

# Mobile Applications of Secret Handshakes over Bluetooth LE

---

Gabriel Capella  
João Henrique

# Fraternidades Secretas

---


Gabriel Capella  
João Henrique

# Annual International Conference on Mobile Computing and Networking (MobiCom 2016)

Yan Michalevsky (Stanford University)

Suman Nath (Microsoft Research)

Jie Liu Microsoft (Microsoft Research)




# Mission

How can we form secure communities at mobile nodes

perform privacy preserving handovering

or communicate with our vehicles or things being tracked?



# Annual International Conference on Mobile Computing and Networking (MobiCom 2016)

Yan Michalevsky (Stanford University)

Suman Nath (Microsoft Research)

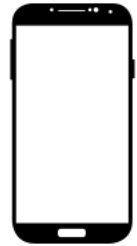
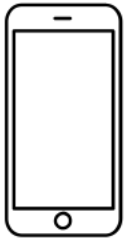
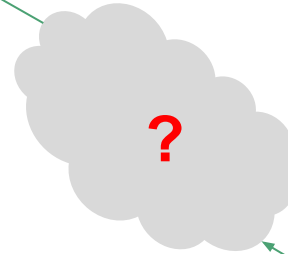
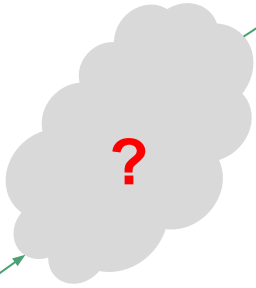
Jie Liu Microsoft (Microsoft Research)



# Comunidades Secretas

- Membros querem identificar-se uns aos outros
- Anonimato para pessoas externas à comunidade
- As mensagens podem ser secretas



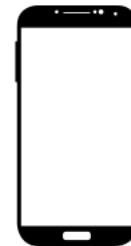
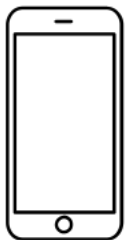


O servidor é seguro?

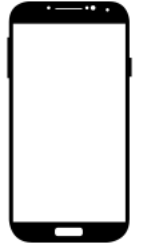
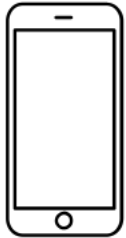


	Seg	Ter	Qua	Qui	Sex	Sab	Dom
<b>7:00 - 8:00</b>	0	0	0	0	0	0	0
<b>8:00 - 9:00</b>	0	0	30	0	0	0	0
<b>9:00 - 10:00</b>	0	0	42	0	0	0	0
<b>10:00 - 11:00</b>	0	0	5	0	0	0	0
<b>11:00 - 12:00</b>	0	0	0	0	0	0	0
<b>12:00 - 13:00</b>	0	0	0	0	0	0	0
<b>13:00 - 14:00</b>	0	1	0	0	0	0	0
<b>14:00 - 15:00</b>	0	20	0	0	0	0	0
<b>15:00 - 16:00</b>	0	13	0	0	0	0	0
<b>16:00 - 17:00</b>	0	2	0	5	0	0	0
<b>17:00 - 18:00</b>	0	0	0	0	0	0	10

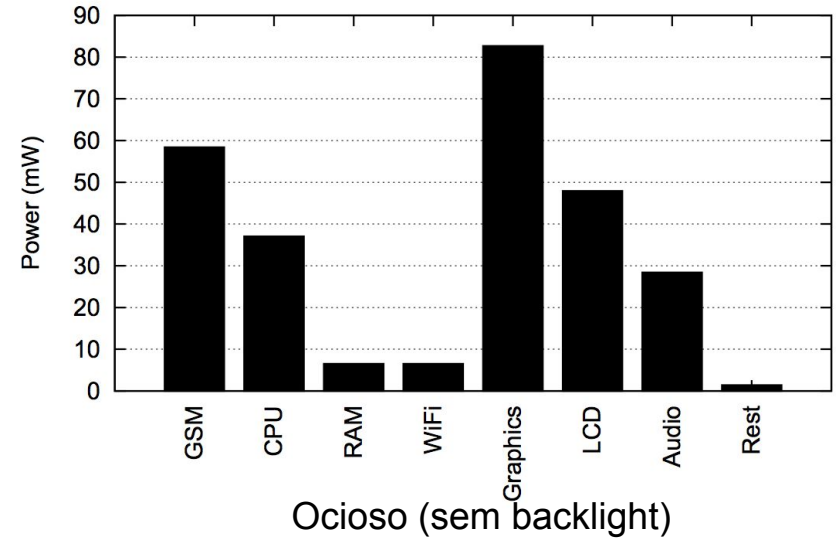
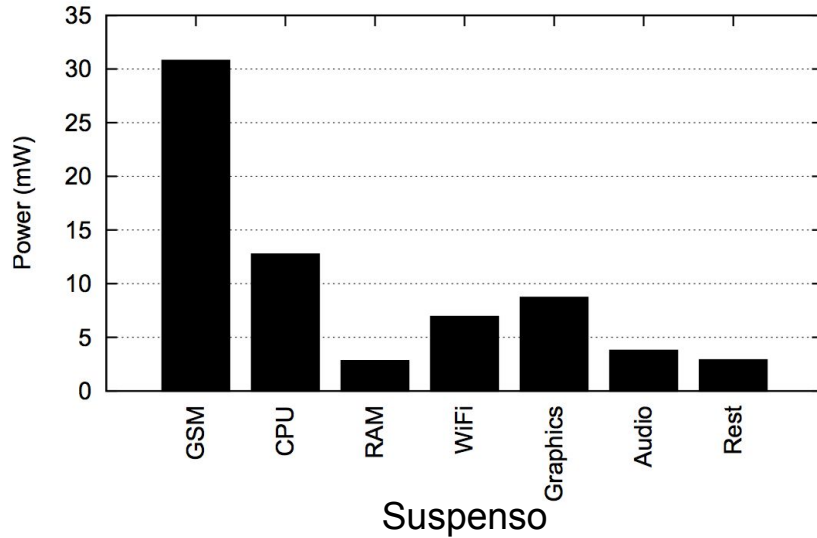
Mensagens trocadas entre João e Capella em determinados horários do dia



Há sempre conexão?



Bluetooth LE



Consumo?

# Objetivos do artigo

- Não utilizar servidor central
  - Comunicação peer-to-peer
- Economizar energia
  - Utilizando bluetooth de baixa energia (BLE)
- Ser possível no contexto atual
  - Em vários dispositivos e com a tecnologia já existente neles

# Bluetooth Low Energy (BLE)

## Prós

- Baixíssimo consumo de bateria
- Presente na maior parte dos aparelhos atuais

## Contras

- Limitação superior na quantidade de dados transmitida
- Modo que o pareamento atual é feito é inseguro

# Comunicando via Bluetooth

## Pareado

- O protocolo atual permite que seja feito o pareamento das seguintes formas:
  - Sem proteção
  - Comparação numérica
  - Senha
  - Método Externo

## Conectado

- Momento em que o dispositivo já está pareado, possibilitando a troca de mensagens

# Anunciando

## Conectado

- O protocolo Bluetooth LE tem a capacidade de anunciar sua existência de tempos em tempos (*advertising*)
- Existe uma opção onde, para cada anúncio, gera-se um endereço MAC diferente, evitando assim personificação



# Handshakes Secretos

- *Handshake*: reconhecimento mútuo de aparelhos para começar o protocolo de comunicação
- Um dispositivo não conhece o outro
- Realizam um procedimento para saber se é confiável falar com o outro
  - Se falhar, nenhum sabe nada sobre o outro
  - Se funcionar, descobrem que pertencem ao mesmo grupo



*“Consider a CIA agent who wants to authenticate herself to a server, but does not want to reveal her CIA credentials unless the server is a genuine CIA outlet. Consider also that the CIA server does not want to reveal its CIA credentials to anyone but CIA agents – not even to other CIA servers.”*

# Álgebra

Sejam  $G_1$ ,  $G_2$  e  $G_3$  grupos cíclicos,  $u \in G_1$ ,  $v \in G_2$  e  $a, b \in \mathbb{Z}_n$ . Seja  $(\cdot)$  uma operação nesse grupo, por exemplo uma multiplicação sobre uma curva elíptica. Um emparelhamento  $(e)$  é uma função  $G_1 \times G_2 \rightarrow G_3$ , tal que:

$$e(a \cdot u, b \cdot v) = (e(u, v))^{ab}$$

Master secret  
 $t \in \mathbb{Z}_Q$

$$(P_A \in G, T_A = t \cdot P_A)$$

$$(P_B \in G, T_B = t \cdot P_B)$$



Alice



Bob



Alice



Bob

$$s \cdot P_B$$

$$r \cdot P_A$$

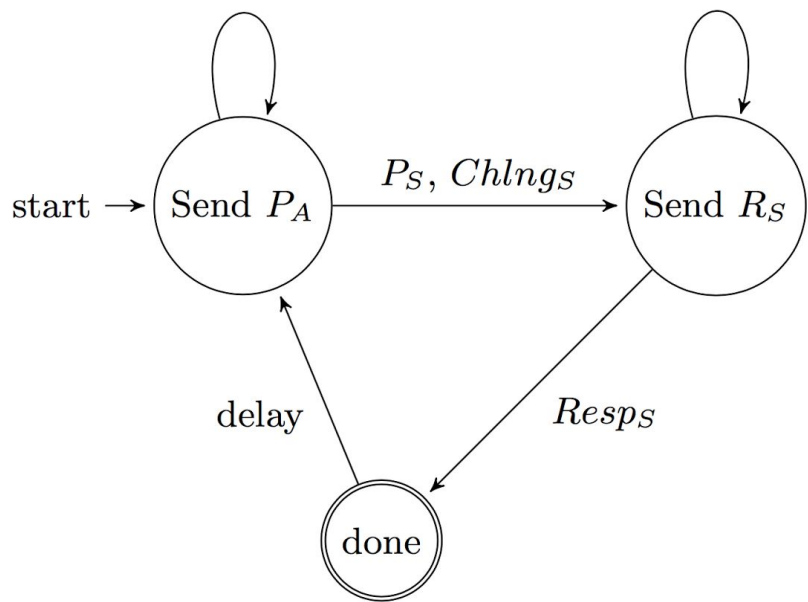
$$K_A = e(s \cdot P_B, r \cdot T_A) = e(P_B, P_A)^{rst}$$

$$K_B = e(s \cdot T_B, r \cdot P_A) = e(P_B, P_A)^{rst}$$

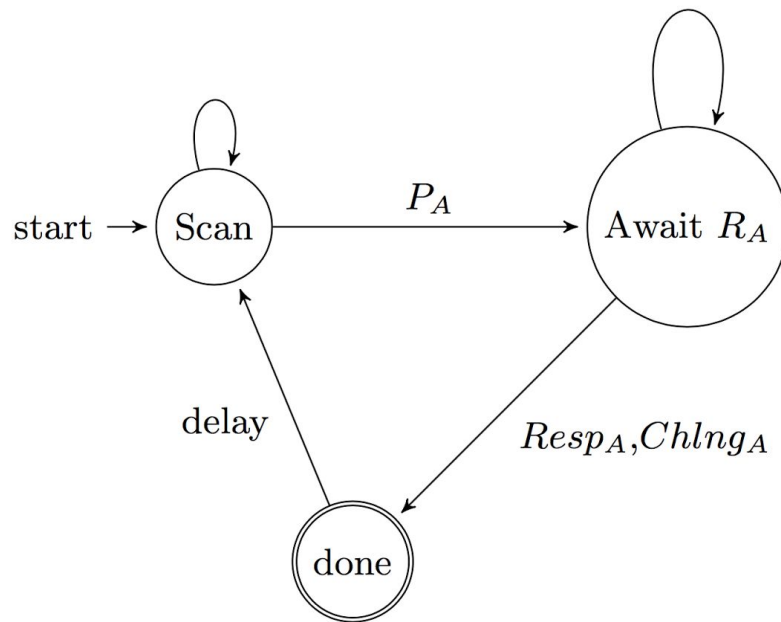
$$Enc_{K_A}(challenge_A)$$

$$response_A, Enc_{K_B}(challenge_B)$$

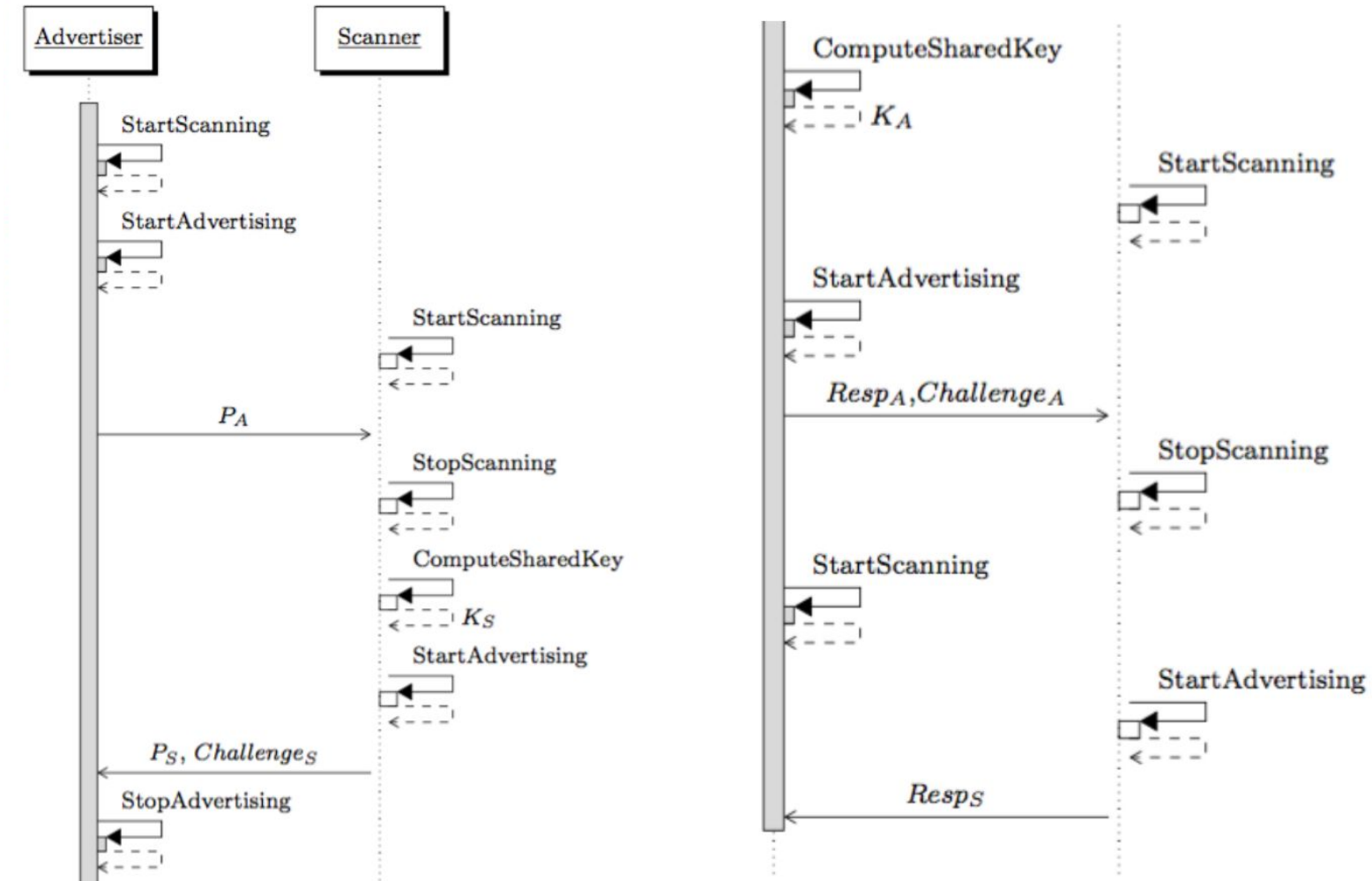
$$response_B$$



**(a) Advertiser**



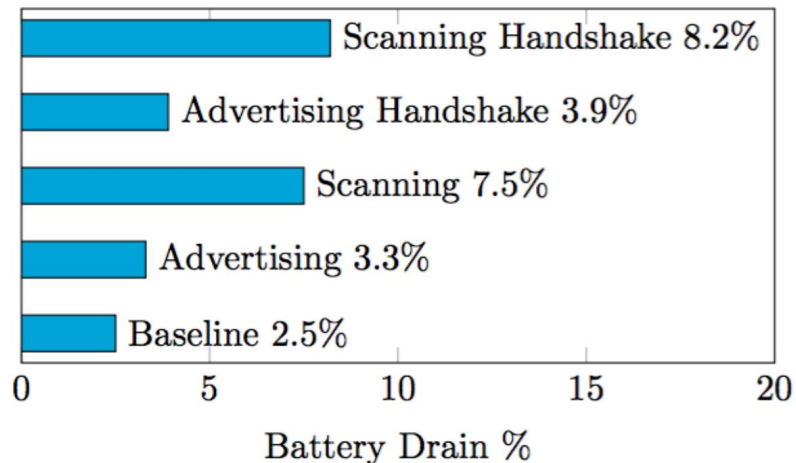
**(b) Scanner**



# Resultados Experimentais

Dois smartphones com Windows Phone, com 1 handshake a cada 8 segundos, por 8296 segundos (aprox. 2 horas e 18 minutos)

- 96% de sucesso usando o handshake secreto como protocolo de pareamento.
- Baixo overhead na comunicação
- Baixo consumo energético





# Conclusões

- Comunicação e reconhecimento anônimos entre entidades
- Canal de comunicação autenticado, encriptado e seguro
- Consumo de energia viável para uma aplicação móvel
- Handshakes secretos são práticos para o pareamento no protocolo BLE

# Perguntas?

---

## Referências:

- “*An Analysis of Power Consumption in a Smartphone*” -  
[https://www.usenix.org/legacy/event/atc10/tech/full\\_papers/Carroll.pdf](https://www.usenix.org/legacy/event/atc10/tech/full_papers/Carroll.pdf)
- “*MASHaBLE: Mobile Applications of Secret Handshakes over Bluetooth Low Energy*” -  
<https://web.stanford.edu/~yanm2/files/sechandble.pdf>
- “*Secret Handshakes from Paired-Based Key Agreements*” -  
<http://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/hcwong/Pdfs/handshakes.pdf>