Security Principles & Approaches

Security Principle

A fundamental statement that serves as the foundation for security design decisions in order to enable the achievement of business objectives and goals.

Security Design Principles

- OWASP
- Open Group (Jericho Forum Commandments)
- NIST 800-160
- "Ten Guiding Principles of Software Security" - John Viega & Gary McGraw+
- Cyber Security Design Principles
- "High Assurance Design" - Clifford J. Berg

OWASP

- Minimize the attack surface
- Apply defence-in-depth
- Avoid security by obscurity
- Enforce least privilege
- Secure defaults

OPEN GROUP

- Fundamentals (level of protection should be appropriate)
- Surviving in a hostile world (devices communicate using secure protocols)
- The need for trust (transparency at all levels)
- Identity, management and federation (AAA)
- Access to data (controlled, private and secured at all times)

NIST

- Least privilege
- Hierarchal trust
- Hierarchal protection
- Minimize sharing
- Reduce complexity

TTGPSS

- Secure the weakest link
- Defence-in-depth
- Keep it simple
- Promote privacy
- Be reluctant to trust

NCSC

- Establish the context before design
- Make compromise difficult
- Make disruption difficult
- Make compromise detection easier
- Reduce the impact of a compromise

High Assurance Design

- Security design patterns must be verifiable
- Deploy and run securely
- Embed intrustion detection at multiple points
- Logs are secured and reliable
- Segment data and resources according to risk

Principles of Secure Design

- Least privilege principle
- Strong authentication
- Fail-safe
- Layered Defence / Defence-in-depth
- Simplicity
- Sensitive data is protected at all times (rest, transit and in use)
- Effective incident response

Approaches to Security

- Security through Obscurity
- Security through Obsolescence
- Security through Minority
- Security through Diversity
- Security by Design

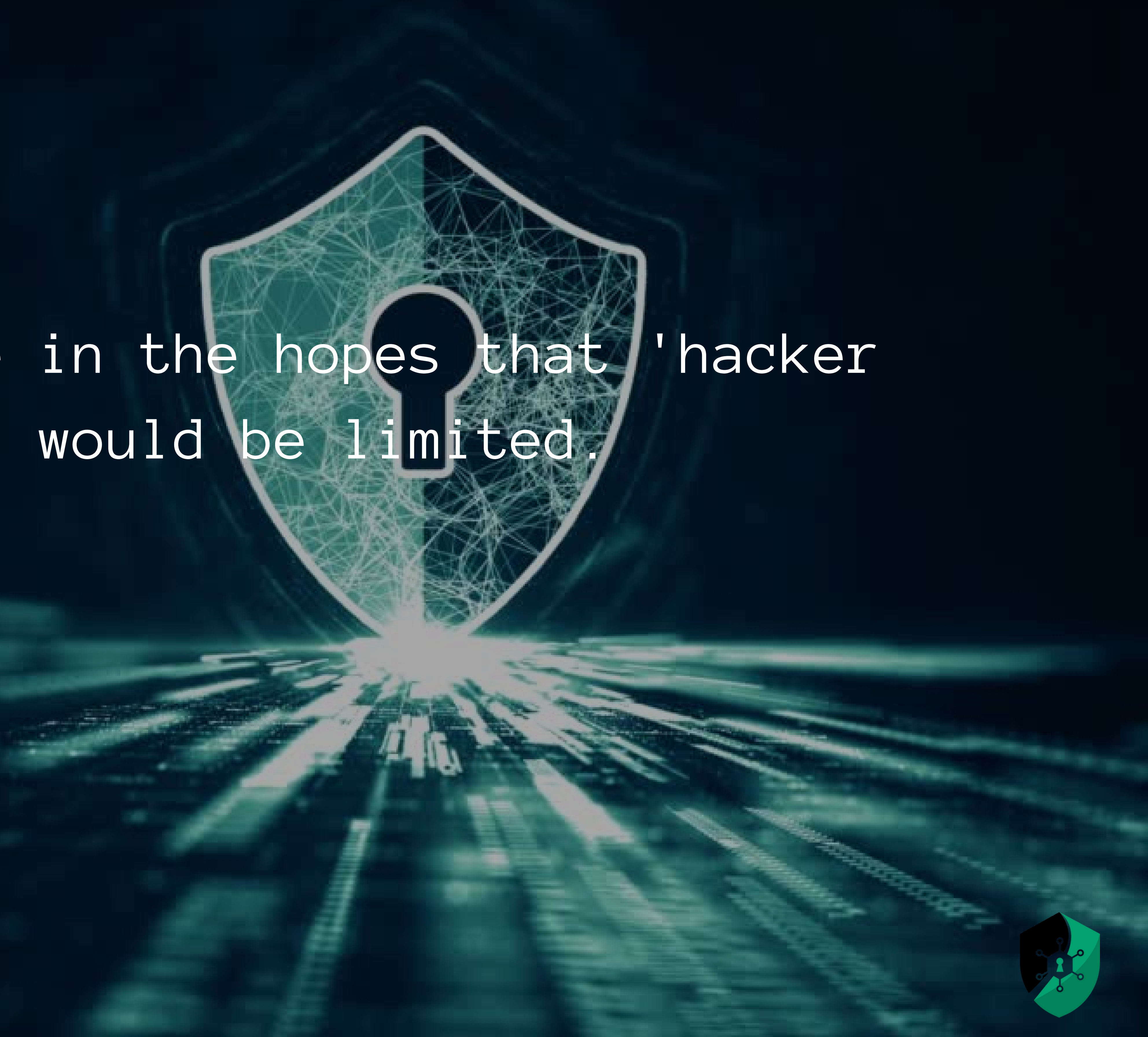
Security through Obscurity

Keeping a system secure by keeping its very existence or vulnerabilities secret.

Security through Obsolescence

Using an outdated operating system (windows XP) on a device to prevent hackers from intruding.

Security through Minority

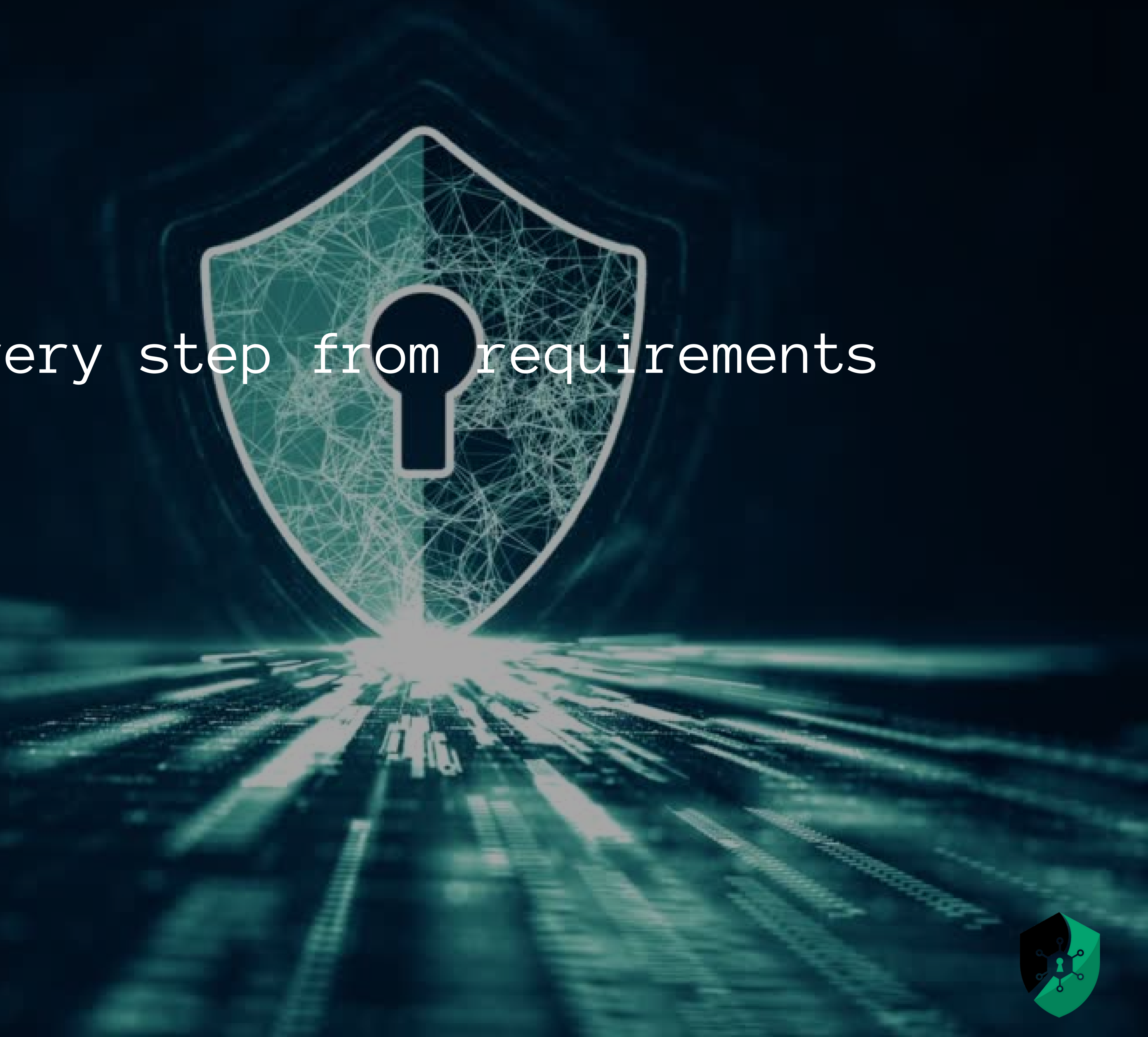


Using very uncommon software in the hopes that 'hacker material' available for such would be limited.

Security through Diversity

Using a very wide variety of systems and apps to confuse the attacker.

Security by Design



Security is considered in every step from requirements to design to deployment.