SIP SECURITY

AUTHENTICATION, ENCRYPTION, IDENTITY

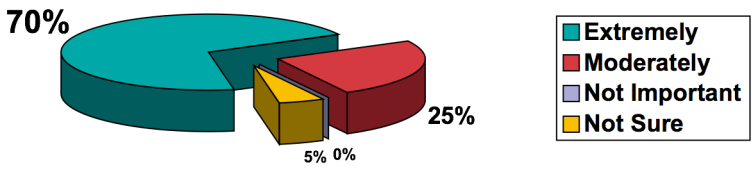
Cullen Jennings, PhD

fluffy@cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.

Does Anyone Care?

To what extent is the relative security of an IP telephony solution important within your purchase decision?



Source: Cisco Systems survey, April, 2004

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Secure SIP Systems

Cisco.com

© 2005 Cisco Systems, Inc. All rights reserved.

Agenda

Cisco.com

- This talk is about the protocol security in VoIP
  - Introduction to SIP
  - Threats
  - Channel Security
  - Object Security
  - Media Security
  - Certificate Management
  - State of Implementations & Standards

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

THREAT MODEL

© 2004, Cisco Systems, Inc. All rights reserved.

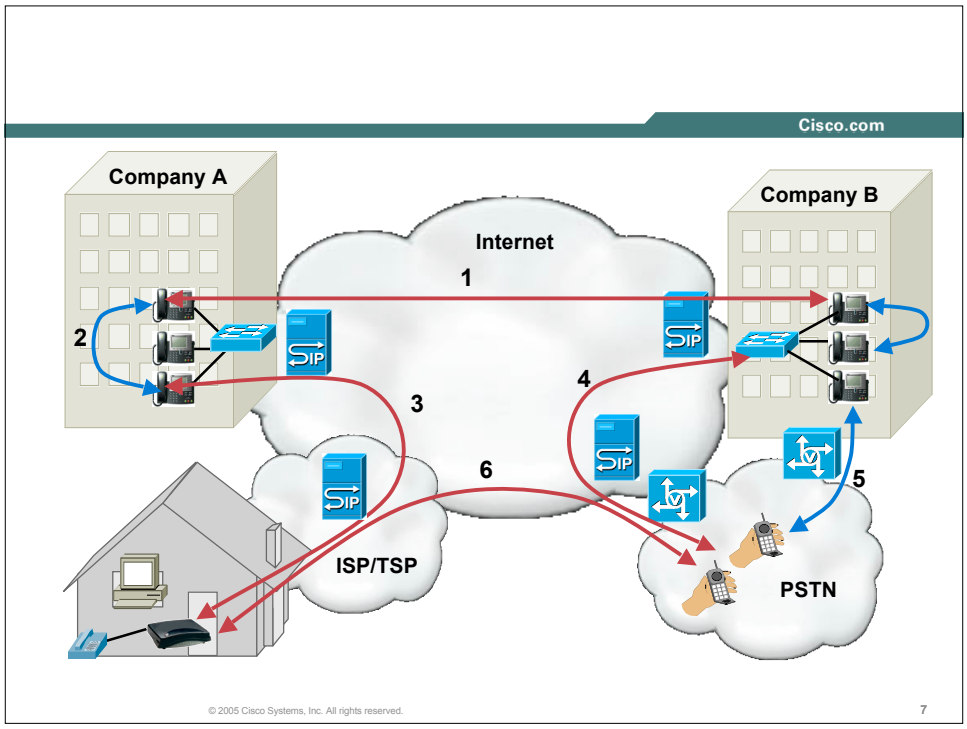
SIP Introduction

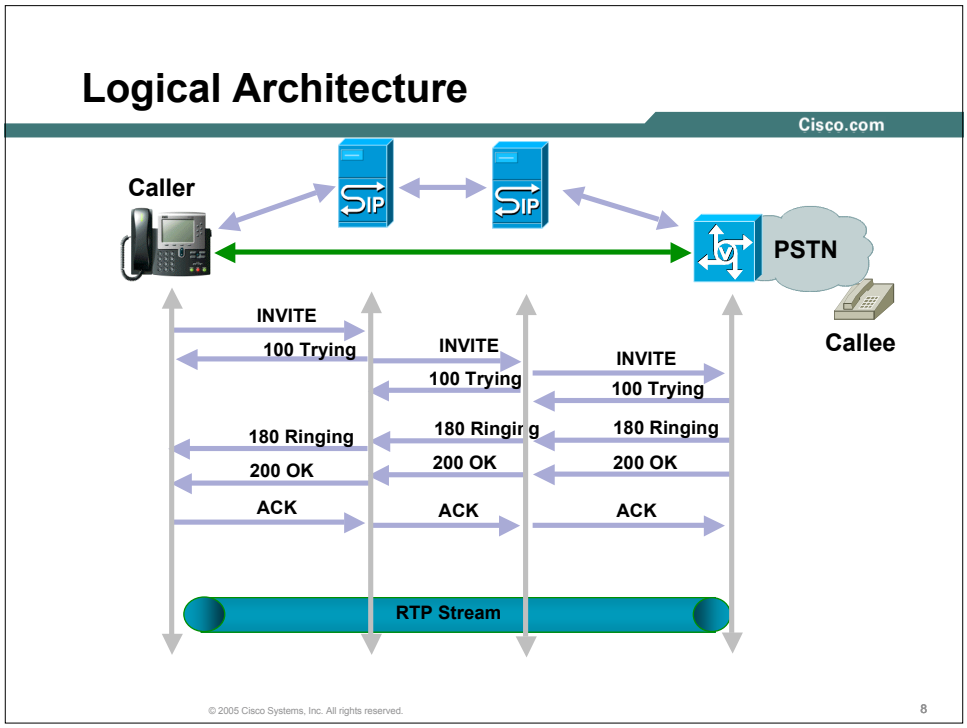
- Used for Voice and Video over IP
  - Toll Arbitrage
  - Residential / IpCentrex
  - Enterprise / IpPBX
- SIP/SIMPLE for Instant Messaging
- Used for Application, Whiteboard, and Web sharing

- How SIP works
  - Peer to Peer System
  - Rendezvous points to find others
  - Separation of media and signaling
  - Negotiation of rich media

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.





Copyright © 2005, Cisco Systems, Inc. All rights reserved.

VoIP Threats

Cisco.com

- Toll fraud
  - Unauthorized or unbillable resource utilization
- Eavesdropping
  - Listening to another's call
- Learning private information
  - caller ID, DTMF password/accounts, calling patterns
- Session replay
  - Replay a session, such as a bank transaction
- Fake identity
- Media tampering
- Denial of service
  - Hanging up other people's conversations
  - Contributing to other DOS attacks
- Impersonating others
- Hijacking calls
- SPAM
  - SPIM, SPIT, and more SPAM

Why SIP Security is Hard

Cisco.com

- SIP is a rendezvous protocol, communicates with peers in any domain with no previous security relationship
- Deals with multiple intermediaries and endpoints with different trust for each (need both channel and object security)
- Multiple endpoints can be involved (eg. forwarding, forking, conferencing, transfer)
- Supports anonymity, call trace, legal intercept, and privacy (simultaneously)
- Complicated by: NATs, firewalls, high reliability, large scale, choice of transport protocol (eg. TCP, UDP, TLS, SCTP, DCCP)

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

On Path / Off Path

Cisco.com

- On Path Attacks:

  An attack that is only possible when the attacker can control one of the network elements or connections over which the the call traverses

- Can be prevented by controlling access to the network component

- On path DOS attacks are well known and uninteresting

© 2005 Cisco Systems, Inc. All rights reserved.

Solutions to Threats

Cisco.com

- Authentication/Authorization from:
  - client to server
  - server to server
  - server to client
- Privacy and integrity hop by hop (Channel Security)
- Privacy and integrity end to end (Object Security)
- Client and server assertion of user identity (can be different)
- Server removal of identity for anonymous calls
- End to end assertion of identity
- Signaling end to end integrity and privacy
- Media end to end integrity and privacy

© 2005 Cisco Systems, Inc. All rights reserved.

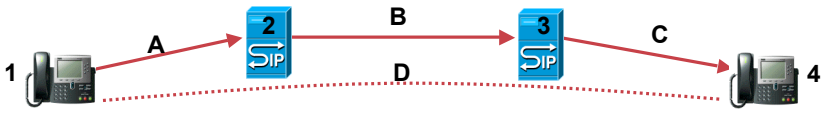
Copyright © 2005, Cisco Systems, Inc. All rights reserved.

AUTHORIZATION & AUTHENTICATION

© 2004, Cisco Systems, Inc. All rights reserved.

Authentication & Authorization

Cisco.com



- **Authentication - Who sent me this?**
  - **over link A: Proxy checks the user (Digest or mutual TLS)**
  - **over link B: Proxies check each other (mutual TLS)**
  - **over link C: UA may verify request came from "its" proxy (TLS)**
  - **end to end (D): UAS may verify UAC (SMIME)**
- **Trust is not transitive: even if 1 trusts 2 and 2 trusts 3, it does not follow that 1 trusts 3**
  - **MCI might carry Vonage calls - Cullen has an account with Vonage, but MCI does not have any trust relationship with Cullen**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Digest Authentication

Cisco.com

- Can only challenge a request from UA to Proxy
  - UAC to UAS is possible but seldom used
- Used to authenticate for requests such as outbound calls
- Used to authenticate for requests such as registration for inbound call
- Does not work proxy to proxy
- About the same as a HTTP Digest authentication from web browser to web server

© 2005 Cisco Systems, Inc. All rights reserved.

TLS Authentication

Cisco.com

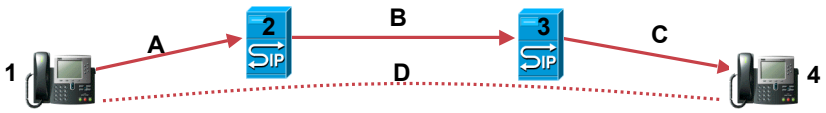
- The certificate in SIP TLS asserts the DNS name of the host
- This is in the Subject Alternative Name field
- Phones typically don't have a stable DNS name and don't have a certificate that can be used for TLS
- Mutual TLS is useful for proxy to proxy authentication
- Devices that do TLS need to have a Root Trust List compiled in. It must be possible to replace this with a customer specific list
- Session resumption mode is critical for avoiding "Start of Service" avalanche restart problem

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Encryption and Integrity

Cisco.com



- Follows the web model and uses TLS on a hop by hop basis
- Follows the email model and uses S/MIME on end to end basis
- TLS creates an authenticated, encrypted, integrity-checked channel
  - Crypto generally: RSA, 3DES or AES, SHA-1
- Use S/MIME to sign and encrypt portions of the SIP body
  - Crypto generally: RSA, 3DES (moving to AES), SHA-1
- Use SRTP to protect RTP/RTCP media (audio, video)
  - Crypto generally: AES-CM, SHA1

© 2005 Cisco Systems, Inc. All rights reserved.

IDENTITY

© 2004, Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Identity

Cisco.com

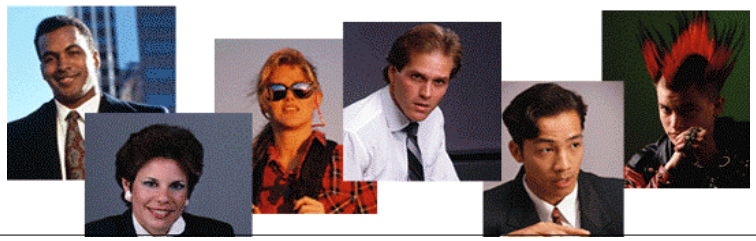
- Goal is to understand who are you communicating with
- Requires strong cryptographic assertions
- Represents the most promising approach for dealing with SPAM, SPIM, and SPIT
  - White lists
  - Reputation services
- Needed for B2B and B2C transactions

© 2005 Cisco Systems, Inc. All rights reserved.

Who is fluffy@cisco.com

Cisco.com

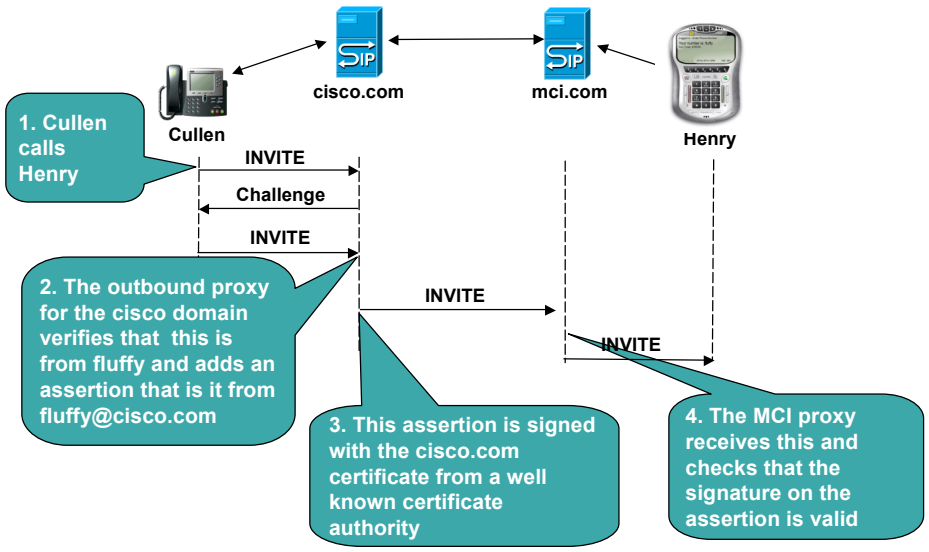
- Who is in the best position to make strong assertions about who fluffy@cisco.com is?
  - Cisco.com allocated the address fluffy to Cullen
  - They provided a way for Cullen to prove his identity with logon password, secure token card, etc.
  - Having Verisign assert that some random person can receive email sent to fluffy@cisco.com is a weak assertion of identity
- Who knows who cisco.com is?
  - Verisign can verify with DNS registrars who has been given that name and can get appropriate contacts for it



Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Identity Service for SIP

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

Signed Portion of Message

Cisco.com

```
INVITE sip:bob@biloxi.org SIP/2.0
        Via: SIP/2.0/TLS pc33.atlanta.com;branch=z9hG4bKnashds8
        To: Bob <sip:bob@biloxi.org>
        From: Alice <sip:alice@atlanta.com>;tag=1928301774
        Call-ID: a84b4c76e66710
        CSeq: 314159 INVITE
        Max-Forwards: 70
        Date: Thu, 21 Feb 2002 13:02:03 GMT
        Contact: <sip:alice@pc33.atlanta.com>
        Content-Type: application/sdp
        Content-Length: 147

        v=0
        o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.com
        s=Session SDP
        c=IN IP4 pc33.atlanta.com
        t=0 0
        m=audio 49172 RTP/AVP 0
        a=rtpmap:0 PCMU/8000
```

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Identity Headers

Cisco.com

- **Identity is SHA1 hash with RSA signature**

```
Identity:
  "CyI4+nAkHrH3ntmaxgr01TMxTmtjP7MASwliNRdupRI1vpkXRvZXx1ja
    9k0nB2sW+v1PDsy32MaqZi0M5WfEkXxbgTnPYW0jIoK8HMyY1VT7egt0kk4
     XrKFCHYWGClsM9CG4hq+YJZTMaSROoMUBhikVIjnQ8ykeD6UXNOyfI="
Identity-Info: <https://atlanta.com/cert02.cer>;alg=rsa-sha1
```

- **Extensible to other algorithms with additional header**
- **Identity-Info is place TLS connection can be formed to fetch certificate**
- **Can migrate to DNS Sec**

© 2005 Cisco Systems, Inc. All rights reserved.

Signature Assertion

Cisco.com

- **The authentication service authenticates the UA and validates that the UA is authorized to populate the value of the From header field**
- **The authentication may happen by sending a Digest authentication challenge**
- **The value of the From header field may be the user's AoR, or it may be some other value that the policy of the proxy server permits the UA to use**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Results

Cisco.com

- Caller ID that works (unlike PSTN)
- Enterprises and service providers need one web server style certificate rather than one certificate per user
- White lists can authorize communications with people we talk to frequently
  - Address books and buddy lists are examples of white lists
- Communications with new parties can benefit from
  - reputation services
  - friend of friend introduction services
  - social networking systems
- Reduction of SPAM/SPIM/SPIT

© 2005 Cisco Systems, Inc. All rights reserved.

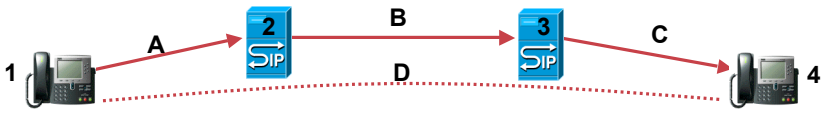
CERTIFICATES
END TO END ENCRYPTION

© 2004, Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Object (End to End) Security

Cisco.com



- Use S/MIME to sign and encrypt portions of the SIP body
- Protect private information from intermediaries
- Assertion of far end identity in a certificate
  - Know who you end up communicating with
- Before saying S/MIME was a failure ….
  - It has been widely implemented, it works, security is good. Technically works well. Deployment is sparse but this relates to the difficulty and cost of an end user getting a certificate. More on this later…
- Crypto generally: RSA, 3DES (moving to AES), SHA-1

© 2005 Cisco Systems, Inc. All rights reserved.

Certificates for Encryption

Cisco.com

- SIP needs certificates for end to end encryption
- Can use traditional capital “PKI” certificates (like Verisign)
  - Problem: enrollment is difficult and expensive
- Can use private CA signed certificates
  - Problem: only works in limited trust domain. Can’t get others to use this CA root as a trust anchor
- Can use self signed certs
  - Problem: need a way to automatically distribute and vouch for these
  - SSH style “leap of faith” first time model
  - Transitive Trust Introduction model

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

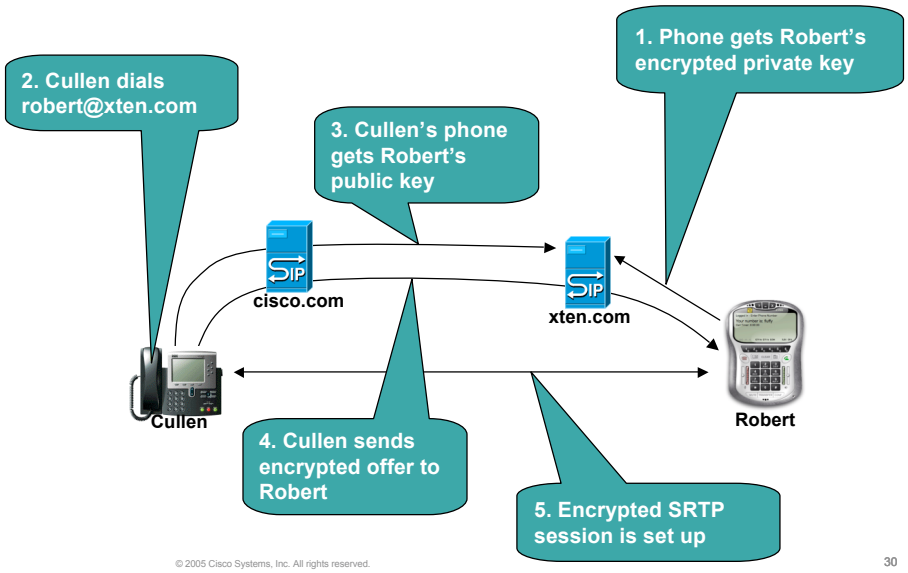
Don't Take ~~Candy~~ Calls From Strangers

Cisco.com

- When you don't know who you are talking to, you don't know if there is a man in the middle even when the voice verifies
- In some important calls, we don't recognize the voice of the person on the other end; and we need to phone people we have never communicated with before
- Encrypted media is far more valuable when coupled with strong cryptographic identity

Who Can Listen to Your Packets? Certificate Management Service for SIP

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Details

Cisco.com

- Fetching certificate done with SUB/NOT
- Allows invalidation of certificates with NOTIFY
- Would typically get certificate at time of subscribing to buddy presence not at time of call
- Phone can PUBLISH a credential (certificate + private key) to the certificate store
- Supports model where certificate store does not know private key as well as models where it does

© 2005 Cisco Systems, Inc. All rights reserved.

Benefits

Cisco.com

- Absolutely no extra work on the part of the end user
- No extra cost to end user
  - Each enterprise or Service provider must have one web server style certificate for the domain
- Makes strong end to end encryption possible
- Avoids IPR entanglement
- Enterprises are comfortable running this type of service
  - It is very similar to presence server or https web server

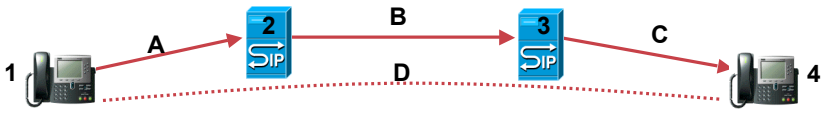
© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

MEDIA ENCRYPTION

© 2004, Cisco Systems, Inc. All rights reserved.

Media Encryption



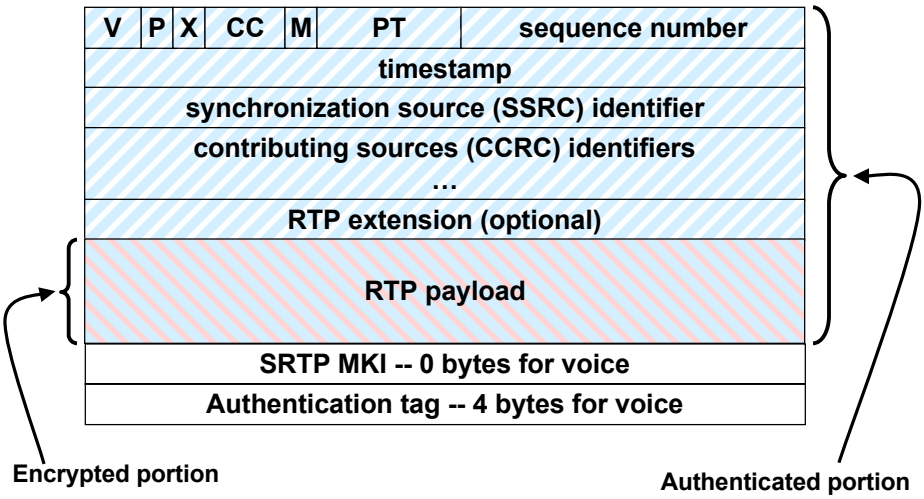
- Use SRTP to protect RTP/RTCP media (audio, video)
  - Keying material is passed in SIP signaling
  - AES Counter Mode
    - counter derived from 16 bit RTP sequence number
    - 32 bit rollover counter provided in RTCP
  - Crypto generally: AES-CM, SHA1
- Protect Instant Messaging with S/MIME
  - Crypto generally: RSA, AES, SHA1

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

SRTP: voice encryption and authentication

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

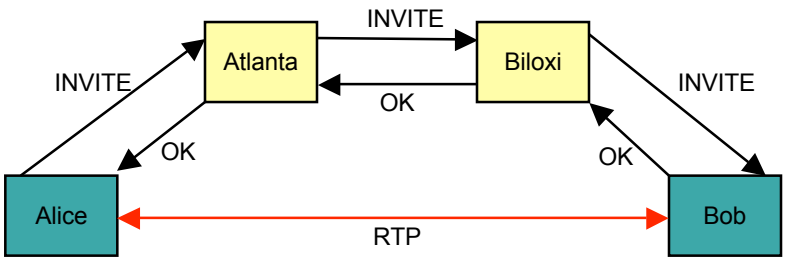
MEDIA KEYING

© 2004, Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Reminder: Basic Topology

Cisco.com

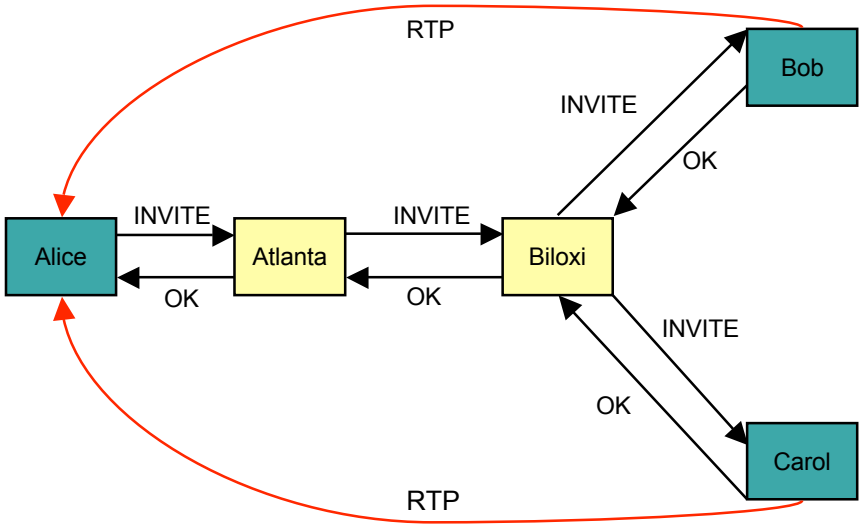


- **SIP and RTP follow different paths**
  - **SIP: Signaling path**
  - **RTP: Media path**
- **Media path is often faster (fewer hops)**

© 2005 Cisco Systems, Inc. All rights reserved.

Forking

Cisco.com

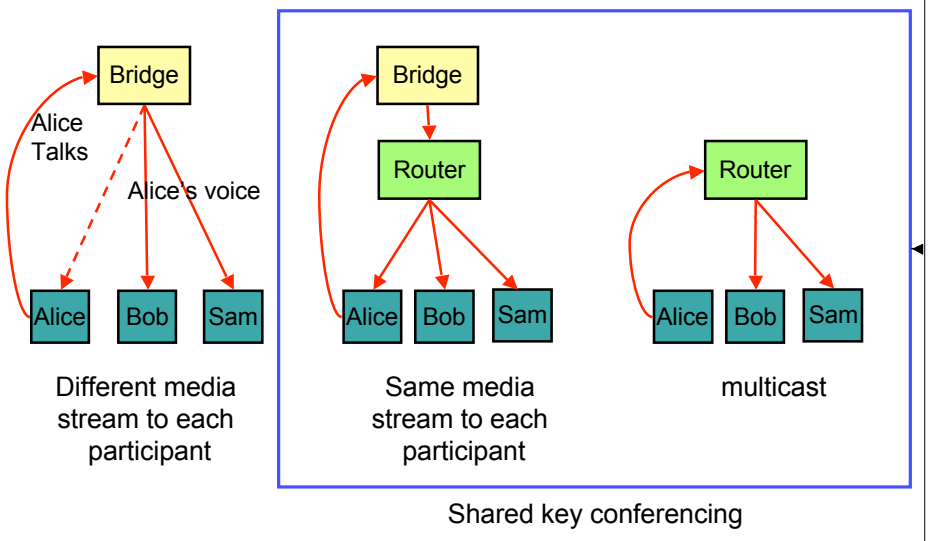


© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Conferencing Architectures

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

Media Keying: Standards Work in Progress

Cisco.com

	Sig. Conf.	Forking	Media before Answer	Shared-key conf.	PKI?	Rekey	Bid-down protection
MIKEY-PSK	**No**	**No**	**Yes**	**Yes**	**No***	**Yes**	**Yes**
MIKEY-RSA	**No**	**No**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
MIKEY-DH	**No**	**No**	**No**	**No**	**Yes**	**Yes**	**Yes**
MIKEY-DHHMAC	**No**	**No**	**No**	**No**	**No***	**Yes**	**Yes**
MIKEY-RSA-R	**No**	**Yes**	**No**	**Yes**	**Yes**	**Yes**	**Yes**
SDES	**Yes**	**Yes***	**No**	**Yes**	**No**	**Yes***	**No**
SDES-EM	**Yes**	**Yes***	**Yes**	**Yes**	**No**	**Yes**	**No**
EKT	**Yes***	**Yes***	**Yes**	**Yes**	**No**	**Yes**	*
SDP-DH	**No**	**No**	**No**	**No**	**No**	**No**	**No**
ZRTP	**No**	**Yes**	**Yes**	**No**	**No**	**Yes**	**Yes**
DTLS	**No**	**Yes**	**Yes**	**No**	**No**	**Yes**	**Yes**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

HOT TOPICS

© 2004, Cisco Systems, Inc. All rights reserved.

What Are SBC Good For?

- **Making a UA do something that the UA should do but is not yet implemented**
  - **Converting SIP over UDP to SIP over TLS**
  - **Converting RTP to SRTP**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

The Basic Facts About Firewall ALGs

Cisco.com

- **The Good**
  - It's nice that a firewall at the gate is only allowing in things that look like gifts
- **The Bad**
  - There is no way for the ALG to know what is OK in the context of this network
- **The Ugly**
  - ALGs break SIP and don't work with encrypted signaling

Do use Firewalls, but don't expect them to solve all problems

© 2005 Cisco Systems, Inc. All rights reserved.

What Are ALGs Good For?

Cisco.com

- **Protecting your hosts from classes of traffic they should not receive**
  - Letting HTTP to Web Server is OK
  - Stopping outside packet to the data base server is Good

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

DENIAL OF SERVICE

© 2005 Cisco Systems, Inc. All rights reserved.

DoS

- DoS attacks are very hard to protect against in any system that allows data exchanges between parties with no previous relationship
- This is a key requirement of voice systems
- Goal is to keep the cost to the attacker as high as the cost to the target
- Many systems are vulnerable to TCP connection depletion
- Many load generators can trivially do tens of thousands of transactions per second, but signaling systems do more in the order of one thousand transactions per second. However bandwidth is symmetrical
- Critical not to allow devices in the core of the network to act as amplifiers (i.e. to receive one message and send many)
  - This is the key problem holding up much of the Push To Talk (PTT) work at IETF

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Solutions to DoS

Cisco.com

- Track the packets back towards the source
- Do one of the following on the source
  - Rate limit the source
  - Disconnect the source
  - Beat the source with a very large stick
- Important to be able to identify and find the source

© 2005 Cisco Systems, Inc. All rights reserved.

DDoS

Cisco.com

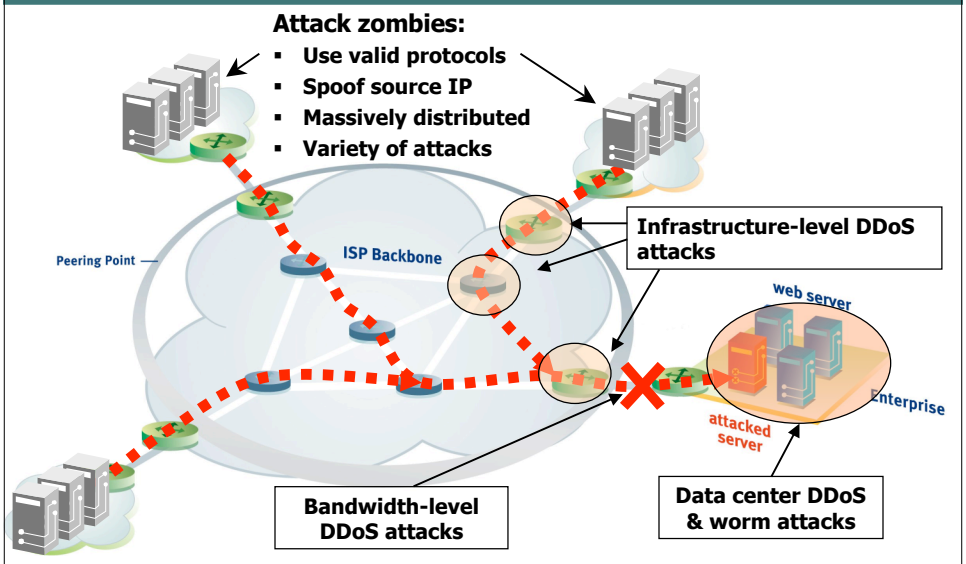
- Harder than DoS because it obfuscates the source and makes many apparent sources
- Solutions mostly involve making sure that if a SIP device forwards a packet on behalf of some sender, it records the original sender in the forwarded packet. Allows the real source to be identified
- Solutions are similar to DoS but harder to implement automatically

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

DDoS Attacks

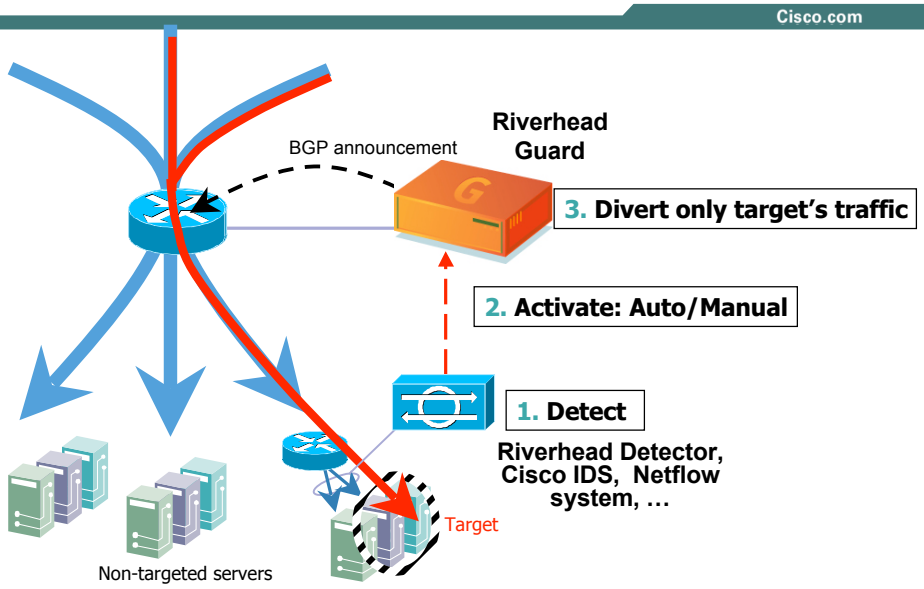
Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

DDoS Solution Attack Starts

Cisco.com

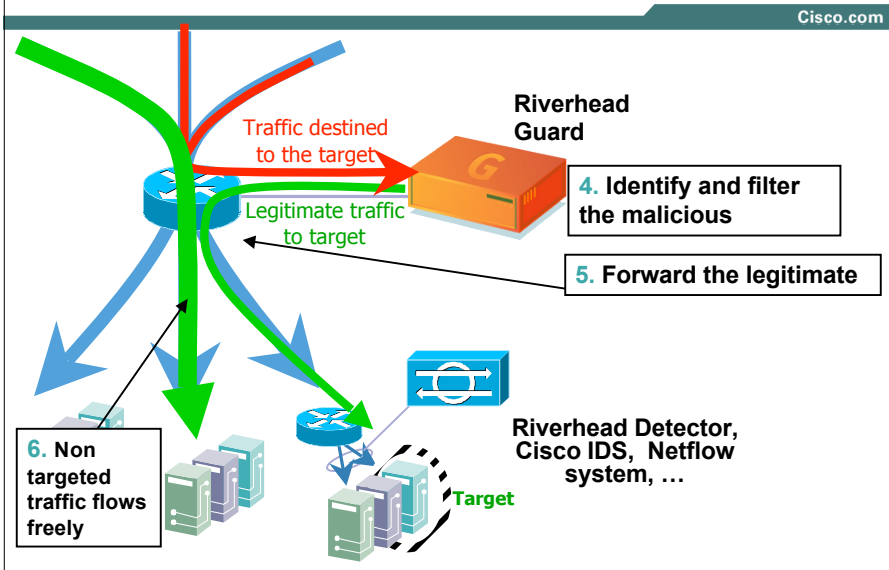


© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

DDoS Solution Attack Blocked

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

DoS & DDoS Summary

Cisco.com

- Know who the packets are coming from
- Ensure Return Routable on packets
- Rate limit as close to source as possible
- Use large stick

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

RISK & COST

© 2004, Cisco Systems, Inc. All rights reserved.

Comparison to PSTN

Cisco.com

- In many ways PSTN is good with respect to toll fraud
  - Still a very large amount of toll fraud on PSTN
- No voice crypto
  - Person in wiring closet can listen to calls
  - Anyone willing to poke around can listen to calls

- Caller ID is bogus (see *38)
  - Anyone can produce fake caller id for a few hundred dollars
- Is the security of the PSTN good enough?
  - Will you give you credit card number over the telephone?
  - Discuss a merger?

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Comparison: Email, PSTN, & VoIP

Cisco.com

	PSTN	EMAIL	VoIP
Hijack protection	OK	good (relies on DNS)	excellent
Off path snooping	good	ok	good
On path snooping	very bad	bad	good if using TLS & SRTP
Fake identity	bad	very very bad	good with Identity (bad otherwise)
Encryption	no	not used	some use and very good with TLS & SRTP

© 2005 Cisco Systems, Inc. All rights reserved.

STATE of the INDUSTRY

© 2004, Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Ongoing Work at IETF

Cisco.com

- SRTP Keying
- Voice/Video/IM SPAM prevention
- Retargeting traceability (History)
- Certificate management
- Models for enrollment
- BEHAVE NAT design guidelines
- Delegation of authorization to 3rd parties
- Passing credentials to middle boxes such as firewalls
- ….. and many more :-)

© 2005 Cisco Systems, Inc. All rights reserved.

VoIP Security Checklist

Cisco.com

- How does the system authenticate users?
  - Digest and Mutual TLS are good answers
- How does the system protect privacy of signaling?
  - TLS is a good answer
- How does the system do media privacy?
  - SRTP and S/MIME are good answers
- Do you know who you are talking to?
  - Identity is a good answer
- Can devices easily be enrolled in the system?

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Summary

Cisco.com

- **Voice security is complex but necessary and feasible**
  - **SIP networks are complex. SIP is a multi-domain, multi-party, peer-to-peer rendezvous system**
  - **The internet community has never secured a protocol this broad before**
- **The tools exist to secure this system. SIP and RTP address threats using:**
  - **Digest**
  - **TLS**
  - **S/MIME**
  - **SRTP**
  - **STUN**

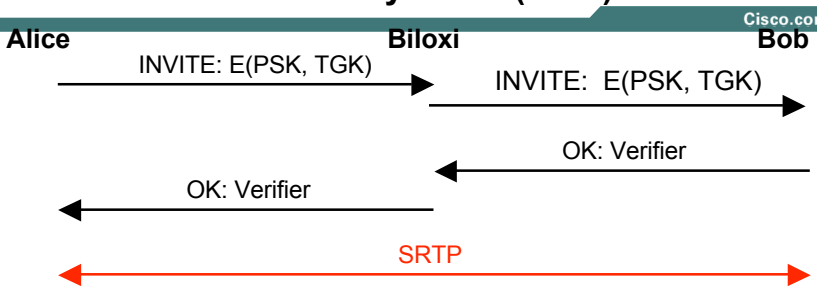
© 2005 Cisco Systems, Inc. All rights reserved.

© 2002, Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

MIKEY Pre-Shared Key Mode (3830)

Cisco.com

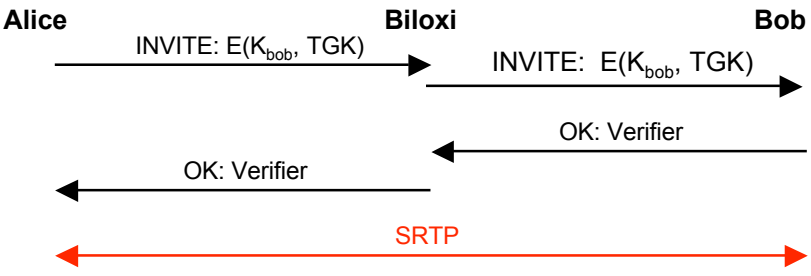


Requires signalling confidentiality	No
Forking	No
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	No (but pre shared key)
Rekeying	Yes
Downgrade attack protection	Yes

© 2005 Cisco Systems, Inc. All rights reserved.

MIKEY Public Key Mode (3830)

Cisco.com



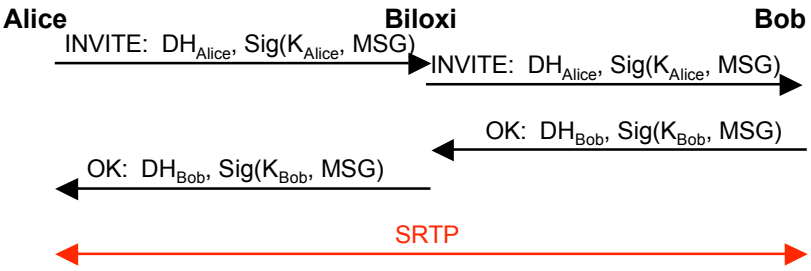
Requires signalling confidentiality	No
Forking	No
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	Yes
Rekeying	Yes
Downgrade attack protection	Yes

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

MIKEY Diffie-Hellman Mode (3830)

Cisco.com

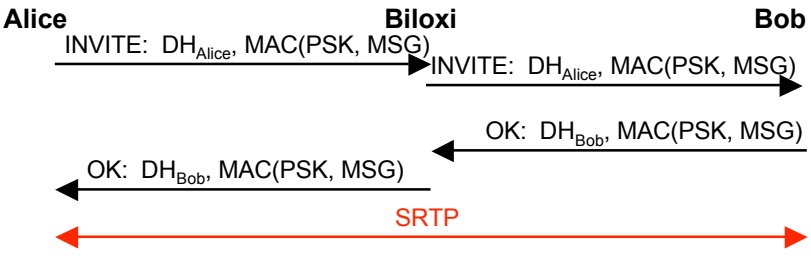


Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	No
Shared-key conferencing	No
Requires PKI	Yes
Rekeying	Yes
Downgrade attack protection	Yes

© 2005 Cisco Systems, Inc. All rights reserved.

MIKEY Diffie-Hellman HMAC Mode (draft-ietf-msec-mikey-dhhmac-11)

Cisco.com



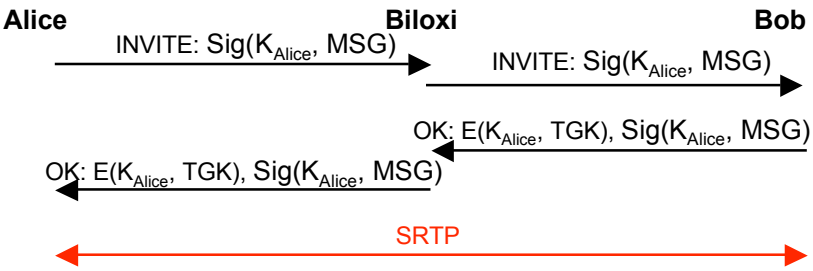
Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	No
Shared-key conferencing	No
Requires PKI	No (pre-shared key)
Rekeying	Yes
Downgrade attack protection	Yes

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

MIKEY RSA-R Mode (draft-ietf-msec-mikey-rsa-r-02)

Cisco.com

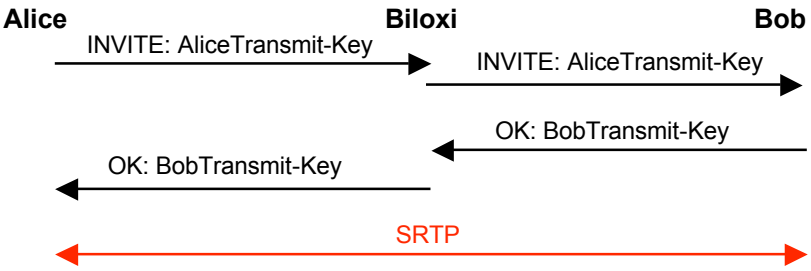


Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	No
Shared-key conferencing	Yes
Requires PKI	Yes
Rekeying	Yes
Downgrade attack protection	Yes

© 2005 Cisco Systems, Inc. All rights reserved.

SDESCRIPTIONS (draft-ietf-mmusic-sdescriptions-12)

Cisco.com



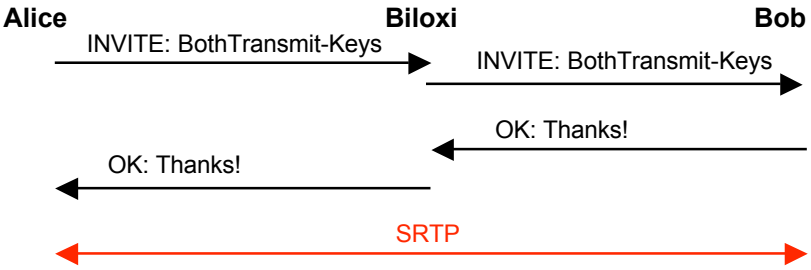
Requires signalling confidentiality	Yes
Forking	Yes (insecure)
Media before SDP answer	No
Shared-key conferencing	Yes
Requires PKI	No
Rekeying	Yes (New Offer)
Downgrade attack protection	No

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

SDES Early Media Mode (draft-wing-mmusic-sdes-early-media-00)

Cisco.com

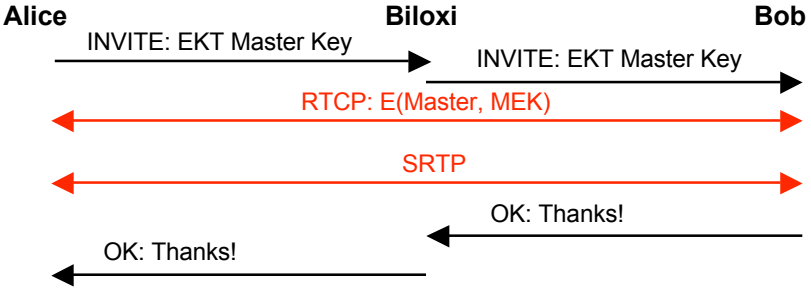


Requires signalling confidentiality	Yes
Forking	Yes (insecure)
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	No
Rekeying	Yes (New Offer)
Downgrade attack protection	No

© 2005 Cisco Systems, Inc. All rights reserved.

Encrypted Key Transport w/ SDES (draft-mcgrew-srtp-ekt-00)

Cisco.com



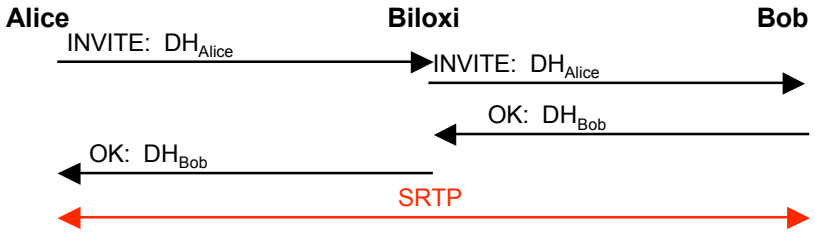
Requires signalling confidentiality	In SDES mode
Forking	Yes (insecure)
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	No
Rekeying	Yes
Downgrade attack protection	Depends on base handshake

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

SDP DH Mode (draft-baugher-mmusic-sdp-00)

Cisco.com

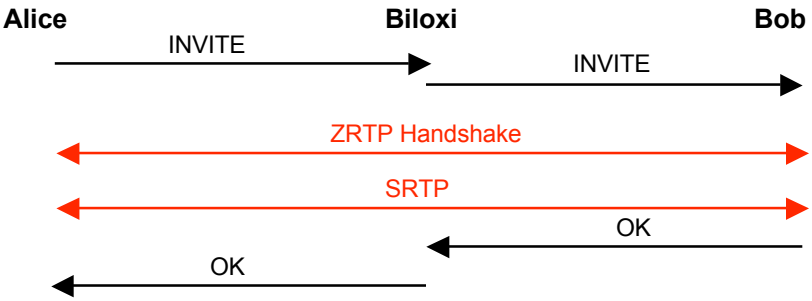


Requires signalling confidentiality	No
Forking	No
Media before SDP answer	No
Shared-key conferencing	No
Requires PKI	No
Rekeying	No
Downgrade attack protection	No

© 2005 Cisco Systems, Inc. All rights reserved.

ZRTP (draft-zimmermann-avt-zrtp-01)

Cisco.com



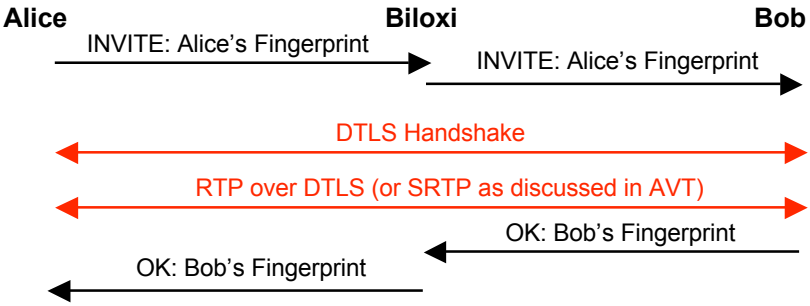
Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	Yes
Shared-key conferencing	No
Requires PKI	No
Rekeying	Yes
Downgrade attack protection	Yes

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

DTLS/RTP (draft-tschofenig-avt-rtp-dtls-00, etc.)

Cisco.com



Requires signalling confidentiality	**No**
Forking	**Yes**
Media before SDP answer	**Yes**
Shared-key conferencing	**No**
Requires PKI	**No**
Rekeying	**Yes**
Downgrade attack protection	**Yes**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc. All rights reserved.