Christian Wieser

Vulnerabilities in VoIP systems

c07-sip
injRTP

Motivation

Software vulnerabilities prevail:

"Fragile and insecure software continues to be a major threat to a society increasingly reliant on complex software systems."
- Anup Ghosh [Risks Digest 21.30]

Our purpose:

*"To study, evaluate and develop methods of implementing and testing application and system software in order to prevent, discover and eliminate implementation level security vulnerabilities in a **pro-active** fashion.*
*Our focus is on **implementation level** security issues and software security testing."*

Dominant security problems

From ICAT vulnerability statics

Vulnerability Type	2003	2002	2001	2000
Input Validation Error	526 (52%)	661 (51%)	744 (49%)	359 (36%)
(Boundary Condition Error)	81 (8%)	22 (2%)	51 (3%)	66 (7%)
(Buffer Overflow)	236 (23%)	288 (22%)	316 (21%)	190 (19%)
Access Validation Error	92 (9%)	121 (9%)	126 (8%)	168 (17%)
Exceptional Condition Error	152 (15%)	117 (9%)	146 (10%)	119 (12%)
Environment Error	3 (0%)	10 (1%)	36 (2%)	19 (2%)
Configuration Error	49 (5%)	67 (5%)	74 (5%)	82 (8%)
Race Condition	17 (2%)	22 (2%)	50 (3%)	21 (2%)
Design Error	266 (26%)	407 (31%)	339 (26%)	166 (17%)
Other	18 (2%)	2 (0%)	8 (1%)	14 (1%)

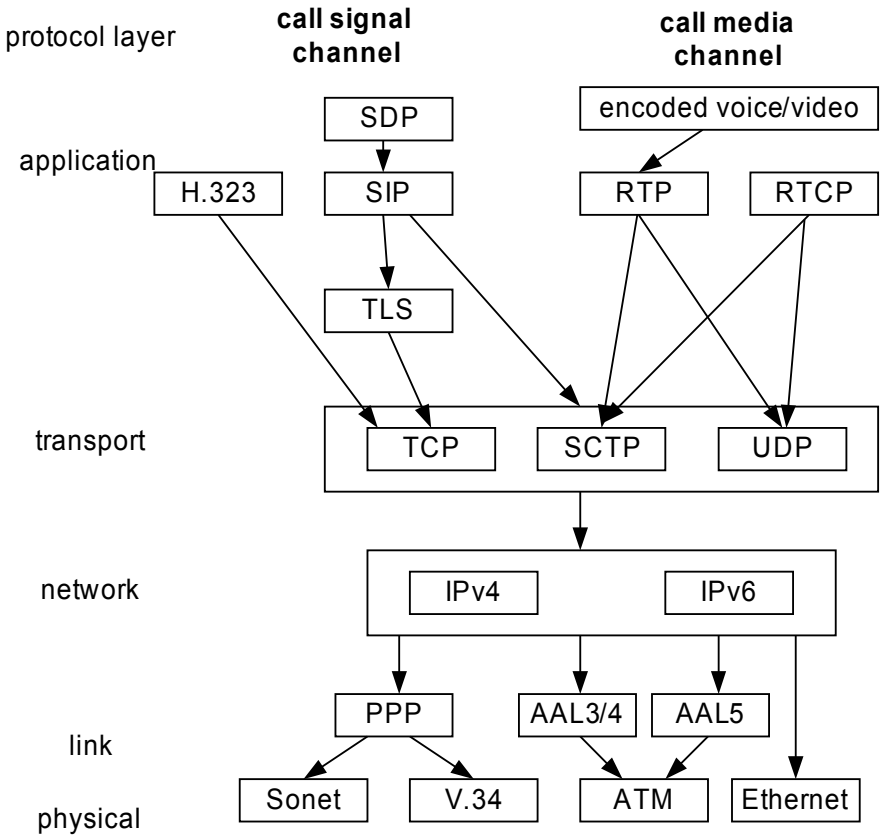
Dominance of “Input Validation Error”

VoIP systems

Typical SIP VoIP stack (simplified)

- different protocols for the transmission of voice and call control

This presentation covers findings on SIP, H.323 and RTP implementations



SIP, H.323 robustness test-suite

a.k.a

PROTOS c07-sip

PROTOS c07-h2250v4

PROTOS project

Security Testing of Protocol Implementations

Results:

- A novel (mini-simulation) vulnerability black box testing method developed
- Several papers and test suites published

Continuation:

- Spin-off company Codenomicon Ltd
- OUSPG will continue with public research

c07-sip design

Mutating SIP INVITE-requests to simulate attacks to the Software Under Test (SUT).

- 54 test groups
- 4527 test cases

Available as Java JAR-package

UDP used on transport layer

Teardown with

- CANCEL/ACK messages

Valid-case as minimal instrumentation

c07-sip results

- Approach new to SIP scene
- Alarming rates of failed subjects
  - Nine implementations (6 UA, 3 servers) tested
    - 1 passed
    - 8 failed in various test-groups
  - For demonstration purpose
    - 2 working exploits

"Hitting the Granny with a stick"?

Vulnerability Process

Vulnerability process: Phases

- Development
  - Creating and wrapping-up the test-suite
  - Internally testing the available implementations
- Pre-release
  - Involvement of neutral third party (in this case CERT/CC)
  - Notifying respective vendors of any vulnerabilities found
  - Distributing the test-suite to identified vendors implementing the chosen protocol
  - Vulnerability and advisory coordination
  - Grace period
- Release
  - Deploying the test-suite for public perusal
  - Collecting feedback
  - Reiterating either with same or next protocol

H.323 – looking any better?

c07-h2250v4

subset of H.323

OUSPG created a robustness test-suite

Comparable results:

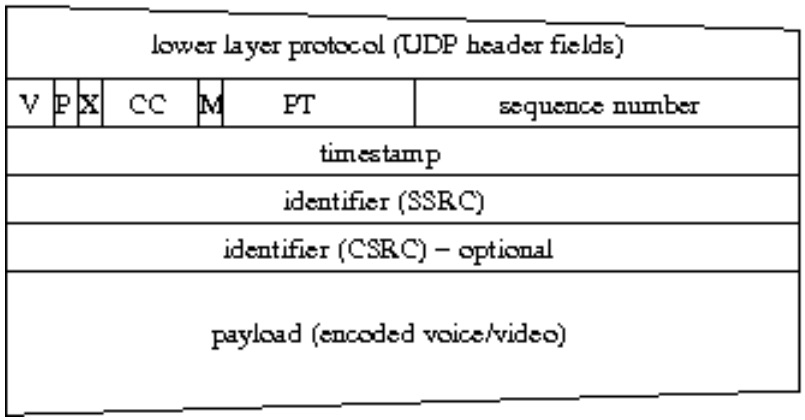
Test-run #	*Total test-cases*	*Failed test-cases*	*Total groups*	*Failed groups (inconclusive)*
tr-001	4497	188	134	45
tr-002	4497	266	134	7
tr-003	4497	221	134	33
tr-004	4497	N	134	4(15)
tr-005	4497	61	134	13
tr-006	4497	2	134	1
tr-007	4497	N	134	N
tr-008	4497	0	134	0

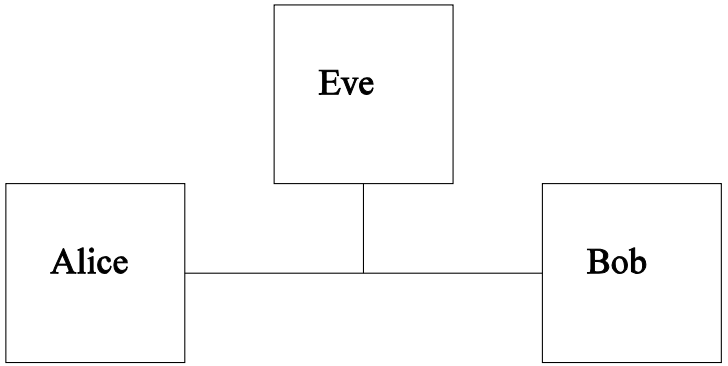
RTP injection

Project name: injRtp3

Introduction

- Purpose: Inject a third party voice into an ongoing VoIP session
- Involved protocol: Real Time Protocol (RTP)
  - Used by SIP and H.323 to transmit voice/video
  - Typically used over UDP
  - Included headers
    - Sequence number
    - Time stamp
    - Identifier (SSRC)
- Classical test bed
  - Alice calls Bob, Eve interferes
- 6 different implementations tested
- Checking for InfoSec implications





Test cases

Confidentiality

- Eve can eavesdrop into the ongoing call

Integrity

- Eve injects her own voice, adapting RTP headers and payload.
  - Two samples: 1 and 10 seconds
  - Is Eves voice understandable on the tested implementation?

Implementation	1s duration	10s duration
001	good	good
002	understandable	understandable
003	poor	poor
004	good	good
005	understandable	understandable
006	good	good

Test cases (II)

Eve simplifies attack, not adopting RTP header values

Do implementations evaluate RTP header values?

Implementation	SSRC	Timestamp	Sequence number
001	no	partly	partly
002	no	no	no
003	yes	partly	partly
004	no	no	no
005	no	no	no
006	no	no	no

She only needs to know/guess the payload encoding

Test cases (III)

Eve checks transfer layer dependence

Does the attack still work when different UDP parameters are incorrect?

Implementation	Accepts broadcast destination IP	Incorrect source IP	Incorrect source UDP port
001	yes	yes	yes
002	yes	yes	yes
003	no	no	no
004	yes	yes	yes
005	yes	yes	yes
006	no	no	no

Test cases (IV)

Eve tries to guess the UDP destination port

Implementation	Start up	Next call
001	fixed (49608)	newPort = oldPort - 2
002	fixed (5004)	fixed (newPort = OldPort)
003	fixed (5000)	newPort = oldPort + 2
004	fixed (49152)	newPort = oldPort + 2
005	fixed (5000)	newPort = oldPort + 4
006	fixed (32782)	fixed (newPort = OldPort)

A combination of missing UDP and RTP evaluation allows the attack to work without tapping into the call.

A new way to distribute Spam over IP telephony (SPIT)?

Accessibility

Eve floods the call with arbitrary RTP packets and succeeds to jam the ongoing connection

Summary

Implementation Level Vulnerabilities show relevant for VoIP

c07-sip, c07-h2250v4

- Noticeable amount of vulnerabilities found
- Awareness among vendors was non equally distributed
- Vulnerability process seems new to VoIP community
- Fair amount of interest
- Further information:
- http://www.ee.oulu.fi/research/ouspg/protos/testing/

injRTP

- Voice injection into an ongoing call via RTP is possible
- Information security could be preached in all 6 tested cases