Communication and Network Security

EECE 571B “Computer Security”

Konstantin Beznosov

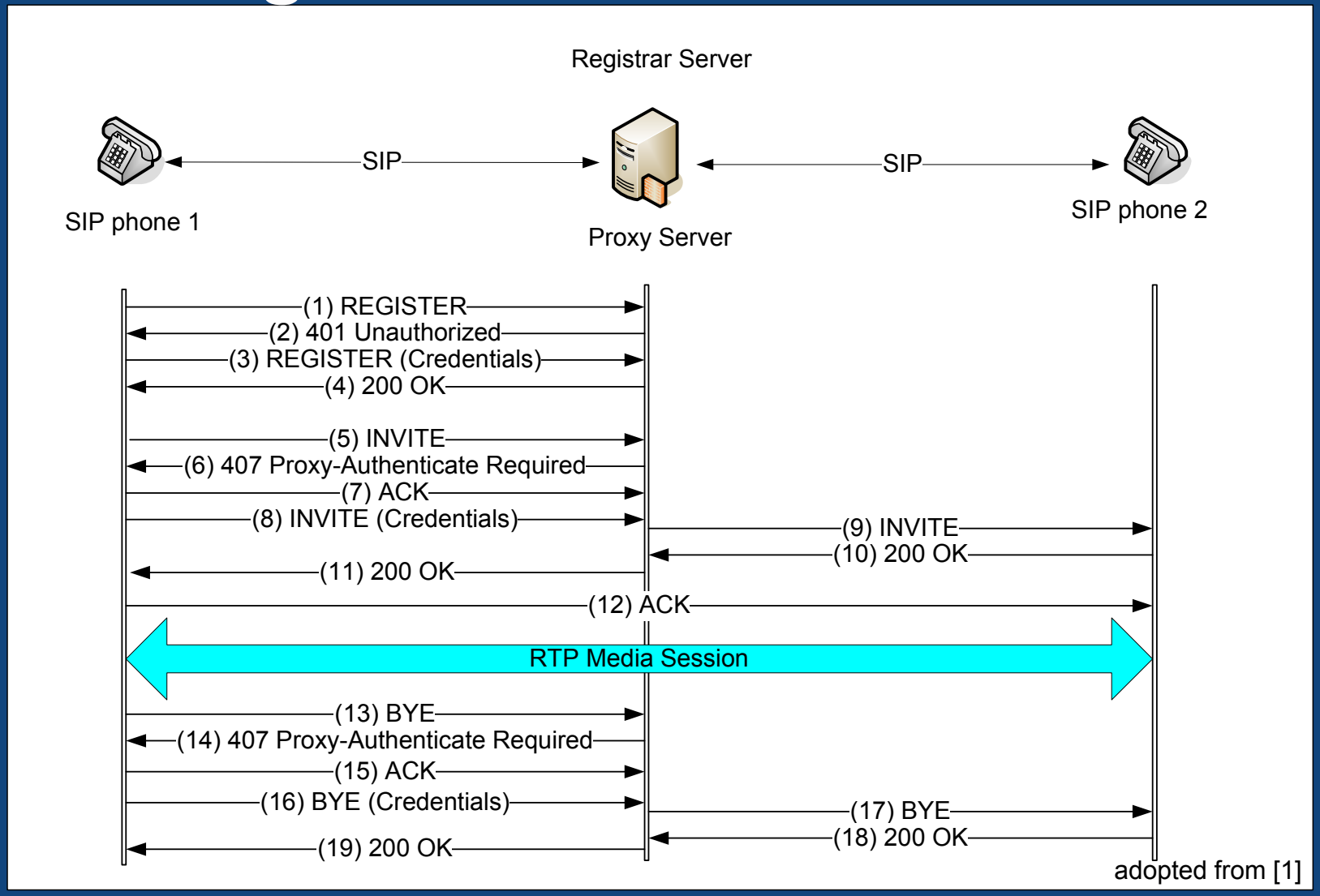
DOS of senders caused by receivers

Sherwood, R., Bhattacharjee, B., and Braud, R. 2005. **"Misbehaving TCP receivers can cause internet-wide congestion collapse**," In Proceedings of the 12th ACM Conference on Computer and Communications Security (Alexandria, VA, USA, November 07 – 11, 2005). CCS '05. ACM, New York, NY, 383-392.

MITM Attacks on VoIP

R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang. "**On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers**," In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09).

message flow of SIP authentication



credentials = MD5(request-URI, username, shared password between the phone and the SIP server, realm, nonce)

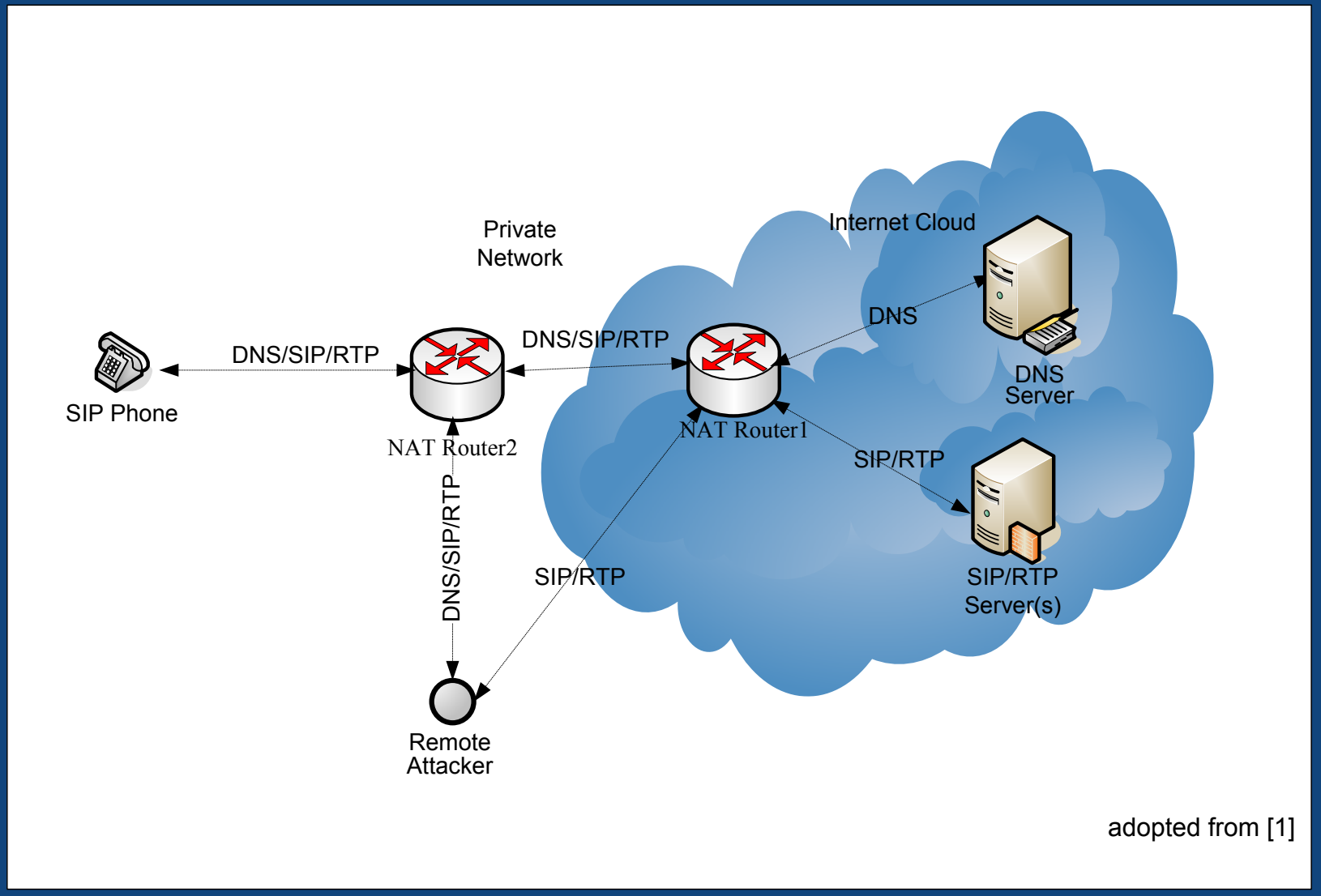
how can an adversary exploit these?

- no integrity protection of the traffic between SIP phone and SIP server
- (Vonage) SIP phone obtains SIP server's IP address via DNS query
  - SIP phone uses static ID and the range of 1,100 port numbers for DNS queries
- SIP phone sends DNS query each time it restarts
- SIP phone crashes when receives an INVITE message

setup

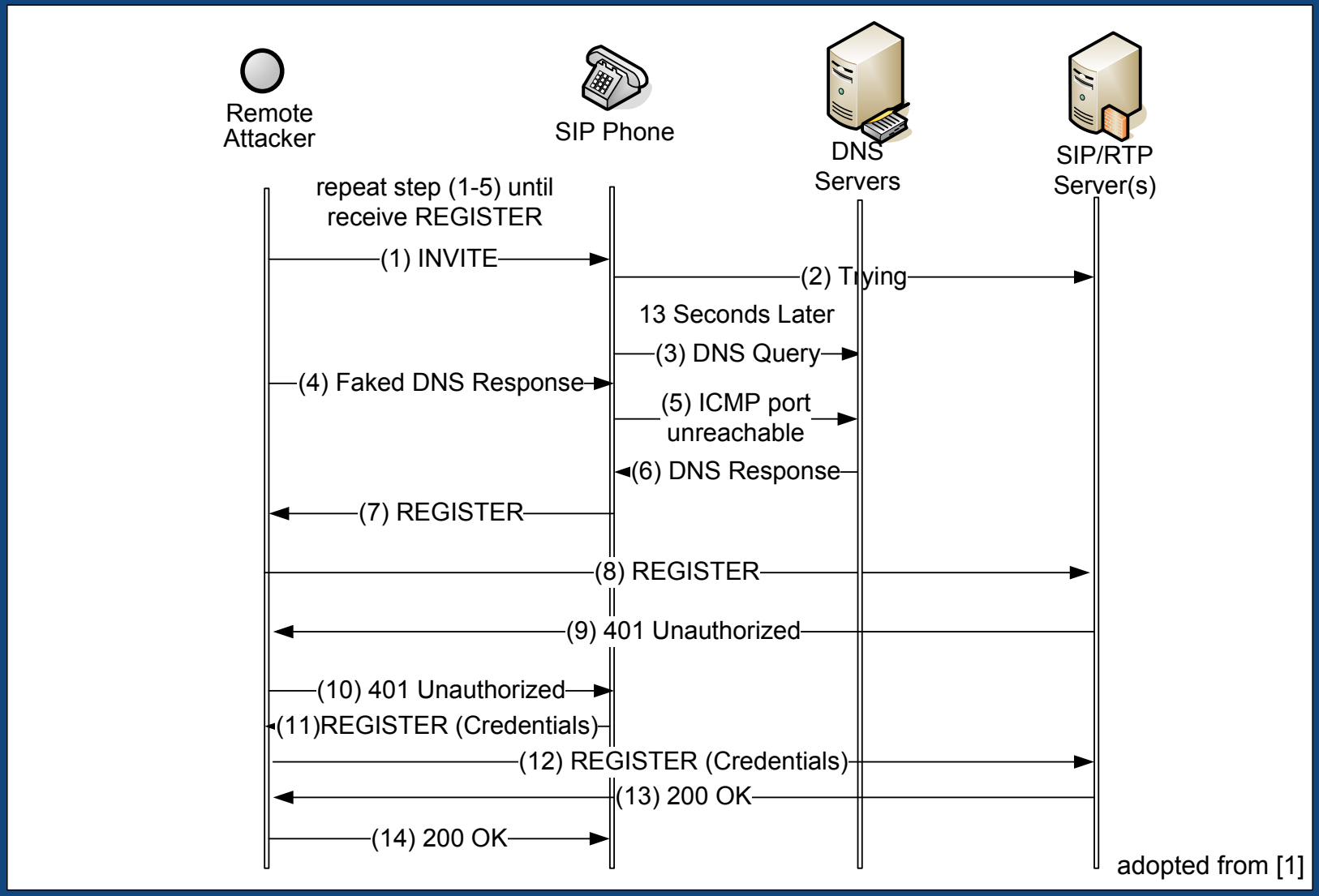
- MITM attacker in the path of a VoIP traffic can
  - wiretap
  - divert
  - hijack
- [1] shows that
  - the attacker outside of VoIP traffic can become a MITM
  - the remote attacker can
    - crash and reboot the targeted Vonage SIP phone
    - trick the Vonage SIP phone into taking any IP address as that of the Vonage SIP server via spoofed DNS responses.
    - “inject” itself in the VoIP traffic of the victim Vonage SIP phone

testbed

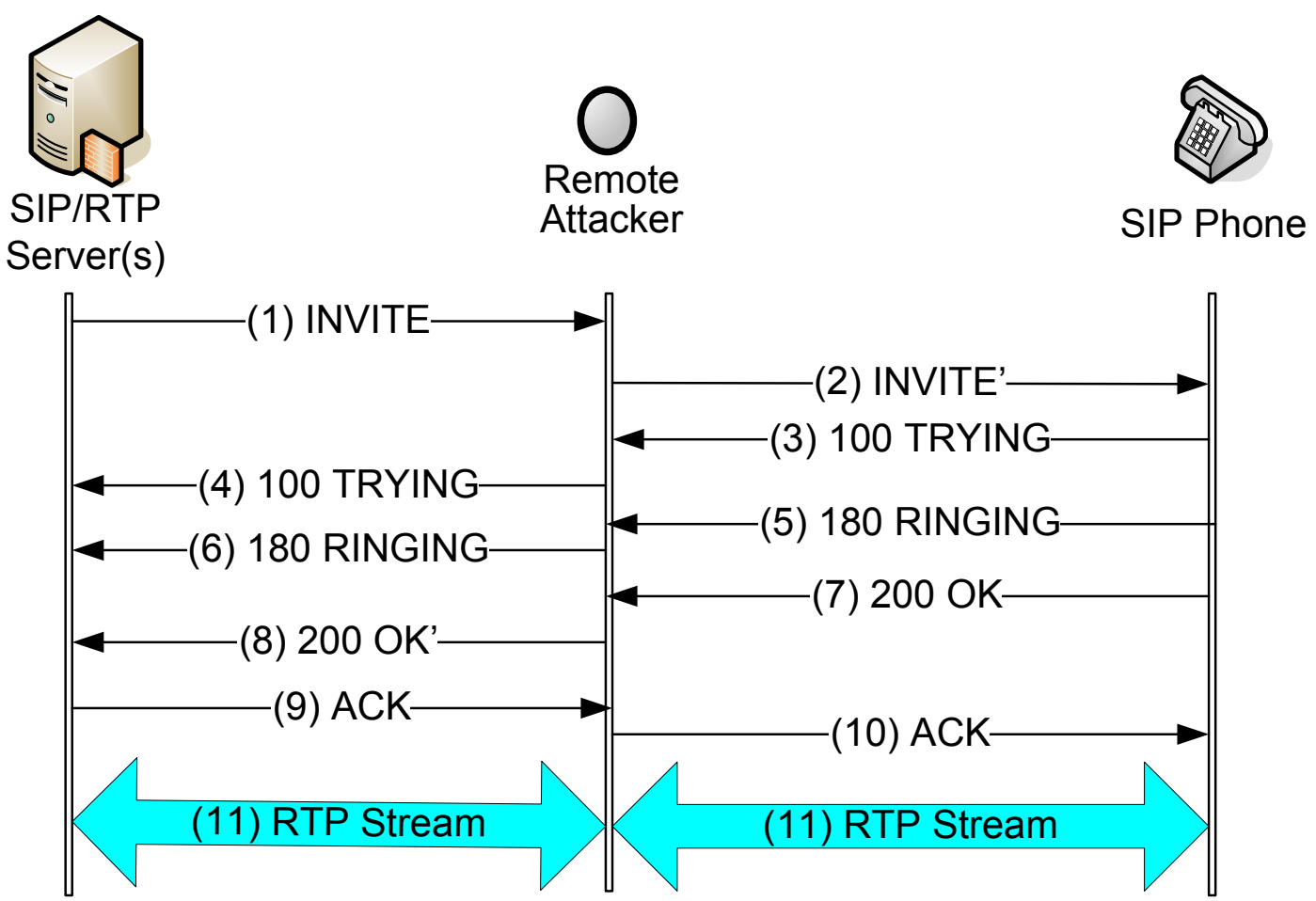


adopted from [1]

DNS spoofing attack



wiretapping calls



adopted from [1]

how to avoid such attacks?

references

1. R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang. “On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers,” In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09). ACM, New York, NY, USA, 61-69. DOI=10.1145/1533057.1533069 http://doi.acm.org/10.1145/1533057.1533069