BEYOND CRYPTOGRAPHY TRUSTED SECURITY

Designing Cryptographic Products That Meet World-Class Security Standards

ST Engineering

Contents

> “Today more than ever, **systems vulnerabilities, design flaws, and backdoors** are the main reasons behind the surge in cybersecurity incidents. Governments and enterprises have to constantly review, upgrade and change their security policies and systems to protect their high-value data, sensitive information, revenue, intellectual property and reputation.”

Goh Eng Choon,
EVP/General Manager,
Info-security,
ST Engineering Electronics

Executive Summary

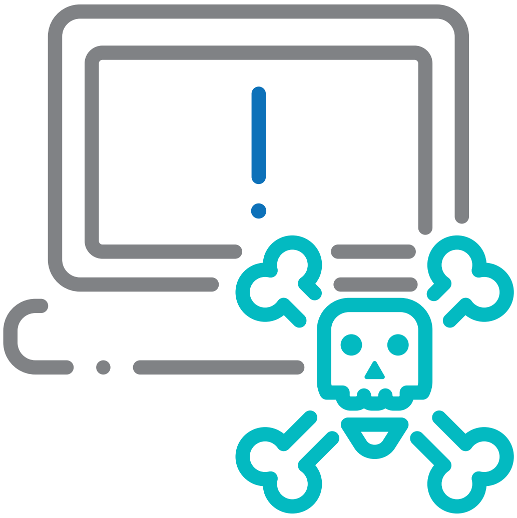
This white paper outlines key security features that IP Encryptors should have for them to be effective in helping organizations with data-sensitive operations protect data-in-transit, prevent unauthorized intrusions into private networks and overcome denial-of-service attacks.

This paper subsequently examines why it is necessary, in the interest of data protection and confidentiality, for IP Encryptors to be resilient against backdoor and side-channel attacks. Consequently, this paper then introduces **The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC)** as an international security standard (ISO/IEC 15408) against which such cryptographic products can be rigorously tested and certified as being resistant against such attacks.

The fundamental question is this:

“In a world of relentless cyber-attacks and threats, have we exercised the same rigor towards improving the assurance and resilience of our security systems by controlling design flaws and weaknesses?”

Threats at the Network Edge



The point at which an organization's internal private network connects to a third-party network (often the Internet) is termed the "**Network Edge**". Without proper established security controls here, organizations risk exposing their entire network infrastructures to a whole host of threats, which include:

Data breaches from unsecured communication channels

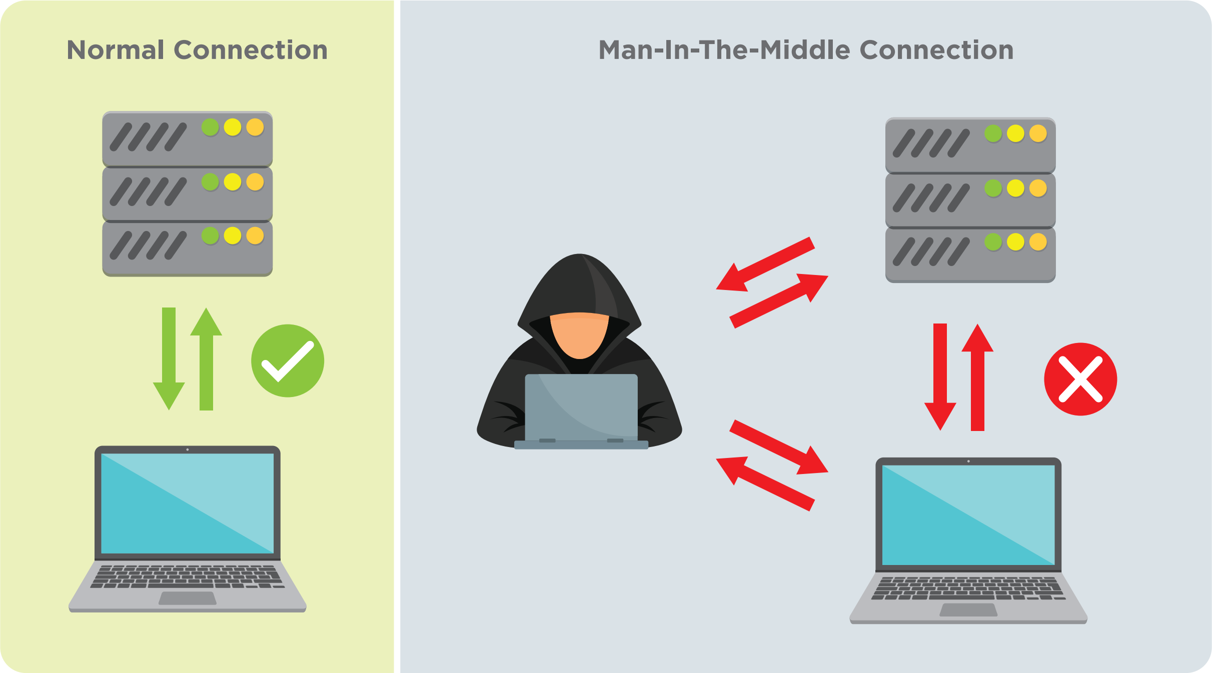


Figure 1: Passive-Man-In-The-Middle attack

When data is transferred between two internal private networks across public infrastructure, one cannot rule out the possibility of having a malicious actor penetrate into the network, intercepting the data traffic, duplicating its contents and passing it on (Passive Man-In-The-Middle attack)

Unauthorised intrusions by external parties into private networks

Rather than targeting data-in-transit, a hacker might attempt to gain unauthorized access to a private network directly. Having penetrated into a network, a hacker can then monitor and redirect network traffic, steal credentials and gain control of more network resources.

Denial of Service attacks (Dos)

Hackers can disrupt the services of private servers and networks connected to the internet by flooding them with superfluous requests.

Malwares

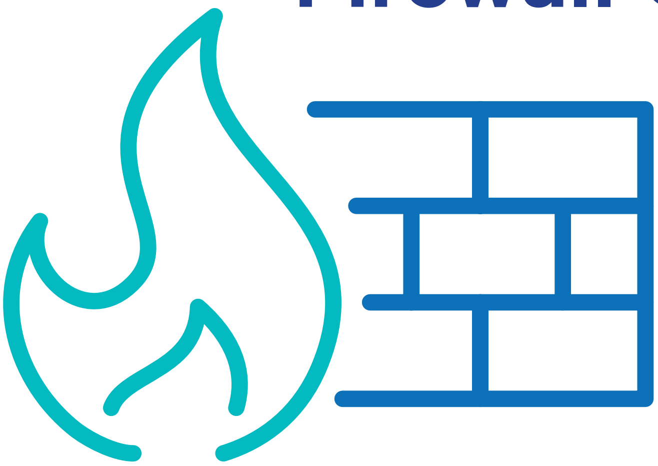
Hackers have often attempted to open up the backdoors to a private network by infecting a network device (e.g. workstation) with a backdoor Malware disguised in the form of a Trojan. As Malwares appear harmless at the first glance and are often equipped with rootkits that allow hackers to have continued access to an infected system, they are threats that are particularly difficult to detect and remedy.

Side-channel and Backdoor attacks

Hackers might also conduct side-channel attacks to circumvent devices deployed at a network edge. For example, against a cryptographic device, one might conduct an attack based on information gained from implementation of the system, rather than the weaknesses in the implemented algorithm itself. Alternatively, hackers might exploit Backdoors and Design Flaws to bypass authentication measures or an encryption process covertly.

IP encryptors stand as the first line of defence against these threats. In the following section, we will outline the security features required of IP encryptors to mitigate the abovementioned network threats successfully.

IP Encryptors with **Firewall Capabilities**



IP encryptors allow users to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. For an IP Encryptor to operate effectively a few core features are needed – **Encryption, Firewall capabilities and Denial of service (Dos) countermeasures**.

Confidentiality protection

Data breaches from unsecured communication channels

Encryption

IP encryptors encode outgoing data before it transits through public networks using an encryption algorithm, making it only accessible to users with the correct encryption key. When selecting an encryption algorithm, it is important to choose one that is reasonably strong yet computationally efficient.

In the current world of cryptography, the AES[1] family of encryption algorithms fit these two criteria and are by far are the most widely adopted, with AES-CBC and AES-CTR being the two most commonly used encryption algorithms.

The other reason why these algorithms are commonly used is that most cryptographic experts regard them to be computationally secure. For example, guessing an AES-256 CBC encryption key using a brute-force attack is near impossible, as there are 2^{256} possible combinations, and even modern supercomputers cannot crack that in a reasonable timeframe.

Integrity protection

IP encryptors often employ hashing functions (usually SHA[2]-256 or HMAC SHA-256) to create a hash (a unique signature) of the transmitted data. By matching the hash of the received data and to the transmitted hash value, encryption devices can verify that there were no signs of tampering to the data.

[1] *Advanced Encryption Standard, a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.*

[2] *Secure Hash Algorithms, a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST)*

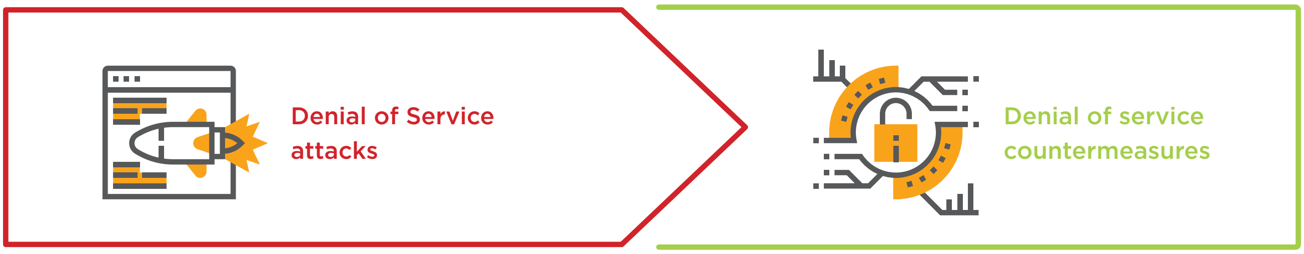
Authentication

IP encryptors also require some form of mutual authentication measures, and often use some form of public-key encryption schemes; with ECC[3] and RSA[4] Public Key Signature Verification (up to 4096 bit being the maximum key size for typical use) being the most widely used.

Unauthorised intrusions by external parties into private networks

Firewall

IP encryptors often rely upon some form of built-in firewall to monitor and control incoming and outgoing traffic. For example, a firewall might perform packet filtering, allowing packets whose source and destination IP addresses, protocols and ports match predetermined security rules to pass, and subsequently discarding all other unauthorised traffic. As a means of strengthening network security, encryptors ought to perform Network Address Translation by concealing the IP addresses of devices connected within the private network.


Denial of Service attacks

Denial of service countermeasures

To thwart possible DoS attacks, IP encryptors should have denial of service countermeasures. Certain tunneling protocols, like the IPsec standard, have inherent features that protect against packet replay for 64-bit replay window implementations.

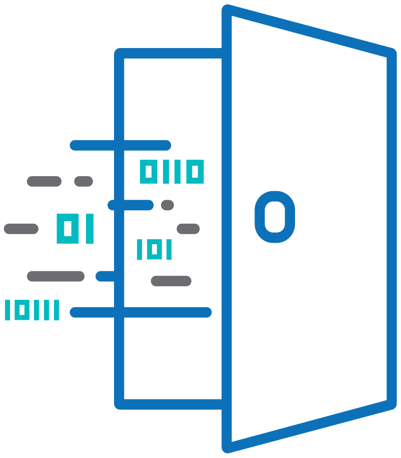
Other security features

An effective IP Encryptor needs to demonstrate tamper-resistance capabilities (triggering of active erasure of SRAM & DRAM to prevent hackers from retrieving the encryption key even with direct physical access to the device.

With these robust security implementations in place, breaking IP encryptors via traditional means would be a near impossible task. However, there are side channel and backdoor attacks, which hackers might attempt to break into such cryptographic products.

[3] *Elliptic-curve cryptography*

[4] *RSA (Rivest–Shamir–Adleman), one of the first public-key cryptosystems widely used for secure data transmission*



Side Channel and Backdoor Attacks

In cryptanalysis (the process of deciphering coded messages knowing the encryption key), **Side-Channel attacks** can include:

Traffic analysis attacks	Hackers intercept and examine patterns found in the communication, such as the frequency and timing of network packets to deduce information about the content of the messages.
Electromagnetic attacks	Hackers measure the electromagnetic radiation emitted from a device and perform signal analysis on it. For a cryptographic system, each operation the cryptographic implementation performs on data emits different amounts of radiation. Hence, tracing this can allow a hacker to deduce the exact sequence of operations, and by doing so, retrieving the encryption key partially or fully.
Power Monitoring attacks	Hackers observe the power consumption by the hardware or cryptographic circuit during computation (either through simple power analysis or differential power analysis) to extract cryptographic keys and other secret information from the device.
Timing attacks	Hackers monitor data movement in and out of the CPU or memory on the hardware running the cryptosystem or algorithm. From careful observation of the variations in how long it takes to perform various cryptographic operations (which involve statistical analysis of timing measurements), it might be possible to determine the secret key.

In addition, **Backdoor attacks** include:

Encryption Backdoors	Using encryption algorithms with backdoors allows attackers to bypass cryptographic systems or decrypt encrypted data much quicker.
Application Backdoors	Hackers exploit bugs in software applications used to configure these cryptographic systems (e.g. skipping password verification process and obtaining root access).
Malware Backdoors	Hackers disguise backdoor malwares in the form of Trojans, which create backdoors in a target system upon installation. These backdoor malwares allow a hacker to bypass security mechanisms enforced by the system.
Supply Chain Infiltration	A system might become vulnerable due to a software or hardware backdoor introduced at some point in the supply chain by an unknown actor. Similarly, using free repositories of code from open source libraries allows for rapid software development but is inherently dangerous as there might be forms of malicious code embedded within.
Design Flaw Backdoors	Backdoors introduced during the development process may find their way into the final release by accident, which hackers can exploit to compromise a cryptographic system.

Because design weaknesses and vulnerabilities create opportunities for hackers to recover encryption keys and extract sensitive information through side-channel attacks and backdoors, strong cryptography alone is insufficient, and forms only half of any data protection and confidentiality solution. The other half comes from rigorous security testing to ensure implementation correctness of the security features mentioned above (Encryption, Firewall Capabilities and Denial-of-service countermeasures) alongside security features which provide IP encryptors' resistance against side-channel and backdoor attacks.

In the following section, we look at what the 'gold' standard for this process is, the Common Criteria – a well-documented international standard that provides certifiable security baseline to security products.

Security Beyond Cryptography - Common Criteria Certification

The Common Criteria is an international standard (ISO/IEC 15408) for IT product security certification. What the Common Criteria security framework offers is independent, scalable and globally recognized security inspections for IT products (e.g. verifying product performance and security claims). In particular, the scheme benefits organizations with limited expertise in cybersecurity in building their cybersecurity portfolios, by providing them a platform for fair comparison of products according to their security requirements. To date, over 30 nations have cooperated and adopted this framework.

The process of specification, implementation and evaluation of all products is a rigorous and repeatable one, as verified by a third-party evaluation lab and the standardization of procedures is beneficial to companies selling computer products as they only need have them evaluated against one set of standards.

To become Common Criteria certified, organizations must complete a Security Target (ST) description and provide other supporting documents, including an overview of the product and its security features, an evaluation of potential security threats and a self-assessment detailing how the product conforms to the relevant Protection Profile at the Evaluation Assurance Level against which it is tested. Next, organizations must find an independently licensed laboratory to evaluate their product and determine if it meets security properties to a satisfactory level. Lastly, if the product passes the evaluation, the various Certificate Authorizing Schemes can be issued with a certification for those security properties.

Achievement of Common Criteria Certification signifies the ability to be on par with international standard and quality benchmarks. Thus, many government agencies and organizations are increasingly using the Common Criteria to evaluate and assess the security posture and integrity of its IT products.

Case Study

NetCrypt's CC Certification Process

NetCrypt Series

Layer 3 (IP network multi-point, support routing)

COMMON CRITERIA CERTIFIED EAL2

NetCrypt S20

- Up to 50 tunnels
- 100 Mbps

NetCrypt R100

- Ruggedized for military use
- 100 Mbps

NetCrypt U1000

- Up to 300 tunnels
- 50 Mbps

NetCrypt U2000

- Up to 800 tunnels
- 1 Gbps

Excerpt from the NetCrypt family series Certification Report[5]:

> *The Family of TOE [6]consists of portable (NetCrypt S20) and rack mounted (NetCrypt R100/U1000/U2000) hardware IP Encryptor that enables the user to leverage on public Ethernet/IP infrastructure to form a secure VPN between itself and a peer TOE. It employs AES algorithm for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as Internet Key Exchange (IKE) protocols for keys derivations and authentications. All models provide the same security functionalities. The evaluated configuration is a gateway-to gateway configuration with only local management.*
>
> *The evaluation of the TOE has been carried out by An Security Pte Ltd[7], an approved CC test laboratory, at the assurance level CC EAL2 and completed on 25 June 2018. The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.*

[5] The certification report can be viewed here: https://www.commoncriteriaportal.org/files/epfiles/NETCRYPT%20CERTIFICATION%20REPORT%20v2.0.pdf

[6] Target of Evaluation – The product or system that is the subject of evaluation

[7] An Security Pte Ltd website: https://www.an-security.cornm/

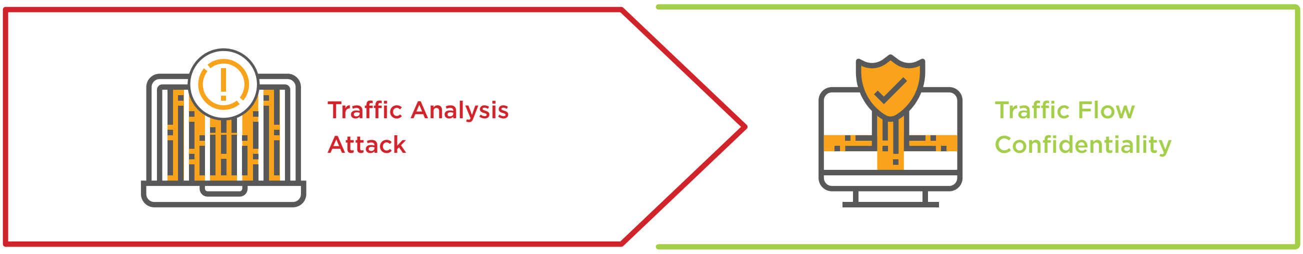
Security Functionalities	What was Verified
Encryption	Correct implementation of AES-256-CBC
Integrity	Correct implementation of SHA-256 and HMAC SHA-256
Authentication	Correct implementation of RSA signature generation, secure values for p, q and d of RSA algorithm modulus 2048 and quality of random number generated by TOE
Firewall	TOE's External Port only accepts IKEv2 packets and IPSec traffic with destination IP addressed to its External port IP

Note: Side channel attacks are normally conducted for mobile devices (Common Criteria EAL4+ and above) where it has higher chance of falling into the hand of an adversary, whereas for device that are deployed in a physically protected environment, it may not be a requirement to do so.

NetCrypt Series Security Features

To address the vulnerabilities as identified in "**Side Channel and Backdoor attacks**" section, certain security features for the NetCrypt were included in its design, which include the following:

Traffic Analysis

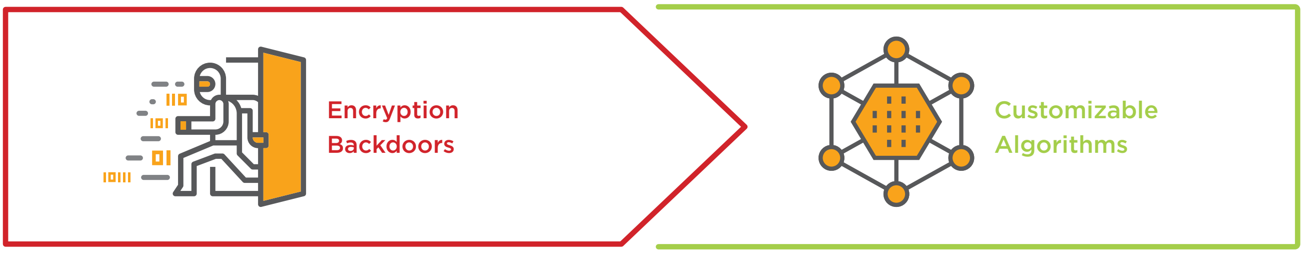


Traffic Analysis Attack

Traffic Flow Confidentiality

Traffic Flow confidentiality is enforced by padding packets to a given packet size, and keeping traffic flow at a constant throughput.

Encryption Backdoors

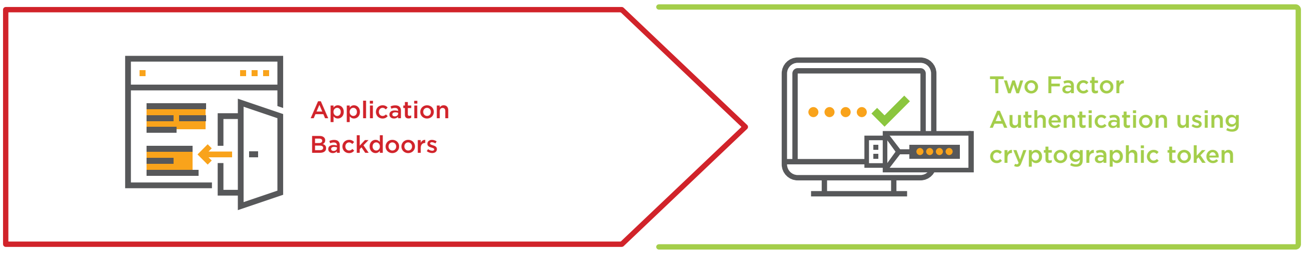


Encryption Backdoors

Customizable Algorithms

Although the Advanced Encryption Standard has thus far proven to be computationally secure, used by even the Western governments to encrypt sensitive data and have no known encryption backdoors, users have the option to introduce their own customizable encryption algorithms if desired.

Application Backdoors

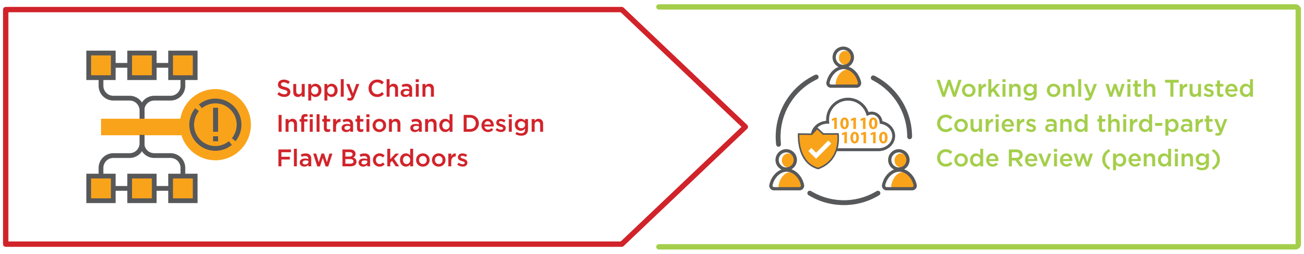


Application Backdoors

Two Factor Authentication using cryptographic token

To protect against application backdoors, the NetCrypt Admin application can enforce the use of two-factor (2FA) authentication using a cryptographic token for user authentication. This ensures that even if the input password step is bypassed (or known to a hacker), a hacker is still unable to access the device.

Supply Chain Infiltration/Design Flaw Backdoors



Supply Chain Infiltration and Design Flaw Backdoors

Working only with Trusted Couriers and third-party Code Review (pending)

To protect against supply chain infiltration and backdoors, delivery of NetCrypt products is conducted through its own In-house courier channel for local delivery. This applies to overseas deliveries where similarly, only trusted couriers are used. In addition, the NetCrypt is currently undergoing thorough code review by a government agency (a separate process that does not fall under CC EAL2 Certification) for Trusted System Vetting.

Lastly, to address the possibility of Electromagnetic, Power Monitoring and Timing attacks, an assumption had to be regarding NetCrypt's operating environment, which is that: The physical environment of the provisioning and deployment site shall prevent unauthorised physical and logical access to the TOE.

NetCrypt Series- A Development by ST Engineering Cybersecurity

ST Engineering is the first local company in Singapore to achieve CC certification, for its NetCrypt Series - a suite of high-assurance network encryptors. The entire series has been CC certified at EAL2, with new developments underway. ST Engineering's commitment to high quality and standards for its products through the adoption of Common Criteria (CC) certification stands alongside its own rigorous internal testing processes and provision of robust technical support and engineering services. Beyond building our IP encryptors on these two pillars of cryptography and certification, we also believe that a third pillar, that of trust, is critical to establishing a strong foundation in systems security engineering.

Paradigm Shift

Risk Management to Trust Validation[8]

The shift towards security certification is, in some way, an attestation of the shortcomings of current model of security assessment based on risk management. Using risk model and process (where one assigns risk scores based on conceptual system vulnerabilities, likelihood of attacks and projected impact of the damage caused), one adopts a reactive approach and is resigned to a passive acceptance of the impact one is prepared to bear.

In contrast, trust validation pivots on thorough security evaluation to give assurance that a product will behave in a known and predictable manner under specified circumstances. Through independent product evaluations and verifications of implementation correctness, a stronger focus is given towards improving inherent design, tightening security considerations and provision of safeguards against vulnerabilities and side channel attacks.

Alongside technological advancements comes the evolution of ideas and creation of new paradigms. In this ever-evolving cyber-physical world, a comprehensive security solution therefore needs to transcend cryptography and random numbers, to embrace security by design and, on top of providing security functionality, incorporate the element of trustworthiness from the start of the design to the entire development process.

[8] This was a focus area of Singapore International Cyber Week/International Common Criteria Conference in October 2019, "Leveraging Common Criteria for Paradigm Shift from Risk Management to Trust Validation" addressed by President of ST Engineering's Cybersecurity Systems Group, Goh Eng Choon https://www.iccc2019.com/programme

Conclusion

What will the future of cryptographic products look like? While no one knows for sure, we predict that data-driven organizations and government agencies (both having tight data security requirements) will be the key players that will continue to press for conformance to cybersecurity standards. In efforts to meet such requirements and standards then, security-by-design might become a more popoular approach to software and hardware development, whereby product vendors prioritize designing and building security throughout the entire product development lifecycle to minimize system vulnerabilties. We believe all encryptors ought to be designed with such an approach such that they go beyond being cryptographic products that function well to being verifiable and trusted security solutions.

References

Common Criteria. (1 Feburary, 2019). *NetCrypt Family Series S20/R100/U1000/U2000 v2.6.4 Certification Report*. Retrieved from Common Criteria Web site: https://www.commoncriteriaportal.org/files/epfiles/NETCRYPT%20CERTIFICATION%20REPORT%20v2.0.pdf

Goh, E. C. (September, 2019). *First Mover's Perspective – Taking on the Common Criteria Certification Journey.* Retrieved from Agil Blog - A ST Engineering Electronics Web site: https://agilblog.com/tech-views/cybersecurity/first-mover-s-perspective-taking-on-the-common-criteria-certification-journey/

Jefcoat, K. M. (8 December, 2017). *What is Common Criteria Certification, and Why Is It Important?* Retrieved from Blancco Web Site: https://

About

ST Engineering Cybersecurity

With digital technology and highly connected economies come new vulnerabilities from a proliferation of cyber threats. To strengthen cyber resilience, it requires a system of cybersecurity capabilities that comprises of People, Process and Technology. Backed by indigenous capabilities and deep domain expertise, we offer robust cyber-secure products and services in cryptography, cybersecurity engineering, digital authentication, SCADA protection, audit and compliance.

We specialise in the design and build of security operations centre, provide cybersecurity professional and managed security services customers in national, government, critical information infrastructures and commercial enterprises. To-date, the cybersecurity academy have certified and trained cybersecurity professionals in more than 150 organisations.

100 Jurong East Street 21,
ST Engineering Jurong East Building,
Singapore 609602

☎ (65) 6568 7118

✉ cybersecurity@stengg.com

www.stengg.com
cybersecurity@stengg.com

V0922

www.stengg.com/cybersecurity