



Blackhat 2004



IKE-Test

Testing IKE Implementations

Ralf Spenneberg

Open Source Security
Training & Consulting
ralf@spenneberg.net



IPsec-based VPNs



- Most VPNs today are based on IPsec
- IPsec protocols
 - Authentication Header (AH)
 - Encapsulated Security Payload (ESP)
 - These protocols do not exchange any keys
- Key exchange is handled by external protocols
 - Internet Key Exchange (most often used)
 - Photuris



Internet Key Exchange (IKE) Protocol



- based on several other protocols and frameworks

ISAKMP (RFC2408) provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchanges.

Oakley (RFC2412) describes a series of key exchanges-- called "modes"-- and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication).

SKEME describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment.



... continued



- IKE (RFC2409)

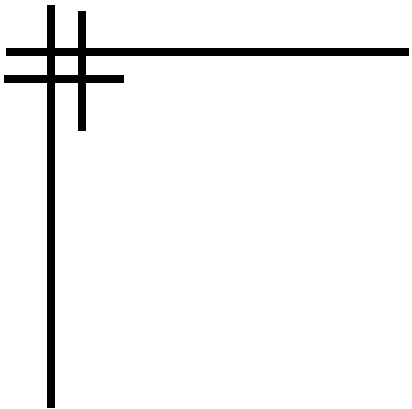
IKE is a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.



IKE Complexity

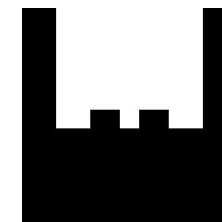


- Phase 1
 - At least two modes
 - Aggressive Mode (3 messages)
 - Main Mode (6 messages, offers identity protection)
 - All parameters are negotiated
- Phase 2
 - Quick Mode
 - relies on the security of Phase 1

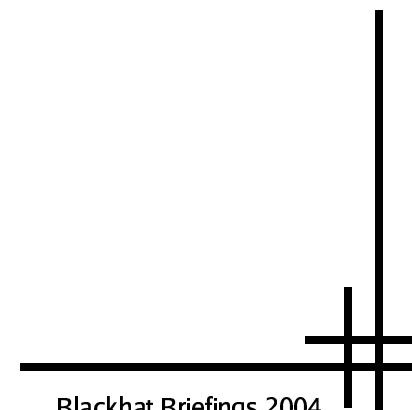
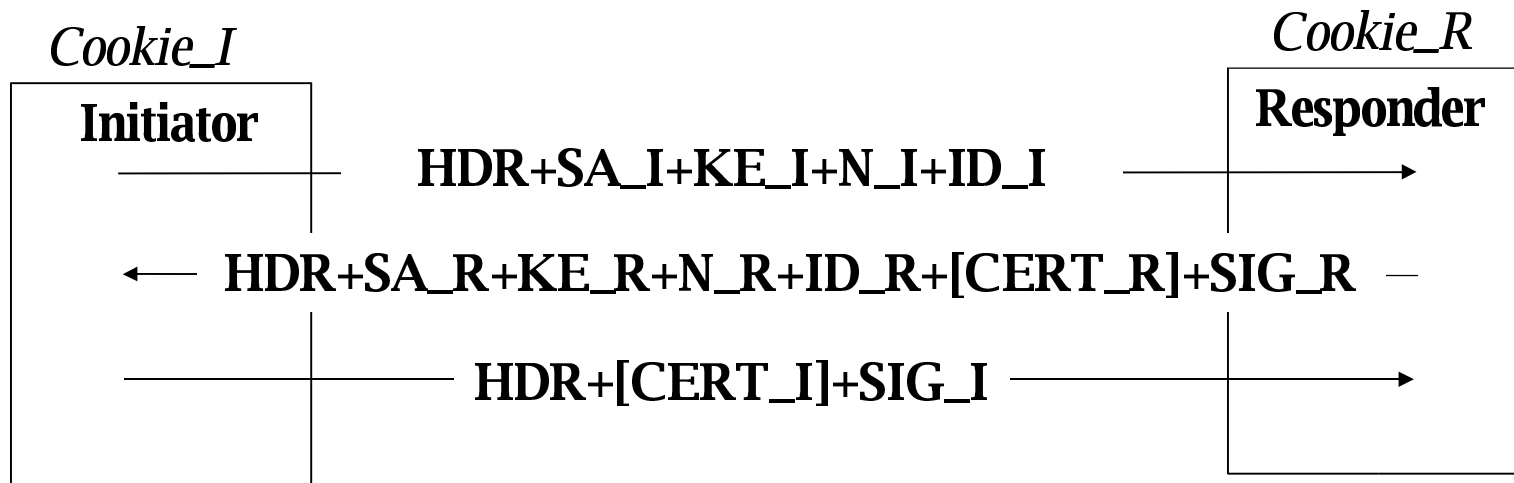


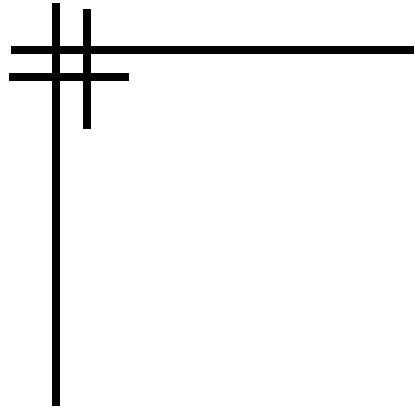
Aggressive Mode

(Using Signatures)

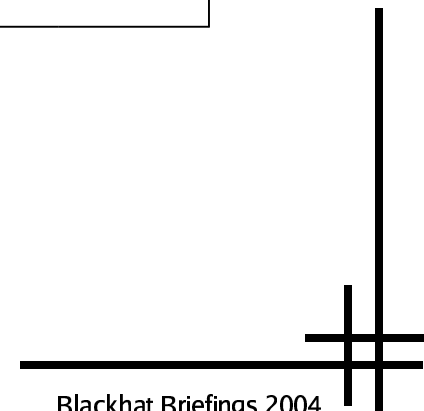
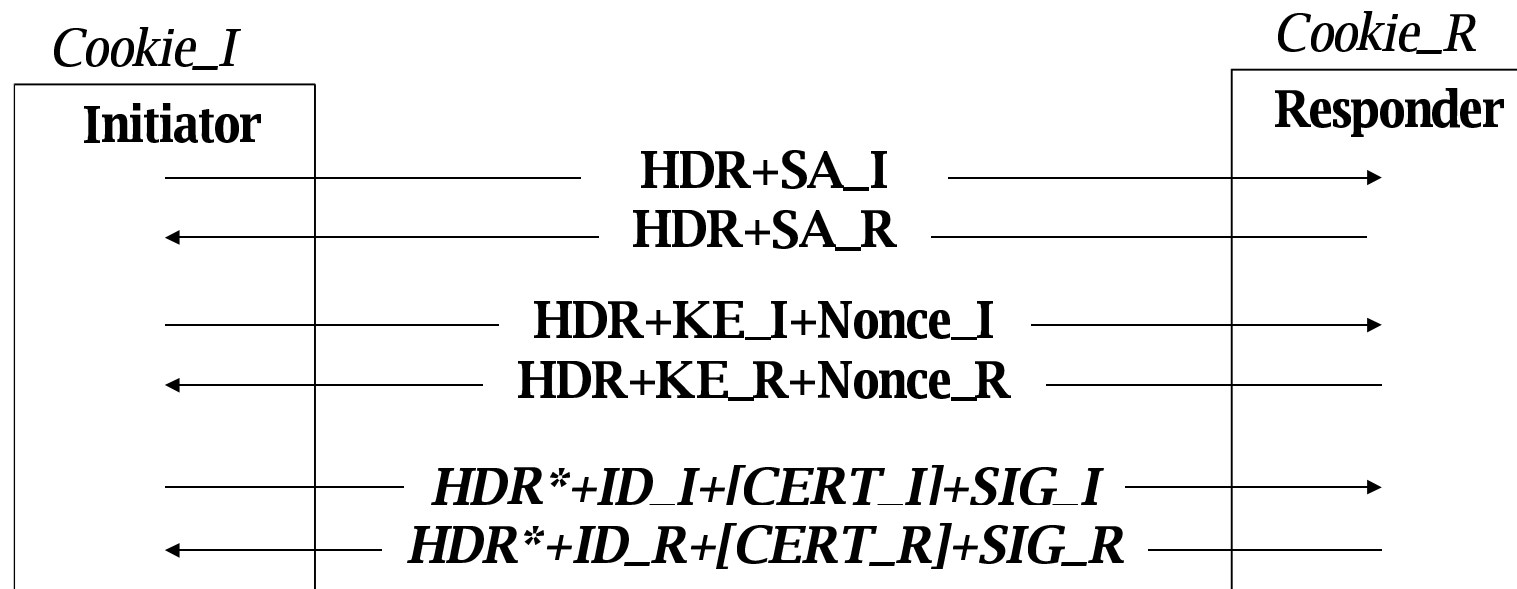


Open Source Security
Training & Consulting
Ralf Spenneberg





Main Mode





IKE Importance



- IKE exchanges the keys in almost all IPsec based VPNs today
- Compromising the IKE exchange attacks the Achilles heel of the VPN
- Often full access to the internal network is provided by the VPN device
 - Boss needs database access from his home!



IKE Design Flaw



- Aggressive Mode with PSKs
 - No identity protection available
 - brute-force or dictionary attack on the used PSK possible
 - First found by Anton T. Rager and implemented in ikecrack



Further IKE Vulnerabilities



- Multiple Vendor IKE Insecure XAUTH Implementation Vulnerabilities (Bid9209)
- OpenBSD isakmpd IKE Payloads Denial Of Service Vulnerability (Bid5589)
- VPN Client IKE Packet Excessive Payloads Vulnerability (Bid5443,5668)
- Multiple Vendor IKE Implementation Certificate Authenticity Verification Vulnerability (Bid9208)



... continued



- Securityfocus vulndb lists 32 IKE vulnerabilities
- Even simple bugs are not found if nobody looks for them

Simple Bugs in Racoon



- Racoon IKE Daemon Unauthorized X.509 Certificate Connection Vulnerability (Bid10072)
 - Authentication succeeds using a valid certificate without the proper private key
- KAME Racoon IDE Daemon X.509 Improper Certificate Verification Vulnerability (Bid10546)
 - Authentication succeeds when using an expired or self-signed certificate



We need a tool!



- Numerous IKE implementations out there
 - Numerous buffer overflows
 - Strange or wrong certificate handling
 - straight forward bugs
- Most IKE implementations are closed source
 - Rigorous testing is needed



Available Tools



- **ikecrack-snarf-1.00.pl / ikeprober.pl**
 - Cracks preshared keys used in aggressive mode
 - <http://ikecrack.sf.net>
- **ikeprobe**
 - <http://www.ernw.de/download/ikeprobe.zip>
- **ikescan**
 - Discovery and fingerprinting
 - <http://www.nta-monitor.com/ike-scan/>



IKE-Test



- Written in Perl
 - uses Net::RawIP
 - fast prototyping
 - easy to extend and modify
- Strives to implement all different IKE messages
- Available at <http://www.spenneberg.com/iketest>

Examples



```
$ sudo iketest.pl --initiate --certificate test.pem  
--key testkey.pem --target vpngw.example.com  
  
$ sudo iketest.pl --initiate --psk 'kennwort' --target  
vpngw.example.com  
  
$ sudo iketest.pl --respond --target vpngw.example.com  
--psk 'kennwort'  
  
$ sudo iketest.pl --initiate --psk 'kennwort' --target  
vpngw.example.com --no_qm_encrypt  
  
$ sudo iketest.pl --initiate --cookie-crumbs --target  
vpngw.example.com
```



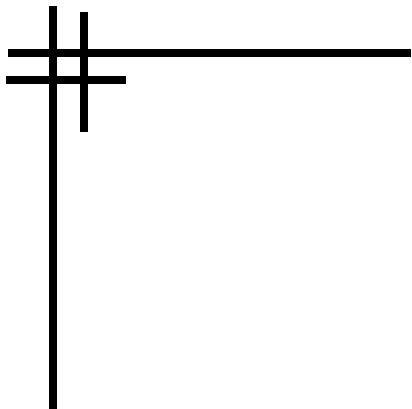

ToDo



Open Source Security
Training & Consulting
Ralf Spenneberg

- Full overhaul
 - object oriented approach
- More RFC-compliance tests
- More modes and algorithms

- Attacking more (commercial) products



Open Source Security
Training & Consulting
Ralf Spenneberg

Thanks.

Ralf Spenneberg
ralf@spenneberg.net

Questions
ike-test@spenneberg.net

