Intended Consequences

Beyond the Box-Ticking Exercise

Mika Boström
<mika.bostrom@iki.fi> / <mika.bostrom@smarkets.com>

About Me

- In the field since 1992
- Head of security at Smarkets
- Data Protection Officer
- SecDevOps advocate

About Me

- In the field since 1992
- Head of security at Smarkets
- Data Protection Officer
- SecDevOps advocate
- Moved to London for the weather

Agenda

- Reality check: theory vs. practice
- Usability lessons
- Way forward

Theory

People want security

Practice

People ask for security but choose convenience

Dirty Secret of Infosec Industry

Compliance

Source: http://sweetclipart.com/silhouette-hands-air-970

Getting Security Team Involved

- < 1 day

Getting Security Team Involved

- < 1 day
- < 3 days

Getting Security Team Involved

- < 1 day
- < 3 days
- < 1 week

Getting Security Team Involved

- < 1 day
- < 3 days
- < 1 week
- ≥ 1 week

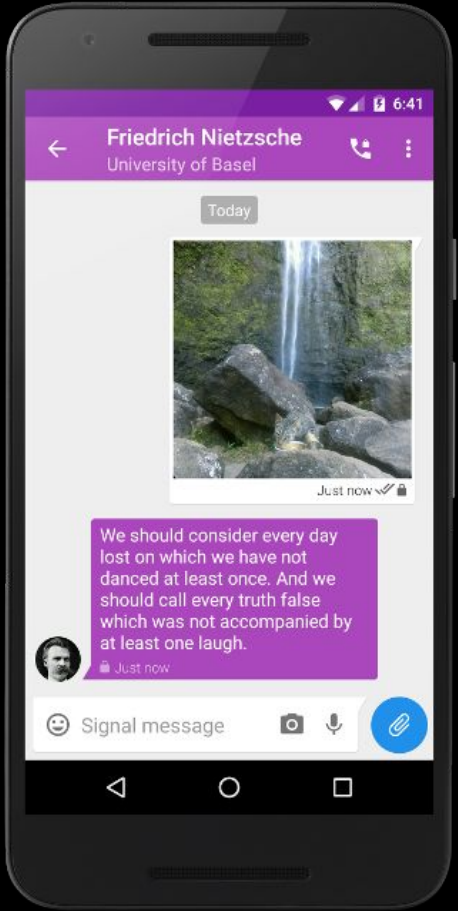
What Was Your Intention?

Usability is everything

```
gpg --armor --recipient
arthur.dent@planet.earth
--sign --output [...]
```

Usability is everything

```
gpg --armor --recipient
arthur.dent@planet.earth
--sign --output [...]
```



Bad Ideas, Worse Practices

Your password must contain …

Example - London School of Economics

LSE's password policy means that passwords must:

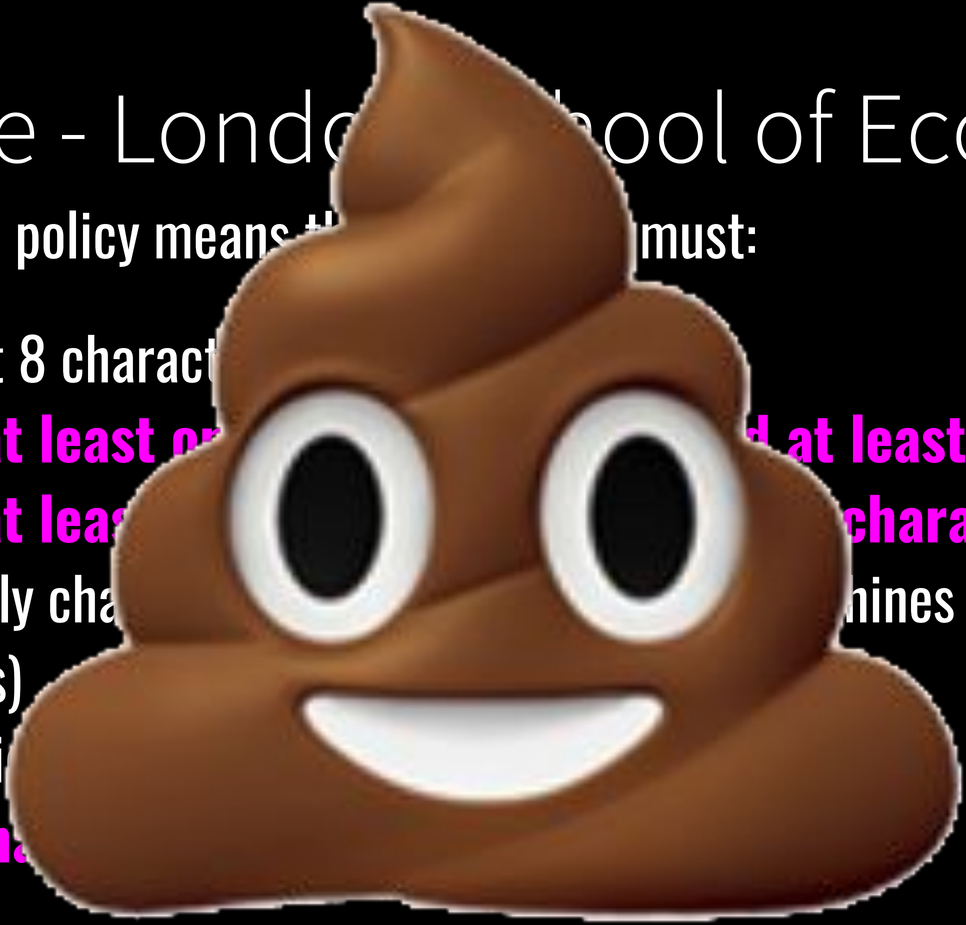
- be at least 8 characters long
- **contain at least one uppercase letter and at least one lower case letter**
- **contain at least one number *or* punctuation character**
- include only characters supported on campus machines (avoid international characters)
- not be a dictionary word
- **be less than 12 months old**

From: http://www.lse.ac.uk/intranet/LSEServices/IMT/guides/accounts/chooseStrongPassword.aspx

Example - Londo hool of Economics

LSE's password policy means th must:

- be at least 8 charact
- **contain at least o at least one lower case letter**
- **contain at leas character**
- include only cha hines (avoid international characters)
- not be a di
- **be less tha**



From: http://www.lse.ac.uk/intranet/LSEServices/IMT/guides/accounts/chooseStrongPassword.aspx

Rest Of The World Finally Catching Up

NIST Recommendations:

- **Allow at least 64 characters**
- **No composition rules**
- **No arbitrary rotation**

NCSC Guidelines:

- **No regular expiration**
- **Use 2-Factor Auth**
- **Reject known-broken passwords**

Rest Of The World Finally Catching Up

NIST Recommendations:

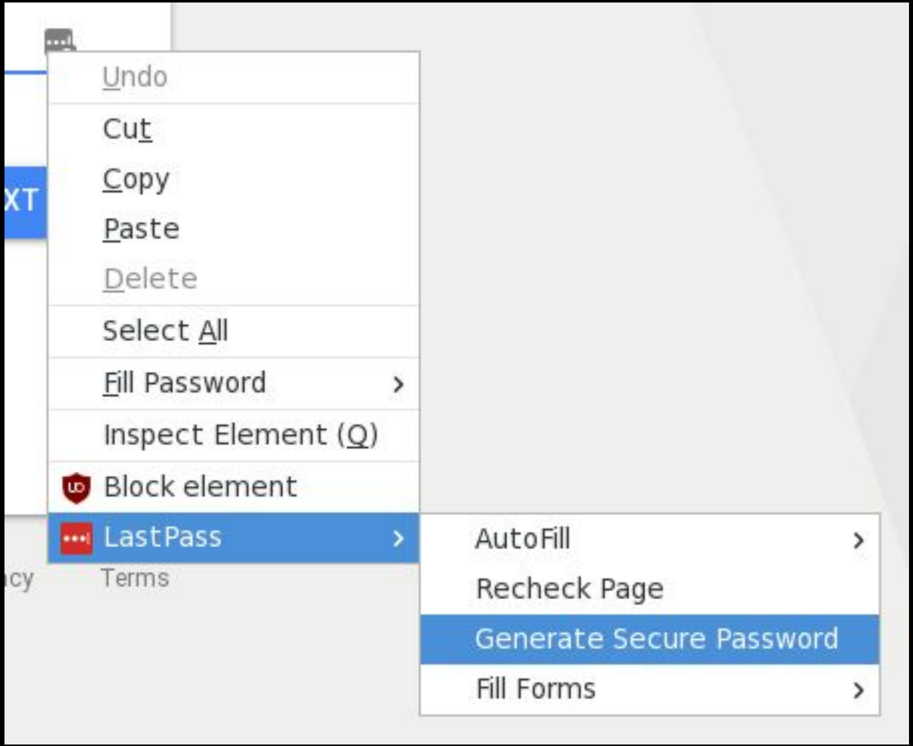
- **Allow at least 64 characters**
- **No composition rules**
- **No arbitrary rotation**

NCSC Guidelines:

- **No regular expiration**
- **Use 2-Factor Auth**
- **Reject known-broken passwords**

Watershed, 2010: *The True Cost of Unusable Password Policies: Password Use in the Wild* (https://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf)

How To Handle Lots Of Passwords



Plus Of Course..

fido CERTIFIED U2F

What Was Your Intention?

BEST PASSWORD IS ONE YOU DO NOT KNOW - OR REMEMBER

Auditors Can Make Insane Demands

Security. Usability. Sanity.

Pick at most one.

Dealing With Dubious Auditor Demands

- **Show research**
- **Educate**
- **Provide reading material**
- ***CONTEST***

Smarkets’s Policy Review 2018

```
% git show --pretty=fuller --reverse
--since=2017-01-01 --until=2018-01-01

% git diff --since=2017-01-01
--until=2018-01-01
```

Time: 20 minutes total

What Can We Do?

COMPANIES:

- Publish your research
- Understand auditor demands
- Never just tick boxes
- Security teams are not gatekeepers

INDIVIDUALS:

- Educate auditors
- Demand usability
- Write blog posts

Why Publish Corporate Research?

- We need better arsenal
- We need more public data
- Auditors understand black-on-white evidence

Few Things Generate More Data …

Few Things Generate More Data …

… than an academic who wants to prove you wrong

Unless...

… they want to prove that **another academic** is wrong

What Was Your Intention?

Theory vs. Practice - take 2

People ask for security but choose convenience

Make the secure option more convenient and you can not keep people away

Thank you

Email: <mika.bostrom@smarkets.com>
IRC: (please ask)
Twitter: **n/a**
Facebook: **n/a**