Snake.li: privacy nell'era del social web

Michele Beretta
mik@snake.li

Alessandro Di Federico
ale@snake.li

Politecnico Open unix Labs

Conferenza Privacy & Sicurezza 2014

Indice

Indice

Il problema

Privacy

In che stato è la privacy su Internet?

- Le rivelazioni di Snowden lo mostrano chiaramente
- L'NSA ha un sofisticato sistema di sorveglianza di massa
- Se non sei americano, peggio ancora[1]

[1] http://tinyurl.com/datagate-summary

Cina

- Fino a qualche tempo fa Skype in Cina non era disponibile
- Al suo posto si usava TOM Online
- TOM censurava alcune keyword nelle conversazioni
- E le uploadava su alcuni server in Cina[2]

[2] http://tinyurl.com/tom-skype-upload

Overly-targeted ads

- Facebook e altri fondano il loro business sulla pubblicità
- La pubblicità è sempre di più targhettizzata
- Quello che condividiamo viene usato per identificarci
- Viene effettuato non solo dai social network

Abbiamo bisogno di qualcosa di meglio

Indice

Possibili soluzioni

Quali caratteristiche deve avere un protocollo?

Sicurezza dell'informazione

- Riservatezza
- Integrità
- Autenticazione

Sicurezza dell'informazione

- Riservatezza
- Integrità
- Autenticazione

Excursus crittografia asimmetrica

Metadati

- Non solo il contenuto del messaggio va protetto
- Anche le meta-informazioni, quali:
  - Mittente
  - Destinatario
  - Data e ora

Sicurezza di default

- Molti sistemi richiedono di attivare la “sicurezza”
- Se l’utente lo trova complicato non lo farà
- Un osservatore individua facilmente messaggi sensibili
- E così pure individui sensibili

Usabilità e scalabilità

- La sicurezza rischia di compromettere l'usabilità
- Deve essere possibile comunicare in gruppi, anche grandi
- Le questioni richiedono un'attenzione specifica

Da chi ci stiamo difendendo?

- L'obiettivo è difendersi da:
  - Cracker
  - Governi
  - Il provider del servizio stesso

Domande?

Indice

Lo stato attuale

Facciamo una rapida analisi dei servizi attuali rispetto a:

- Riservatezza dei dati
- Possibilità di impersonare un altro utente
- Accesso ai metadati
- Comunicazione sicura in gruppo
- Comunicazioni sicure di default

Instant messaging

- La privacy è un problema anche per queste applicazioni

Instant messaging

- La privacy è un problema anche per queste applicazioni
- Di recente sono comparse molte nuove applacazioni

Instant messaging

- La privacy è un problema anche per queste applicazioni
- Di recente sono comparse molte nuove applacazioni
- Poche si focalizzano sulle problematiche legate alla privacy

Analisi di alcune applicazioni

Riservatezza
Autenticazione
Comunicazione di gruppo sicura
Metadati protetti
Sicuro di default

Whatsapp

	Whatsapp
Riservatezza	×
Autenticazione	×
Comunicazione di gruppo sicura	×
Metadati protetti	×
Sicuro di default	×

Telegram

	Whatsapp	Telegram
Riservatezza	×	✓
Autenticazione	×	(✓)
Comunicazione di gruppo sicura	×	(✓)
Metadati protetti	×	×
Sicuro di default	×	(✓)

Threema

	Whatsapp	Telegram	Threema
Riservatezza	×	✓	✓
Comunicazione di gruppo sicura	×	(✓)	(✓)
Autenticazione	×	(✓)	✓
Metadati protetti	×	×	×
Sicuro di default	×	(✓)	✓

Social

	Facebook
Riservatezza	×
Autenticazione	×
Comunicazione di gruppo sicura	×
Metadati protetti	×
Sicuro di default	×

Social

	Facebook	Diaspora
Riservatezza	×	×
Autenticazione	×	×
Comunicazione di gruppo sicura	×	×
Metadati protetti	×	×
Sicuro di default	×	×

Social

	Facebook	Diaspora	Syme
Riservatezza	×	×	✓
Autenticazione	×	×	(✓)
Comunicazione di gruppo sicura	×	×	(✓)
Metadati protetti	×	×	×
Sicuro di default	×	×	✓

Ispirazione

- Abbiamo preso ispirazione principalmente da:
  - PGP
  - OTR

PGP

PGP

- Spesso usato per scambiare e-mail in maniera sicura

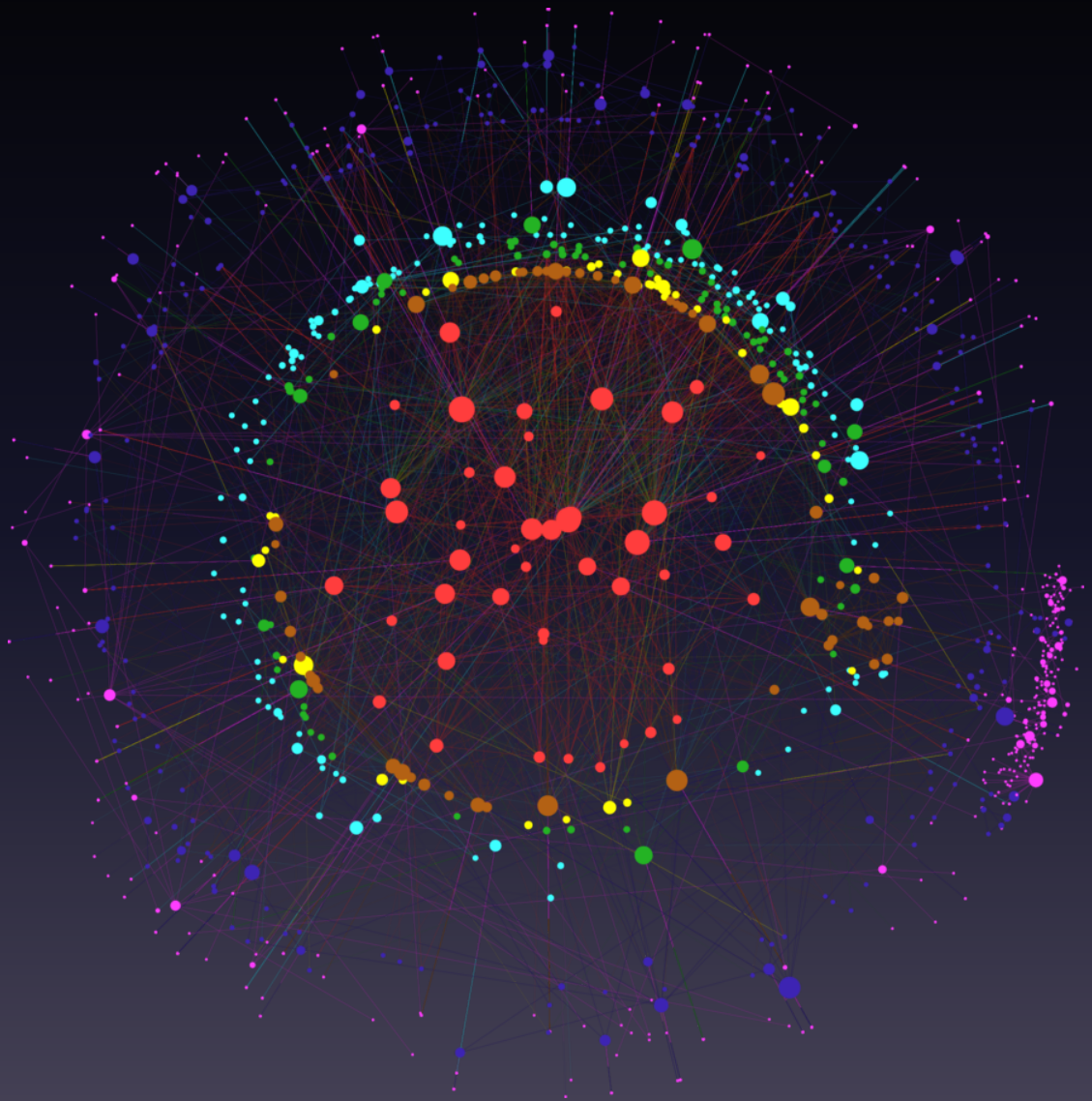
PGP

- Spesso usato per scambiare e-mail in maniera sicura
- Garantisce le seguenti proprietà:
  - Confidenzialità
  - Autenticità
  - Integrità

PGP: autenticazione

Verifica manuale
della chiave pubblica

PGP: Web of Trust



2 7 25 98 390

7 6 5 4 3 2 1

PGP: Web of Trust

2 7 25 98 390

7 6 5 4 3 2 1

Comunicazione di gruppo

Non scala

OTR

Off-the-Record Messaging

OTR

Off-the-Record Messaging

- Protocollo cifrato per sistemi di IM

OTR

Off-the-Record Messaging

- Protocollo cifrato per sistemi di IM
- Autenticazione in-band

OTR

Off-the-Record Messaging

- Protocollo cifrato per sistemi di IM
- Autenticazione in-band
- Soltanto messaggistica uno-ad-uno

PGP e OTR

	PGP	OTR
Riservatezza	✓	✓
Autenticazione	✓	✓
Comunicazione di gruppo sicura	(✓)	×
Metadati protetti	×	×
Sicuro di default	×	×

Domande?

Indice

Indice

Snake

- Piattaforma per lo scambio di messaggi tra utenti fortemente orientata alla privacy

Snake

- Piattaforma per lo scambio di messaggi tra utenti fortemente orientata alla privacy
- Architettura client-server

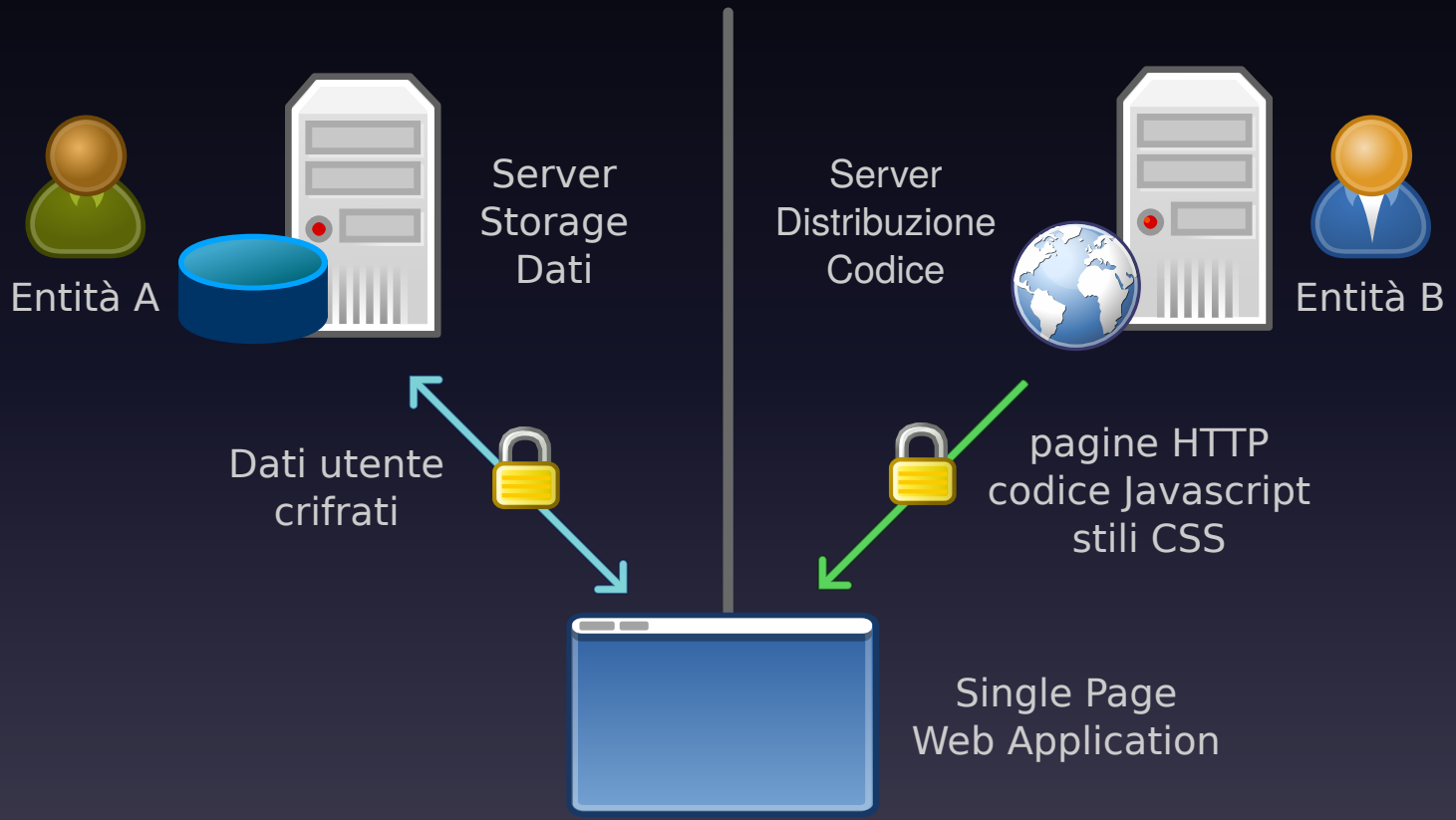
Snake

- Piattaforma per lo scambio di messaggi tra utenti fortemente orientata alla privacy
- Architettura client-server
- Cifratura end-to-end delle conversazoni e autenticazione delle chiavi pubbliche in-band

Snake

- Piattaforma per lo scambio di messaggi tra utenti fortemente orientata alla privacy
- Architettura client-server
- Cifratura end-to-end delle conversazoni e autenticazione delle chiavi pubbliche in-band
- Codice rilasciato con licenza opensource, client e server

Architettura



Client

- È una HTML5 in-browser Single Page Application

Client

- È una HTML5 in-browser Single Page Application
- Tutte le comunicazioni sono cifrate end-to-end
- L’autenticazione delle chiavi è in-band

Client

- È una HTML5 in-browser Single Page Application
- Tutte le comunicazioni sono cifrate end-to-end
- L'autenticazione delle chiavi è in-band
- WebCrypto API, W3C standard
  - PBKDF2 per la derivazione di chiavi da password
  - AES-GCM per la cifratura/decifratura simmetrica
  - SHA-256 per l'hash crittografico
  - ECDSA per generazione e verifica di firme

Server distribuzione del codice

- Il codice distribuito ha licenza opensource

Server distribuzione del codice

- Il codice distribuito ha licenza opensource
- È personalizzabile per aggiungere nuove funzioni

Server distribuzione del codice

- Il codice distribuito ha licenza opensource
- È personalizzabile per aggiungere nuove funzioni
- Il server garantisce l'integrità del codice

Storage server

- È una semplice interfaccia HTTP ad un database per effettuare delle operazioni CRUD

Storage server

- È una semplice interfaccia HTTP ad un database per effettuare delle operazioni CRUD
- Non può leggere i contenuti dei messaggi scambiati

Storage server

- È una semplice interfaccia HTTP ad un database per effettuare delle operazioni CRUD
- Non può leggere i contenuti dei messaggi scambiati
- Ogni eventuale modifica maligna dei dati può essere facilmente rilevata dal client

Domande?

Indice

Autenticazione di chiavi pubbliche

L'approccio adottato in SNAKE

Ci siamo focalizzati su due aspetti:

Autenticazione di chiavi pubbliche

L'approccio adottato in SNAKE

Ci siamo focalizzati su due aspetti:

- Un metodo di autenticazione diretta **in-band**

Autenticazione di chiavi pubbliche

L'approccio adottato in Snake

Ci siamo focalizzati su due aspetti:

- Un metodo di autenticazione diretta **in-band**
- Una versione del Web of Trust privata

Autenticazione diretta

Protocollo del socialista milionario (SMP)

Autenticazione diretta

Protocollo del socialista milionario (SMP)

- Sfrutta segreti pre-condivisi implicitamente

Autenticazione diretta

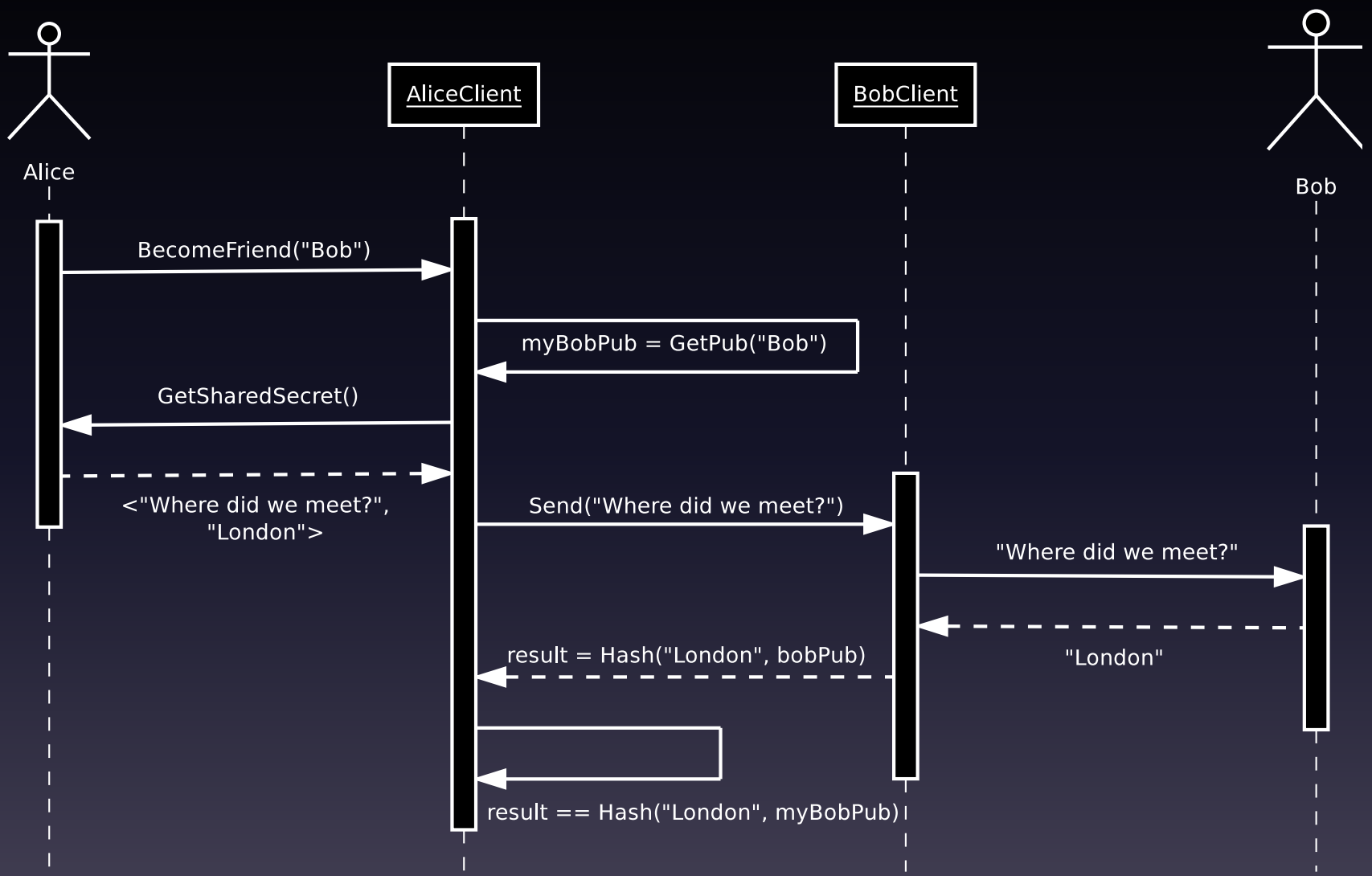
Protocollo del socialista milionario (SMP)

- Sfrutta segreti pre-condivisi implicitamente
- Non richiede di incontrarsi di persona

Autenticazione diretta

Protocollo del socialista milionario (SMP)

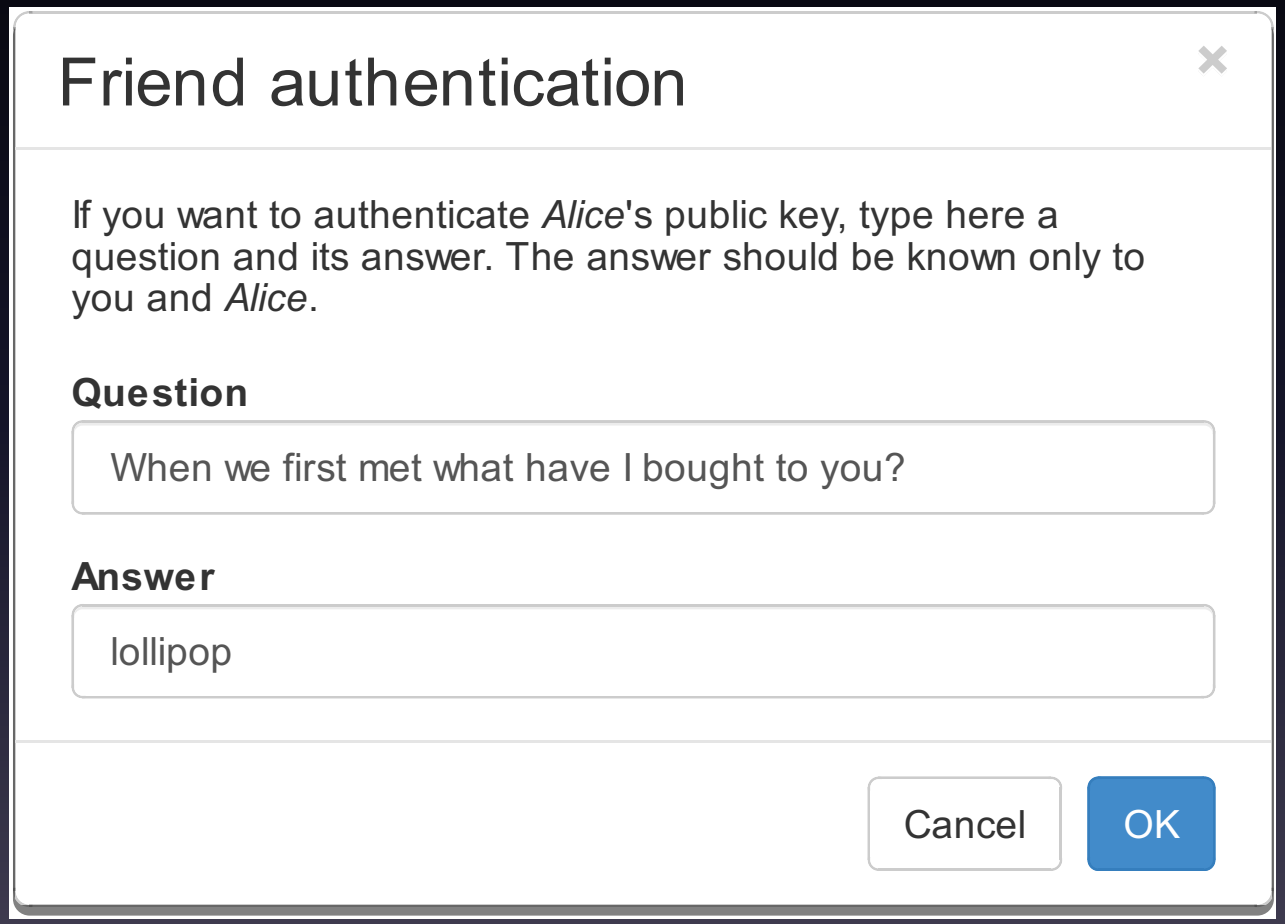
- Sfrutta segreti pre-condivisi implicitamente
- Non richiede di incontrarsi di persona
- Non rivela nulla a proposito del segreto condiviso


Alice
AliceClient
BobClient
Bob
BecomeFriend("Bob")
myBobPub = GetPub("Bob")
GetSharedSecret()
<"Where did we meet?",
"London">
Send("Where did we meet?")
"Where did we meet?"
"London"
result = Hash("London", bobPub)
result == Hash("London", myBobPub)

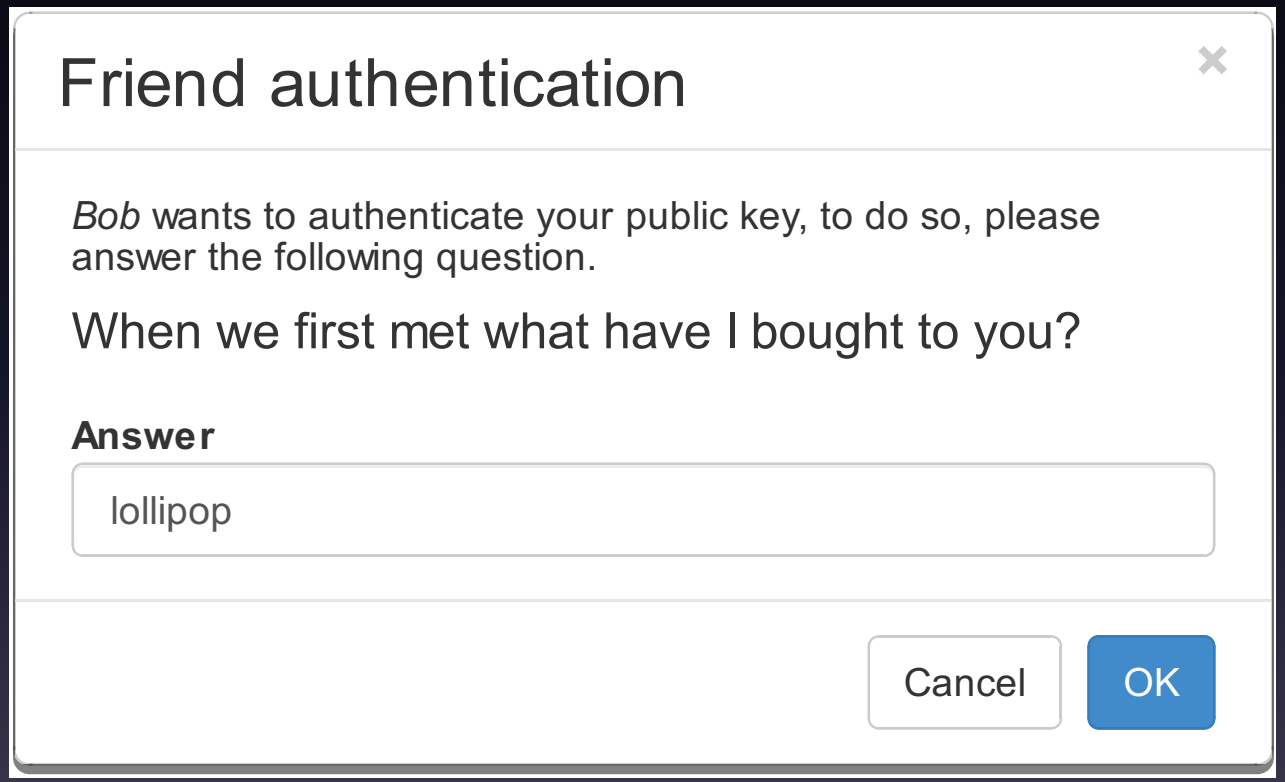
Caratteristiche

- Non è possibile forgiare il valore senza la risposta corretta
- I tentativi di risposta richiedono un'interazione dall'altro lato
- Non è possibile effettuare un attacco di tipo brute-force

Domanda


Friend authentication
If you want to authenticate *Alice*'s public key, type here a question and its answer. The answer should be known only to you and *Alice*.
Question
When we first met what have I bought to you?
Answer
lollipop
Cancel
OK

Risposta


Friend authentication
Bob wants to authenticate your public key, to do so, please answer the following question.
When we first met what have I bought to you?
Answer
lollipop
Cancel
OK

Domande?

Indice

Qual è il problema

- Il problema non esiste quando il server gestisce i dati

Qual è il problema

- Il problema non esiste quando il server gestisce i dati
- È un problema non banale in tutti i sistemi con cifratura end-to-end
  - Numero di copie da inviare per ogni singolo messaggio
  - Aggiunta e rimozione di utenti al gruppo

Soluzioni attuali

- PGP
  - Ogni messaggio destinato ad un gruppo deve essere cifrato singolrmente per ogni destinatario

Soluzioni attuali

- PGP
  - Ogni messaggio destinato ad un gruppo deve essere cifrato singolrmente per ogni destinatario
- OTR
  - Non è prevista la comunicazione di gruppo

Soluzioni attuali

- PGP
  - Ogni messaggio destinato ad un gruppo deve essere cifrato singolrmente per ogni destinatario
- OTR
  - Non è prevista la comunicazione di gruppo
- Altre soluzioni
  - Limitano il numero di utenti massimo del gruppo
  - Limitano l'aggiunta o la rimozione di utenti nel gruppo

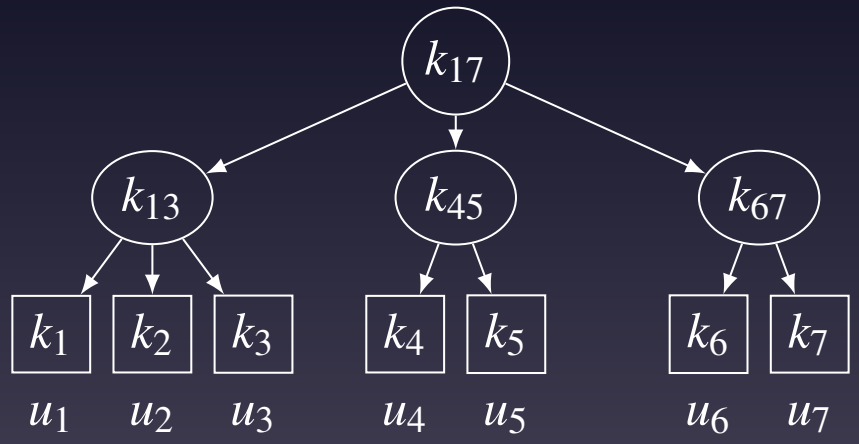

ENGINEERING:
OUR BIG PROBLEM IS HEAT DISSIPATION
HAVE YOU TRIED LOGARITHMS?
40 SECONDS

Nostra soluzione

- Soluzione scalabile
  - Gruppi arbitrariamente grandi
  - Possiblità di aggiungere o rimuovere utenti in modo efficiente (costo logaritmico nella dimensione del gruppo)

Nostra soluzione

- Soluzione scalabile
  - Gruppi arbitrariamente grandi
  - Possiblità di aggiungere o rimuovere utenti in modo efficiente (costo logaritmico nella dimensione del gruppo)
- Utitilizzo di una gerarchia di chiavi per la gestione di gruppi



Domande?

Indice

Non solo riservatezza del contenuto

SNAKE offre anche l'anonimato dei dati
tramite la soppressione dei metadati pubblici superflui

I metadati

Osservando i dati immagazzinati sul database non è possibile:

I metadati

Osservando i dati immagazzinati sul database non è possibile:

- Stabilire chi sia il mittente di un messaggio

I metadati

Osservando i dati immagazzinati sul database non è possibile:

- Stabilire chi sia il mittente di un messaggio
- Stabilire chi sia il destinatario

I metadati

Osservando i dati immagazzinati sul database non è possibile:

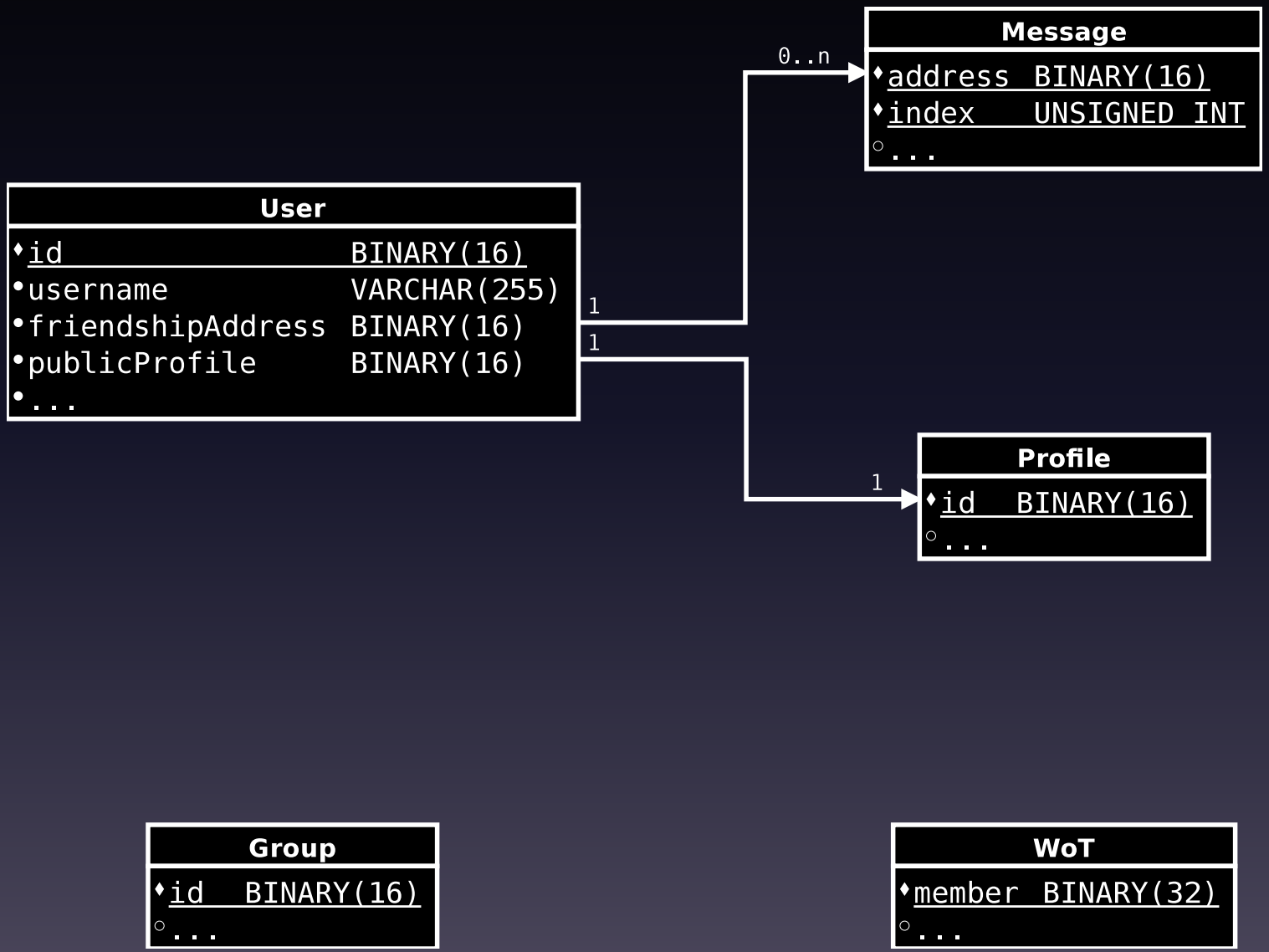
- Stabilire chi sia il mittente di un messaggio
- Stabilire chi sia il destinatario
- Stabilire se un utente sia amico di un altro

I metadati

Osservando i dati immagazzinati sul database non è possibile:

- Stabilire chi sia il mittente di un messaggio
- Stabilire chi sia il destinatario
- Stabilire se un utente sia amico di un altro
- Stabilire se un utente sia membro di un gruppo

Percorsi di join superstiti



Anonimato

SNAKE garantisce l'anonimato sui dati **a riposo**

Lo scenario

L’anonimato è garantito se il server di storage è onesto

Domande?

Indice

Possibili sviluppi

- La struttura attuale permette lo scambio sicuro di messaggi tra uno o più utenti

Possibili sviluppi

- La struttura attuale permette lo scambio sicuro di messaggi tra uno o più utenti
- Sono già previste funzionalità più orientate ad un uso da social network (amicizie, bacheca, . . .)

Possibili sviluppi

- La struttura attuale permette lo scambio sicuro di messaggi tra uno o più utenti
- Sono già previste funzionalità più orientate ad un uso da social network (amicizie, bacheca, . . .)
- Altri interessanti sviluppi
  - Chat realtime
  - Condivisione di file sicura
  - Suite Office collaborativa

Indice

Snake in breve

- Applicazione semplice e sicura per lo scambio di messaggi usabile direttamente nel proprio browser

Snake in breve

- Applicazione semplice e sicura per lo scambio di messaggi usabile direttamente nel proprio browser
- Pensata e realizzata con la privacy dei dati in mente

Snake in breve

- Applicazione semplice e sicura per lo scambio di messaggi usabile direttamente nel proprio browser
- Pensata e realizzata con la privacy dei dati in mente
- Autenticazione delle chiavi pubbliche in-band e privata

Snake in breve

- Applicazione semplice e sicura per lo scambio di messaggi usabile direttamente nel proprio browser
- Pensata e realizzata con la privacy dei dati in mente
- Autenticazione delle chiavi pubbliche in-band e privata
- Comunicazione in gruppo efficiente e scalabile

Snake in breve

- Applicazione semplice e sicura per lo scambio di messaggi usabile direttamente nel proprio browser
- Pensata e realizzata con la privacy dei dati in mente
- Autenticazione delle chiavi pubbliche in-band e privata
- Comunicazione in gruppo efficiente e scalabile
- Anonimato dei dati a riposo

Concludendo

- La privacy dei propri dati è un tema da non sottovalutare

Concludendo

- La privacy dei propri dati è un tema da non sottovalutare
- Bisogna essere consapevoli di come i nostri dati vengono usati

Concludendo

- La privacy dei propri dati è un tema da non sottovalutare
- Bisogna essere consapevoli di come i nostri dati vengono usati
- Molti software non affrontano tutte le problematiche di privacy

Concludendo

- La privacy dei propri dati è un tema da non sottovalutare
- Bisogna essere consapevoli di come i nostri dati vengono usati
- Molti software non affrontano tutte le problematiche di privacy
- Noi proponiamo una soluzione usabile e sicura

Domande?

Licenza