ES94N-15 Crypto-systems & Data Protection

23/24

Department
    WMG
Level
    Taught Postgraduate Level
Module leader
    Harjinder Lallie
Credit value
    15
Module duration
    1 week
Assessment
    100% coursework
Study location
    University of Warwick main campus, Coventry

Description

Introductory description

Cryptography has a variety of roles to play within the cyber security domain. At its core, this module aims to give students insight into how to select the appropriate cryptographic solution to solve the information assurance problem at hand.

It is given that a small community of gifted mathematicians have already refined some really sophisticated cryptographic primitives, protocols and algorithms. Other gifted engineers have realised these protocols and made them available on a range of platforms from dedicated crypto-hardware to general purpose computers. Then these implementations are used to protect information assets.

The properties and uses of cryptographic hashes are analysed. Particular attention is given to their role in assuring data integrity and in password management. Different attacks (brute force, dictionary, rainbow tables, synthetic collisions) and mitigations (salting, stretching, large keyspace) are also analysed.

Symmetric encryption is compared and contrasted with public key encryption. Particular attention is paid to the use of hybrid systems to address the key exchange problem in a computationally efficient manner, securing confidentiality over time and in transit. This is developed to show how a

public key infrastructure also offers assurance through digital signatures. The significance of "looking after the keys" is emphasised throughout. The challenge of having the relevant key available for authorised use, yet unavailable for unauthorised use is a common theme.

Different trust models are exemplified through the hierarchical X509 PKI and the PGP web of trust PKI. The SSL/TLS and IPSec protocols are analysed to determine the extent to which they assure the appropriate attributes of a data asset.

And again, key management is emphasised.

Module aims

To equip students to use cryptography to good effect.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Cryptographic hashes:

- terminology- hash, digest, Message Authentication Code, function
- properties- irreversible, deterministic, collision resistance, length
- applications in the cybe domain- authentication, known good/ bad files, file integrity,
- attacks- brute force, rainbow tables, password salting/ stretching, collisions
- specific hashes- MD5 (and collisions), SHA1, SHA2** series
- practical application of specific algorithms to specific tasks

Encryption theory:

- terminology- plaintext, ciphertext, key, algorithm, protocol,
- concepts- entropy, one time pad, complexity, modular arithmetic, initialisation vectors

Symmetric encryption:

- encryption over distance or time- the key exchange problem
- example algorithms- DES, Triple DES, AES,

Asymmetric encryption:

- properties- encrypting for known recipient, signing by authentic sender,
- establishing trust- hierarchy (X509) and web (OpenPGP), certificates,
- consequences of loss of key control- revocation certificates.

Hybrid encryption:

- Using asymmetric encryption to share symmetric key,
- SSL/TLS

Other specific protocols:

- Kerberos.
- IPSEC.

Data protection:

- at rest, in transit

Learning outcomes

By the end of the module, students should be able to:

- Apply cryptographic techniques to achieve desired information assurance objectives.
- Articulate the properties of different cryptographic primitives, techniques and algorithms to a non-specialist audience so that information owners can make informed decisions about how to protect data assets and manage information risk.
- Critically analyse the cryptographic needs of a particular scenario.
- Critically evaluate competing cryptographic solutions to an information assurance problem, recommending the most appropriate.

Indicative reading list

Schneier, B; Applied Cryptography; Wiley (2ed)
Anderson, R; Security Engineering; Wiley, (2ed).
Pfleeger, CP and Pfleeger, SL; Security in computing; Prentice Hall, (4ed).
Gollman, D; Computer Security; John Wiley and Sons, (3ed).

Ferguson, N Schneier, B & Kohno T; Cryptography Engineering: Design Principles and Practical Applications; John Wiley and Sons

Subject specific skills

Protect information using cryptography.

Transferable skills

critical thinking, problem solving, digital literacy

Study

Study time

Type	Required
Lectures	5 sessions of 1 hour (3%)
Tutorials	(0%)
Total	150 hours

Type	Required
Demonstrations	10 sessions of 1 hour (7%)
Practical classes	15 sessions of 1 hour (10%)
Online learning (independent)	10 sessions of 1 hour (7%)
Assessment	110 hours (73%)
Total	150 hours

Private study description

No private study requirements defined for this module.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A1

	Weighting	Study time
Coursework	100%	110 hours

Implementation of a solution to a cryptographic problem with demo / viva on completion.

Feedback on assessment

Verbal feedback via recorded demo / viva over MSTeams or equivalent.
Written feedback provided with the mark via tabula.

Availability

Anti-requisite modules

If you take this module, you cannot also take:

- ES94N-10 Crypto-systems & Data Protection

Courses

This module is Core optional for:

- Year 1 of TWMA-H6C7 Postgraduate Taught Cyber Security Engineering