PrimaryKey ASSOCIATES

Cryptography

Cryptography underpins digital security

Cryptography is ubiquitous in a modern digital society, for example it protects our online activities by securing our web browser connections to online stores and our personal data both in transit and when stored on our laptops, tablets and phones.

If you are a company developing or implementing information systems with security requirements to protect sensitive data (due to GDPR or other regulatory factors) you will need to use cryptography to secure those assets and associated processes.

In the rapidly expanding 'Internet of Things' (IoT) properly designed, implemented and tested cryptography will be critical to protecting our digitally connected daily lives.

Proper design, implementation and testing is critical

Cryptography is used in application security enforcing and securing relevant functions. The overall security of your systems will depend on the completeness and correctness of your design, implementation and testing. We have seen many instances where designers have failed to appreciate the necessary scope of a cryptographic system and relied on 'black box' engineering to integrate third party code and applications without understanding completely the implications of doing so.

This situation is further complicated where such systems rely on other parties such as a Cloud service or embedded systems firmware suppliers.

Design

Your cryptographic design must be complete, correct and meet all your business and security requirements. It is vital that it includes and addresses all aspects of operation over the full lifetime of your systems and users and includes provision for in-service maintenance and upgrades both planned and unplanned. Your design should take account of your system threat model and demonstrate how it mitigates those threats.

Sometimes limitations in system components can make it challenging to choose a cryptographic solution that adequately meets the threats on its own; this is particularly true where there is limited processing power available in, for example, IoT devices or when you need to integrate with legacy systems. Under those circumstances any design trade-offs must be properly understood and the associated threats mitigated using a combination of other countermeasures that work together.

Underpinning all cryptographic systems is a key hierarchy and key management system, compromise of which would completely undermine the secure operation of the system. Many of the system failures that we have seen are associated with compromise of the key management system.

Cryptographic systems are regularly the subject of sophisticated attacks whose mechanisms may remain unknown or may be disclosed by those who discover them. In any event it is important that the design takes into account the likelihood that it may need to change the underlying algorithms, keys and key lengths or modes of operation in the event of compromise.

Implementation

Implementing cryptographic systems needs a different approach to that typically followed by many developers when working on an area outside their immediate expertise (do an Internet search for suitable code examples and libraries, download code from Github and incorporate it into your application). Unfortunately this approach is inherently unreliable, not least because without detailed cryptographic experience it is virtually impossible to distinguish a 'secure' suite of code from a defective one.

In the same way as the design needs to take into account the potential for having to change the underlying algorithms, keys, key lengths and modes of operation, so too should the implementation. For example it should avoid any hard-coded 'magic numbers' that make updating the code challenging – it's better to abstract such values so that the system software can be upgraded with minimal development impact.

Testing

Testing cryptographic systems can be very challenging and requires different approaches to conventional system testing. For example, just because an encryption function using a random session key successfully turns plaintext into unintelligible ciphertext and then back again doesn't mean that it had not leaked information in the process. Was the key 'weak'? Did the key value leak in a side channel?

We have the right team to help you

As experts in security and cryptography we can help you address the complexity of properly designing, implementing and testing your cryptographic systems.

We have been engaged in the design, development, integration, testing and analysis of mission critical cryptographic systems since the mid 1980's. We were among the first in the UK to demonstrate Differential Power Analysis (DPA) attacks against smart cards to recover their cryptographic keys.

We maintain active engagement with the cryptographic research community to understand both best practice in cryptography and the art of the possible in cryptanalysis.

One of our founding directors, Andrew Clark, is a past President of the International Association for Cryptologic Research (IACR) the leading organisation on worldwide cryptographic research for the commercial sector.

We work flexibly

We work hard to make it easy to do business with us and stay flexible in our approach so that we can respond together to those unexpected developments that crop up from time to time. We use a simple letter of engagement to get to work alongside you … fast.

We would like to talk to you

We find that the best way to deliver what you need is to schedule a free-of charge initial exploratory teleconference between us so we can understand your requirements and learn more of your business needs and drivers. We use this initial discussion to draw up a short proposal in the form of a letter of engagement that lets us work together quickly on a series of short time and budget-bound sprints for your approval.

Contact us

We look forward to hearing from you:

t: +44 1403 599900

e: webfb@primarykey.co.uk

a: PO Box 2254, Pulborough, West Sussex, RH20 9AW, UK

