
    /* Further specification */
```

Test bed deployment



Upper-level agent uses API to affect IUT (add/remove SA/SP, etc)

Data link agent captures outgoing IPv6 datagrams

Mediators development

- Mediator links specification and implementation
  - Pass test inputs to target system
  - Capture outputs of Implementation Under Test
  - Translate conceptual data structures to concrete ones and vice versa

Test scenarios

- Test scenarios specify how to iterate parameters of test inputs depending on the state of the model
- The actual test inputs are built “on the fly” during test execution
- Coverage-driven iteration
  - Do not iterate all possible inputs, only “interesting” ones that improve coverage

Current state

- Upper-level and data link agents for FreeBSD and OpenBSD ready
- Specification under development
  - Inbound and outbound
  - Manual key management
- Test scenarios under development

Agenda

- Work Background
- Specification based testing in IPsec
- **Discussion**
- Future work

CTesK applications

- API and message-based interfaces
    - MSR IPv6
        - Basic IPv6 features
    - Mobile IPv6 for Windows CE 4.1
        - Mobile IPv6, draft 13
    - Sensor networks (TinyOS)
        - Embedded software

Discussion

- Strengths of the approach
  - Strong modularity of Test Scenario
  - Relatively easy way to model complex features of IPv6
  - Incremental design of Test Suite
- Weaknesses
  - New paradigm (implicit specs / FSM test)
  - Relatively long way to first tests

Alternatives

- Manual test suite development
  - Project TAHI
- TTCN-based approaches
  - Commercial test suites (presumably TTCN-2)
  - Work in progress in the EU
    - TTCN-3, scheduled for 3 years, in the early beginning

Alternatives (2)

- All known industrial alternatives are test-case based
- Strengths
  - Well known and established technologies (e.g. ISO 9646)
  - Relatively quick way to first tests
- Weaknesses
  - Intensive manual work
    - Test purposes elicitation
    - Test cases development
  - Problems with IPsec output prediction (IPsec is VERY complex)
  - Problems with maintenance and extensions
  - Less thorough study of official specification

Agenda

- Work Background
- Specification based testing in IPsec
- Discussion
- **<u>Future work</u>**

Future work

- Full IPsec conformance test suite
  - Inbound / Outbound traffic
  - IKE v1
- Mobile IPv6 conformance test suite development
- Mobile IPv6 security conformance testing
- Open for collaboration

Links

- UniTesK http://www.unitesk.com/
  - CTesK http://www.unitesk.com/products/ctesk/
- Institute for System Programming RAS http://www.ispras.ru/
  - Network research group http://ipv6.ispras.ru/
- Contact: Nickolay Pakoulin mailto:npak@ispras.ru

END

Questions?