Implementing Ad-hoc Message Authentication in Social Media Platforms

Charles A. Clarke
Faculty of Science, Engineering and Computing
Kingston University

About This Research

Research Outline

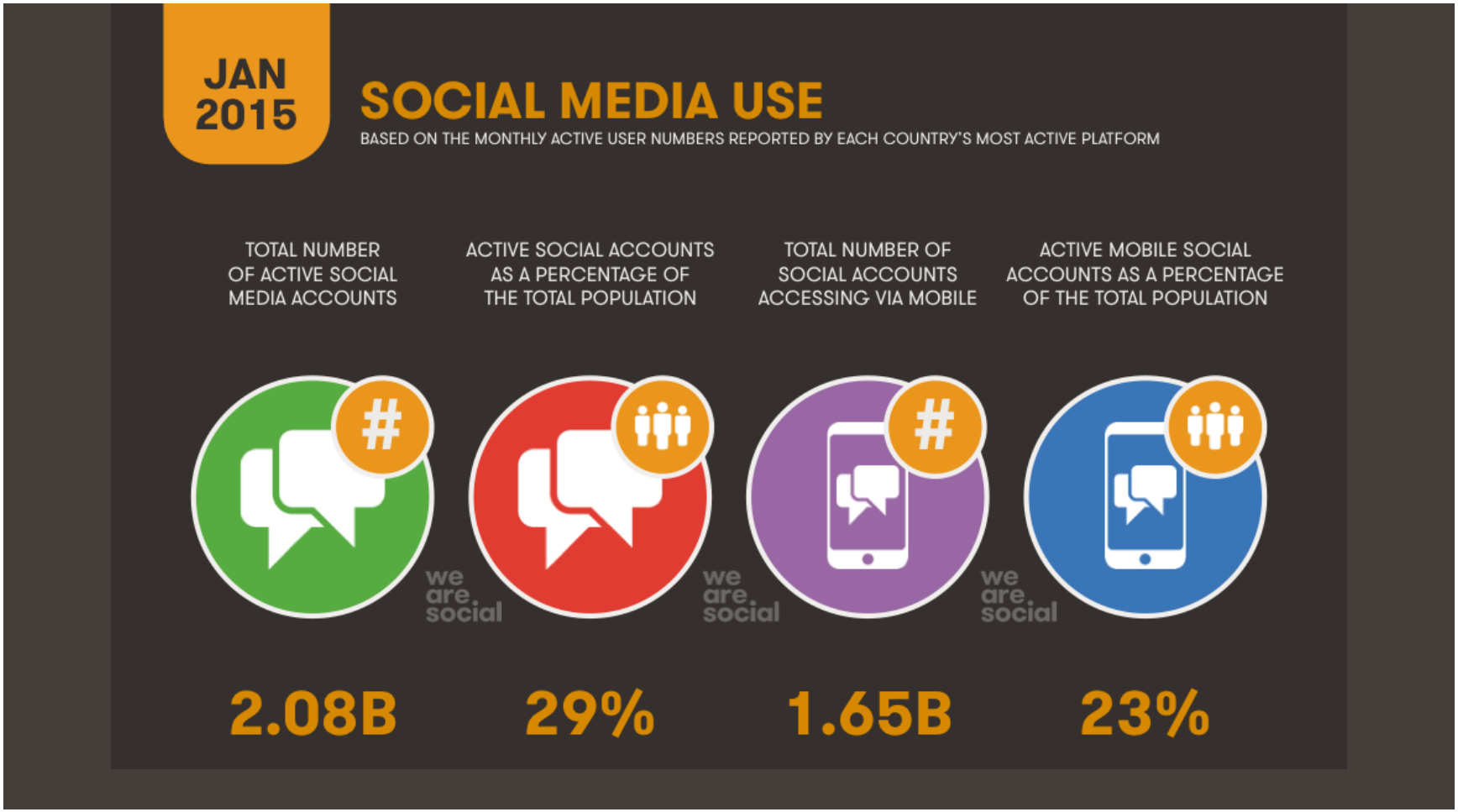
- **Domain**
  Social Media Platforms (SMPs)
- **Problem Addressed**
  Validating the integrity of content shared between SMP users (Message Authentication)
- **Research Contribution**
  Characterised as a multi-channel overlay authentication protocol

Introduction

What are social media platforms (SMPs) and how are they used?

Introduction

Social media activity is conducted on a global scale



SOURCE: http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/sd

Research Problem

Routine SMP modifications pose integrity threats to user content

- Content Reformatting
  - E.g. YouTube videos converted during upload
- Image cropping, resizing etc
  - Images are changed to comply with a specific SMP presentation format
- Watermarking and metadata changes
  - Metadata added or changed to for the purposes of identification, ad delivery and tracking etc

Research Problem

Why is message authentication important in the context of SMPs?

- Message authentication is relevant to scenarios that include the sharing of legal, time stamped, forensic and journalistic content, where statements, images and videos may need to be validated as *original* (i.e. unaltered and genuine).

Research Problem

Some SMPs apply functional constraints

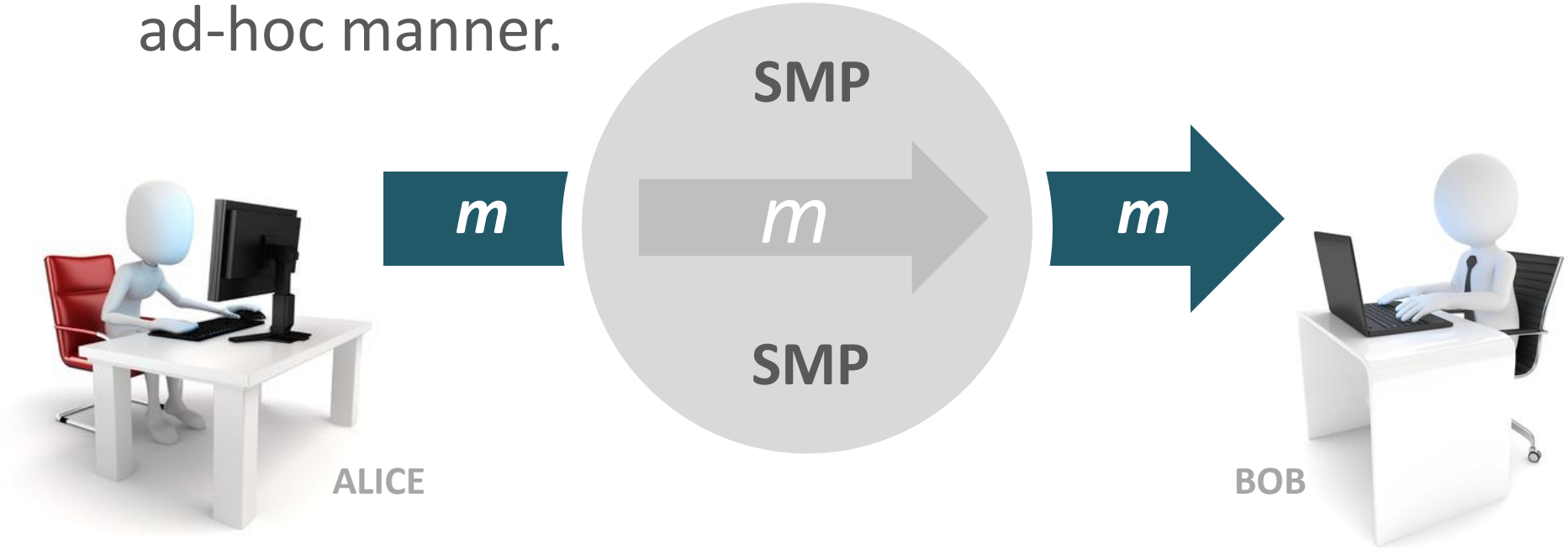
- **Capacity constraints** restrict content size
  - E.g. Twitter 140 character limit
- **Format constraints** limit types of content
  - E.g. WhatsApp, Viber, Line allow sharing of text, image, audio and video formats, but not pdf, word, excel etc
- **Contextual constraints** require appropriate content for the environment
  - E.g. Publishing cipher-text would appear conspicuous

Research Contribution

Synopsis

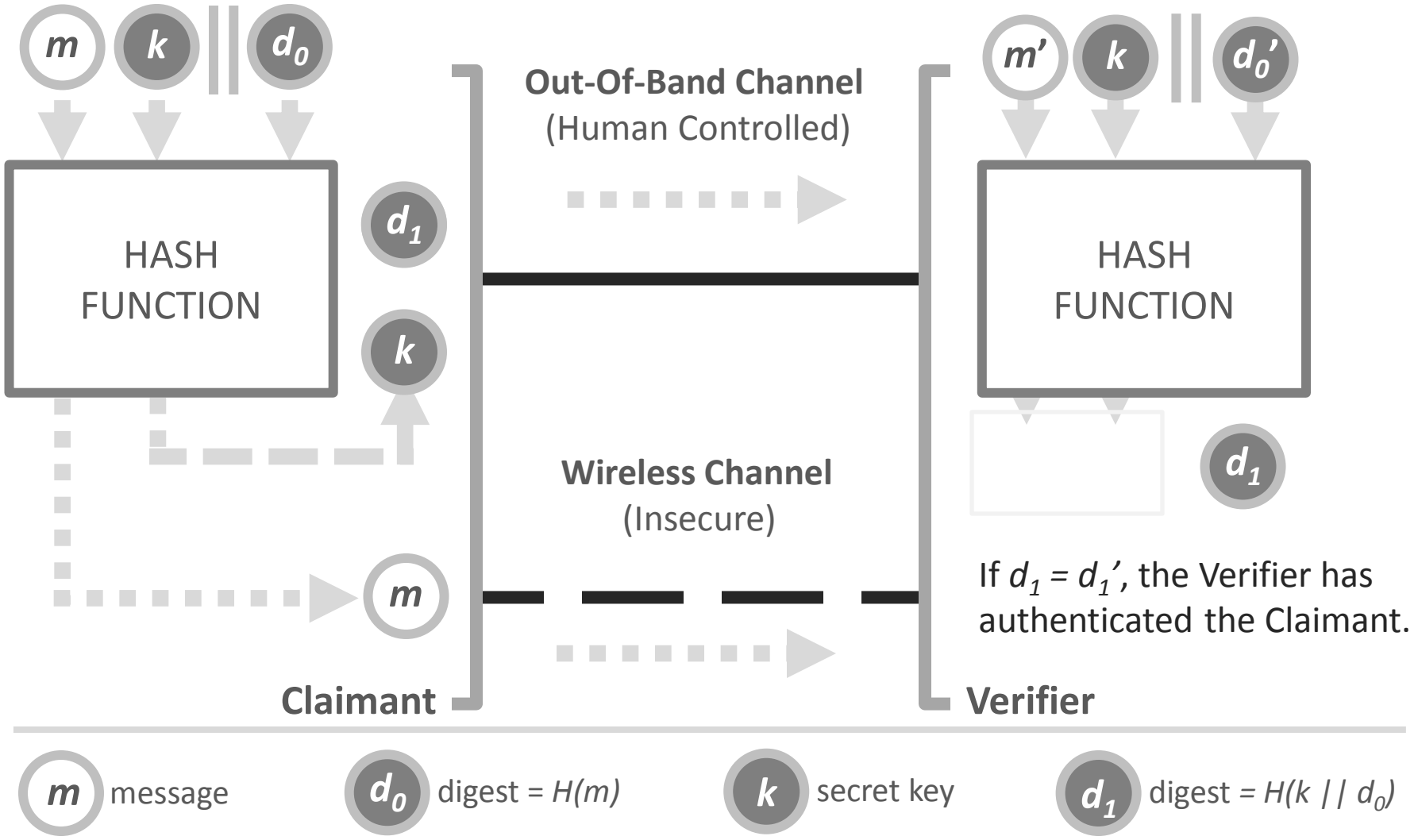
Message Authentication

- Alice transmits a message *m* to Bob where *m* is subject to SMP threats and constraints.
- Goal? Find a way for Bob to authenticate *m* in an ad-hoc manner.



Research Contribution

Related Work – Hash Based Ad-hoc Device Pairing Concept



Research Contribution

Our Approach - Concepts

Our approach generally mirrors device pairing, with some notable differences:

- Authenticate *content* and not entities
- Multiple untrusted SMP channels…no OOB
- No secret key.

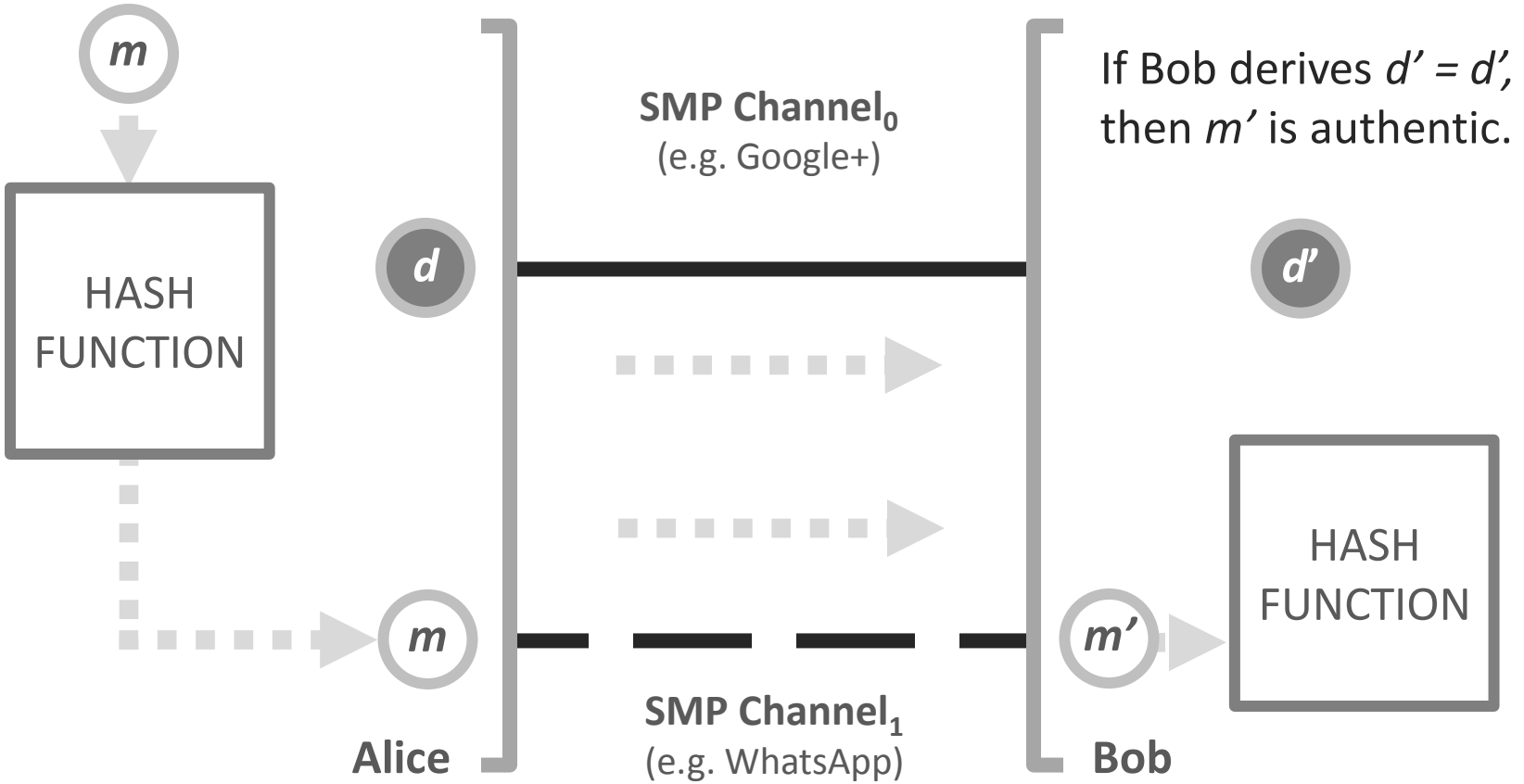
Research Contribution

Our Approach - Implementation Assumptions

- SMP channels are independent and non colluding.
- Links between users and SMPs are https secured.
- SMPs establish entity authentication
- We assume that SMPs may eavesdrop on content and may modify it.
- Users trust each other and have appropriate accounts on common SMPs.

Research Contribution

Our Approach – Multi-channel Message Authentication Concept



m message

d digest = *H(m)*

Research Contribution

Summary of Benefits and Limitations

Benefits

- Approach is easy and intuitive to implement
- Scalable
- Can be used as a ‘probe’ to identify SMPs that modify content

Limitation

- Message authentications (e.g. digests) must be contextually relevant. Can be mitigated by concealing digests using steganography (e.g. jpg dct, text DLSB).

Research Contribution

Summary of Implementation Requisites

Participants require access to:

- Accounts on pre-agreed SMPs
- A cryptographic hash function tool
- An agreed steganography tool

Conclusions

Summary

- Approach is characterised as a *multi-channel overlay protocol*, for ad-hoc authentication of content shared between users in SMPs.
- Relevant to scenarios that include the sharing of Legal, time stamped, forensic and journalistic content, where statements, images and videos may need to be validated as *original.*

References

References

[1] C. Heller Baird and G. Parasnis, “From social media to social customer relationship management,” Strategy & Leadership, vol. 39, no. 5, pp. 30–37, 2011.

[2] C. Clarke, E. Pfluegel, and D. Tsaptsinos, “Confidential communication techniques for virtual private social networks,” in Distributed Computing and Applications to Business, Engineering & Science (DCABES), 2013 12th International Symposium on. IEEE, 2013, pp. 212–216.

[3] M. Conti, A. Hasani, and B. Crispo, “Virtual private social networks,” in Proceedings of the first ACM conference on Data and application security and privacy. ACM, 2011, pp. 39–50.

[4] D. P. Maher, “Secure communication method and apparatus,” Sep. 12 1995, uS Patent 5,450,493.

[5] F. Stajano, “The resurrecting duckling,” in Security Protocols. Springer, 2000, pp. 183–194.

[6] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, “Talking to strangers: Authentication in ad-hoc wireless networks.” in NDSS, 2002.

[7] C. Gehrmann, C. J. Mitchell, and K. Nyberg, “Manual authentication for wireless devices,” RSA Cryptobytes, vol. 7, no. 1, pp. 29–37, 2004.

[8] S. Vaudenay, “Secure communications over insecure channels based on short authenticated strings,” in Advances in cryptology–CRYPTO 2005. Springer, 2005, pp. 309–326.

[9] F.-L. Wong and F. Stajano, “Multi-channel protocols,” in Security Protocols. Springer, 2007, pp. 112-127.

Questions