Using Classified Intelligence to Defend Unclassified Networks

B. Michael Thomas, Neal L. Ziring
National Security Agency
bmthoma@nsa.gov, nlzirin@nsa.gov

Abstract
Intelligence services have access to unique information about adversarial cyber-exploitation and -attack capabilities. Nations such as the United States should be employing this unique but sensitive information in the defense of national security, government, critical infrastructure, and other networks, but doing so may expose the sources and methods behind the intelligence. Once exposed, access to that unique information may be lost. This paper describes the dilemma, presents a partial taxonomy of use cases for which solutions are needed, and offers avenues for supplying those solutions. In particular, solutions to the problem of using classified intelligence for defense of unclassified networks fall into three approaches. Properties and examples for each approach are presented and assessed.

1. Introduction
Cyber-threat actors and cyber defenders engage in a continual competition, both improving their technologies, tools, and tradecraft in response to the other’s successes. In the competition, the attacker has great freedom of action and enjoys a significant advantages when the defender lacks insight into their plans and intentions [13][14][29].

Intelligence services use specialized, and often clandestine, sources and methods to gather information about their targets. In the cyber realm, intelligence targets may include a variety of cyber threat actors (usually foreign nations or trans-national groups), and the intelligence gained may include critical details about a threat actor’s software, command-and-control, and other assets. The intelligence services of the United States and other nations face a dilemma: intelligence-derived information, if used properly, can help shift the advantage back to the defender, but it is also highly sensitive and correspondingly classified. To employ the information in network defense exposes it to leakage or theft, particularly by cyber threat actors. Once such information is compromised, it loses its unique defensive value because actors can modify their plans or adjust their tradecraft. More importantly, compromise of defensive information based on intelligence can also compromise the sources and methods used to get it, eliminating future intelligence.

Therefore, national security communities need mechanisms that will allow effective use of sensitive intelligence information for defense of a broad range of networks, but which can also protect that information from unauthorized access, leakage, and theft.

1.1. Scope
The discussion and solution approaches in this paper are focused on intelligence information useful for directly detecting actions against a defended network or system. This includes the kinds of artifacts that network defenders derive today from forensic analysis of successful attacks, such as file and network signatures, communication addresses, and credentials. Higher-level intelligence, such as threat-actor goals and intentions, can also be very useful for defensive strategy, but are outside the scope of this paper.

1.2. General properties of solutions
Solutions for using classified intelligence information in defense should exhibit three main properties.

1. **Defensive Effectiveness**: the solution should meet the same criteria for accuracy, timeliness, and flexibility that apply to conventional defensive techniques. For intrusion detection, such criteria are well understood [1][26].

2. **Confidentiality**: the solution must protect the content of the intelligence information, and even its very existence, from unauthorized parties.

3. **Operational Relevance**: the solution must be usable in one or more operational use cases (see ‘Use Cases’ section below).

Defense is more than detection. An authorized operator who receives detection events based on classified information might choose to take a response action or to configure a system to take action. In many cases, taking such an action will allow an external observer, or the attacker, to learn something about the intelligence information. For example, if the
intelligence included a malicious document that an attacker planned to send, then blocking it could reveal to the attacker that the defender had advance warning about that document. The authorized defender must choose a response based on risk management and cost/benefit analysis. But a critical aspect of the confidentiality property is that the solution must protect all that it can—prior to defender action, the attacker and other observers must not be able to gain any knowledge of the intelligence information. Even after a defensive response, the exact content must remain secret. Confidentiality about defensive information can provide a powerful advantage for the defender. Means for maintaining that advantage, even in very hostile conditions, are the focus of this paper.

2. Related Work

The dilemma identified in the ‘Introduction’ presents a specific case of a more general problem: using information for a task without revealing that information. This section provides an overview of some of the considerable research and development devoted to solutions for specific problems in this vein.

Private Information Retrieval (PIR) and privacy-preserving queries are active research areas. The usual problem involves extracting information from a database or stream of data, without revealing the query or extraction criteria. Many proposed solutions apply cryptographic techniques. Kushilevitz and Ostrovsky demonstrated computationally private database retrieval in 1997. Other early work on PIR was performed by Chor, Goldreich, Kushilevitz, and Sudan [6]. Boneh et al. applied partially homomorphic encryption (encrypted computation) to private database queries [4], and homomorphic techniques have also been applied for secure pattern matching [30]. Surveys of PIR work are available: a general survey in 2004 [10] and a more focused database PIR survey in 2007 [25].

Privacy-preserving cryptographic techniques have been applied directly to network defense research. A classic problem in that area is correlation of security events while preserving the privacy of individual events. Lincoln, Porras, and Shmatikov reported on a privacy-preserving system for sharing alerts [17]. Ma, Chen, and Li presented an approach for privacy-preserving alert correlation [18], and Li, Liang, Lu, Shen, Lin, and Zhu proposed applying privacy-preserving techniques to aggregation of critical infrastructure monitoring data [16]. Most recently, Niksefat et al. reported on a privacy-preserving intrusion detection system built on secure 2-party computation [23].

There has also been substantial research and development on computational platforms that can isolate or protect certain computations, ensuring integrity and/or confidentiality. Early work on this topic was performed in the 1970s, for example, on virtual machines for isolation [19]. NSA researchers reported on NetTop™, which used a commercial hypervisor to support execution of multiple classification levels of processing, mutually isolated, on a single host [22]. More recently, frameworks for isolating and protecting specific computations and processes within a host without using virtualization have been codified by industry consortia [12] and by particular companies [3][21].

Sometimes, the cryptographic and isolated computation approaches have been combined. For example, Wang and colleagues reported on implementing PIR on trusted hardware [28].

3. Use Cases

There are many situations in which sensitive or classified information may be applied in cyber defense. This section presents a partial taxonomy of such situations, which may be used to assess the suitability of a particular solution to a candidate application. To illustrate the taxonomy, several specific use cases, which have arisen in practice, are presented and categorized.

3.1 Application taxonomy

The following factors are important to describing and understanding the network defense use cases for the application of classified information in the defense of unclassified systems.

The use cases differ greatly depending on the existence of ‘connectivity’ between the classified systems where the classified information originates and the unclassified systems to be protected. Even when connected, the ‘bandwidth’ between these systems plays a major factor in the solution space. ‘High-bandwidth’ connections (that is, well connected) offer the most flexibility. ‘Low-bandwidth’ connections, such as those available to Forward Operating Bases (FOBs) in combat zones, are more challenging. The most challenging case is the defense of ‘disconnected’ unclassified systems that have no connectivity back to any classified systems.

To deal with the challenges of low-bandwidth connectivity, security assessments or incident responses can be conducted locally by deployed,
cleared security personnel or remotely, albeit slowly. In the case of disconnected systems, there is little choice but to deploy cleared security personnel to conduct a local assessment. In both cases, the cleared security personnel will have access to classified information during the security assessment or incident response. The use cases are summarized in Table 1.

<table>
<thead>
<tr>
<th></th>
<th>High-Bandwidth</th>
<th>Low-Bandwidth</th>
<th>Disconnected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local operations</td>
<td>Use Case 2</td>
<td>Use Case 4</td>
<td></td>
</tr>
<tr>
<td>Remote operations</td>
<td>Use Case 1</td>
<td>Use Case 3</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Use case summary

3.2. Use case 1: High-bandwidth remote monitoring

In this use case, connectivity exists from the classified systems to the unclassified systems to be protected via appropriate cryptographic and boundary protection mechanisms. The cleared security operators work on classified networks and have full access to classified adversarial indicators. They do not need to travel to field locations where the unclassified systems reside, and they can remotely manage the sensor suites that implement the detection capabilities. The core challenge is to enable the sensor suite to search for adversary indicators on classified or unclassified networks, using sensitive intelligence information, without exposing that information to compromise. Typically the on-site IT staff and network defenders do not have access to the remotely managed sensor suites. Figure 2 illustrates the structure of Use Case 1.

Figure 2. Use case 1: high-bandwidth remote monitoring

3.3. Use case 2: Low-bandwidth local assessment

In this use case, connectivity exists from the classified systems to the unclassified systems to be protected, but that connectivity is low-bandwidth. Defensive-operations personnel are deployed to the field location, and may have access to secure communications, but are limited to low-bandwidth. For example, they often have modest classified communications access, such as e-mail or web, via a classified network. There is usually no direct communication between classification levels other than the team members themselves or media which can be moved manually (for instance, CD-Rs). Figure 3 illustrates the low-bandwidth local assessment use case.

Figure 3. Use case 2: low-bandwidth local assessment

For example, NSA defensive operators are cleared and are trained and authorized to handle sensitive intelligence data. But they conduct a wide variety of operational assessments and incident responses. Every evaluation is different: the degree of access, convenience, timeliness, and bandwidth all vary. Some sites may have only unclassified or only secret and unclassified networks. When the operation involves deploying a team to a remote site, team members typically cannot carry sensitive intelligence information to the site, because most sites lack Sensitive Compartmented Information Facility (SCIF) facilities. The goal for the assessment team is to use its physical presence, and deep access to site assets, to search for adversary traces on networks, servers, and workstations at all classification levels.

3.4. Use case 3: Low-bandwidth remote monitoring

In this use case, connectivity exists, at low-bandwidth, from the classified systems to the unclassified systems to be protected. The security analysts work on classified networks and have full access to classified adversarial indicators. They do not need to reside at or deploy to the field locations where the unclassified systems reside. They are able to manage the sensor suites remotely. There are two core challenges. The first is shared with the use case 1, which is the challenge to enable the sensor suite to search for adversary indicators on classified or unclassified systems.
networks, using classified adversary information, without exposing that information to possible compromise. Secondly performance is greatly reduced due to the low-bandwidth, which makes even simple tasks, such as scanning a network and returning the results, difficult and slow. Typically the on-site IT staff and defenders have little, if any, access to the advanced detection capabilities. Figure 4 illustrates the structure of this use case.

Figure 4. Use case 3: Low-bandwidth remote monitoring

3.5. Use case 4: Disconnected incident response

In this use case, connectivity does not exist between the classified systems and the unclassified systems to be protected. Security personnel must be deployed to the field location to provide incident response services. There is no direct communication between classification levels other than the knowledge and experience of the team members. The team members have no secure communications and they cannot carry classified information to such sites, due to lack of a SCIF. The goal for the team members is to use their physical presence, and deep access to site assets, to search for adversary traces on networks, servers, and workstations at all classification levels (especially unclassified). Figure 5 illustrates the disconnected incident response use case.

Figure 5. Use case 4: disconnected incident response

4. Solution Approaches

This section describes three approaches for addressing the dilemma of using sensitive information in cyber defense, while meeting the general requirements discussed in the introductory section of the paper. The approaches may be characterized roughly on the primary mechanisms that protect the sensitive information: physical isolation, software (computation) isolation, and cryptographic isolation. Each approach has advantages and short-comings. An important consideration for solutions is whether the approach works well for network intrusion detection, host intrusion detection, or both.

4.1. Physical-isolation approach: secure appliances

A traditional means of protecting a secret is to lock it in a strong box. This means can be used to protect intelligence information while using it for defense, by building a defensive appliance as a discrete device (for example, a network sensor). In this model, the sensitive information stays in the box and is processed against network data. Such an appliance can operate in-line at the boundary between two networks, or via a passive tap that copies information from one or more network domains to the appliance [26]. Secure appliances must have the following properties:

- They must support access control and secure communications for secure use by authorized parties.
- They must accept input from the defended systems or networks, and use the intelligence information to detect malicious events or behaviors.
- They must notify authorized parties of detection in a timely and secure manner. They do not reveal the intelligence information or detection notifications to any unauthorized parties.
- They are highly resistant to physical tampering and other forms of close-access attack. All sensitive information should be erased if attempts at physical attack are detected [24].

Figure 6 shows how a secure appliance acts as an extension of the classified systems, operating attached to the local unclassified network. It is controlled and managed solely by cleared operators.
**Figure 6: Employing a secure appliance**

Most commercial network appliances, such as intrusion-detection systems, satisfy properties 1-4 to some degree. To be considered sufficiently secure to protect classified intelligence, the mechanisms used must meet relevant standards (e.g., for the US, [9]). Only a few commercial network devices are built with these properties. To illustrate this approach, two devices designed with all five properties in mind are described as examples below.

**Example 1: Cloud Shield CS-4000 trusted network security platform**
The CS-4000 is a commercial Deep Packet Inspection (DPI) network device. It incorporates features for protecting the signatures and detection methods loaded into it, protecting communication with authorized users, and resisting physical attacks [7]. It implements IPSec with Suite B-compliant cryptography for communication, giving cryptographic strength of function sufficient to protect classified information [9].

**Example 2: KG-175G trusted sensor**
The KG-175G is a commercial network sensor and network encryptor, built specifically to satisfy U.S. Government requirements for protection of classified information. It uses network packet signatures to detect particular activity on a network link, and protects the signatures inside its tamper-resistant chassis. The KG-175G implements the U.S. government standard HAIEP network-layer encryption protocol for protecting communication between the appliance and authorized users; its implementation of HAIEP is certified by NSA as sufficient for protecting classified information [11].

**Assessment of secure appliance approach**
Both examples share some features that help them support the use cases outlined in section 3. First, sensitive information is stored inside the appliance during operation, within the tamper-resistant boundary of the device. Second, the device must have long-term cryptographic credentials, which are stored internally, cannot be exported, and are erased if physical tampering is detected. Third, the device uses the credentials to establish secure communication with cleared, authorized operators (who must possess a credential that the device has been configured to trust). Fourth, notifications of activity detection, and management functions, occur only over the secure link.

The secure appliance approach can satisfy all three general properties for solutions to a substantial degree. Defensive effectiveness will depend on the features of the particular appliance, but as long as the defensive signatures and detection methods are downloaded into the appliance, then it should be able to perform the same operations as other network defense appliances. Confidentiality will depend on three factors: 1) assurance provided by the secure communications between the appliance and the cleared operators; 2) resistance to close-access attacks, including physical anti-tamper and integrity; and 3) software integrity and resistance to attacks from the defended network. Operation relevance can be judged by the breadth of operational use cases that the secure appliance can support. This combination of features allows the example secure appliances to support use case 1, well-connected monitoring, very effectively, and should also be usable for use cases 2 and 3. But secure appliances such as the examples above are not suitable for use case 4, disconnected-incident response, because they require real-time connectivity to a SCIF for reporting results.

Because the secure appliance is a separate device on the network, it is most suited to performing detection against network activity; applying this approach to detecting malicious activities on individual hosts would require sending all relevant activity from the hosts to the appliance. While this is possible, it does not match current practice for host-intrusion detection, and poses scaling issues for large collections of hosts.

### 4.2. Computation-isolation approach: secure execution environments

Another approach to supporting the use of sensitive intelligence is to perform detection computations within a trusted, isolated compute environment or ‘secure enclave’. The enclave must provide assurance of three critical properties: 1) sensitive information cannot leak out to, or be extracted by, unauthorized parties; 2) only authorized parties can configure, or add new sensitive information, to the enclave; and 3) the software used to perform the detection is the authorized, correct software, which can be confirmed by external authorized parties.
In general, a secure enclave acts as a trusted proxy that can act on behalf of cleared defenders, performing detection using the sensitive information, but isolating the information, computations, and results from any other processing or users on the platform. To support defensive-use cases, the secure environment must also have some means to support secure communication with the cleared defenders, to accept new detection settings, and deliver results. Figure 7 shows how the secure enclave would work.

**Figure 7: Employing computation isolation**

Many different mechanisms have been proposed and studied for creating trusted, isolated computation environments; the topic has a long history, for example, see Madnick and Donovan (1973) and later Meushaw and Simard (2000). Many modern processors are built with hardware virtualization or domain separation features which can isolate computation and data (for instance, ARM TrustZone [3]), which can then be leveraged to satisfy properties 1 and 2.

**Example: Intel Software Guard Extensions™**

Software Guard Extensions (SGX) allow an application to create a protected container—an enclave—which is a separate area in the application’s address space that provides confidentiality and integrity assurances [21]. SGX integrity and confidentiality guarantees are enforced by the processor, even against fully privileged software running on the same processor. Further, an SGX enclave has cryptographic keys that allow it to store data encrypted only for itself. Together, the execution and storage features allow an SGX enclave to satisfy property 1. Launching an enclave initiates a process of measurement which allows the enclave to attest to its integrity to a remote party and securely exchange information with that party [2]. These features allow an SGX enclave to satisfy properties 2 and 3.

**Assessment of computation isolation approach**

A secure-compute-environment implementation that satisfies the three properties above can support all four use cases. The sensitive data is accessible only to the software running in the enclave, but the enclave can accept data from its local host and/or network environment. Detection computations using the sensitive data proceed in isolation, and stored results are protected. For use cases 1 and 3, results are reported to the remote cleared operators. For use cases 2 and 4, results can be reported locally only to authorized users, or wrapped for later unwrapping back in a SCIF. For use case 4, in particular, sensitive information can be provisioned into the enclave before the incident response.

When used for network detection, the enclave simply acts like the secure appliance. For host detection, the enclave runs on the host, protecting the sensitive information but performing computation against local host conditions and behavior. Note that, in both cases, the local software environment can prevent the secure enclave from detecting behavior simply by corrupting the information passed to it, but it cannot extract the sensitive information or masquerade as the trusted computation to external authorized parties.

**4.3 Cryptographic-isolation approach: encrypted computation**

The cryptographic isolation approach protects sensitive information by provisioning it to the unclassified environment only in encrypted form, performing cryptographically masked computations, and returning an encrypted result to the classified environment. Inside the SCIF, the sensor-control system can decrypt the results and inform the cleared operators of any positive detection events. Unauthorized parties in the unclassified environment see only cipher text; if the cryptography is strong, then they can gain no knowledge about the sensitive information. Figure 8 shows a simplified overview of how the detection computations would work. This form of encrypted computation for intrusion detection is Private Information Retrieval (PIR) [6]; in particular it is single-database PIR (1dPIR), where the state of the unclassified environment, or network traffic passing through it, is the ‘database’ from which a result must be privately retrieved.

For example, a PIR scheme suitable for protecting sensitive information and operating as a sensor requires that a system in the unclassified environment be provisioned with a public key; the associated private key is held back in the SCIF. To deploy a particular set of sensitive information to the unclassified environment, the cleared operators use the private key to encrypt it, and send the encrypted block (the ‘query’) to the detector. For each set of local state data
(for instance, events, packets, file properties) in the unclassified environment, the detector computes an encrypted result from the dataset using the encrypted query and the public key, and returns the encrypted result to the SCIF, as shown in Figure 8.

There have been a number of cryptographic algorithms described in the literature that can support PIR in the way shown in Figure 8. They offer a variety of detection power and efficiency trade-offs in terms of computational overhead and the size of the encrypted query and result. (Note: most such systems are ‘partially homomorphic’, meaning that the encrypted computation can only include certain operations. A ‘fully homomorphic’ system can perform any computation; only a few such systems have been reported, and all impose high computational overhead which limits their capacity.)

Assessment of cryptographic-isolation approach
Because the private key must not leave the SCIF, the cryptographic-isolation approach is most suitable for use cases 1 and 3. Depending on the efficiency of the particular PIR scheme selected, application to use case 3 must be assessed to see whether available bandwidth will support necessary detection performance. For use case 4, a system could be provisioned with encrypted queries, and the encrypted responses could be decrypted when the system is returned to the SCIF. The cryptographic-isolation approach works for both host and network detection.

At present, the homomorphic encryption techniques used for encrypted computation impose substantial computational overhead. Even recent work specifically optimized for intrusion detection shows significant latency [23]. Further research and optimization will be required before cryptographic-isolation approaches will offer sufficient performance for general-purpose intrusion detection, but they may be adequate for specialized niche applications.

5. Implementation Experiences
Several prototypes and pilots have been developed to test the approaches described in Section 4. This section describes two, along with some of the lessons learned from them.

5.1. Network Detection Using Physical-isolation Approach
The authors’ organization is developing a defensive system for detecting and mitigating advanced persistent threats by leveraging a combination of commercially available and sensitive government threat information. Figure 9 shows the basic structure of the design, which employs two secure appliances to manage traffic and perform network detection.

Figure 8. Employing cryptographic isolation
Example: using single-database PIR
The single-database PIR scheme described by Chang [5], allows the sensor to store a database of $N$ strings, and the detection system in the SCIF to retrieve for any single string of index $n < N$, without revealing $n$ to the sensor. It uses the Paillier encryption system and supports efficient communication between a deployed sensor and the control system in the SCIF. By using a hash bucket scheme, this fundamental 1dPIR functionality can be turned into a private hash table lookup. For example, if the sensitive information being queried were the MD5 hash value of a file, the sensor system could group the MD5 values into a set of $N$ buckets using, perhaps, the 16 bit prefix of each value. Using the PIR scheme, the control system in the SCIF could retrieve the subset of MD5 values matching a given prefix and search that subset for the sensitive value, without revealing even the prefix to the sensor.
This design uses one secure appliance as the interface to the defended network; it copies traffic and forwards copies to various detection systems, while enforcing traffic flow policy. The second secure appliance hosts a detection application, which can accept threat information which includes a sensitive government portion. Both secure appliances maintain secure communication with the trusted sensor management infrastructure. In the current pilot, both secure appliances are CloudShield CS-4000 devices [7].

This design reveals one way to compose multiple secure appliances to support functions beyond the capacity of a single appliance. But the design does require that forwarding traffic between the components use dedicated links, because the forwarded traffic is not cryptographically secured.

5.2. Network Detection Using Computational-isolation Approach

The secure sensor prototype project, led by one of the authors, employed virtualization and integrity attestation mechanisms to create a computational isolation environment in which classified network signatures could be deployed. The intent of the prototype was to assess the strength and practicality of the mechanisms.

Figure 10 shows the basic structure of the sensor prototype; each element is running in its own virtual machine (VM).

![Figure 10. High-level structure of a secure sensor prototype using computational isolation](image)

Detection using sensitive signatures is performed in the detection VM, which is the only VM that can accept data from the defended network. Communication with the cleared operators in the SCIF is handled by the secure communication VM; it uses IPSec with Suite B-compliant cryptography [9]. The prototype uses the Xen virtualization framework [20]. Computational isolation assurance is provided by two mechanisms: the Xen hypervisor itself, and the Xen security modules (XSM) facility [8]. The hypervisor ensures memory and execution isolation; XSM enforces communication policy.

The integrity of software running in the individual VMs is essential to the computational isolation model. The prototype uses a Trusted Platform Module (TPM) [27] to perform measurement of the BIOS, the boot loader, hypervisor itself, and each VM during the boot process. The results of the measurement are used to unlock the key to the encrypted data; only if all components measure correctly can the data be decrypted successfully.

The secure sensor prototype revealed that it is very complex to combine multiple technologies to assure all three properties listed in Section 4.2. All three depend on the hypervisor isolation combined with data encryption. The encryption keys are protected by the integrity measurement process, which required integration of integrity measurement with key management. Binding of the keys to the entire chain of integrity measurement makes the system brittle; the slightest change to any component necessitates re-measuring and re-wrapping the keys.

6. Directions for Future Work

All three approaches offer practical means to perform detection for sensitive classified data in an unclassified environment, while protecting the sensitive data. But only the secure-appliance approach is currently realized in available implementations.

For the computational-isolation approach, a small number of potentially viable technology platforms are available. Initial research must focus on building a variety of host and network detection facilities on top of these platforms, and characterizing their security, functionality, and performance. The results can be used to improve the platforms, and to build commercial implementations for government defense pilot programs.

For the cryptographic-isolation approach, numerous PIR schemes have been published that can support various detection scenarios. More research is needed to characterize the computation and communication overhead of these schemes in realistic network defense scenarios. Next, developers need to integrate the PIR schemes into sensors and their control systems, to
make the cryptographic assurance they offer available for government and private sector operations.

7. Conclusions

Classified information can provide a unique benefit to defense of unclassified networks, but only if the confidentiality of that information (and the source and methods behind it) can be protected. Three basic approaches are being explored in the research and development community for supporting this. Table 2 summarizes those three basic approaches and their current maturity.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Security Foundations</th>
<th>Applicability</th>
<th>Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Appliance</td>
<td>Physical isolation, secure communication path</td>
<td>Use cases 1-3, Network, broad functionality</td>
<td>High – products available</td>
</tr>
<tr>
<td>Secure Execution Environment</td>
<td>Software isolation, secure communication path</td>
<td>Use cases 1-4, Network and host, broad functionality</td>
<td>Medium – technology available, products not yet available</td>
</tr>
<tr>
<td>Encrypted Computation</td>
<td>Cryptographic isolation</td>
<td>Use case 1-4, Network and host, limited functionality</td>
<td>Low – algorithms available but may not scale; toolkits not yet available</td>
</tr>
</tbody>
</table>

Table 2. Summary of solution approaches

At the moment, only the secure-appliance approach is ready for operational use, and the range of products specifically designed for protecting classified defensive information is modest. The computation-isolation approach shows great promise. It appears to be the most flexible of the three approaches, and relevant secure execution features are being offered on modern processors. However, no products or applications that employ this approach are yet available for defenders to deploy. The encrypted-computation approach has the potential to offer very high assurance of confidentiality because the classified information is never exposed unencrypted on the defended network. But limitations imposed by performance and functionality constraints make it the least flexible of the three.

By deploying secure appliances, it is possible today to use classified intelligence information for defense of unclassified networks, as long as suitable communications with cleared operators can be provided. It is not yet feasible to employ classified information for defensive operations on unclassified hosts. The computation-isolation and cryptographic-isolation approaches offer means to support hosts, but further development of products and applications is needed. In the case of encrypted computation, further research is on-going to improve performance and breadth of functionality.

As these technologies continue to develop, national intelligence and cyber-defense communities must create the policies and practices to take advantage of them. This will give these nations a powerful ability to apply their significant intelligence capabilities to defending critical networks, while managing the risks such application could pose to those capabilities.

8. Acknowledgments

An earlier, shorter version of this paper appeared in The Journal of Information Warfare (http://www.jiw.org). The authors wish to thank the Journal editors for their guidance and advice.

9. References


