SPEECHSC

Eric Burger
eburger@brooktrout.com
Dave Oran
oran@cisco.com

Note Well
(The Fine Print)

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- the IETF plenary session,
- any IETF working group or portion thereof,
- the IESG, or any member thereof on behalf of the IESG,
- the IAB or any member thereof on behalf of the IAB,
- any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,
- the RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of BCP 78 and BCP 79. Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult BCP 78 for details.

Administrivia

- Note Well (Done)
- Minute Taker
- Jabber Talker
  - How-to: http://www.xmpp.org/ietf-chat.html
  - Server: `ietf.xmpp.org`
  - Room: `speechsc`
- mp3 Web Stream (live)
  - http://videolab.uoregon.edu/events/ietf/ietf626.m3u
- Blue Sheets

Speechsc Agenda

- 5 Intro and Agenda Bashing
- 25 Push to Last Call for MRCPv2
  draft-ietf-speechsc-mrcpv2-06.txt
- 20 Discussion of Security Issues on Requirements
  draft-ietf-speechsc-reqts-06.txt
- 10 Wrap-Up and Action Items

MRCPv2 Push to Last Call

Sarvi Shanmugham

Requirements Security Issues

Dave Oran

Security Issues in SI/SV

- Privacy
  - Main concern is potential for large scale theft of voiceprints and concomitant privacy loss
- Security of protocols
  - Usual questions about confidentiality, integrity, and authentication/authorization
- Threats/Vulnerabilities of a biometric for authentication/authorization

What the CSTA Report Says

"Recommendation: Biometric technologies should not be used to authenticate users via remote authentication servers because of the potential for large-scale privacy and security compromises in the event of a successful attack (either internal or external) against such servers. The use of biometrics for local authentication (for example, to control access to a private key on a smart card) is a more appropriate type of use for biometrics."

Threats to SI/SV Protocols

- External Threats
  - Attacks can be foiled by well-understood security means
  - Speechsc employs
    - TLS encryption of the control channel,
    - SRTP encryption of the media channel, and
    - authentication/authorization of all elements in the chain from the speaker to the server holding the voiceprints.

Threats to SI/SV Servers

- Internal Attacks
  - Stealing the voiceprint database
  - Compromise of the server system, including its keying material.
- Server with voiceprints like a /etc/passwd file
  - Prudent to store the data encrypted to foil theft by removal/copying stolen en masse.
  - Speechsc a protocol standard, so not clear what we need to do about this
  - Server compromise can leak voiceprint information.
    - Same situation as passwords in Radius

Biometric Considerations

- Replay and impersonation attacks.
  - Not a static biometrics (e.g. retina, face geometry, fingerprints,
    - speaker verification can (and is) done via challenge response protocols
      - Subject asked to say a number of words or a phrase *chosen by the verification system*,
      - result matched against the the voiceprint.
  - Possession of a stolen voiceprint does not by itself enable impersonation
  - Accurate voiceprint has similar confidence to a fingerprint, retina scan, etc., but…can't be used unless you can be induced to speak enough to allow a match

Privacy

- Voiceprints of varying quality can be obtained by anything which can record your voice.
  - Voiceprint used for identification/verification needs to be protected, but not all recording devices will be super-secure
  - Question: is it really useful to require servers holding voiceprints to be more secure than those holding speech recordings, especially if those recordings have meta-data allowing the source to be identified (e.g. calling phone number, logged in user id)?
  - Is the consequence of this to revisit all the specs like RTSP, SIP, XCON, etc. to ensure that they cannot be used to make recordings that can be turned offline into voiceprints?

Additional Considerations

- If you speak in a non-secure session, there are obvious problems (e.g. eavesdropping and surreptitious recording)
- Secure sessions -generally have authentication by means other than speaker verification
  - implicit agreement that your identity can be ascertained by the participants?
  - What about a secure session with explicit anonymity? Speaker identification does limit privacy somewhat, but is it out of line with common expectations of privacy
  - If ndirect methods of identification (such as speaker identification) need to be thwarted there are things like voice distorting devices which rendering the identification and verification systems impotent.

Next Steps

- Discussion on list -
  - have we raised all the relevant issues
  - What tradeoffs are appropriate
  - How to make the case for those tradeoffs
- Work with Area Directors (Transport & Security) to resolve these issues
- If needed, establish an on-going “security advisor” function to help get closure on both requirements and MRCPv2 specification.

Milestones
Work Group Progress

NOV 02 *Done*	Requirements ID submitted to IESG for publication (info)
APR 03 *Done*	Submit Internet Draft(s) Analyzing Existing Protocols (info)
JUN 03 *Done*	Submit Internet Draft Describing New Protocol (standards track)
OCT 03 *Done*	Submit Drafts to IESG for publication
SEP 04	WGLC MRCPv2 *Late*
Oct 04 *Late*	Submit MRCPv2 Specification to IESG

Proposed Milestone Update

- APR 05 MRCPv2 WGLC
- JUN 05 Submit MRCPv2 to IESG

Thanks!