Modular Over-the-Wire Configurable Security for Long-Lived Critical Infrastructure Monitoring Systems

Erik Solum
School of EECS
Washington State University
Pullman, USA
erik.solum@gmail.com

Carl Hauser
School of EECS
Washington State University
Pullman, USA
chauser@wsu.edu

Dave Bakken
School of EECS
Washington State University
Pullman, USA
bakken@eecs.wsu.edu

Rasika Chakravarthy
School of EECS
Washington State University
Pullman, USA
rmchakra@wsu.edu

ABSTRACT

This paper presents a modular, software-based, over-the-wire configurable, end-to-end security architecture for critical infrastructure monitoring systems. The architecture provides mechanisms allowing it to evolve, during operation, over the long lifetimes typically encountered in these systems by allowing security modules to be securely added and replaced at runtime. Our security architecture addresses these systems' need for high-performance secure multi-cast with modules for confidentiality, integrity, authentication, and obfuscation. The variety of available modules provides tradeoffs between performance and security now and for the future. Experimental performance results for various existing modules, in the context of the architecture, are presented. To achieve long system lifetime a secure management system, using protocols based on symmetric-key cryptography, is described.

1. INTRODUCTION

Critical infrastructure monitoring systems often have highly distributed sensors that measure the state of the system and report their data to several control institutions. A challenge with securing this type of systems is that they have life expectancies of 25 years or more, yet no one can accurately predict the developments in the security field during that time, with respect to how much computational power will be available to attackers and possible breakthroughs in ways to crack specific algorithms. In such environments the security-related components must evolve along with cryptographic developments instead of being at their mercy. Two complicating factors are that the nodes in such systems are often widely distributed and unmanned, while the data that they produce are critical and their flow cannot be interrupted.

DEBS'09,July 6-9, Nashville, TN, USA.

The publish-subscribe paradigm (pub-sub) has been proposed as a solution meeting the functional requirements of critical infrastructure monitoring [12]. It allows loose coupling between producers and consumers of information. It implements a logical, asynchronous bus where events can be pushed in at any point by a publisher and retrieved by any number of subscribers at other points. This makes it ideal for situations where information production is distributed and more than one consumer is interested in each information item.

The widespread use of pub-sub systems in this field is held back by the lack of performance. Conventional, content-based publish-subscribe, in which data are dynamically routed based on the content of each event, cannot achieve the same level of performance as the currently used strictly hierarchical *Supervisory Control and Data Access* (SCADA) systems. This is especially evident when security is added to the equation. *Managed publish-subscribe* [11] uses static routes configured by a management plane, to achieve the performance that critical infrastructures require. However a security solution is also needed. We present a dynamic security architecture for managed publish-subscribe systems that addresses many of the data exchange and related communication needs currently evident in critical infrastructures such as the power grid. We introduce a *security management plane* to dynamically assign sets of interchangeable security modules in order to provide end-to-end confidentiality, integrity, obfuscation, authentication and filtering. The performance of our demonstration modules, described later in the paper, is good enough to allow the system in which it is implemented to meet latency requirements for data delivery.

The rest of the paper is organized as follows: section 2 explores both the managed pub-sub model and the threat model; section 3 presents our architecture; section 4 discusses the performance of our solution using proof-of-concept modules; Section 5 looks into related work and section 6 concludes the paper.

2. MODELS

In this section we define the system model for managed pub-sub systems and we describe a threat model, against which

our modular security system protects.

2.1 Managed Publish-Subscribe

Managed pub-sub could be considered a compromise between the conventional hierarchical SCADA systems and content-based pub-sub systems. The managed pub-sub model provides a flat, wide-area, asynchronous data bus where information can be inserted and extracted anywhere, but instead of routing the events dynamically based on their content, a hierarchical *management plane* is added that statically controls the routing based on publication identities. By leveraging static routing, managed pub-sub systems are able to provide the low-latencies needed for critical infrastructure monitoring and control, while at the same time providing the convenience of pub-sub systems. The management plane's hierarchy can reflect the geographical and business structure of the critical infrastructure being monitored. The hierarchy provides a place for the cooperating businesses that operate the infrastructure to express and enforce their own policies about resource use and information security.

GridStat[1] is an example of such a managed pub-sub system, as seen in Figure 1. The management hierarchy is made up of quality-of-service (QoS) brokers that operate and configure the data plane's *forwarding engines* so as to provide QoS guarantees such as maximum latency and delivery reliability. GridStat publications are created when a publisher informs the management plane of its intent to produce a periodic stream of update events at a certain rate. Similarly, subscriptions are created when a subscriber informs the management plane of its need to receive update events from a particular publication at a particular rate, latency, and reliability. The management plane configures data plane mechanisms such as multicast, rate filtering, resource control and redundant paths to meet subscriber requirements. Unlike in content-based pub-sub systems, forwarding decisions are made on the basis of the publication identity of each event and subscribers' requirements: access to event contents is not needed. Because of this, end-to-end security mechanisms are possible in managed pub-sub and there is no latency penalty associated with decrypting data at the forwarding engines. GridStat includes middleware components that provide the communication and management interfaces for publishing and subscribing applications.

2.2 Threat Model

The threat model is based upon Wang et al. [22] general security requirements for pub-sub systems. The threat model addressed here has a slightly narrower focus and concentrates on the following aspects of application security:

authentication: subscribers must be able to determine that the events they receive originated at the intended publisher

information integrity: subscribers must be able to check the integrity of received events

information confidentiality: events flowing from publishers to subscribers must be kept secret from the pub-sub infrastructure and from adversaries.

and on the following infrastructure security issues:

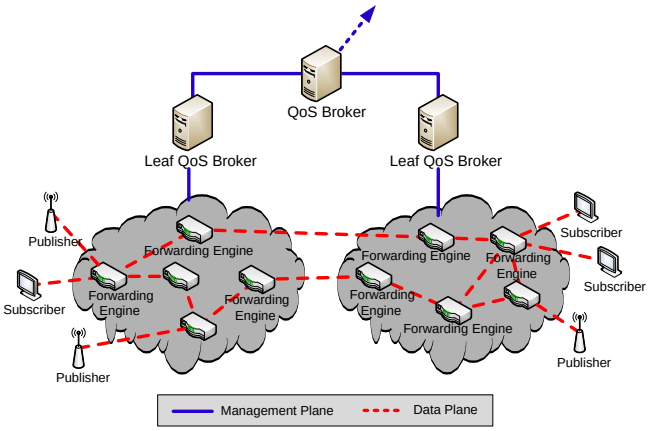

Figure 1: GridStat, a managed pub-sub system for power grid monitoring and control

publication confidentiality: publishers must be assured that only authorized subscribers gain access to publications

service integrity: protect against attackers mimicking infrastructure level components

availability: reduce the risk that malicious publications and subscriptions can be used to overload the system.

We address an adversary who will try to compromise these areas using access to the network traffic by observing, inserting, deleting, modifying, replaying, delaying or reordering both data plane and security management communication. In this work we do not address the problem of securing the system against attacks directed at nodes themselves. In order to survive over the long lifetime associated with wide-area critical infrastructure monitoring systems the architecture must be adaptable as developments in cryptography and processing power occur over a period of decades.

3. APPROACH

The security architecture uses a dynamic approach to addressing the security of managed pub-sub systems by reusing the QoS management idea and institutionalizing a security management infrastructure. The approach is applied to securing both the multicast streams of events from publishers to subscribers, i.e, the publications, and also to securing management communication links between data plane nodes and security management nodes.

3.1 Interchangeable Transparent Software Security Modules

The security architecture is built upon the idea of using transparent interchangeable software security modules to achieve the needed confidentiality, integrity, authentication and to a lesser degree availability. A security extension to the management plane, henceforth called the *security management plane* (SMP), generates keys and assign sets of modules from a module repository to publishers and subscribers, on a per-flow granularity according to dynamic policies as illustrated in Figure 2.

Assigning sets of modules and keys on a per-stream granularity enables the security system to address the different needs of each different multicast stream (publication). For some publications the need for confidentiality might be the strongest concern, requiring strong encryption modules; others might emphasize integrity and obfuscation; yet others might have strict real-time requirements so that weaker, but faster, security modules are needed. These requirements are specified in *publication policies* and corresponding *subscription policies*.

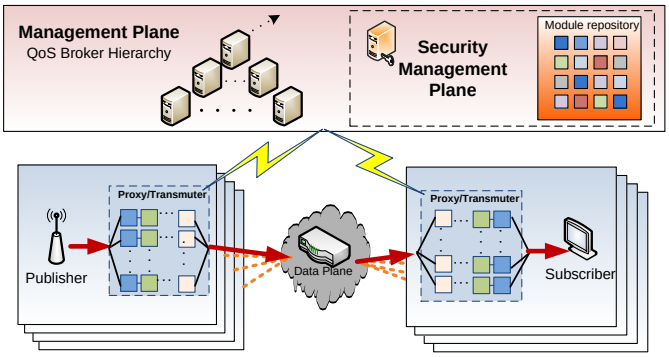

Figure 2: Interchangeable Transparent Modules for the Data Plane

Publishers and subscribers are assigned one publication or subscription policy for each of their respective publications and subscriptions. Based on these policies they download the security modules that they need from a security management server and instantiate them with the keys specified in the policy. Once the modules are installed they are transparently (to the publishing or subscribing application) applied to each of the publisher's or subscriber's event streams using a security management component incorporated in the management middleware for publishers and subscribers.

The SMP's repository of modules can be changed over time by adding new modules at runtime. These new modules can be assigned both to new and to existing publications through adjusting their policies stored in the management plane. All modules added to the module repository need to have two separate parts: a file containing the actual code which does the module's work and a *module policy* specifying the properties and behavior of the module. An optional third component, a *key generator*, is included if the module needs a special type of key generation not supported by the default key generator.

The strength of a modular approach is that new security modules can be implemented with varied functionality and performance attributes. By allowing modules to be combined in different ways the security architecture provides a toolset for easily making and enforcing tradeoffs between different security and performance properties at a small granularity. It also enables system administrators to respond to changes in the security field by introducing new modules to replace old ones whenever necessary.

3.1.1 Types of Modules

There are almost an infinite number of modules that could be implemented and deployed. We have created proof-of-concept implementations of five major kinds of modules, each of which has a clear and differentiated goal from the others:

encryption modules: Modules that encrypt information to achieve confidentiality

authentication modules: Modules that use digital signatures to let receivers of the information authenticate its origin

integrity modules: Error checking and error correcting modules whose goal is to assert the integrity of the information or correct integrity faults

obfuscation modules: Modules whose goal is to mask recognizable patterns in data that could be used to break the confidentiality achieved by the encryption module

filtering modules: Modules that try to reduce the risk of denial of service by filtering published events so that only events that are needed are pushed into the data plane.

By assigning stacks of modules from these groups to different publications, the security and performance aspects can be optimized to fit each of their needs. The proof-of-concept modules and performance experiments combining them according to various policies are described in Section 4.

3.2 Communication Security for the Security Management Plane

As described above, security for the data plane is achieved using module configurations and keys provided to data plane entities by the security management plane. The communications related to this provisioning also need to be secured with long-lived mechanisms that will support evolution of cryptographic techniques. Security management communication needs to be secured between data plane nodes and *Security Management Servers* (SMS) and between SMSs themselves. Unlike the data plane, the security management plane has no external choreographer of its communication security and has to rely on agreement protocols to coordinate key change and module change actions. The protocols described below exploit the hierarchical nature of the security management plane and the assumption that parents in the hierarchy will direct the security policies used in communicating with children. (For this purpose, the security management component of each forwarding engine is a child of some SMS.) Since we assume that new security modules will be required during the life of the system and these need to be distributed securely according to policy, we provide a way for children to acquire new modules from parents. Providing the necessary keys, however, is problematic. We consider approaches based on PKI techniques and symmetric pre-shared keys.

3.2.1 The PKI approach

PKI security is built upon public-key cryptographic algorithms and assumptions about the value of authentication

provided by a securely distributed root certificate. Secure distribution of root certificates typically involves out of band loading [24], so they cannot easily be updated once installed. Even root certificates with the recommended 4096-bit keys do not have eternal lifecycles and need to be updated. Microsoft recommends replacing a standalone root certificate every 20 years [3]. This is more than long enough for this to be a non-issue for conventional Internet use since users replace their browsers and operating systems long before they reach 20 years of age. The recommendation poses a significant problem, however, for systems where out-of-band updates are difficult and infrequent. Information systems for the power grid, for example, are highly distributed with large numbers of unmanned devices and a life expectancy well above the recommended root certificate life cycle. This further emphasizes the need for a security architecture that does not rely on system-wide keys that are only replaceable out-of-band. One might attempt to solve this problem by pre-loading multiple root certificates with different validity periods. That approach, however, does nothing to address the concern that the cryptographic algorithms used for the PKI are at risk of being broken over the long life of the system. Pre-loaded certificates could become obsolete before they were ever used. We have therefore adopted the following approach based on symmetric cryptography and pre-shared keys for securing the security management plane's communication.

3.2.2 The pre-loaded keys approach

When a new node is added to the managed publish-subscribe network it and its parent are provided with a large random pad and an initial encryption module, as shown in Figure 3. The random pad can be thought of as comprising $k = \frac{sizeOfPad}{sizeOfKey}$ keys. The pad contains many more bits than needed for any key. Unlike PKI-based approaches, many symmetric-key cryptographic algorithms make no special demands on the form of the keys used with them: the next sequence of bits from the random pad will do. As the system evolves and encryption modules are replaced the number of bits used for each key may change. The parent shares a *different random pad* with each of its children. (Thus a direct attack on a field node (child) does not result in compromise of its siblings' communications.) Having pre-loaded key material makes it possible to build a dynamic solution that can recover from compromised keys and modules.

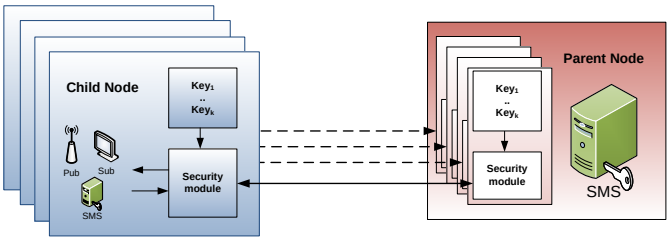

Figure 3: The pre-loading architecture

Pre-loading k keys makes it possible to switch keys $k-1$ times even if the current key is compromised. This is possible since there is no need to send any keys over the wire, hence no possibility for an attacker to gain access to the new key through sniffing. The only mischief an attacker can try is to provoke a situation that forces the child and parent node out of key-synchronization. That can either be attempted by initiating false key switches or attempting to interrupt valid ongoing switches. These possibilities are addressed by the re-keying and the key re-synchronization protocols.

Pre-loading a pad of keys out of band is an expensive operation and it should ideally be done only once during the lifetime of each node. Adopting the standard practice of generating session keys for protecting the communication not only preserves the pre-loaded keys for longer, but also increases the number of keys dynamically.

3.2.3 Security Management Communication Re-keying Protocol

Protocol 1 illustrates how a parent node initiates a key switch for the management communication link by sending a key-switch command together with a random number encoded with the current key. The child node decrypts the number with the current key, increments the number by one, and returns it together with a new random number encrypted with the next key in the key list. This concludes phase one. If it could be assumed that the child never would receive false key change commands from attackers masquerading as the parent trying to push the child out of key synchronization with the real parent, the protocol could finish here. But since this cannot be assumed, the parent node initiates phase two of the protocol which asserts that both sides completed the key change successfully by first checking that the child node correctly incremented the first random number. Then the parent decrypts, increments and re-encrypts the second random number and sends it back to the child. The child checks that the random number is incremented correctly, increments it a second time and sends it back to the parent. The child now assumes that the key switch is complete and moves permanently to the new key. The parent assumes the same when it receives the random number incremented for a second time.

Protocol 1 Key switch protocol using pre-loaded keys

1. **Parent:** $\{Switch\ to\ new\ key, \{RN_p\}_{K1}\}$
2. **Child:** $\{RN_p + 1, RN_c\}_{K2}$
3. **Parent:** $\{RN_c + 1\}_{K2}$
4. **Child:** $\{RN_c + 2\}_{K2}$

Forcing both parties in the key switch to prove their possession of the next key in the list makes it impossible for an attacker to successfully initiate key switches without possessing the *next* key in the list. Hence when the pre-loaded key set is safe, it is impossible to maliciously provoke a continuous change. It is also not possible to use a replay attack without knowing the *next* key in the list. If either of the random number checks fails, or if either the first message or its reply isn't received, both the child and the parent revert back to the old key after a short timeout.

To combat the chance that interruptions or loss of the last reply from the child to the parent causes the nodes to go out of key sync, the last message has to be treated differently

than the others. Since the child assumes the key switch was successful when it returns the second random number incremented by 2 without checking whether the parent node received it, the parent cannot follow the pattern of the other messages and reset back to the old key if it does not receive it. The parent now has to determine whether the child node has completed the key switch or not.

If the child did not receive the last message from the parent it will revert to the old key after a given timeout. During this timeout the parent will try to repeat the last message in an effort to successfully complete the key change. If the parent has not received any responses, or only invalid ones, when the timeout kicks in, nothing can be asserted about which key the child node uses, the old or the new. To resolve this question the parent initiates a series of *next-key-probes*, as illustrated in Protocol 2, with alternating base keys. First the parent sends a probe using the old key as base, if no reply is received, or the reply number is wrong, a new probe using the new key is sent. The parent will continue to do this until it gets a correct reply.

Protocol 2 Key re-synchronization protocol

1. **Parent:** $\{Key\ probe, \{RND\}_{K_{Index_p}}\}$
2. **Child:** $\{RND\}^{-1}_{K_{Index_c}}$; $\{RND+1\}_{K_{Index_c+1}}$
3. **Parent:** $\{RND+1\}^{-1}_{K_{Index_p+1}}$;
   Verify the decrypted value $RND+1$

Since the child has to use either the new key or the old key there can be only two reasons for the parent not receiving a correct response. Either there is a network failure, which means that when the network is fixed the probes will re-synchronize the keys, or a man-in-the-middle keeps intercepting the commands. In the case of the man-in-the-middle attack, the attacker needs to be able to continuously intercept all the commands between the child and the parent to keep such a denial of service attack up. As soon as the interception stops, the nodes will re-synchronize. Worth noting is that if the attacker has enough control over the network to accomplish such denial of service it can completely sever the communication between the two nodes without the need to attack specific protocols.

3.2.4 Security Management Communication Re-moduling Protocol

Key switches in themselves cannot handle the case where the current key is compromised as a result of the current module being compromisable. When a security module is compromisable the attacker can, by listening to the message-flow, extract the key used. This means that in general all messages that are sent using this encryption module, no matter the number of key switches, are insecure and open to man-in-the-middle attacks after some amount of time.

It is possible to extend the key switch protocol to also replace the current module even though it is compromised. Successfully replacing a compromised module with a new module necessitates the transfer of the new module from the parent to the child without any men-in-the-middle compromising the new module's integrity. To create a special case where the chance of such a successful man-in-the middle attack is below acceptable levels the following assumptions about what preconditions an attacker needs to satisfy to extract a new key from the currently used module have been exploited:

1. Assumption: A relatively large number of processing cycles, which takes time.
2. Assumption: A significant amount of data encrypted with a given key.

These assumptions are used as follows. First, by switching keys when sending a new encryption module the attacker is denied two things:

1. It cannot use any key it previously may have decoded from the communication stream.
2. It has to discard all previously collected data about the stream and start from the beginning.

Since the amount of data needed to transfer a new module is relatively small, the chance of the attacker getting enough data from that transfer alone to decode the new key is very low. Observe that for a man-in-the-middle attack to successfully compromise the integrity of a module transfer the attacker needs to be able to replace the real module with a fake module that it has encrypted with the currently active key. By switching to a new key just before sending the module the attacker's workload can be significantly increased by forcing it to extract the new key on very little data before being able to do the encryption. If the attacker gets enough information in that single message with the new module to extract the new key, it still needs some time to calculate it. By adding strict time limits on these transitions the attacker would need to accomplish all this without adding a significant level of latency. (Note that encryption of the module here is used to authenticate the module rather than to keep it secret – modules are presumed to be public knowledge.)

To further enhance the protocol, keys should be switched a second time after the new module is transferred. This ensures that when the security management communication link starts using the new module, it has a new key that has not been used with the old module. Assuming the new module is secure this makes it impossible for the attacker to use information gleaned from the use of the old module with the new module. Protocol 3 depicts the module switch protocol, messages `A, B` symbolize messages encrypted with the old key and module, message `C` is encrypted with the temporary key and old module, and messsages `D, E` and `F` are safely communicated using the new key and the new module.

The protocol in detail is: first the parent sends a replace module command encrypted with the old key and module. Both the parent and the child move to the next key in the list, which becomes a temporary key. Then the parent sends the new module and a random number, encrypted with the

Protocol 3 Module switch protocol using pre-loaded keys

1. **Message A - Parent:** $\{Replace\ module\}_{K1}$
2. **Message B - Child:** $\{Acknowledge\}_{K1}$
3. **Message C - Parent:** $\{\texttt{New Module}, RN_p\}_{K2}$
   Parent and Child change to new module
4. **Message D - Child:** $\{RN_p + 1, RN_c\}_{K3}$
5. **Message E - Parent:** $\{RN_c + 1\}_{K3}$
6. **Message F - Child:** $\{RN_c + 2\}_{K3}$

temporary key and the old module. When the child receives message `C` it decrypts the new module and random number, installs the new module, increments the random number, generates a new random number and then changes keys again to a new key. Finally the child replies to the parent with the two random numbers encrypted with the new module and the new key. Receiving message `D` the parent also moves from the temporary key to the next key and decrypts the message.

This module switch protocol is designed to make it extremely hard to perform a man in the middle attack and reduce the chance of a successful attack to acceptable levels. The key here is to enforce a tight time requirement on a response to message `C`. If the parent does not receive message `D` within a set time it red-flags the node and aborts the operation. To be able to do a successful man in the middle attack the attacker must be able to extract the temporary key from the single message `C` in a short enough time to encrypt its false module with this key and send it to the child without exceeding the time limit.

The third phase in the protocol is added to assert that the module switch was successful and avoid the problem of loss of the last confirming message, regardless of whether caused by an attacker or by mundane network problems, resulting in the child and parent going out of module and key synchronization. Loss of any intermediate messages can easily be solved by letting both parties reset to old keys and modules after a timeout, effectively re-synchronizing the parties. If the parent does not receive F, or the response is invalid, a similar approach to handling the loss of the last message in the key switch protocol illustrated in Protocol 2 can be employed to re-synchronize the child and parent.

As shown it is possible to replace a module $k/2$ times over the life of the child, if the child is preloaded with k keys. Even though this definitely imposes a finite limitation on the dynamic aspects of the security architecture, it can be argued that with the correct size of k this would not hamper the security significantly. The only reason for needing an infinite number of keys is that the keys and modules keep getting compromised indefinitely. For this to be true there has to be another weakness in the security system that no amount of key or module switches can remedy. Assuming a finite life expectancy there exists a k such that there are enough keys to switch modules as many times as needed during the deployment of the managed pub-sub infrastructure.

4. DATA PLANE PERFORMANCE

A security extension to the GridStat managed pub-sub system has been developed based on the security architecture described above. The extension includes an SMS implementation and security components incorporated in the publisher and subscriber middleware. In the resulting prototype systems we have measured the communication latencies in the data plane to evaluate the ability of the architecture to meet the latency requirements for power grid monitoring and control. Since communication in the security management plane occurs only for configuring and initializing data plane communication it does not have stringent latency requirements and we have not evaluated it.

Several proof-of-concept modules were developed, many based on Sun's *Java Cryptographic Extension* (JCE), see Table 1. JCE has a very limited interface that is not compatible with GridStat's event publication format. As a result the modules employ costly translation logic between the two formats that copies the data at least two times. This means that the numbers presented in Tables 1 and 2 have a lot of potential for improvement. The latency requirements for electric power substation automation, range from 4ms to 16ms internal to a substation and from 8ms to 10s external to a substation [1]. So, even with room for improvement the security architecture is able to provide security with low added latency.

By employing an end-to-end security approach the latency associated with each module is independent of the length of the paths that events travel so the added latency is presented without taking the path length into account in Table 1. Since the size of the event obviously affects the number of processor cycles each module needs to perform its task, an experiment is run for each of the modules with messages containing a single integer update and messages containing a 200-byte string update. The updates or events would, in a deployment of GridStat, represent readings from sensors. These readings are, as a norm, primitive types such as integers, longs and floats, or small collections of primitive types. However, larger, compound data values are sometimes needed and thus they are supported.

The data plane performance experiments were run on a simple GridStat topology having a single leaf-QoS Broker, one leaf-SMS, one status router, one publisher, one subscriber. A single publication was set up between the publisher and the subscriber. The whole setup was run on a single machine with a 2.4 GHz Intel E6600 dual-core processor and 2 gigabytes of RAM running Ubuntu Linux with kernel version 2.6.20-16. All GridStat components were compiled and run with java2SE 6 (version 1.6.0-02).

Of the encryption modules, `Blowfish` [20] performed best with `AES` [8] as a close second. The experiments show that both can apply a 128-bit encryption key on the stream of integers while adding below 17 microseconds of end-to-end latency and handle the 200-byte updates within 50 microseconds. `DES` [9] and `TripleDES` [7] on the other hand performed much poorer with the larger data samples. DES, with only 58-bit effective encryption, added an average of 65 microsec-

[1]Modules implemented based on Sun's JCE [23, 13]

Module	Publisher side latency		Subscriber side latency		End-to-end latency	
	Integer	200 bytes	Integer	200 bytes	Integer	200 bytes
Blowfish[1]	7,336	16,091	9,318	32,263	16,654	48,354
AES[1]	8,341	16,203	8,101	33,231	16442	49,434
DES[1]	8,059	22,945	9,561	42,486	17,620	65,431
TripleDES[1]	9,748	43,642	12,473	70,439	22,221	114,081
OneTimePadObf	8,303	34,314	7,489	28,314	15,792	47,959
AESObfusccation[1]	52,804	57,260	34,134	58,800	86,938	116,060
SimpleAuth	2,161	2,189	2,332	2,414	4,492	4,603
RSA[1]	$114*10^6$	$114*10^6$	933,402	944,225	$114*10^6$	$114*10^6$
Crc	2,589	16,789	2,654	17,075	5,243	33,863
MD5ErrorCheck[1]	5,197	7,721	4,815	6,804	10,002	14,525
SHAErrorCheck[1]	6,490	9,823	5,938	9,423	12,428	19,246
SHA512ErrorCheck[1]	11,051	17,698	12,481	19,028	23,532	36,726

Table 1: Proof-of-concept modules and the underlying module logic latencies in nanoseconds

onds latency on the 200-byte events and `TripleDES` used as much as 114 microseconds. Clearly the `AES` and `Blowfish` modules are the better choice for achieving confidentiality.

The two evaluated obfuscation modules follow two different approaches to obfuscation. The `AESObfuscation` module randomly generates a new key for each event and uses this key to encrypt the event with the AES algorithm, before the random key is appended to the event to allow the receiver to de-obfuscate. As the experiments show this carries a great performance cost. Since a new key is used for each published event, the module needs to re-initialize its encryption cipher for each event, and the performance is much worse than that of the `AES` encryption module that uses the same key each time. This corresponds to the findings of Opyrchal and Prakash [16]. The `OneTimePadObf` module, on the other hand, performs much better, especially with small events. It generates a one-time-pad of equal size to the event and applies it to the event with simple bitwise Caesar Ciphering. After the one-time-pad has been applied it is appended to the event in order to allow the subscribers to reverse the process. The integer experiment shows that data in an event can be completely obfuscated within only 16 microseconds and since the chance of repeating events are greater on smaller data samples one time pad obfuscation seems the more viable obfuscation alternative.

The experiments show that the authentication modules, `RSA` and `SimpleAuth`, based on the asymmetric RSA algorithm and the static signature scheme respectively, have hugely different performance impacts. The `RSA` module with a 2048-bit key adds as much as 113 milliseconds of latency which far exceeds the latency requirements for some power system applications, while the `SimpleAuth` module, because of its simplistic logic only adds 4.5 microseconds in the 200-byte event experiment. The `SimpleAuth` algorithm simply adds a set of secret identification bytes to each event in order to sign them. Though such an approach in itself would achieve little, since an attacker easily could replicate such a signature, the experiment based on it serves as a performance comparison measure.

The four integrity modules implemented and evaluated are error checking modules that use different hash algorithms to assert the integrity of received information. The `Crc` module uses a 16-bit *cyclic redundancy check* (CRC) optimized for small events, while the `MD5ErrorCheck` [19] module generates

#	Module set	Publisher side latency		Subscriber side latency		End-to-end latency	
		Integer	200 bytes	Integer	200 bytes	Integer	200 bytes
1	MD5ErrorCheck Blowfish	16,612	27,208	14,736	35,231	31,348	62,439
2	Blowfish MD5ErrorCheck	12,746	24,588	10,412	34,434	23,158	59,022
3	OneTimePadObf Blowfish MD5ErrorCheck	14,042	54,404	14,736	52,885	28,778	107,289
4	OneTimePadObf AES SHA	15,376	60,701	15,946	60,111	31,322	120,813
5	SimpleAuth OneTimePadObf Blowfish	13,393	46,717	11,392	39,115	24,785	85,833
6	AESObfuscation TripleDES SHA512	70,602	135,048	59,304	108,073	129,906	243,121
8	SimpleAuth OneTimePadObf Crc Blowfish	15,765	121,353	13,280	96,782	28,348	218,136
7	SimpleAuth OneTimePadObf Blowfish SHA	15,068	59,583	16,577	49,986	32,342	109,569

Table 2: Module set latencies in nanoseconds

a 128-bit hash, the `SHAErrorCheck` [10] uses 160-bit hash, the `SHA512ErrorCheck` module employs a 512-bit hash to achieve a varying degree of integrity checks. The varying length of the hash impacts the added end-to-end delay, but they scale well from the integer size experiments to the 200-byte event experiment and show that 200-byte events on average can be error checked with either a MD5 hash or a SHA hash within 20 micro seconds of added end-to-end latency.

To test how the performance was affected by stacking these modules, the experiments presented in Table 2 were undertaken. As the two first experiments show, the order in which modules are used affects the latency that they add. This is due to the different inflation of the data size, e.g. applying a hash module before applying an encryption module will require the encryption module to encrypt the hash and thus increase the latency.

Experiment 3 and 4 in Table 2 show that combinations of one-time-pad obfuscation, Blowfish/AES encryption and MD5/SHA integrity modules can be applied to a stream of integer events with an average added latency of below 32 microseconds (120 microseconds for the 200-byte event stream). Experiment 5, on the other hand, shows that if we are interested in group membership authentication instead of error checking then the added latency can be reduced to 85 microseconds for the 200-bytes stream.

To show a worst-case scenario experiment 6 combines the three slowest symmetric-key modules namely, `AESObfuscation`, `TripleDES` and the `SHA512-ErrorCheck`. As a result the added latency gets as high as 130 microseconds for integers and 243 microseconds for 200-bytes. This clearly is not an optimum combination of modules, but nevertheless provides results that are tolerable in a wide area setting.

Experiment 7 takes it one step further and shows that we

are able to provide authentication, obfuscation, encryption and integrity while adding only 32 microseconds of latency for the integer stream and 110 microseconds for the 200-bytes stream by combining the `SimpleAuth`, `OneTimePadObf`, `Blowfish` and `SHAErrorCheck` modules. This clearly shows, even with these non-optimized, proof-of-concept modules, that the modular approach is able to provide the security needed for the event streams while adhering to real-time industry standards in critical infrastructure such as the IEC 61850 4 millisecond inter-intelligent controller requirement [4]. Future optimization will only further reduce the added latency and enable even higher levels of encryption.

5. RELATED WORK

Publish-subscribe research tends to focus on performance, scalability and expressiveness [22] and the research on security related matters that is being done is mainly concentrated on *content-based* publish subscribe (CBPS)[14, 16, 17, 18]. In CBPS systems the subscribers register filter functions and events are routed based on evaluations of these functions applied to the, usually complexly structured, events. Since the brokers in a CBPS require full or partial knowledge of the content of the events to route correctly, the introduction of confidentiality poses challenging research questions in that setting. Most published approaches to these requirements have been variations on encrypting each attribute of an event with a different key, thus allowing brokers with different needs to decrypt just what is needed to route the event successfully [16]. Khurana [14] presents an extension to this approach that supports events that have an XML structure. Others employ end-to-end techniques such as only encrypting the values of events, while keeping the attribute types in clear text to route the information [18].

While most research on security in CBPS is not directly applicable to managed publish-subscribe, some of it can be useful such as Wang et al. [22] which does not present a security architecture, but explores the issues related to security in the publish-subscribe paradigm that can be used as part of the threat model. Pesonen et al. [17] present a security architecture for multi-domain CBPSs that acknowledges that providing confidentiality in multiple security domains warrants special considerations, such as what the intermediate brokers are allowed to know about the content of routed events and where the access control to the events should be placed.

A common trait of the security architectures published for CBPS is that they all employ PKI in some fashion. This introduces weaknesses that were explored in Section 3.2.1. Other security standards such as IPSEC, TLS and Kerberos which are candidate PCS security architectures were found to be unsuitable for GridStat. IPSEC currently expects the security modules to be available at compile time. Hence supporting dynamic change of modules is not possible with IPSEC, TLS and Kerberos. TLS does not have datagram support and DTLS which added datagram support to TLS does not support all algorithms as it does not maintain state. In addition, support of multicast and rate-filtering requirements is not supported by the security standards explored [5, 6, 15, 21]. The dynamic re-moduling techniques described in this paper may be adaptable for use with IPSec and TLS in long-lived systems, but this is a subject for further research. In particular, our re-moduling protocol relies on clearly distinguished, a priori, parent and child roles which do not exist, in general, between IPSec or TLS nodes.

6. CONCLUSIONS

This paper has presented a security architecture that, through the use of transparent interchangeable software modules, can provide confidentiality, integrity, obfuscation, authentication and filtering to managed pub-sub systems. This is accomplished, while adhering to critical infrastructures' low latency requirements, by taking advantage of managed pub-sub systems ability to support an end-to-end approach that is not available in CBPSs.

The architecture's support for secure re-keying and re-moduling of both data plane and management plane communication, without relying on root-certificates, provides service integrity without locking the system to a single set of security algorithms. The leaf-SMSs provide publication confidentiality by only allowing authenticated subscribers with the right credentials to access the needed modules and keys to read the event streams.

The scalability analysis and the experiments showed that the architecture can support large scales and still provide the necessary performance for encryption, obfuscation, and integrity while keeping all data access control local to each security domain. The experiments also showed that per-update authentication using RSA is too expensive for many power-grid applications. We are currently extending our techniques to support intechangeable authentication protocol modules for use during session establishment. This means that we will continue to support evolution of the authentication infrastructure over the long life of the system but will not suffer the high cost of RSA authentication on every update. This ongoing work includes validation, using so-called BAN authentication logic [2] and other formal techniques, to ensure correctness and security of the protocols.

It is not possible to predict the advances in technology and hence the types of attacks possible in future. However, having an architecture independent of specific modules and keys allows evolution of the system to adapt to new techniques and to resist even currently unknown attacks. We believe that this makes the use of the presented security architecture a ideal tool for providing managed pub-sub with the security it needs to be utilized in critical infrastructures.

7. ACKNOWLEDGEMENTS

This work was funded in part by the U.S. Department of Energy, Office of Electricity Delivery, via subcontract 49944 with Pacific Northwest National Laboratory, and by National Science Foundation Grant CNS 05-24695 (CT-CS: Trustworthy Cyber Infrastructure for the Power Grid(TCIP)).

8. REFERENCES

[1] D. E. Bakken, C. H. Hauser, H. Gjermundrød, and A. Bose. Towards more flexible and robust data delivery for monitoring and control of the electric power grid. Technical Report EECS-GS-009, Washington State University, May 2007.

[2] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

[3] "Microsoft TechNet. Certificate Life Cycle, URL: http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/dist

[4] F. Cleveland. IEC TC57 security standards for the power system's information-infrastructure beyond simple encryption. URL: http://xanthus-consulting.com/Publications/, June 2007.

[5] T. Dierks and C.Allen. The TLS protocol. RFC 2246, 1999. http://www.ietf.org/rfc/rfc2246.txt.

[6] N. Doraswamy and D. Harkins. *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Prentice Hall PTR, 2003.

[7] National Institute of Standards and Technology (NIST). Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. NIST Special Publication (NIST SP) 800-67, May 2004.

[8] National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES). Federal Information Processing Standards Publication (FIPS PUB) 197, Nov 2001.

[9] National Institute of Standards and Technology (NIST). Data Encryption Standard (DES). Federal Information Processing Standards Publication (FIPS PUB) 46-3, October 1999.

[10] National Institute of Standards and Technology (NIST). Secure Hash Signature Standard (SHS). Federal Information Processing Standards Publication (FIPS PUB) 180-2, August 2002.

[11] K. H. Gjermundrød. *Flexible QoS-Managed Status Dissemination Middleware Framwork for the Power Grid*. PhD thesis, Washington State University, August 2006.

[12] C. H. Hauser, D. E. Bakken, and A. Bose. A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid. *Power and Energy Magazine, IEEE*, 3(2):47–55, April 2005.

[13] Sun Microsystems. Java SE Security, Sun Developer Network URL: http://java.sun.com/javase/technologies/security Last checked 05.15.09.

[14] H. Khurana. Scalable security and accounting services for content-based publish/subscribe systems. In *SAC '05: Proceedings of the 2005 ACM symposium on Applied computing*, pages 801–807, New York, NY, USA, 2005. ACM.

[15] N. Modadugu and E. Rescorla. The design and implementation of datagram TLS. In *11th Annual Network and Distributed System Security Symposium*, San Diego, CA„ February 2004. http://crypto.stanford.edu/ nagendra/papers/dtls.pdf, Last checked 05.15.09.

[16] L. Opyrchal and A. Prakash. Secure distribution of events in content-based publish subscribe systems. In *SSYM'01: Proceedings of the 10th conference on USENIX Security Symposium*, pages 21–21, Berkeley, CA, USA, 2001. USENIX Association.

[17] L. I. W. Pesonen, D. M. Eyers, and J. Bacon. Encryption-enforced access control in dynamic multi-domain publish/subscribe networks. In *DEBS '07: Proceedings of the 2007 inaugural international conference on distributed event-based systems*, pages 104–115, New York, NY, USA, 2007. ACM Press.

[18] C. Raiciu and D. Rosenblum. Enabling confidentiality in content-based publish/subscribe infrastructures. In *Proc. Second IEEE Communications Society/CreateNet Int. Conf. on Security and Privacy in Communication Networks (SecureComm 2006)*, Aug.-Sep. 2006.

[19] R. Rivest. RFC 1321: The MD5 message-digest algorithm, April 1992. MIT Laboratory for Computer Science and RSA Data Security, Inc.

[20] B. Schneier. Description of a new variable-length key, 64-bit block cipher (blowfish). In *Fast Software Encryption, Cambridge Security Workshop Proceedings*, pages 191–204. Springer-Verlag, December 1993.

[21] J. G. Steiner, B. C. Neuman, and J. I. Schiller. Kerberos: An authentication service for open network systems. In *Winter 1988 Usenix Conference*, pages 191–202, Dallas, February 1988.

[22] C. Wang, A. Carzaniga, D. Evans, and A. Wolf. Security issues and requirements for internet-scale publish-subscribe systems. In *HICSS '02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 9*, page 303, Washington, DC, USA, 2002. IEEE Computer Society.

[23] J. Weiss. *Java Cryptography Extensions: Practical Guide for Programmers*. Morgan Kaufmann, 1 edition, 2004.

[24] ITU Telecommunication Standardization Sector (ITI-T). ITU-T RECOMMENDATION X.509, July 2005, URL: http://www.itu.int/rec/T-REC-X.509-200508-I/en.