Anonymity summary

vrijdag 6 januari 2023 19:34

TCP/IP and TLS do not provide anonymity. IPSec only provides anonymity in tunnel modes, and only for the part between gateways.

Dining cryptographers problem: 3 cryptographers on dinner; someone paid; want to figure out if it was one of them without revealing who paid (if anyone).

- Share pairwise secret bits (between AB, BC, AC)
- Everyone prepares as message the XOR of their shared bits
- If someone paid, they XOR that message with 1.
- Broadcast all messages
- XOR over all messages is 0 if none paid and 1 if someone paid.

Cryptographic mixing: to send message m from A to B, m is sent to the mix in the format $E_{K_M}\left(B, E_{K_B}(m)\right)$. M forwards the message to B, who can decrypt it.

Flushing modes:

- Message threshold: wait until n messages are received, then release all.
- Message pool: pool size n, probability p. After n messages in pool, shuffle, then send each with probability p. Unsent messages remain in pool.
- Stop and go: sender determines waiting time for each mix

Adversary properties:

- Internal-External: can compromise communication medium (external) and mix nodes/recipients/senders (internal)
- Passive-Active: active can arbitrarily modify computations & messages (insert/delete); passive can only listen
- Static-Adaptive: Static chooses compromised resources upfront; adaptive can change resources under control during protocol execution.

Countermeasures:

- Padding
- Dummy traffic

Re-encryption mixnets: re-randomize ciphertext at each node instead of decrypting. Based on a re-randomizable form of ElGamal encryption.