Hycat: More Performant Full Disk Encryption with Chacha and Poly1305

Bernard Dickens
University of Chicago

Hank Hoffmann
University of Chicago

Ariel Feldman
University of Chicago

Abstract

Summarize introduction/contributions, methodology, conclusion in 250? interesting words or less.

1 Introduction

Is this worth it? Why? Argue project meaningfulness. Status quo disk encryption has a non-trivial cost. Show empirically. This cost can be lessened, a trade-off made. What tradeoff(s)? Tease apart and enumerate different contributions.

Characterize cost. "We save X at the cost of Y". DE is the proiblem. The solution is Z. It costs Y. If willing to pay.

Caveats, limitations, and how they're handled.

2 Related Works

2.1 AES-XTS

2.2 Salsa20/Chacha20

3 Threat Model

4 Design and Implementation

5 Evaluation

6 Results

7 Conclusion

8 Acknowledgments

A polite author always includes acknowledgments. Thank everyone, especially those who funded the work.

9 Availability

It's great when this section says that MyWonderfulApp is free software, available via anonymous FTP from

```
ftp.site.dom/pub/myname/Wonderful
```

Also, it's even greater when you can write that information is also available on the Wonderful homepage at

```
http://www.site.dom/~myname/SWIG
```

References