

Message Conformance for Security of Protocol Implementations

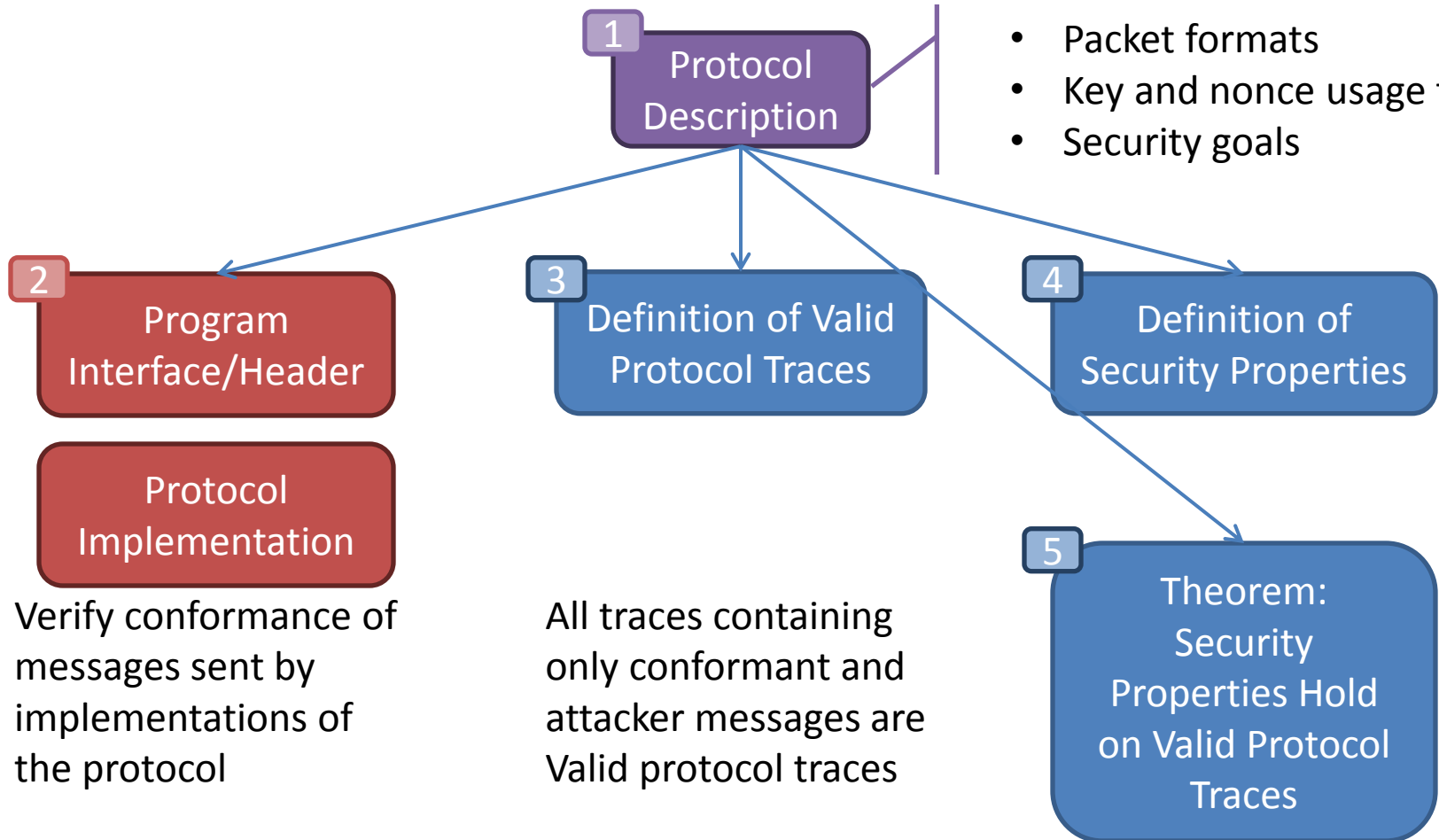
François Dupressoir
Andy Gordon
Bart Jacobs
and others

Verifying Implementations

- Previous methods (POPL'10,CSF'11) geared towards symbolic security verification without independent formal specification
 - Semi-formal partial spec produced in the process
 - Program verification (in particular for C) is a hard problem by itself
 - Getting computational security out of symbolic security results can be problematic
- We take a step back and separate program and security verification

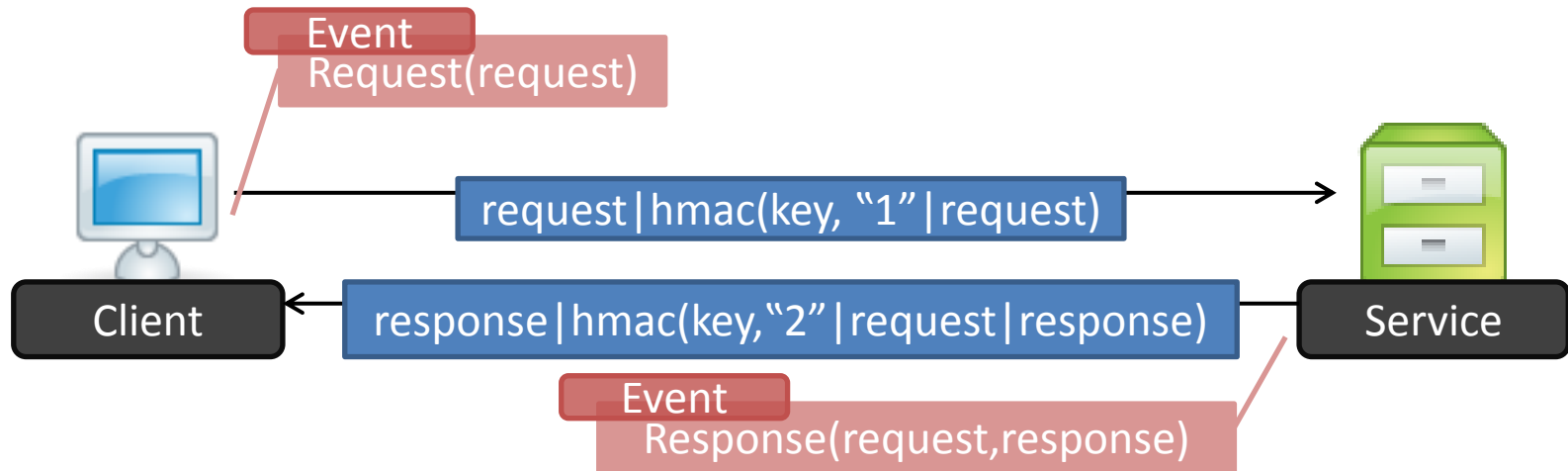
Goals

- Packet formats
- Key and nonce usage types
- Security goals



1

Running Example: Authenticated RPC



Protocol Events:

- Request(a,b,req)
- Response(a,b,req,resp)
- Bad(a)

Key Types:

- KeyAB(a,b): HmacKey KeyABPayload(a,b) KeyABComp(a,b)
- Where:
- KeyABPayload(a,b) =
 $(\text{Is}("1" | \text{req}) \ \&\& \ \text{Request}(a,b,\text{req})) \ ||$
 $(\text{Is}("2" | \text{request} | \text{response}) \ \&\& \ \text{Response}(a,b,\text{req},\text{resp}))$
 - KeyABComp(a,b) =
 $\text{Bad}(a) \ || \ \text{Bad}(b)$

2 Verifying Conformance of Code

- The protocol implementation is verified with the following precondition on the network send function

$$\begin{aligned} \text{CanSend}(R,m,L) = & \\ & (R = \text{Client}(a,b,k) \ \&\& \\ & \text{Request}(a,b,r) \in L \ \&\& \\ & m = \text{msg1}(r,k)) \\ & || \\ & (R = \text{Server}(a,b,k) \ \&\& \\ & \text{Received}(\text{msg1}(r,k)) \ \&\& \\ & \text{Response}(a,b,r,r') \in L \ \&\& \\ & m = \text{msg2}(r,r',k)) \end{aligned}$$

Valid Traces

- Inductively define a notion of Valid trace:
 - The empty log is Valid
 - Inductive rules modelling attacker capabilities
 - Protocol operations are modelled using a single rule:

$$\frac{\text{CanSend}(R, m, L) \quad \text{Valid}(L)}{\text{Valid}(L \cup \{\text{Msg } m\})}$$

- Intuition: All logs produced during execution of a verified implementation are Valid traces

5

Security Properties of Valid Traces

- We then formally prove that the correspondence properties hold on Valid traces
 - Example Theorem:
IsKeyAB(a,b,k,L) &&
Valid(L) &&
Msg(msg1(r,k)) ∈ L ==>
Request(a,b,r) ∈ L || Bad(a) ∈ L || Bad(b) ∈ L

Conclusion

- We provide a formal framework for separate verification of conformance and security
- We automatically generate both conformance and security models from the same protocol description
- We expect improvements on our previous methods:
 - Performance: no need to model the attacker when verifying the program
 - Security proof done once and for all; can be reused for several implementations of the same protocol
 - Theory: proving computational security properties of the protocol model should yield computational security properties of the implementation