IA 315: INFORMATION SECURITY AUDITING AND ASSURANCE

- Instructor Name: Dr. Jabhera Matogoro
- Office Number: B13
- Contact: jabhera.matogoro@udom.ac.tz
- ORCID: https://orcid.org/0000-0002-3546-5743

Aims of the Course

- The course aims at enabling students to get knowledge, tools and skills to conduct security audit on organization's network, wireless network, applications, database, software, web server and email security.
- Also enable student to write security auditing report

Course Objectives

- Students will understand security of different access points,
- Students will understand and acquire knowledge and skills for analyzing and managing vulnerability
- Students will be imparted with the knowledge of how exactly to go about auditing the security of an enterprise
- Students will be able to acquire skills and ability to analyze practical development processes in terms of their prospects and problems.

Learning Outcomes

- Upon completion of this course, students should be able to:
  - ✓ Perform a comprehensive audit
  - ✓ Provides excellent information to operations for improve network
  - ✓ Answering questions on audit planning, reporting on audit findings, and making recommendations to key stakeholders to communicate the results and effect change when necessary.

What is Information assurance (IA)

- Information assurance (IA) is actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation.
- This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.
- Defined by the United States (US) Department of Defense In 1996, IA all about protecting your information assets from destruction, degradation, manipulation and exploitation by an opponent.
- Information assurance can be considered at three levels: physical, information infrastructure and perceptual.

What is Information warfare

- This involves the managing of the opponent's perception through deception operations and psychological operations. Within military circles this type of IW is often called Truth Projection.
- This involves denying, destroying, degrading or distorting the opponent's information flows in order to break down their organization and their ability to co-ordinate operations.
- This type of information warfare gathers intelligence by exploiting the opponent's use of information systems.

Information and Competitive Advantage

- Within the proprietary advantage strategy an organization develops a distinctive technology, one that sets it apart from the rest of the industry. It then protects this lead, which is based of course on such things as barriers, e.g. patents, extraordinary investment, long lead times or rare skill base.
- The one step ahead strategy demands that an organization continually releases new and improved technology. This ongoing innovation keeps it just ahead of the competition, despite the ability of rivals to duplicate particular aspects of the technology.

Information and Competitive Advantage

- Within the discontinuity strategy an organization applies technology to produce a quick, decisive shift in the market it serves. For example: Citibank was the first bank in the US to install ATMs.
- Within the implementation strategy an organization applies commonly available technology uncommonly well. This strategy can offer a double pay-off, both delivering a competitive advantage in itself and improving the performance of other strategies.

Cryptographic Key Management

Key topics from NIST's general guidance, from keying relationships to compromise recovery

KEY MANAGEMENT

What key management is

> A set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties.
>
> NIST: the process of managing a key throughout its lifecycle, from secure generation to storage, distribution, use and destruction.

01	02	03	04	05
Generation	**Storage**	**Distribution**	**Use**	**Destruction**

Keys are like a safe’s combination: poor key management can easily compromise even strong algorithms.

TYPES OF KEY MANAGEMENT

Manual, automated and establishment methods

HOW IT IS RUN

Manual

People handle keys directly: key loaders, trusted couriers and split-knowledge key shares. Prone to human error.

Automated

A key management system oversees, automates and secures the lifecycle. Often required at scale (SP 800-130, SP 800-152).

HOW KEYS ARE ESTABLISHED

Key agreement

Two or more parties contribute information, so the key itself is never sent.

Key transport

The sender selects and encrypts (wraps) the key, using the receiver’s public key or a shared wrapping key.

Key derivation

Keys derived from a master key, a shared secret or a password with an approved function.

CRYPTOGRAPHIC PRIMITIVES

Four building blocks behind every key

NO KEY

Hash functions

Produce a fixed-length digest and resist pre-image and collision attacks. A building block for MACs, signatures and key derivation.

ONE SHARED KEY

Symmetric-key algorithms

The same secret key does an operation and its inverse: encryption (AES), MACs, key derivation and key wrapping.

PUBLIC AND PRIVATE KEY

Asymmetric-key algorithms

Digital signatures for source, identity and integrity authentication, plus key agreement and key transport.

SEEDED WITH ENTROPY

Random bit generation

Needed to generate keys, IVs, nonces and challenges. Approved generators are in the SP 800-90 series.

Valuable information beyond keys

Information	Role
Domain parameters	Used to generate key pairs, create signatures and establish keys
Initialization vectors (IVs)	Starting point for encryption and MAC modes of operation
Shared secrets	Produced during key agreement, then used to derive keys
RBG seeds	Initialize random bit generators; must stay secret
Other public information	For example, a nonce used in key establishment
Other secret information	Used when seeding an RBG or establishing keying material
Intermediate results	Outputs of internal steps in cryptographic operations
Key-control information / metadata	Identifier, purpose, counter, owner and key state
Random numbers (or bits)	Output of a random bit generator
Passwords	Authenticate identity or derive keys that protect stored data
Audit information	Record of key-management events

How long to keep it, and whether to back it up

Information	Retention	Back up / archive
Domain parameters	Remain in effect until changed	OK
Initialization vector	Until the protected data no longer needs processing	OK, if necessary
Shared secret	Destroy once keying material is derived	No
RBG seed	Destroy immediately after use	No
Other public information	No longer than needed	OK
Other secret information	No longer than necessary	OK
Intermediate result	Destroy immediately after use	No

Shared secrets, RBG seeds and intermediate results are never backed up or archived.

CRYPTOPERIODS

Risk factors that shape a cryptoperiod

Mechanism strength

Algorithm, key length, block size and mode, and how it is embodied (FIPS 140 Level 4 module or PC software).

Environment and people

Secure facility or open office, and turnover of system administrators and CA staff.

Data and usage

Volume of data or transactions, security life of the data, algorithm limits such as nonce reuse, and the security function.

Re-keying and sharing

Re-keying method and process, nodes sharing a key, and the number and distribution of key copies.

Threats

Adversary capabilities and resources, and new technologies such as quantum computers.

Rule of thumb

Short cryptoperiods generally help, but access protection often matters more than key size.

CRYPTOPERIODS · TABLE 1

Suggested cryptoperiods by key type

Key type	Originator-usage	Recipient-usage
Private signature key	1 to 3 years	–
Private authentication key	1 to 2 years	–
Symmetric authentication key	Under 2 years	Up to OUP + 3 years
Symmetric data-encryption key	Under 2 years	Up to OUP + 3 years
Symmetric key-wrapping key	Under 2 years	Up to OUP + 3 years
Symmetric master / key-derivation key	About 1 year	–
Private key-transport key	Under 2 years	–
Ephemeral key-agreement keys	One key-agreement transaction	–

Rough order-of-magnitude guidance (OUP = originator-usage period). Keys encrypting large volumes quickly, such as link encryption, suggest a day or a week. Longer periods call for serious risk review.

DESIGNING A NEW SYSTEM

Factors to consider for a new algorithm suite

1 Sensitivity and lifetime

Don’t underestimate system lifetime or data sensitivity.

2 Algorithm selection

Meet or exceed requirements; consult an expert.

3 System design

Balance performance and security; stay flexible for updates.

4 Evaluate first

Strong cryptography can be poorly implemented.

5 Testing

Test any system before it is deployed.

6 Training

Train people on any new key-management tasks.

7 Implementation

Follow the design closely; note any exceptions.

8 Transition plan

Follow a plan so the changeover runs smoothly.

9 Post-launch evaluation

Verify the system meets its security requirements.

Comparable security strengths

Bits	Symmetric	Finite field (DSA, DH, MQV)	RSA	Elliptic curve
≤ 80	2TDEA	L=1024, N=160	k=1024	f=160–223
112	3TDEA	L=2048, N=224	k=2048	f=224–255
128	AES-128	L=3072, N=256	k=3072	f=256–383
192	AES-192	L=7680, N=384	k=7680	f=384–511
256	AES-256	L=15360, N=512	k=15360	f=512+

80 bits is no longer approved for applying protection, and 3TDEA is deprecated and disallowed after 2023. Estimates will change once practical quantum computers exist.

ALGORITHMS, KEY SIZES AND STRENGTHS

Effective strength is the weakest link

112

BITS OF SECURITY

A 224-bit ECC key establishing an AES-128 key gives no more than 112 bits.

112

BITS OF SECURITY

SHA-256 with a 2048-bit RSA key: RSA limits the signature to 112 bits.

128

BITS OF SECURITY

A 256-bit key wrapped with AES-128 drops to 128 bits.

Strength	Through 2030	2031 and beyond
Below 112 bits	Disallowed to apply; legacy to process	Disallowed to apply; legacy to process
112 bits	Acceptable	Disallowed to apply; legacy to process
128, 192, 256 bits	Acceptable	Acceptable

KEY COMPROMISE

What a key compromise means

The protective mechanisms for a key fail, and it can no longer be trusted.

WHEN IT HAPPENS

Stop applying protection with the key.

Revoke the key.

Use it only to process data already protected, under controlled conditions.

Disclosure. Others can use the key to read past or future data, or to encrypt false data. A leaked private signature key makes signed data suspect; a leaked CA key allows fraudulent certificates and CRLs.

Lost integrity. The key was modified, substituted or deleted, so what it protected is in doubt.

Wrong usage. The key may be used for the wrong purpose or application.

Wrong owner. The identity of the entity can’t be assured.

Wrong association. The key is tied to the wrong information, so services fail or data is lost.

PROTECTIVE MEASURES

Reducing the likelihood and impact of compromise

01 Limit the time a key sits in plaintext form

02 Prevent humans from viewing plaintext secret and private keys

03 Keep plaintext keys in protected containers: HSMs, key loaders, crypto modules

04 Wrap keys so changes to the key or its metadata are detected

05 Use key confirmation to check the right key was established

06 Log every access to plaintext keys (accountability)

07 Add a MAC or digital signature as a key integrity check

08 Use trusted timestamps for signed data

09 Destroy keys as soon as they are no longer needed

10 Create a compromise-recovery plan, especially for CA keys

> The worst compromise is the one that goes undetected, so design the system so that one key exposes as little data as possible.

COMPROMISE RECOVERY

What a compromise-recovery plan contains

The plan shall be documented and easily accessible, for example within the Key-Management Practices Statement.

A Who to notify, and what the notice says

B Who performs the recovery actions

C How a new key is obtained (re-keying)

D Inventory of all keys and certificates, and where they are

E Education of all personnel on the procedures

F All personnel needed to support recovery

G Policies requiring key-revocation checking

H Monitoring of re-keying so every affected key is replaced

I Other steps: equipment inspection, finding affected data and signatures, new keying material

COMPROMISE RECOVERY

Recovering when many parties are affected

Hardest keys to recover from

- A CA’s private signature key, especially a root CA
- A key-wrapping key shared by many entities
- A master key many entities use to derive keys
- A data-encryption key for a large distributed database
- A symmetric key shared across a network
- A key protecting a large number of stored keys

What recovery requires

1. Revoke every compromised key
2. Replace affected keys where needed
3. Assess damage immediately when sensitive or critical data is affected
4. Notify affected entities promptly, and only them
5. Replace over a secure path: automated is preferred, manual may be unavoidable

SUMMARY

Key takeaways

01 Strong algorithms fail without sound key management across the whole key lifecycle.

02 Protect more than keys: seeds, shared secrets, IVs, metadata and passwords matter too.

03 Match cryptoperiods and algorithm strength to the data’s security life and the threats it faces.

04 Plan for compromise before it happens: inventory, notification, revocation and replacement.