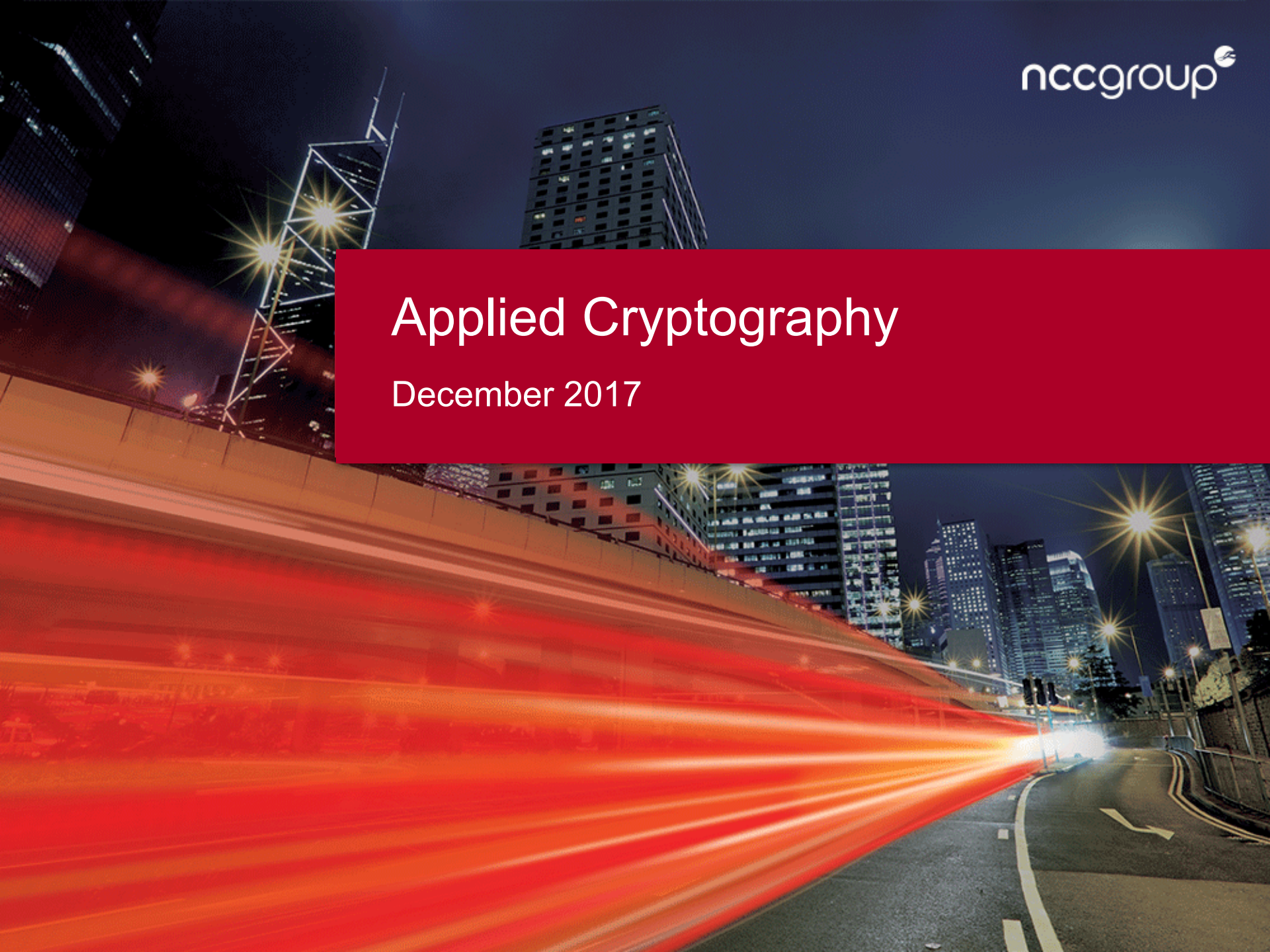


Applied Cryptography

December 2017

…ECDLP is the problem of finding an ECC user's secret key, given the user's public key.

Unfortunately, there is a gap between ECDLP difficulty and ECC security.…There are many attacks that break real-world ECC without solving ECDLP.

The core problem is that if you implement the standard curves, chances are you're doing it wrong.

https://safecurves.cr.yp.to/


nccgroup
The Basics

Use the right primitives

- Encryption != Integrity
- Encryption != Authentication
- Hashing != Encryption
- Hashing != Irreversible (in general)

Garbled != Senseless

Understand your cryptographic libraries

- Understand their purpose
- Understand their assumptions
- Validate input to the libraries
- Check return values

Side Channels

Crypto black box

- Perform complex mathematics
- Fast enough to be suitable
- On general purpose hardware
- Correctly for all inputs

Without any measurable side effect

Side effects?

- Data and error conditions
- Processing time
- Data access time
- Power fluctuations
- Electromagnetic emissions

Acoustic emissions


nccgroup
Password Storage

What could be simpler?

- Take password
- Store in database
- ....?
- Profit!

Step 1 – Hash it!

- Get password
- Store SHA256(password)
- Preimage resistance for the win!

Precomputed dictionary attack

Everything falls*

Step 2 – Hash it with salt!

- Get password
- Store random || SHA256(random|| password)
- No precomputation!

Active dictionary attack

Pretty much everything falls

Step 3 – Expensive hash it with salt!

- Get password
- Store random || PBKDF2(random|| password)
- Slow computation!

Active dictionary attack with acceleration

Normal passwords fail

Step 4 – Argon2d with salt!

- Get password
- Store random || argon2d(random|| password)
- No acceleration!

Active dictionary attack

Bad passwords fail

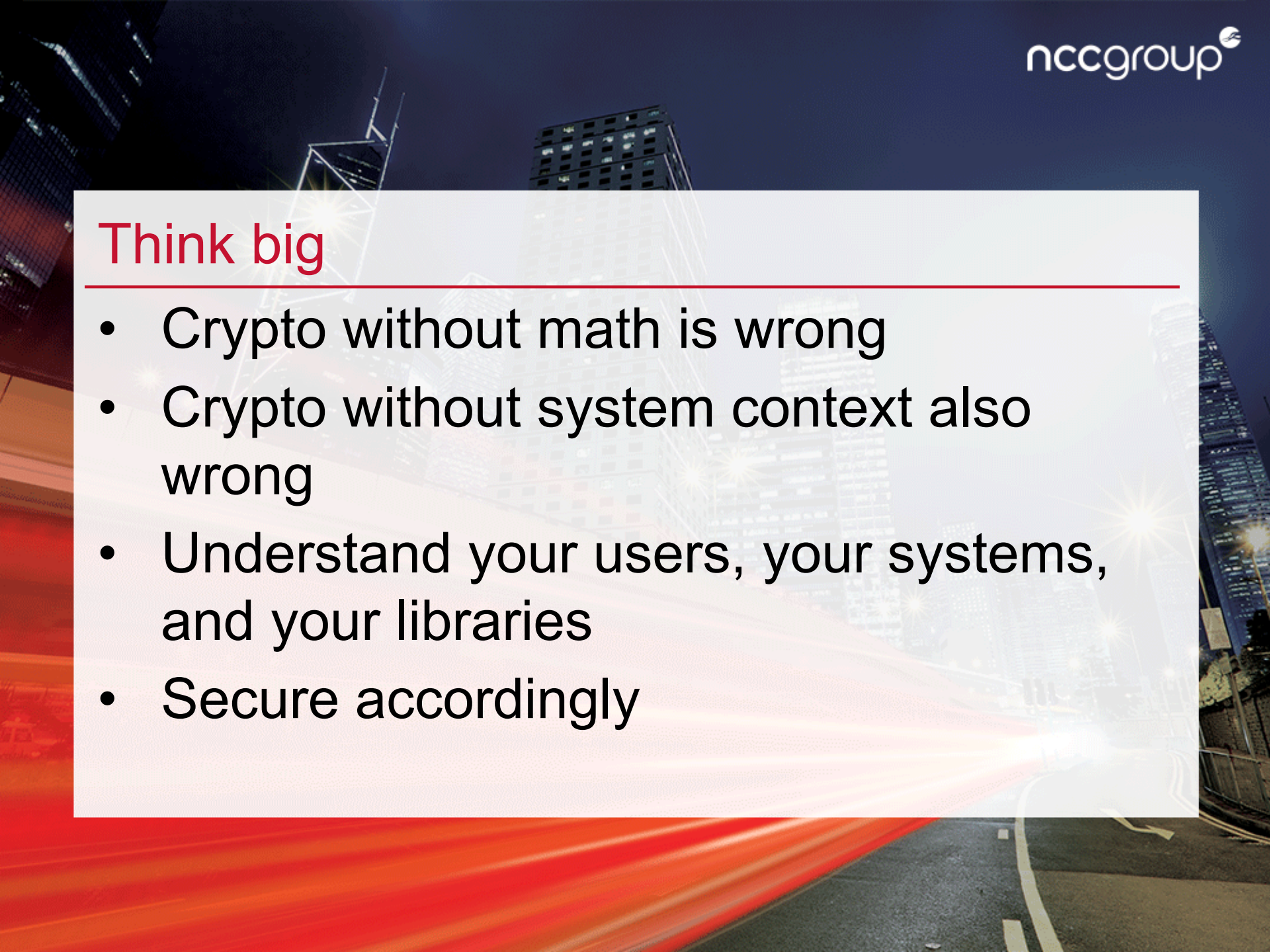
Step 2 – Argon2d with salt!

- Get password
- Store random || argon2d(random|| password)
- *whew*

Denial of Service?

Data independence?

Conclusions



Think big

- Crypto without math is wrong
- Crypto without system context also wrong
- Understand your users, your systems, and your libraries
- Secure accordingly

Thank you!

scott.stender@nccgroup.trust
@scottstender