Lecture 9

zaterdag 10 december 2022 19:43

anonymity → participate in discussion without revealing who you are

↓ protect metadata which can be even more important than the data itself

nobody knows Alice's recipient (not even the recipient itself)

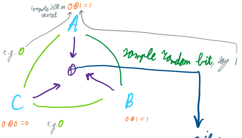
IP address breaks anonymity in TCP/IP

TLS → above network layer → IP address still leaked

IPsec → tunnel mode hides IP from MitM, but not from receiver

dining cryptographers problem: did one of group pay or outside group

without revealing identity



0 if no one paid

if e.g. A paid, A flips their bit → 1 if someone paid

as B does not know the bit shared between A and C ⇒ perfect anonymity

can be extended to longer messages

can be used for any group size

only broadcast

easy to DoS

inefficient

N^2 shared keys

everyone has to participate in every message transmission

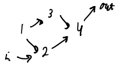
problems when multiple parties paid

Mixnet → route messages through mixes / mixing relay

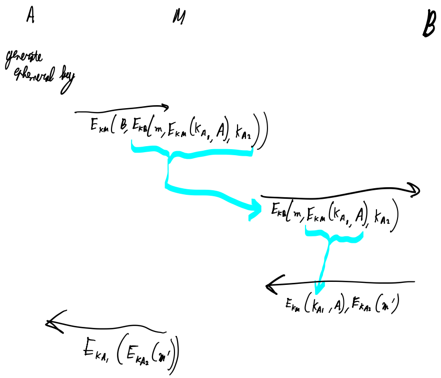
more messages ⇒ more anonymity

cascade in → 1 → 2 → 3 → 4

random order / free routing



sender A
receiver B
mixe M
probabilistic public key encryption Kg, E, D
keygen



generate ephemeral key

$E_{K_M}(B, \underbrace{E_{K_B}(m, E_{K_M}(k_{A_1}, A), k_{A_2})})$

$E_{K_B}(m, \underbrace{E_{K_M}(k_{A_1}, A)}, k_{A_2})$

$E_{K_M}(k_{A_1}, A), E_{K_{A_2}}(m')$

$E_{K_{A_1}}(E_{K_{A_2}}(m'))$

flushing modes

message threshold : wait until N messages are received, then release all of them

message pool : pool size n, probability p → wait until n messages in pool , then send each message with probability p ; unsent message remain in pool

stop and go : sender specifies waiting time for each mixe adversary properties :

internal / external
↓ compromise mix nodes / recipients / senders
↳ compromise network

passive / active
↓ listen only
↓ modify messages

static / adaptive
↓ corrupt resources before attack
↓ change resources during attack

generic attacks :

brute-force → follow all paths message could have taken

node-flushing → send t-1 messages, last message must go to recipient
↑ known recipient, come from attacker

correlation attacks : use e.g. time / size (or other statistics) to correlate incoming + outgoing messages

Countermeasures : padding
dummy traffic

complicate tracing

remove identifiable / recognizable message

decreased bandwidth

authentication allows for quotas

prevents DDoS
prevents flushing attacks

requires pseudonyms

re-Encryption ; instead of decrypting, re-randomize ciphertext

important for exam: hybrid encryption

symmetric + asymmetric

finding find receiver is difficult

El Gamal : $G = \langle g \rangle$

cyclic group

generator

$|G| = p$

order of G

prime

$gen(G): \; x \xleftarrow{\$} \mathbb{Z}_p^*$

uniform random sample

secret key

public key $= g^x$

$enc(g^x): \; r \xleftarrow{\$} \mathbb{Z}_p^*$

$c = (g^r, (g^x)^r \cdot m)$

in ElGamal: looks like random element, even if g^r and g^x are known

$dec(g^r, \overbrace{g^{rx}} \cdot m, x): \quad m = \frac{g^{rx} \cdot m}{(g^r)^x}$

given $c = (g^r, g^{rx} \cdot m)$ and g^x (and r')

we can do :

$r' \xleftarrow{\$} \mathbb{Z}_p^*$

$g^r \cdot g^{r'} = g^{r+r'} = g^{r''}$

$g^{rx} \cdot m \cdot g^{r'x} = g^{rx+r'x} \cdot m$

$g^{rx} \cdot m \, (g^x)^{r'} = g^{r''x} \cdot m$

to hide g^x for anonymity

$g^r, g^{rx} \cdot m, g^s, g^{sx}$

$r', s' \xleftarrow{\$} \mathbb{Z}_p^*$

$g^r \cdot (g^{sr'}) = g^{r+sr'}$

$g^{rx} \cdot m \, (g^{sx})^{r'} = g^{rx+sxr'} \cdot m = g^{x(r+sr')} \cdot m$

$(g^s)^{s'} = g^{ss'}, \; (g^{sx})^{s'} = g^{(ss')x}$

For

server cert $B = (\hat{B}, B)$, system parameters g, G^*

1. $\hat{A}$ creates ephemeral key pair $(x, X \leftarrow g^{x})$
2. $\hat{A}$ initializes connection sending X
3. $\hat{B}$ creates ephemeral key pair $(y, Y \leftarrow g^{y})$
4. $\hat{B}$ sends y
5. $\hat{A}$ computes shared secret $K = (BY)^{x}$ $\boxed{= g^{x(b+y)}}$ flawed...
6. $\hat{B}$ computes shared secret $K = X^{b+y}$

compute $g^{y} = g^{-b} = (g^{b})^{-1}$

or $(b+y) \xleftarrow{\$} \mathbb{Z}_p^*$

then $\dfrac{g^{(b+y)}}{g^{b}} = g^{y}$