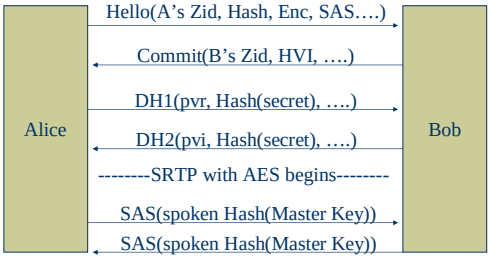
ZFONE

- Philip Zimmermann's new secure VOIP application
- Interoperates with SIP signaling
- Communication with AES by SRTP
- Successor of PGPfone
- Does not rely on a PKI
- Authentication by ZRTP

ZRTP



SRTP
Secure Real Time Transport Protocol

- Goals
  - Confidentiality
  - Message Authentication/Integrity
  - Replay Protection
- Key Refresh / Master Key Expiration
- Entire Packet is MACed
- Payload is encrypted

ZFONE

- Secrecy between 2 parties
- Forward Secrecy
- Authentication (untraditional)
  - No PKI
- Replay protection
- Parties can ***distinguish*** voices

ZFONE
Acknowledged Protocol Properties

- Resourceful adversary can pose as anyone
- Adversary can force a re-SAS
- Privacy
  - ZID's are public
- DOS

Hash Commitment

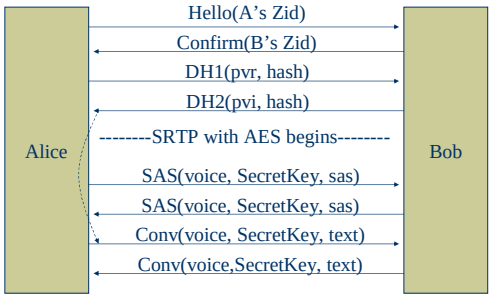
- Hash collision attack on authentication
- Small SAS read aloud
- Attacker needs only to find collision on first 4 bytes of hash(master key)
- Attacker cannot deterministically influence hash(Master Key)

Shared Secrets

- Parties perform SAS once
  - Cache shared secret s1
- Master Secret – s0
  - Based on DH exchange and shared secret
  - Becomes s1 (s1 -> s2, etc…)
- Initiator sends HMAC(s1, “Initiator”)
- Responder sends HMAC(s1, “Responder”)

ZRTP Modeled

Really Really Ridiculously Good Looking



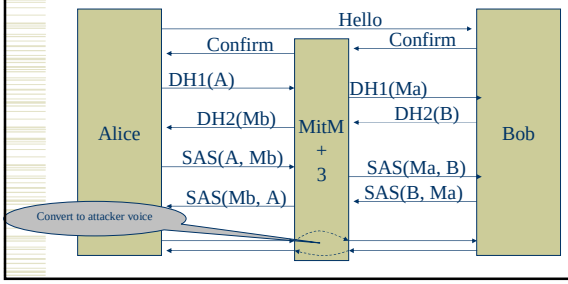
Attack Tensor

- Attacker can simulate Initiator's voice
- Attacker can simulate Responder's voice
- Attacker can convert voice to his own in real time
- Initiator knows Responder's voice in advance
- Responder knows Initiator's voice in advance
- Initiator remembers voice from one session to the next
- Responder remembers voice from one session to the next

Results of Murphi Modeling

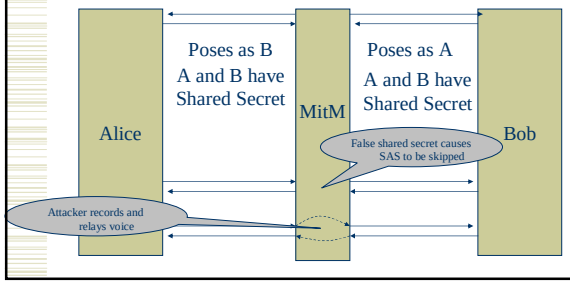
- 61 parameter assignments yielded attacks
- After reduction, 5 independent attacks found!
  - SAS Voice Forgery Attack
  - Bill Clinton Attack
  - 6 Month Attack
  - Court Reporter Attack
  - Hybrid Clinton-Court Reporter Attack

Court Reporter Attack



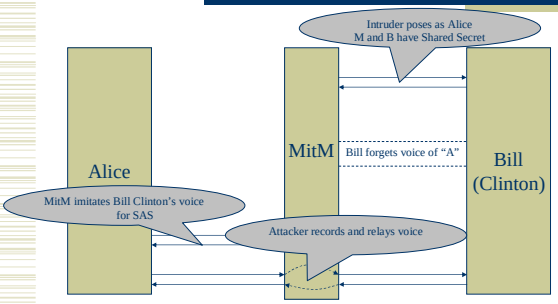
Six Month Attack

A and B don’t remember voices between sessions



Bill Clinton Attack

MitM can imitate the president's voice
Bill doesn't know Alice's voice



Solution: The Chrono-Gambit

- Interpolate Hash(Master Key) between 0 and N seconds
  - N is negotiated in Hello and HashCommit
- Conversation must start ~N seconds from first message exchange
- Probabilistically foils every attack
  - Idea: Hard to interleave conversations starting at different times!

Conclusion

- In normal use cases, ZFone is secure
- In abnormal, but reasonable cases, ZFone can be attacked
  - To mount attacks, adversary needs to be powerful and resourceful
- Questions?