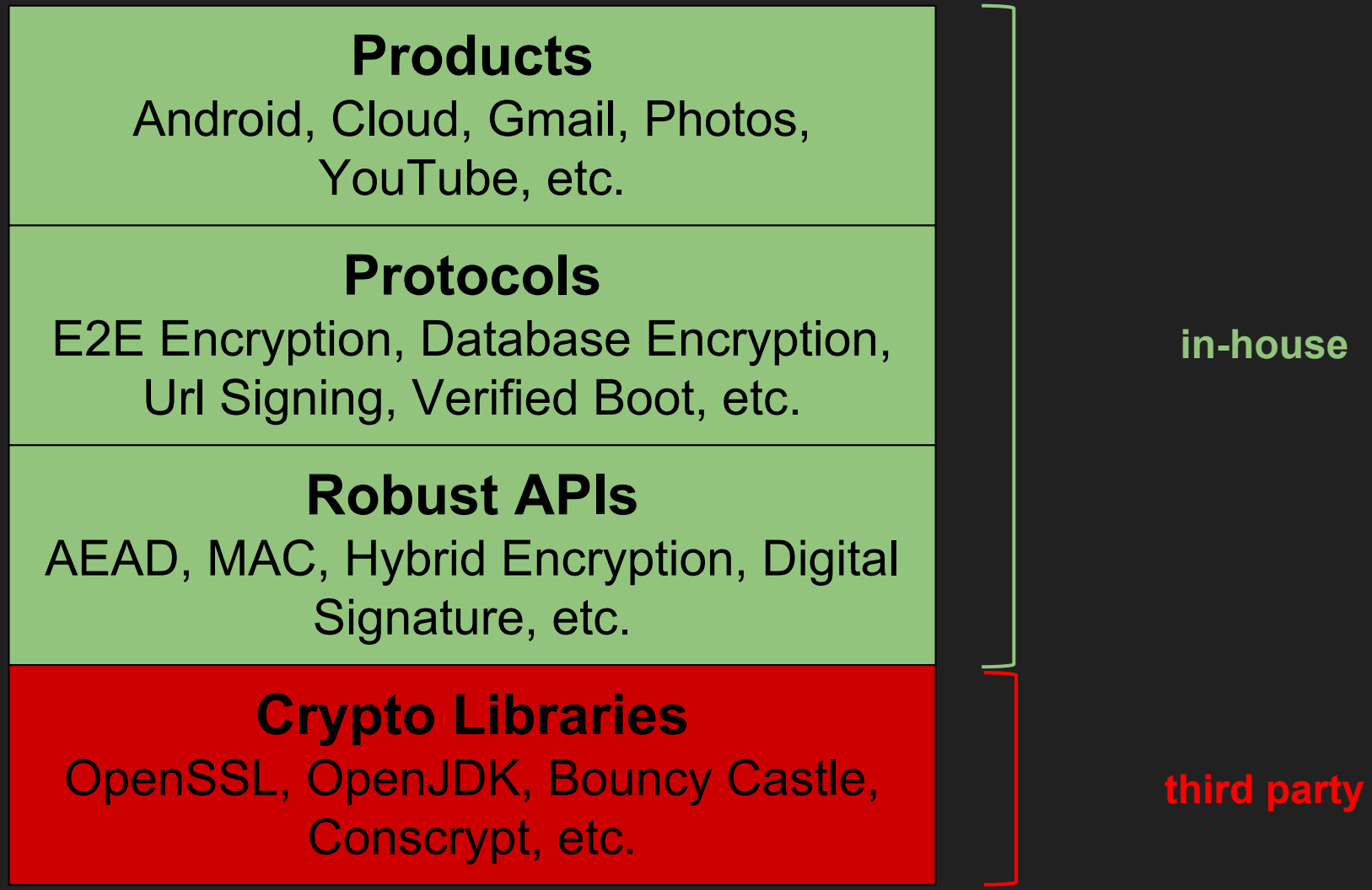
Scaling Crypto Testing with Project Wycheproof


Products
Android, Cloud, Gmail, Photos, YouTube, etc.
Protocols
E2E Encryption, Database Encryption, Url Signing, Verified Boot, etc.
Robust APIs
AEAD, MAC, Hybrid Encryption, Digital Signature, etc.
Crypto Libraries
OpenSSL, OpenJDK, Bouncy Castle, Conscrypt, etc.
in-house
third party

Problems

- Bugs happen too often and for much too long
- Good crypto implementation guidelines are hard to come by

Project Wycheproof

- 80+ open source unit tests uncovering 40+ bugs in popular implementations of ECC, RSA, DH, DSA, AEAD, etc.
- Defense in depth tests
- Out of box test runners for Bouncy Castle, Spongy Castle, and OpenJDK
  - bazel test BouncyCastleAllTests
  - bazel test BouncyCastleAllTests_1_52

Notable bug: key recovery in OpenJDK's DSA

```
generator = KeyPairGenerator.getInstance("DSA");
generator.initialize(2048);
keyPair = generator.generateKeyPair();
priv = (DSAPrivateKey) keyPair.getPrivate();
signer = Signature.getInstance("DSA");
signer.initSign(priv);
signer.update(messageBytes);
byte[] signature = signer.sign();
```

Notable bug: key recovery in Bouncy Castle's ECDHC

```
pub = (ECPublicKeyParameters)pubKey;
pa = pub.getParameters();
hd = pa.getH().multiply(key.getD()).mod(pa.getN());
ECPoint P = pub.getQ().multiply(hd).normalize();
```

What we want for Christmas

- Common crypto interfaces for C++, Python, Go, Javascript, etc.
- Robust and readable interfaces
  - Allow switching algorithms in an existing application
  - Show crypto properties right in the code
  - Never ask users to provide critical input (e.g., randomness, etc.)

Links

- Apache2 code and documentation
  - https://github.com/google/wycheproof
- Mailing list
  - wycheproof-users@googlegroups.com
  - https://groups.google.com/forum/#!forum/wycheproof-users

Credits

- Daniel Bleichenbacher
- Thai Duong
- Emilia Kasper
- Quan Nguyen

Thank You. Questions or Comments?

We’re hiring ^^! Send your resume to thaidn@google.com