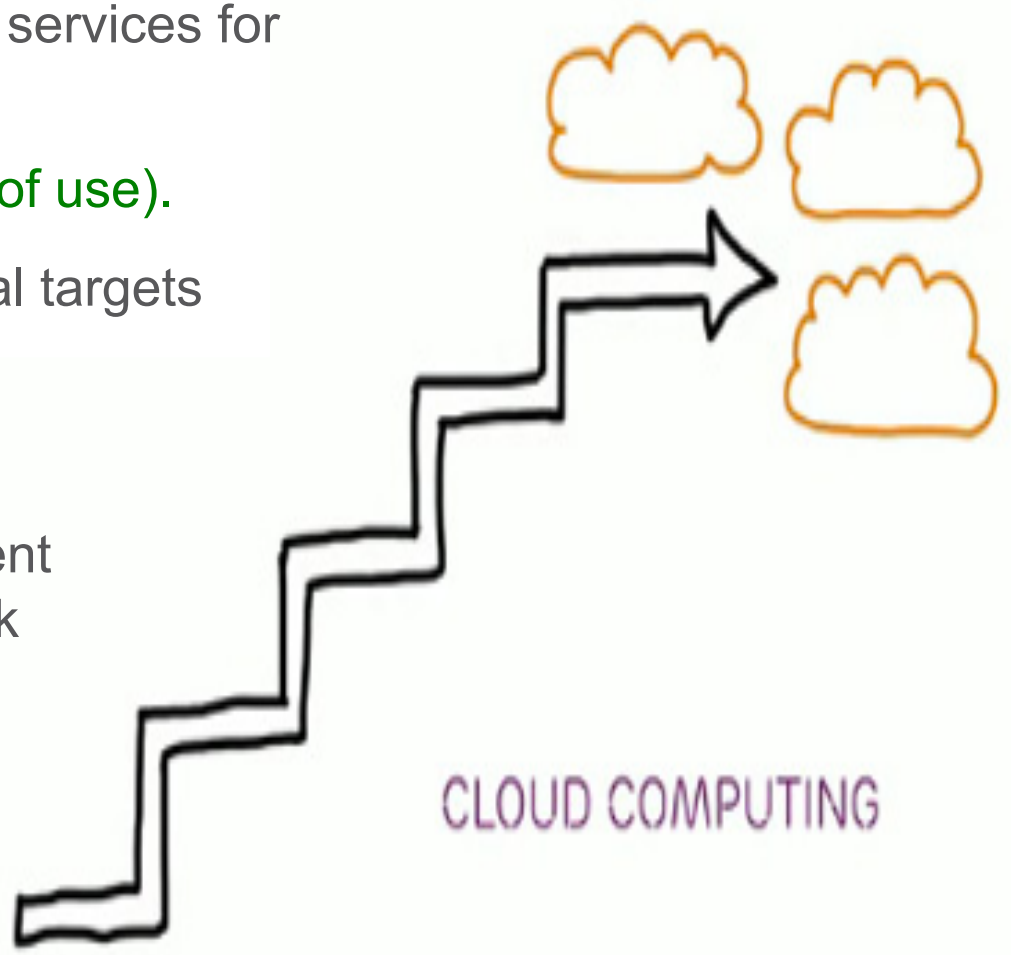
CLOUD PRIVACY IN A PERVASIVE MONITORING LANDSCAPE

JOHN MATTSSON
STEFAN HÅKANSSSON

ERICSSON RESEARCH

INTRODUCTION

- Ongoing transformation towards third-party cloud services for storing and managing information.
  - This has many benefits (cost, flexibility, ease of use).
- Data aggregated in global data centers are natural targets for pervasive surveillance.
  - Also active attacks, e.g. celebrity image theft.
- The market potential for enterprise and government cloud services and web applications are held back by privacy and security concerns.
  - Problematic with servers in other countries and vendors from other countries.



SECURITY MODEL

- WebCrypto uses so called host-based security where the security depends on the security of the host.
  - This alone is not enough in a pervasive monitoring landscape
  - Need to protect against service provider, data breaches, and government demands.
  - Need to shield not just encryption keys, but also plaintext data from the hosting application.
- Similar thoughts have been pursued in WebRTC, Isolated Media Streams, and Encrypted Media Extensions.

EXAMPLES

Cloud storage

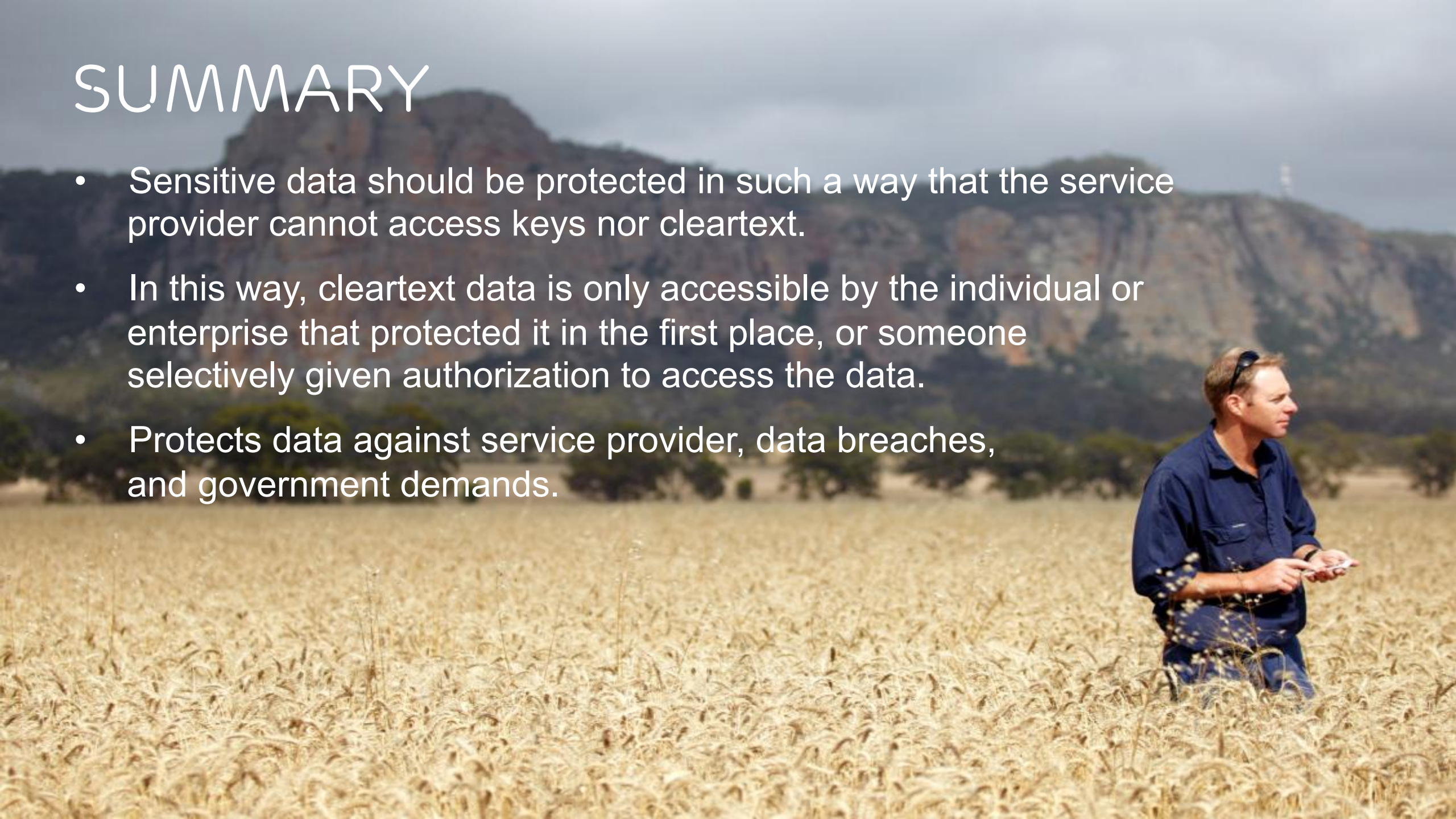
- There is currently no easy way to use cloud storage in a way that ensures privacy.
- Needed: Secure File Input / File Download where cleartext is not accessible by the web application / JavaScript runtime environment.

HTML forms

- Data entered in forms is available to the web application in cleartext.
- Needed: secure forms where the data is not accessible to the application in any other form than encrypted.
- Example: Google Chrome extension End-to-End.

SUMMARY

- Sensitive data should be protected in such a way that the service provider cannot access keys nor cleartext.
- In this way, cleartext data is only accessible by the individual or enterprise that protected it in the first place, or someone selectively given authorization to access the data.
- Protects data against service provider, data breaches, and government demands.



REFERENCES

The presented paper: “Cloud Service Privacy in a Pervasive Monitoring Landscape”
http://www.w3.org/2012/webcrypto/webcrypto-next-workshop/papers/webcrypto2014_submission_9.pdf

TRINT - A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring
http://www.w3.org/TR/WebCryptoAPI/

Barnes et al. “Pervasive Attack: A Threat Model and Problem Statement”
http://tools.ietf.org/html/draft-barnes-pervasive-problem

Cooper, Jennings, “The Trust-to-Trust Model of Cloud Services”
https://www.w3.org/2014/strint/papers/30.pdf

Farrell, Tschofenig, IETF RFC 7258, “Pervasive Monitoring Is an Attack”
https://tools.ietf.org/html/rfc7258

W3C, “Web Cryptography API”
http://www.w3.org/TR/WebCryptoAPI/

W3C, “WebRTC 1.0: Real-time Communication Between Browse
http://www.w3.org/TR/webrtc/

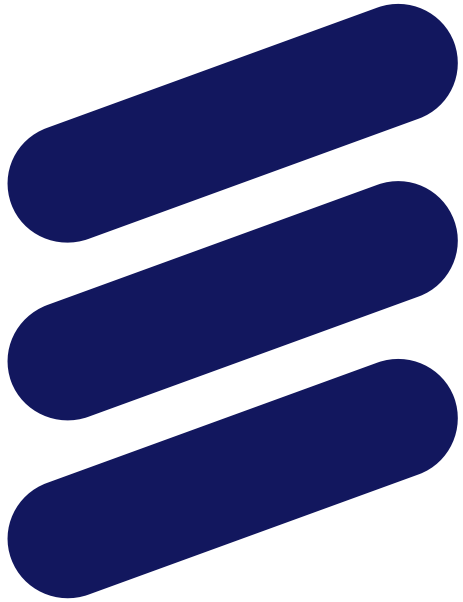
IETF, “Real-Time Communication in WEB-browser
http://tools.ietf.org/wg/rtcweb/

W3C, “Media Capture and Streams”
http://www.w3.org/TR/mediacapture-streams/#isolated-media-streams

W3C, “Encrypted Media Extensions”
http://www.w3.org/TR/encrypted-media/

Google, “End-To-End”
https://code.google.com/p/end-to-end/

Halpin, “The W3C Web Cryptography API: Design and Issues”, 2014
http://ws-rest.org/2014/sites/default/files/wsrest2014_submission_11.pdf



ERICSSON