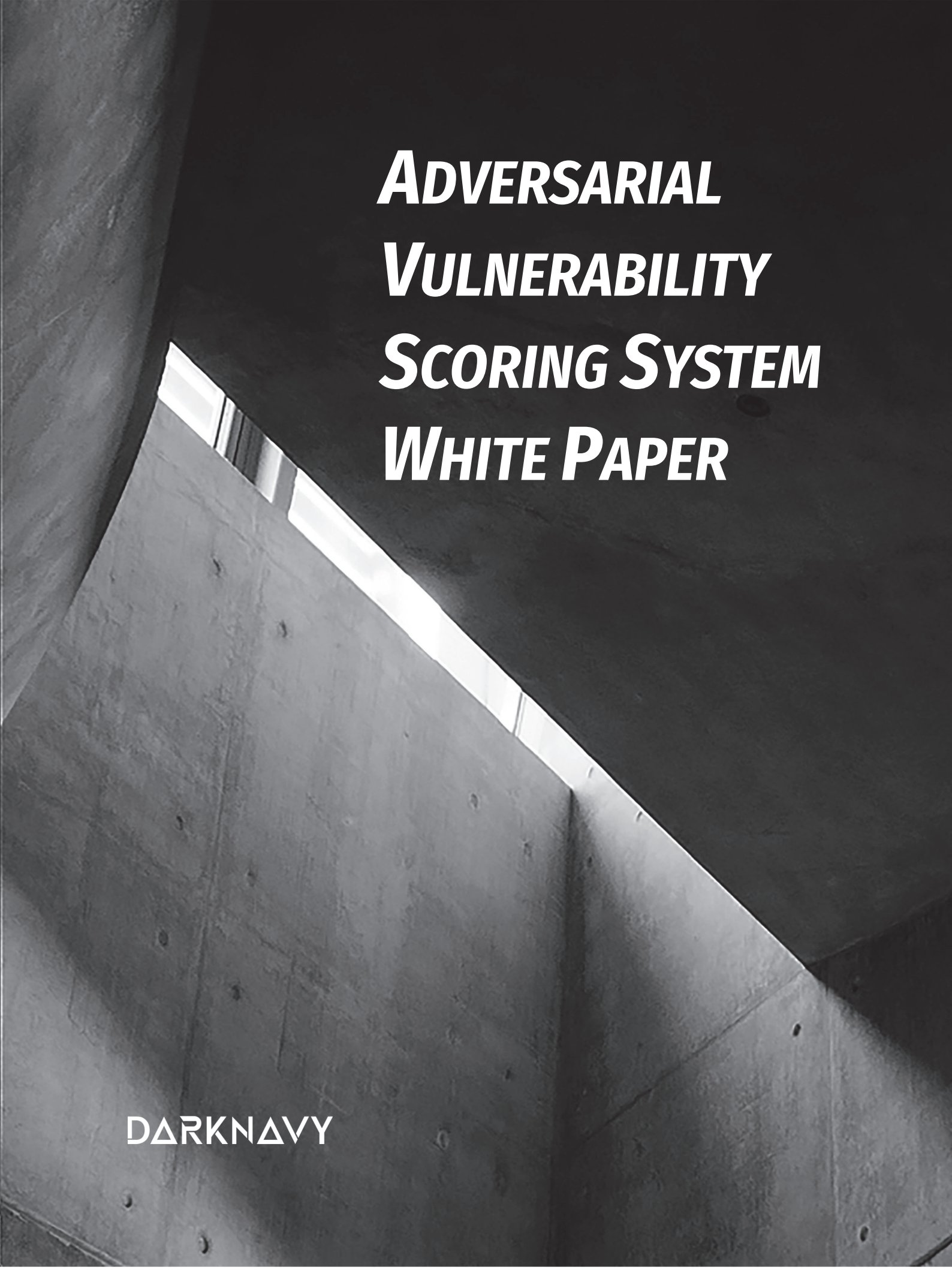
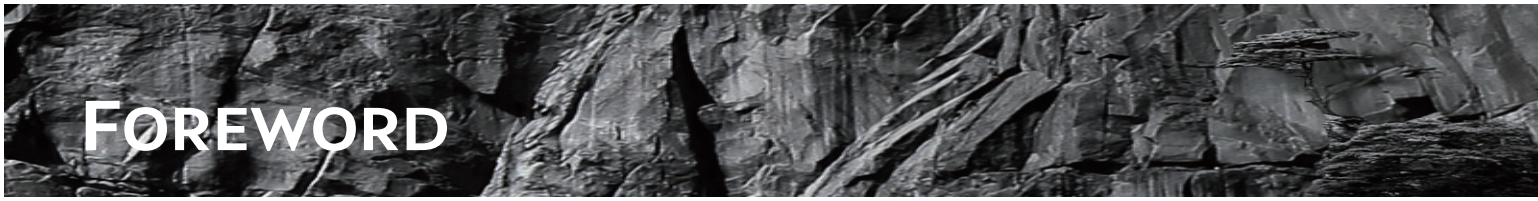


Adversarial Vulnerability Scoring System White Paper

DARKNAVY

An adversary based on attacker's perspective is the only scientific measure proving the level and effectiveness of security defense mechanisms.

Daniel Wang
Founder & CEO, DARKNAVY



Foreword

The essence of cybersecurity lies in the constant battle between attack and defense, where vulnerabilities form the bedrock of all threats. However, it's a universal truth within the cybersecurity community that vulnerabilities can never be entirely eliminated.

Assuming there were an array of three online payment systems, five smartphone models, seven smart car brands, and ten office networks, a sophisticated and persistent attacker would still inevitably detect new vulnerabilities, making these systems susceptible to breaches.

So, where does the value of our considerable security efforts lie?

Security isn't a realm of absolutes; it's not a simple toggle between secure and insecure. Approaching it from a binary perspective oversimplifies a complex issue and does a disservice to enterprises investing in security.

The primary objective of security defenses is to elevate the cost for attackers, making their endeavors as arduous as possible.

For years, DARKNAVY and GEEKCON have delved into the mindset of malicious attackers, aiding numerous enterprises in vulnerability identification. We recognize a harsh reality: penetrating a heavily fortified system often demands the expertise of top security research teams spending hundreds of days, whereas systems with lesser investments may fall prey to attacks within days by ordinary attackers. Through the lens of attackers, DARKNAVY grasps the significance and value of robust security measures. As consumers ourselves, we gravitate toward products or systems that command higher costs on potential attackers. Indeed, for enterprises prioritizing security investments, security emerges as a core competitive advantage, not as an expense.

We urge industries to place security as an essential market advantage. Only then will cybersecurity be on the priority ladder across diverse sectors, safeguarding users effectively.

Consider the traditional automotive industry, where safety underscores competitive advantage. Just as collision testing determines which car can better protects passengers, the ability to prevent online tracking defines a vehicle's security prowess. To become a core competitive advantage, security must be tangible and quantifiable to consumers and business leaders.

Hence, we've developed and championed Adversarial Vulnerability Scoring System (AVSS) — a novel, open, attacker-perspective-based security assessment framework. AVSS not only fortifies defenses but also empowers data-driven decision-making. By quantifying security strengths, AVSS enables businesses to make informed decisions, maximizing their security investments and staying ahead of emerging threats.

Our vision is to forge a robust cybersecurity evaluation ground through collective efforts within the security ecosystem, where AVSS serves as a beacon working with businesses toward resilience and strength in the face of evolving cyber risks.

Daniel Wang
Founder & CEO, DARKNAVY

1. WHAT IS AVSS

Adversarial Vulnerability Scoring System (AVSS) is a quantifying approach to systematically measure security defense capabilities of an evaluated object, from an attacker's perspective, based on vulnerability exploitation and defense confrontation.

Benefits of AVSS

- *Improved security understanding*
- *Resource optimization*
- *Data-driven decisions*

AVSS is a scoring guideline for evaluating the security level of information systems, IoTs, or their subcomponents, based on real-world adversarial activities. It was first proposed, maintained, and managed by the independent security research organization DARKNAVY.

AVSS builds a systematically quantifying evaluation framework from the confrontational perspective of attack-and-defense, to meet the updated requirements of security performance evaluation with the continuous development of information technology. By comparing security evaluation scores of an information system, an IoT device, or their respective subcomponents with other peers or previous versions of themselves, respectively, it helps information system operational

team and R&D team of the IoT device to precisely understand the current security status and to better measure the returns of information security resources, including personnel, funds, and equipment etc., so to methodically evaluate direct outputs of a security investment and its contribution to the business.

AVSS has been practiced in multiple fields such as financial payment, mobile computing, smart manufacturing, and connected vehicles. These projects have helped providing security defense results for an organization's information systems and products, and become an important basis for its business decision-making.

AVSS is designed as an open methodology, which will bring community talents, academia and institutions, research organizations, and manufacturers together to jointly participate and continuously improve, so to promote the development of security ecosystem.

2. AVSS HIGHLIGHTS

2.1 Evaluating Security from a Real Adversarial Perspective

Current security evaluation frameworks mostly focus on the defensive aspect, emphasizing on the completeness and compliance of security defense mechanisms. Those frameworks lack for the adversarial evaluation from an attacker's perspective. The emergence of AVSS provides the industry with a new perspective to examine and help enhance the security of information systems, IoTs, or their subcomponents.

The rapid development of information technology has led to constantly changing demands for security evaluations. The emergence of a security system based on a real attacker's perspective has become an inevitable trend. Security evaluation has evolved from verifying basic security function to confirming cybersecurity assurance (functional effectiveness), and then to the verification of comprehensive security mechanisms and in-depth defense systems. However, even comprehensive defense mechanisms are in place, with the continuous existence of security vulnerabilities, attackers could still successfully penetrate through, which exposes security issues in systems or products.

Vulnerabilities can never be totally eliminated. Defense is to increase the cost of attacks.

Therefore, evaluations from attackers' view became important. Penetration testing, vulnerability mining, and vulnerability evaluation have then been transformed into a new cybersecurity evaluation method named CVSS, that is, reflecting the cybersecurity level of a targeted object based on a number of vulnerabilities found in a system or product.

Period	Features	Evaluation Standard
The early stages of the Operating Systems and Networks.	Confidentiality requirements, prevention of information leakage.	Confidentiality, Integrity, and Availability (CIA) Evaluation
Internet and PC period	Viruses and worms are rampant; systems are full of vulnerabilities	Evaluation of malware detection and removal capabilities.
The maturity of PCs and the rise of mobile platforms	The effectiveness of defense mechanisms begins to manifest, exploiting vulnerabilities to penetrate systems.	With the number of vulnerabilities, Common Vulnerability Scoring System (CVSS) centered on vulnerability assessment, reflecting the level of system security.
Various security solutions emerge, and good security practitioners appear.	Defense mechanisms become mature, and bypassing these mechanisms becomes the core of attacks.	By evaluating the effectiveness of defense mechanisms, the AVSS assessment quantifies system security capabilities and guides entities to make their security investments.

Why AVSS takes a different approach:

- *Focus on attack cost*
- *Beyond vulnerability counts*
- *Attacker simulation: the ultimate test*

The widespread deployment of security defense mechanisms in complex information systems and IoTs has further increased the complexity of attacks. Attackers often need to exploit multiple vulnerabilities simultaneously to form attacking chains, so to gradually approach their targets. In this scenario, individual vulnerabilities may not be sufficient to achieve attacking goals. However, when multiple vulnerabilities are interconnected to form a complete attacking chain, they can pose a serious threat to a system.

Therefore, for security evaluations of information systems, IoTs, or their subcomponents, it is necessary to shift from assessing security mechanism and vulnerability to comprehensive real-world adversarial evaluations. Simulating real attack scenarios for in-depth testing and vulnerability discovery, the evaluation process should focus more on integrating business processes and practical application scenarios. This ensures that information systems and IoTs can effectively resist, detect, and recover quickly when facing malicious attacks in real environments. Such an evaluation system helps organizations better understand and manage information security risks, thus building more resilient and adaptable security safeguards.

Not knowing offense well, how can one shield off attacks?

AVSS

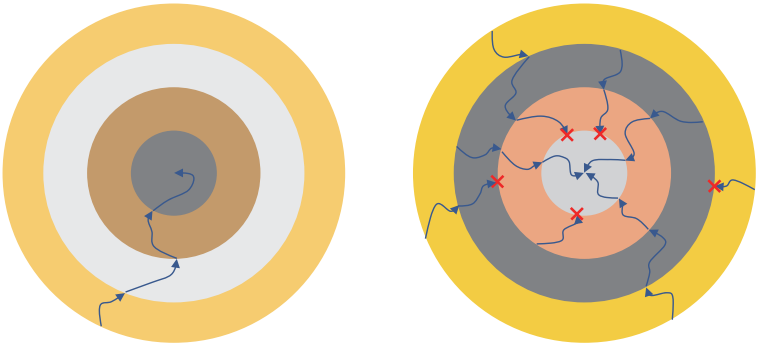
Evaluating Security from a Real Adversarial Perspective

The AVSS believes that:

- Vulnerabilities can never be completely eliminated, and the goal of all security defense efforts is to increase the cost of attacks as much as possible.
- Evaluating the security level of a system based solely on the number of vulnerabilities or whether it has been breached, or even using generic vulnerability scores, lacks scientific rationality.
- An adversary based on attacker's perspective is the only scientific measure proving the level and effectiveness of security defense mechanisms.

2.2 Not only verifying vulnerabilities but also validating the effectiveness of security defense mechanisms

In real-world systems and devices, security vulnerabilities and defense mechanisms coexist. With the continuous improvement of modern security systems, especially the gradually established security defense mechanisms, vulnerabilities can be effectively prevented from being exploited by attackers. However, the existence and discovery of vulnerabilities have randomness and uncertainty, which cannot be fully controlled. Validation of the effectiveness of security defense mechanisms has always been a challenge in security assessments. AVSS not only focuses on real security adversarial testing but also proposes ideas for validating the effectiveness of defense mechanisms. Real-world combat is the only logical method for evaluating the effectiveness of security defense mechanisms. Therefore, actual vulnerabilities and exploits are used to test the effectiveness of security defense mechanisms. By mining vulnerabilities in an evaluated target and conducting exploitation tests, AVSS can conduct in-depth testing of the security defense mechanisms of an evaluated target and provide quantitative indicators of the effectiveness of security defense mechanisms.



Pic 1: Different Outcomes between Vulnerability Mining Attack and AVSS Evaluation

Advantages of AVSS:

- *Bypass outer defenses*
- *Explore deeper weaknesses*
- *More comprehensive evaluation*

Not only verifying vulnerabilities but also validating the effectiveness of security defense mechanisms

More importantly, by placing vulnerabilities in a target before evaluation, AVSS can break through conventional patterns, bypass specific defense mechanisms, and explore and validate deeper vulnerabilities, thereby ensuring the security and stability of the testing system. Typically, the outer layer of a system's protection is the most stringent, with the most comprehensive security defense mechanisms in place. If testing from a perspective of other attackers cannot bypass the outer defense mechanisms, it is impossible to evaluate the system's security level within the outer protection (*Pic 1 Left: pre-condition of vulnerability mining attack is an ability to bypass the outer defense mechanisms*). This makes an evaluation difficult to be comprehensive and lacks for depth, only verifying the outer defense capability. However, with a defense mechanism validation provided by AVSS and with the cooperation of a testing client, more resources of a testing system could be opened up for evaluation, allowing testing from multiple attacking entry points and different attacking levels, thus comprehensively validating the effectiveness of security defense mechanisms.

Therefore, the evaluation results provided by AVSS can depict a panoramic view of system security, providing more comprehensive and in-depth evaluation results for system security (*Pic 1 Right: AVSS Defense and Attack Framework (DAF) collects much more defense mechanisms, and vulnerability evaluation will help identify effectiveness of defense mechanizes*).

2.3 Open Framework Supports Collaborative Improvement by Participating Parties

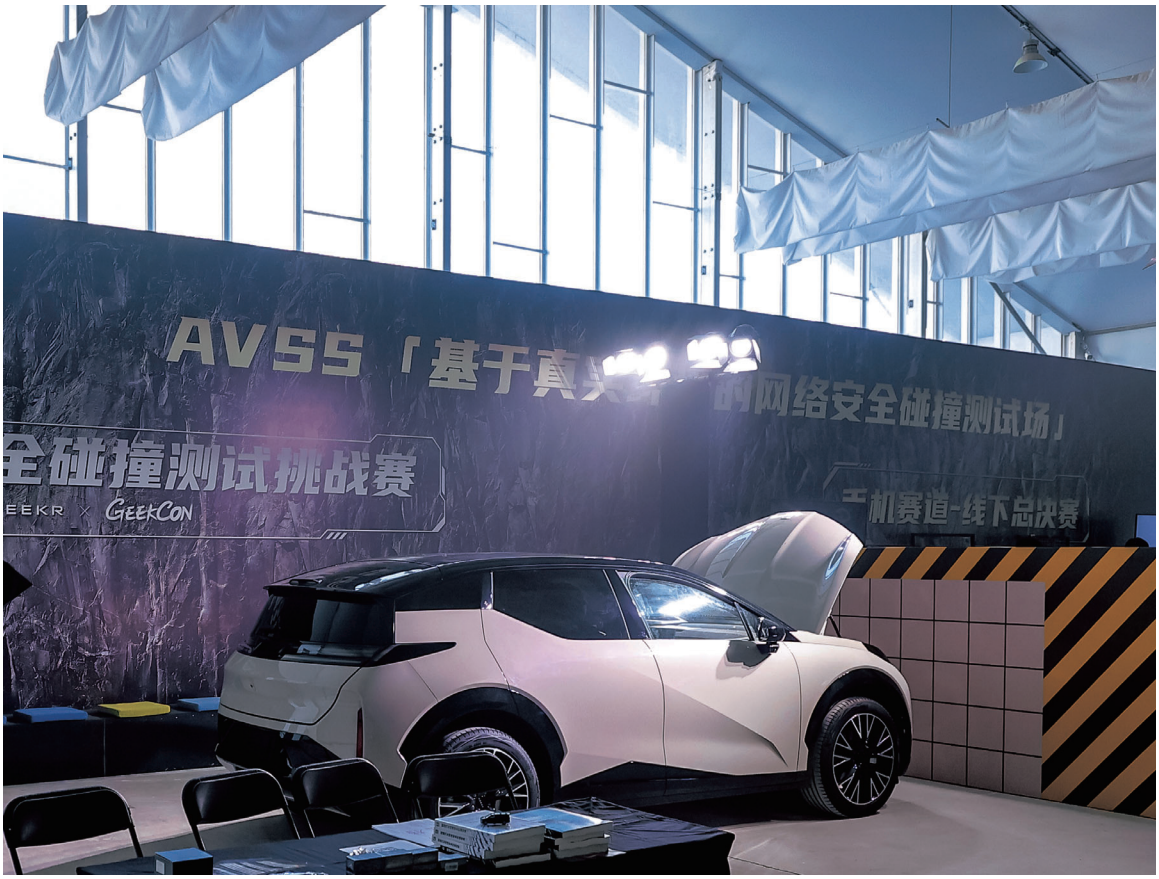
AVSS, as an open framework, actively advocates for collaboration and extensive participation, particularly welcoming various vendors to jointly promote its development and improvement. Information security involves a wide range of fields. Different industries face varying security challenges in their application scenarios. Moreover, characteristics of different IoT technologies also vary, making information security evaluation a complex and diversified task. It requires an evaluation approach to not only have strong scalability but also be flexible to adapt to specific requirements of different domains and scenarios.

To meet the requirements of information security diversity for an evaluation framework, AVSS actively promotes and encourages multi-party participation from regulatory authorities, industry and local entities, research institutions, community forces, and IoT manufacturers etc. Under the AVSS open framework, all participating parties follow a unified methodology, to formulate evaluation criteria and frameworks with regional characteristics, industry features, and unique application scenarios, and combine with regulatory requirements, system product technical characteristics, and security standards from different regions and industries. Through this open and collaborative approach, AVSS applications and frameworks in different regions, industries, and technology fields will continue their enrichments and improvements.

How AVSS achieves open collaboration:

- *Diverse participants*
- *Unified methodology*
- *Customizable frameworks*

With multi-party participation and joint development, AVSS will gradually evolve into a more comprehensive and efficient security evaluation program. Not only will it support the development of information security industry, but it will also promote the advancement of industrial and sectoral ecosystems.



3. The Value of AVSS

AVSS considers:

- *Vulnerability presence*
- *Exploitability of vulnerabilities*
- *Effectiveness of defense mechanisms*

The core value of AVSS lies in its ability to accurately measure the security of systems.

As the era of IoT emerges, various types of systems and devices coexist, each with different levels of technology and security investments. These differences in systems lead to varying capabilities in defending against vulnerabilities. Impacts of the same vulnerability can vary significantly across different systems, depending not only on the specific system environment but also on the attackers' tactics. Therefore, using quantity and severity of vulnerabilities as indicators to evaluate security is not accurate. Just because a vulnerability exists only in newer versions of software does not necessarily mean that the security of the newer version is inferior to that of the older version. While newer versions of software may have specific vulnerabilities, they may also adopt new security mechanisms or architectures that significantly enhance their ability to resist vulnerability exploitation. In such cases, a more accurate and reflective evaluation method of real security situations is needed.

AVSS integrates various aspects such as vulnerabilities, exploitability of vulnerabilities, and effectiveness of defense mechanisms in its evaluation, serving as a reflection of security defense capabilities, and also representing the cost of carrying out attacks.

3.1 Making Security a Core Value of Products

As consumers increasingly place more focus on information security, choosing products with better security performance will become a consensus of more users. The quantitative evaluation provided by AVSS not only enhances the transparency of efforts in information security by IoT manufacturers but also makes security capability a product feature.

In the digital age, information security has undoubtedly become a key factor in the quality and security of IoT products. An excellent product or a reliable IoT device should not only excel in functionality and user experience but also establish a robust information security protection system. This system ensures secure storage and transmission of data, effectively prevents information leakage, tampering, or loss, and safeguards the security of systems and data. AVSS evaluates from multiple dimensions such as defect exploitation and effectiveness of defense mechanisms, presenting evaluation results in quantitative values, allowing for a straightforward understanding of the security level for an evaluated object.

AVSS benefits manufacturers:

- *Security benchmarking*
- *Data-driven decisions*
- *Security as a differentiator*

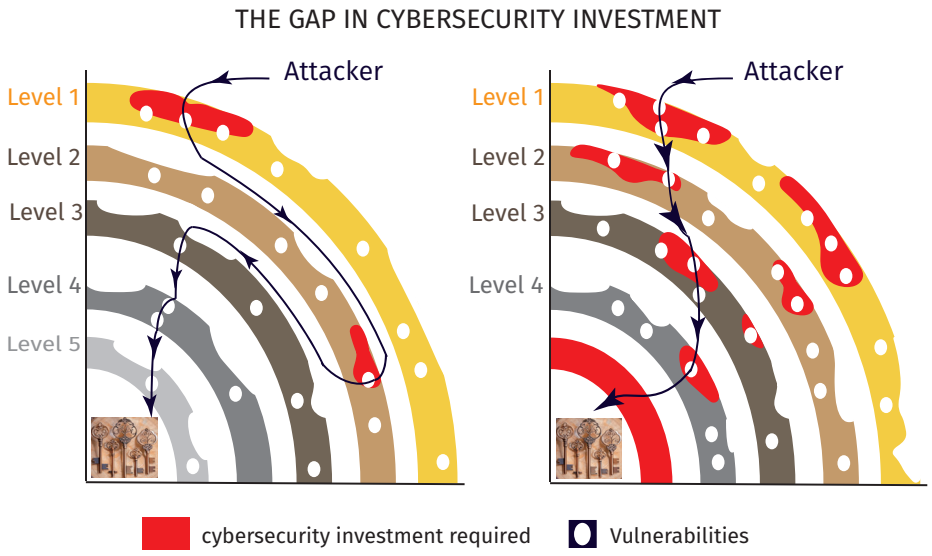
AVSS evaluates various information security indicators of an evaluated object, enabling users to intuitively understand the information security capabilities of the product. With objective evaluation and peer comparison, product security is no longer just an abstract concept but a core valuable attribute of any IoT products.

For product manufacturers, AVSS evaluation results can serve as a reference for product compliance, incorporating information security into the assessment elements of product quality. By comparing a product security with peers or previous versions of the same system, the quantified evaluations can reflect the input-output effectiveness of product information security design, promoting manufacturers to pay more attention to their information security characteristics of products during product development and market promotion processes.

For users, AVSS quantitative evaluation results are intuitive and easy to understand, instilling confidence in end users and encouraging them to choose more secure products.

3.2 Making Security a Key Support for Business Assurance

Information systems are the core support for organizational business operations, carrying various critical data and business processes. Stable and secure operation of information security systems provides basic assurance to the safety of business. With an accurate quantitative scoring approach, AVSS makes security investment visible and measurable, becoming a powerful support for business assurance.



Pic 2: AVSS Evaluation Provides a More Corresponding and Effective Recommendation for Organizations on Where and How to Invest Their Security Resources

Firstly, AVSS's scoring system provides organizations with a clear indicator of their system's information security level. Based on AVSS evaluations, organizations can well understand their security defense mechanism's

AVSS supports a better decision-making based on:

- *Security scorecard*
- *Targeted improvements*
- *Measurable Return on Investment*

performance across multiple dimensions for their information systems, allowing them to make targeted investments and improvements in security. This supports better decision-making on where should be improved and how to allocate resources for information security management, avoiding decision-making challenges caused by differences in information security awareness between security teams and business teams. Organizations can use AVSS evaluation results to formulate and adjust information security strategies, ensuring that information systems can support business operations stably and securely.

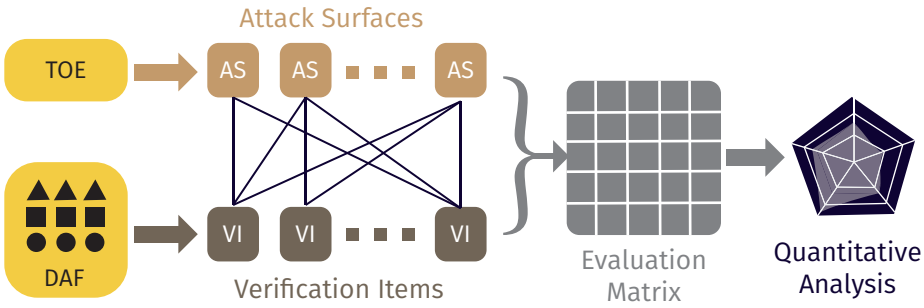
Moreover, AVSS quantitative evaluations make security investment measurable. Typically, information security investment is often difficult to quantify, but AVSS provides organizations with a quantitative and comparable evaluation system. Through horizontal and vertical comparisons of AVSS evaluation results of information systems, organizations can have a clearer understanding of the effectiveness and return on investment of information security investments. (*Pic 2: AVSS Evaluation Provides Clear Supports for Organization's Decision-Making on Directions and Size of Security Investment, Based on Gaps between its Current Systems and the Industry Leading Practices*)

AVSS

4. AVSS Methodology

4.1 Evaluation Framework

AVSS measures and evaluates the security defense level and effectiveness of an evaluated objects from the confrontation perspective of attack-and-defense. It replaces subjective evaluations with technical confrontations in real scenarios. Based on abundant vulnerabilities, exploit methods, and security attack techniques, AVSS conducts comprehensive, systematic, and in-depth adversarial assessments of evaluated objects, representing truthfully their security defense capabilities. (*Pic. 3*)



Pic 3: AVSS Evaluation Framework

4.2 Basic Concepts

Following are the key terms frequently used in AVSS:

Target of Evaluation (TOE)

A target of evaluation in AVSS, can be an information system, IoT, or its functional components, such as enterprise intranet systems, smartphones, connected vehicles, websites, and authentication modules etc. Similar types of evaluated objects can be classified into a TOE class, with each class having similar attack surfaces and security requirements. The establishment of TOE classes aims to better identify, evaluate, and compare evaluated objects, thus these classes are not static and can be adjusted by AVSS based on the evolving nature of the objects.

Attack Surface (AS)

An AS refers to any services, functions, or defense measures and mechanisms within a TOE that could be attacked. Unlike traditional external attack surfaces during an attack-and-defense testing, an AS in AVSS can be decomposed more deeply and finely based on the evaluation purpose. For instance, to verify defense mechanisms at a system level, the interface of that defense mechanism can be directly exposed to form an attack surface to be verified, rather than gradually attacking from peripheral applications.

Defense & Attack Framework (DAF)

DAF is a knowledge-base formed by DARKNAVY for various security vulnerabilities, exploitation methods, technical means, and defense mechanisms related to TOEs. It serves as an important technical support for conducting AVSS security evaluations. DARKNAVY maintains and releases an open DAF, however organizations implementing AVSS can also construct their own DAF according to their needs, product/system characteristics, industry features, and technical research.

Verification Items (VI)

A VI refers to security vulnerabilities and exploitation methods that may affect an AS. These items will be sorted out based on DAF library during AVSS processes by evaluators, or newly discovered during a verification of AS implementations.

Evaluation Matrix (EM)

An AS can be influenced by multiple VIs, and a VI can be applied to multiple AS. After enumerating AS and VI, a comprehensive EM is formed. The EM serves as a basis for evaluators to implement technical attack-and-defense verification and assess the effectiveness of the TOE's defense.

EQuantitative Evaluation (QE)

During technical verification of a TOE based on its EM, evaluators conduct quantitative evaluations according to various evaluation indicators, leading to comparable quantitative conclusions about the TOE's security level, as well as potential security vulnerabilities and improvement suggestions.

4.3 Evaluation Metrics

Once AVSS identifies corresponding attack surfaces and verification items for different evaluated objects, they are combined into an evaluation matrix, including a series of potential attack points and attack paths. AVSS evaluates different attack surfaces based on two sets of indicators: "Exploitation of Defects" and "Impact Consequences".

"Exploitation of Defects" reflects a difficulty level of exploiting defects when implementing verification items attack against a TOE, thus reflecting the defense capabilities of the TOE. "Impact Consequences" assesses all potential harms caused after implementing verification attacks against an attack surface. These results are scored based on different consequences.

AVSS scores security strength based on:

- *Exploiting weaknesses*
- *Impact of attacks*

Exploitation of Defects: This indicator reflects technical defects presenting in an attack surface of a TOE and the likelihood and cost of exploiting these defects. Evaluation is conducted comprehensively based on factors such as personnel capabilities, target information, lead time, and attack resources. Each indicator is divided into multiple levels, such as the capability required for exploiting defects ranging from no computer skills to highly specialized knowledge, and corresponding scores are provided. Higher requirements for personnel capability correspond to higher scores, enabling precise measurement of security.

AVSS calculates attack surface scores considering:

- *Severity of weaknesses*
- *Attack surface characteristics*
- *Attack chain position*
- *System usage*
- *Business logic*
- *Data sensitivity*

Impact Consequences: During verification attacks against an attack surface, TOEs protected by defense mechanisms may be affected, and evaluations are conducted based on multiple dimensions such as data confidentiality, integrity, and availability. Evaluation results also provide corresponding scores based on different consequences.

Attack Surface Evaluation: A TOE's attack surface forms a base for AVSS proceeding. Once implemented verification items attack against each attack surface, an evaluation score is created for that attack surface, integrating factors from both exploitation of defects and impact consequences to accurately reflect the effectiveness of the TOE's defense mechanism.

- Different verification items may have different scoring values, referring to evaluation indicators for exploiting defects.

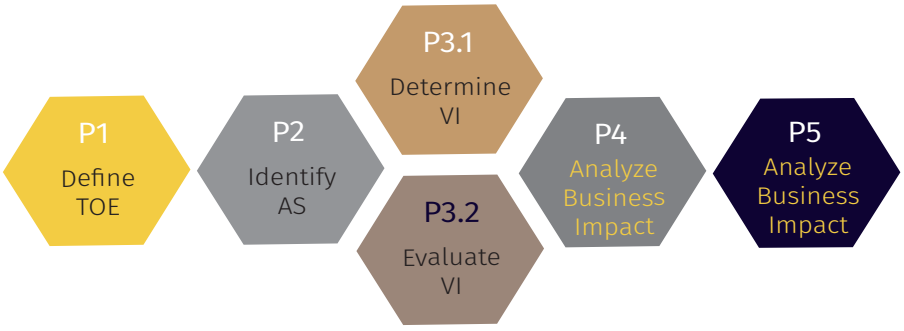
- The score for the same verification item may vary when applied to different attack surfaces, depending on characteristics of the attack surface and its defense mechanism attributes.

- Verification item scores not only consider individual attack surfaces but also consider their position in the attack chain. For example, from consequence of A attack only general information has been obtained, however a certain vulnerability exploit B requires specific information, which happens to be provided by the exploitation A, then the score for this A verification item will not be limited to its own defense ability.

Business Value Analysis: AVSS evaluation approach is based on attack-and-defense analysis, and provides a comprehensive quantitative evaluation of a security level and defense effectiveness of a TOE. However, purely technical evaluations may not fully and accurately reflect security risks of the TOE. The same TOE may have significant differences in potential impacts and consequences under various application scenarios, business logics, associated information and data, necessitating a business value analysis. This analysis combines evaluation results of attack surfaces in different application scenarios with their potential impacts and consequences to form evaluation conclusions in specific scenarios and business attributes.

4.3 Evaluation Metrics

AVSS evaluation framework is divided into five processes: Define TOE (P1), Identify AS (P2), Determine and Evaluate VI (P3), Analyze Business Impact (P4), and Generate Quantitative Report (P5). (*Pic.* 4)



Pic 4: AVSS Evaluation Processes

Define TOE (Target of Evaluation) (P1)

Due to the complexity of information systems, IoTs, or their subcomponents, it is necessary to have a preliminary understanding of TOEs before conducting attack-and-defense analysis, and to determine categories to which the TOEs belong.

AVSS has identified basic attack surface groups for a certain category of TOEs. Therefore, once a TOE is identified and categorized, it has laid a nice foundation for the next process of work.

If a TOE cannot be identified within any currently established category, a new category of TOEs is then needed during this process, and should be created based on the TOE characteristics. Once completing the next process of work, a basic attack surface group of this new TOE category will be formed.

Identify AS (Attack Surface) (P2)

This process builds upon the previous stage's work and ultimately forms a list of attack surfaces for evaluation.

If the TOE is identified and categorized, the work during this process involves assessing matches between the TOE's attack surfaces and the basic attack surface group of the corresponding category. Inapplicable attack surfaces are removed, and any attack surfaces specific to the TOE are added to a final list of attack surfaces.

If the TOE does not belong to any established category, the work during this process involves studying the TOE, identifying all attack surfaces, and analyzing these attack surfaces to construct a basic attack surface group for the newly created TOE category.

Determine and Evaluate VI (Verification Item) (P3)

In this process, verification items are formed based on DAF for different attack surfaces, thereby creating an evaluation matrix. Based on the evaluation matrix, adversarial security verification and technical analysis are conducted on the targeted attack surfaces, with analysis results serving as the main basis for security scoring.

Analyze Business Impact (P4)

During this process, the results of technical adversarial analysis from the evaluation implementation stage are analyzed in conjunction with the TOE's business application scenarios and related business requirements. The process and results of technical analysis are mapped to specific business scenarios to reanalyze and evaluate potential business risks.

Additionally, in this process, a business analysis and evaluation are conducted for resource investment, business support capabilities, and cybersecurity return on investment for information systems, IoTs, or their subcomponents, representing a comprehensive impact of the TOE security on business.

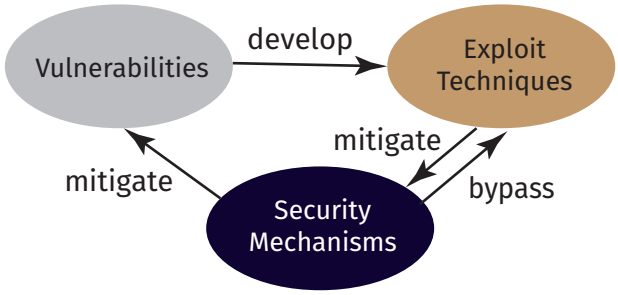
Generate Quantitative Report (P5)

In this stage, the processes and results of technical analysis and value analysis are presented quantitatively. This includes quantifying the overall security results of the TOE and, if necessary, separately quantifying statistics for specific business scenarios or technical components. The evaluation process, technical adversarial results, value analysis, and quantitative presentation constitute the AVSS evaluation report for the TOE, along with corresponding security improvement recommendations.

5. AVSS Implementation

5.1 DAF and its implementation

DAF (Defense & Attack Framework) serves as a technical backbone for AVSS evaluations, encompassing necessary technical elements for AVSS assessments. DAF includes a vulnerability library, exploitation techniques library, and defense mechanism library. (*Pic. 5*)



Pic 5: DAF components: vulnerability, exploitation, security mechanisms

5.1.1 DAF Vulnerability Library

DAF Vulnerability Library comprises a representative collection of vulnerabilities, representing potential vulnerabilities that may occur in a TOE. The library contains collections of vulnerabilities from various scenarios, serving as indicators for conducting AVSS evaluations on different types of systems.

DAF Vulnerability Library exhibits strong specificity to a targeted system, with significant variations in vulnerability sets for different targeted systems. For example, vulnerabilities related to an operating system kernel and browser frameworks in smart phones constitute different vulnerability collections, while vulnerability collections in IoTs differ substantially from those in information systems.

Taking memory corruption vulnerabilities as an example, a the defense capability against memory corruption vulnerabilities is an important component of system security capability. According to data released by MSRC at CppCon 2019, approximately 70% of CVE numbers from 2006 to 2018 correspond to memory corruption vulnerabilities, including common vulnerabilities such as stack overflow and UAF.

When evaluating the core of an operating system as an assessment target, DARKNAVY's existing DAF Vulnerability Library contains many types of vulnerabilities, covering various common vulnerability types found in real system cores, such as stack overflow, heap overflow, Use-After-Free vulnerabilities, and race conditions. These vulnerabilities are quantified in terms of their destructive impact. The DAF Vulnerability Library for the core of the system is then used for AVSS evaluations of the core defense mechanisms, reflecting the defense capabilities of different system cores against the DAF Vulnerability Library.

In contrast, within browsers, the DAF Vulnerability Library covers various common vulnerabilities, including type confusion and out-of-bounds read/write in the JS Engine (e.g., V8 or SpiderMonkey), heap overflow and Use-After-Free vulnerabilities within the rendering engine (e.g., blink and DOM), and Use-After-Free vulnerabilities in the browser process itself.

5.1.2 DAF Exploitation Technique Library

DAF Exploitation Technique Library goes beyond just attack surfaces. It provides a targeted arsenal of techniques attackers might use to exploit vulnerabilities in various security scenarios. These techniques are tailored to specific target systems and reflect real-world attack methods.

For example, when evaluating a browser, the library might include techniques like:

- Bypassing the sandbox, a security mechanism within the browser engine.
- Exploiting the allocator to obtain arbitrary heap allocation primitives, allowing attackers to gain control over memory allocation.
- Exploiting vulnerabilities by cross-thread allocation to compromise data between different parts of the browser.

This targeted approach ensures that AVSS evaluations are more realistic and effective.

5.1.3 DAF Defense Mechanism Library

DAF Defense Mechanism Library serves as a comprehensive catalog of security measures that can counter the attack techniques identified in the Exploitation Technique Library. It categorizes various defense mechanisms based on their effectiveness against different types of vulnerabilities and security scenarios.

This library is crucial for AVSS evaluations as it allows for:

- Identifying Suitable Defenses: Evaluators can assess which defense mechanisms are most effective against the specific vulnerabilities identified in the target system.

- Understanding Mitigation Capabilities: Each defense mechanism is evaluated based on its ability to mitigate different types of vulnerabilities. This helps assess the overall security posture of the system.

Let's take memory corruption vulnerabilities in operating systems as an example. The DAF Defense Mechanism Library includes Stack Cookie, Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), Pointer Authentication Code (PAC), Control Flow Integrity (CFI), and Memory Tagging Extension (MTE) etc. The effectiveness of these defenses varies depending on the specific type of memory corruption vulnerability. However, with sound implementation practices, their combined presence significantly strengthens the overall security of the operating system.

5.2 Best Practices for AVSS Implementation

The concept of in-depth defense has long been widely used in modern information security design, with different levels and types of security defense mechanisms deployed within systems. The core idea of AVSS evaluation is to represent the effectiveness of defense mechanisms by assessing any exploitability of security vulnerabilities, thereby accurately evaluating the overall security of a system.

With sufficient settings, AVSS evaluations require placing certain vulnerability collections from a DAF Vulnerability Library within the attack surface of a targeted system or device. Technical personnel then conduct adversarial assessments based on the correlative DAF Exploitation Technique Library as validation items to assess the exploitability of vulnerabilities of different types and qualities. By quantitatively analyzing the security threats posed by security vulnerabilities in the targeted system, and the defense capabilities of each defense mechanism against the vulnerabilities, evaluate the overall security capability level of the targeted system.

AVSS DAF includes evaluation vulnerability collections for different attack surfaces. By conducting adversarial assessments on the security capabilities of defense mechanisms included in each layer of attack surfaces, a comprehensive evaluation of the in-depth defense protocol can be performed.

5.3 Agile Practices in AVSS

If a technical environment does not support the pre-placement of security vulnerabilities in a TOE and its various levels, entry points for adversarial assessment will be limited, and it may not be possible to complete the best operational practices. However, this doesn't mean the system can't be evaluated. AVSS offers agile practices for such scenarios.

AVSS Agile Practice:

evaluating security without pre-placed vulnerabilities

Agile practices involve analyzing and identifying the attack surfaces of a TOE and conducting evaluations using validation items from a DAF Exploitation Techniques Library. Based on methods such as vulnerability discovery, attack surface management, and penetration testing, the level of threat posed to the TOE by these validation items is assessed. The evaluation process using attack evaluation methods available in a DAF Exploitation Techniques Library quantitatively evaluates the TOE's security defense capabilities.

At the same time, vulnerabilities discovered during this process are treated as a subset of the DAF Vulnerability Library, and their exploitability is assessed through adversarial judgment to verify the TOE's security defense capabilities. The value of defense mechanisms and defense capabilities against attack surfaces is reflected through the effective mitigation of vulnerabilities. Simultaneously, the technical team endeavors to bypass defense mechanisms to delve deeper into the layers of attack surfaces and defense mechanisms.

6. Open Framework

AVSS Open Framework emphasizes the importance of:

- *Continuously improving DAF*
- *Industry-specific standards*
- *Evolving methodology*

AVSS is designed as an open framework, fostering collaboration among various stakeholders in the security community. This collaborative approach ensures systematic and accurate security assessments for TOEs. Therefore, continuing enrichment and improvement of DAF, evaluation standards for different industry domains, and iterative updates of methodologies are necessary prerequisites. Optimizing and updating AVSS relies on collective participations from cybersecurity community, research institutions, academia, and industry vendors.

The openness of AVSS is mainly reflected in the following aspects:

- AVSS Usage: Professional third-party security evaluation organizations can leverage AVSS as an evaluation method to provide security evaluation services for customers; product vendors and organizations can use AVSS for self-assessment of their products, information systems, etc. Undeniably, accuracy and effectiveness of the evaluation results heavily depend on cybersecurity technical capabilities, experiences, and richness and

Cyberspace, like our real world, isn't perfect. We encourage more cybersecurity enthusiasts to discover bugs in the cyberspace, motivates more youth to find future vulnerabilities and responsibly disclose them.

updating speed of DAF content used by an organization implementing AVSS evaluations.

- DAF Contribution: DAF is a technical foundation for ensuring a smooth implementation of AVSS evaluations, containing key attack-and-defense technical elements for security. AVSS supports and encourages individuals and organizations in cybersecurity practices (security researchers, communities, research institutions, and product vendors etc.) to support expansion, improvement, and timely update of DAF. This includes but is not limited to vulnerability information, exploit methods, defense measures, and attack techniques etc.
- AVSS Promotion: AVSS supports all security evaluation activities conducted using the AVSS approach, and encourages evaluators to promote AVSS applications broadly.

Benefits of AVSS Openness

The open nature of AVSS offers several advantages:

- Widespread Adoption: Security evaluation organizations, product vendors, and organizations can all leverage AVSS for their security assessments.
- Improved Evaluations: The richness and update speed of the DAF content directly impacts the accuracy and effectiveness of AVSS evaluations. By encouraging contributions, AVSS ensures a comprehensive and up-to-date knowledge base.

- Community-Driven Enhancement: Security researchers, institutions, and vendors can all contribute to expanding and improving the DAF, leading to a more robust framework.

- Transparency and Trust: AVSS promotes the sharing of best practices and fosters collaboration within the security community.

Maintaining AVSS

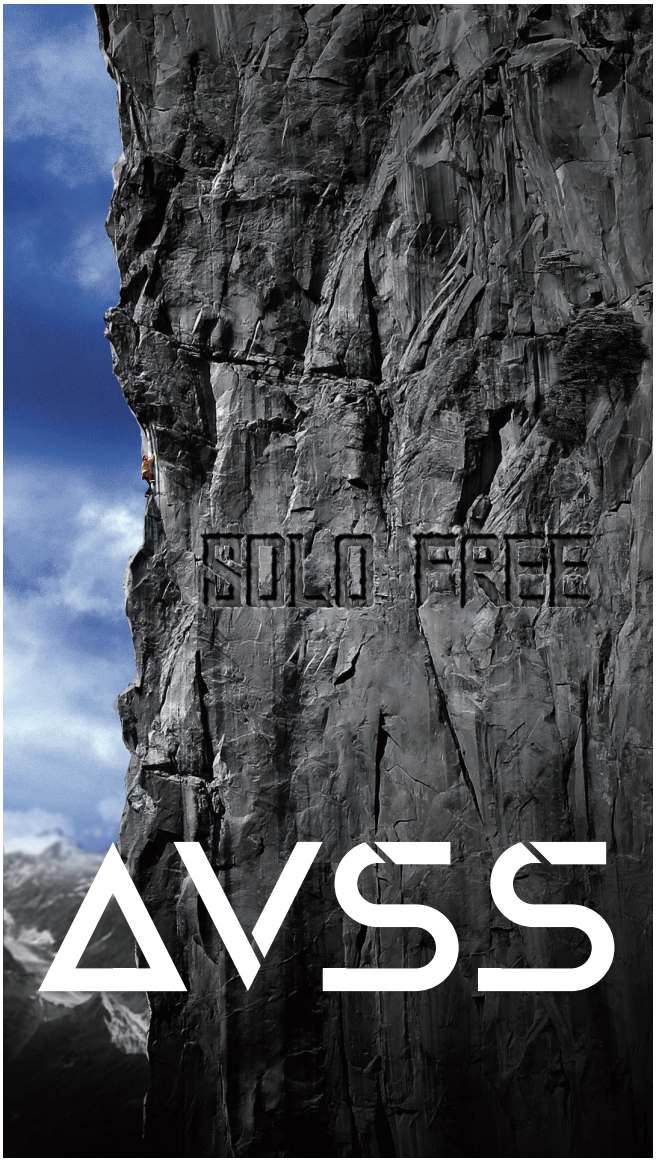
DARKNAVY, the creator of AVSS, takes responsibility for its ongoing maintenance:

- Methodological Updates: the AVSS methodology will be continuously updated to reflect evolving security landscapes.

- Industry Guidance: evaluation indicators will be developed specifically for different industries, ensuring more appropriate assessments.

- Open DAF Management: DAF will be managed and published through the official website (*www.avss.sg*), promoting transparency and accessibility.

White Paper for AVSS v1.0



7. Application Cases

Case Studies: Deep Dive into AVSS Applications

AVSS has been successfully applied in various fields, including financial payments and IoT products, demonstrating its effectiveness in real-world scenarios. Here's a closer look at how AVSS helps enhance security:

Financial Payments: AVSS evaluates the security of payment systems, identifies potential vulnerabilities and recommends improvements. This ensures a more secure environment for financial transactions.

IoT Products: AVSS evaluations play a crucial role in verifying the security of connected devices. This helps manufacturers identify and address security gaps, leading to more reliable and secure IoT products.

The following case studies showcase the practical application of AVSS in evaluating the security of various systems.

7.1 Case Study 1: AVSS Evaluation of Smartphones

Target:

This case study evaluates the security of fingerprint and facial recognition technology on a smartphone.

Evaluation Processes:

- Identified Target: Specific smartphone model and its biometric authentication technology were identified.
- Modeled Threat: A threat model was built based on the smartphone's operating environment.
- Analyzed Attack Surface: Key attack surfaces were determined, including data collection, processing, storage, permission control, and authentication effectiveness.
- Utilized DAF: Relevant test cases and attack methods were retrieved from the DAF for evaluation.
- Tested Adversary: Simulated attacks were conducted to assess the effectiveness of the smartphone's defense mechanisms against identified vulnerabilities.
- Assessed Risk: Security risks for high-value data (e.g., fingerprints) were evaluated from a business perspective.
- Reported Scorecard: Quantitative scores from the evaluation were presented on reports to provide insights into the security posture of the smartphone compared to industry standards.

Outputs:

- Quantitative evaluation of the smartphone's security mechanisms for biometric authentication.
- Identification of potential vulnerabilities, including previously unknown 0-day vulnerabilities.
-
- Comparison with industry best practices to identify improvement areas.

7.2 Case Study 2: AVSS Evaluation of a Financial Payment System

Target:

This case study evaluates the security of a cross-border payment system used by banks and merchants in multiple countries.

Evaluation Processes:

- Identified Attack Surfaces: Evaluation personnel identified different attack surfaces faced by the business system, based on information system security research;
- Tested Vulnerabilities: Security researchers attempted to obtain defects or gathered information using attack surfaces;
- Conducted Simulated Attacks: Verified the business system from multiple attack surfaces via the Internet, suggesting that a fairly strong security was in place, and various typical network attack methods failed to breach the business system's control;
- Verified Security: Evaluation personnel verified that security risks still existed in the office business system by leveraging various vulnerability combinations within the office network;
- Assessed Results and Made Recommendations: Evaluator conducted comprehensive evaluations of the TOE based on the then-current settings of the business and provided suggestions for improvement in the next phase.

Outputs:

- Identification of vulnerabilities and potential attack paths within the payment system.
- Recommendations for system upgrades and security improvements.
- Improved security posture to prevent financial losses and protect sensitive data.

7.3 Case Study 3: AVSS Evaluation of IoT Products

Target:

This case study evaluates the security of a remotely controlled IoT device used in unmanned scenarios.

Evaluation Processes:

- Evaluated Scope: The evaluation focused on device operations, cloud communication channels, and image transmission security.
- Analyzed Attack Surface: Potential attack surfaces were identified, including cloud vulnerabilities, device system vulnerabilities, and service vulnerabilities.
- Utilized DAF: Relevant verification items and test cases were chosen from the DAF for evaluation.
- Tested Security: Identified vulnerabilities were exploited through simulations to assess the device's defense mechanisms.
- Analyzed Business Impact: Security risks were evaluated based on real-world usage scenarios.
- Developed Security Indicator: Security design principles and test indicators were established for future product iterations.

Outputs:

- Identification of potential attack surfaces and vulnerabilities in the IoT device.
- Evaluation of the device's resistance against various attacks.
- Development of security guidelines to improve future product models.

Conclusion: These case studies illustrate the versatility of AVSS in evaluating the security of diverse systems. By combining simulated attacks with a comprehensive vulnerability library, AVSS provides a robust framework for assessing and enhancing the security posture of various products and systems.

With the rapid development of digital technologies, the world has entered into the digital age, bringing unprecedented digital experience to people. Data has become one of the most important and valuable assets. At the same time, information security also faces many challenges such as complex systems, big data, artificial intelligence, and mobile computing etc., which puts forward higher requirements for information security. We believe that the proposal of AVSS can provide a new thinking direction for the value evaluation and technology development of information security. We also believe that AVSS will help businesses to make their information security a competitive advantage!

To this end, we have joined forces with our partners to officially release AVSS version 1.0.

Initiator: *Daniel Wang,* *Founder and CEO of DARKNAVY*

Joint Promulgators:

Philip Yeo, *Former Special Advisor of Technology and Economy, Prime Minister's Office, Singapore; Former Chairman of the Agency for Science, Technology & Research, Singapore; and Former Chairman of the Economic Development Board Singapore*

Chee Yeow Meng, *Co-founder of the Singapore Computer Emergency Response Team (SingCERT); Professor of National University of Singapore; Fellow and Council Member of the Institute of Combinatorics and its Applications; and Senior Member of IEEE*

Yuejin Du, *Former Vice President of Technology and Chief Security Expert of Alibaba Group; and Form Vice Chairman of APCERT (Asia Pacific Computer Emergency Response Organization)*

Xiaosheng Tan, *Founder and CEO of Beijing Genius Cyber Tech Co. Ltd.; and Former CTO of Yahoo, China*

Tao Wei, *Vice President and Chief Technology Security Officer of the Ant Group; and Visiting Professor of Beijing University*

Yang Liu, *Professor of Nanyang Technological University, Singapore; PhD of the National University of Singapore; and Specialist for software verification, security and software engineering*

Tielei Wang, *Renowned vulnerability researcher; and the No.1 Chinese researcher in iOS Jailbreak*

Kang Li, *CSO of CertiK; and tenured professor at the Computer Science Department, University of Georgia*

Yu Wang, *Founder and CEO of Hangzhou Cyberserval Co. Ltd; and the record holder for the most solo presentations at the Black Hat Conference*

Liang Chen, *Director of Huawei Singularity Security Lab; and multiple-time champion winner of world hacking contests*

Qidan He, *Senior Security Director and Chief Security Researcher of NASDAQ:JD; Head of Dawn Security Lab; and Winner of "Master of PWN" & Ownie Awards*

Xuebin Chen, *Independent Researcher*

May 25, 2024 @ Singapore

White Paper for AVSS v1.0

May 25, 2024 @ Singapore

www.avss.sg

contact@avss.sg