nccgroup
freedom from doubt

Mobile apps and security by design

Ollie Whitehouse, Associate Director - NCC Group

Agenda

- **Challenges**
- **Benefits**
  - Features
  - Privacy
  - Product security

- **Assurance and COTS**
- **Response planning**

Problem Statement

“How to develop or purchase COTS mobile apps for my enterprise while ensuring security.”

Real-world challenges

- Cost
- Timelines
- Available security skill-set
- Trust in underlying technologies
- COTS, the big black box

Reality

Last minute security can lead to;

- Poor user experience
- Risk of fundamental flaws
- Implementation issues
- Higher expense and wasted effort
- …. Band-Aid solutions

How do we know this?

Secure Development Life-cycles!

Security earlier is;

- Cheaper
- Easier
- More integrated
- Less likely to be wrong

How do we know this?

Issues found during final testing

- Back to development
- Re-testing (functional)

Issues found after release

- All of the above
- Customer support costs
- Regulatory, press / brand etc.
- …

Put another way..

“Those practicing SDL specifically reported visibly better ROI results than the overall population.“

- Forester research

nccgroup
freedom from doubt

But it's not without cost…

~14% extra effort

What do we care about?

Functionality

- Security has a bad reputation
- Security is seen as impeding

Privacy

- Users and customers

Security

- Risk and regulator
- Integrity and data protection

Feature benefits

- Meet your risk appetite
- User friendly (UX etc.)
- Measured
- Integrated
- Lower risk of fundamental issues

Privacy benefits

Regulatory compliance

Publically acceptable

- Consumer versus employee
- Internet versus VPN
- … concepts like do not track etc …

Consideration around

- What we send, how we send, what we store and how we store

Security benefits

Baked in (intrinsic to the fabric)

Defence in depth

- Easy (automatic?) to upgrade
- Auditing / logging
- Authentication / authorisation
- Transport security
- Data at rest security

Mobile security by design

- User experience
- Authentication
- Authorisation
- Storage
- Logging
- Transport
- Upgradability
- Device / user identification

nccgroup
freedom from doubt

The COTS challenge

- Marketing buzzword bingo
- 3rd party development practices
- Gaining assurance

… in code and processes

… ideally via code access (rare!)

… likely black-box security assessments

… we don't want to outsource risk

If it all goes wrong

- Security response processes
- Internally developed
    - Escalation points?
- Vendor relationships
    - Who would you call?
    - Legal agreements?
    - Security SLAs?
    - Short term mitigations?

nccgroup
freedom from doubt

Summary

- Consider security & risk early
- Design security in from the start
- Test security early, test often
- Bigger locks != better security
- Consider user base
- Consider underlying technologies
- Consider tech/user case constraints
- Coax COTS vendors to improve

Thanks! Questions?

nccgroup
freedom from doubt

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney

European Offices

Amsterdam - Netherlands

Munich - Germany

Zurich - Switzerland

Ollie Whitehouse

ollie.whitehouse@nccgroup.com