Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Cryptography - Business Value Behind the Myth

There are many misconceptions about the role cryptography plays in the world of information security. The purpose of this paper is to help information technology professionals make informed decisions about using cryptographic solutions to secure electronic business transactions. The guidance contained in this paper is organized into three main areas of the cryptographic solution life cycle. These three areas can be described as solution discovery, solution integration and solution maintenance. The following provides a ...

Copyright SANS Institute
Author Retains Full Rights

AD

Cryptography – Business Value Behind the Myth

Jeff Christianson

August 25, 2003

Practical Assignment for SANS GSEC Certification

Assignment version 1.4b, Option 1

Administrivia version 2.6

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

There are many misconceptions about the role cryptography plays in the world of information security. The purpose of this paper is to help information technology professionals make informed decisions about using cryptographic solutions to secure electronic business transactions. The guidance contained in this paper is organized into three main areas of the cryptographic solution life cycle. These three areas can be described as solution discovery, solution integration and solution maintenance. The following provides a consistent approach to cost justify the use of cryptographic security solutions in business applications. Some basic understanding of encryption and cryptography is assumed.

Cryptographic Solution Discovery

In order to define what cryptographic solution discovery is, think about why anyone would want a cryptographic solution in the first place. Cryptographic solutions are defined as any technology that provides business applications with one or more of the four main cryptographic principles. These principles include data confidentiality, data integrity, client accountability, and client authentication. These four principles have been sold over that past few years as the means to a secure computing end. Thus, the discovery takes place when an IT professional is taking action to solve business partner security problems with the promise of cryptographic principles.

The first step an IT professional can take to make a business partner's transaction more secure is to understand that cryptography is only one part of security threat mitigation. Cryptography does not equal security. In fact, that is exactly the myth that must not be propagated. When many security professionals are asked the question "How can we protect this data?" they will provide the simple response "Encrypt it!" The problem is that these security professionals are ignoring the two most difficult parts of discovering the cryptographic solution. First, a solid business case should be documented based on the risk of existing threats and vulnerabilities. These threats and vulnerabilities could lead to negative business impact. Second, potential cryptographic solutions need to be compared with other non-cryptographic alternatives. This comparison will take into account the actual security value the solution provides in a production environment. Cost-benefit analysis over the solution's life cycle will determine the best security solution.

Business Case via Risk Assessment

Creating a valid business case for a cryptographic solution is not complex in theory. What can make the business case creation painful is the complex application environment to be analyzed.[1] In the end, all business cases come down to dollars and cents. Therefore, some intangible things like "risk" have to be defined in these monetary terms.

Risk assessment is not elementary but it becomes a surmountable task with assistance from tools that have been proven. The Information Security

[1] See Schneier, Bruce "Risk, Complexity, and Network Security"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Forum is one such organization that has produced risk assessment models.[2] Do not invent your own risk assessment methodology from scratch. At the very least take some input from professionals that are veterans in this space and adopt their ideas to fit your needs.[3]

A valid business case will include the documented risk assessment along with the direct business value a specific cryptographic solution provides. The risk assessment describes potential vulnerabilities in a business application and the likelihood that one of these vulnerabilities could result in a compromise. The risk assessment will also document possible negative impact to the business if a compromise does occur. True business value of a security solution is the amount of risk mitigation provided compared to the cost of solution implementation and maintenance. In other words, how well does the cryptographic solution protect the business from costs related to a compromise of confidentiality, integrity, accountability, or authentication? These questions can only be answered through direct conversation with the actual business partners.

Data Confidentiality

Confidentiality seems to be one of the most common benefits that cryptographic solutions provide via encryption. The need for cryptographic confidentiality usually stems from data classification and the risk of unauthorized access to certain classes of data.[4]

Data classification can be a complex task. Many organizations underestimate the resources and effort that go into data classification. The simplest case is the small business scenario where business ownership of data is usually well defined. Data classification is also much simpler if the number of data types is relatively few. Unfortunately, most large enterprise data classification tasks are a huge undertaking filled with political red tape.

First, it is necessary to define what classifications exist. The easy route is simply public versus private. All public data is unprotected and all private data is access controlled to a specific group of individuals. This bipolar classification scheme is over simplistic and almost never applicable. In the real world there are always more than two data classifications and they are organized to be gradually more restrictive in access. An example of graduated data classifications might start with private data as a grouping. Everything outside of private data would be publicly accessible. A subset of the private data may be considered proprietary. A subset of the proprietary data could be confidential. The confidential classification could be the most restrictive.

The next logical step is to classify every bit of data used by business applications. These data elements and their classification can be maintained in a catalog for easy reference. One of the road bumps that will slow down this process is the large number of data types that need classification. When databases reach into the terabytes of storage the number of elements can be overwhelming. An even bigger roadblock is determining which business partner actually owns the data. There may be many business applications that share the

[2] See "The Standard of Good Practice for Information Security"
[3] See "Information Security Risk Assessment Practices of Leading Organizations"
[4] See Parker, Donn B. "Fighting Computer Crime"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

data. Here is where the politics and red tape come into play. Suddenly, the area tagged with the job of classifying data realizes it will cost them 5,000 people hours. On top of that, the task was never planned for. This type of resource expense will most likely result in finger pointing and passing the buck.

Calculating the return on investment of data classification is not any easier than the data classification itself. One of the best ways to sell the data classification task to management is the concept of reuse. Multiple efforts will not waste valuable time re-classifying data if there is an enterprise standard. Think of how much time and money is saved by having a consistent answer to the classification of certain data types. Once an organization has a consistent way to classify their business data, they have a significant head start on answering the data confidentiality question. Risk assessment can happen much faster when there is an enterprise data classification to reference. Still, even when a solid data classification model is defined, risk assessments should not always conclude that cryptography is the best answer.

What security does the encryption really provide? Encryption provides access control based on key management. Are there other ways to provide a similar level of access control without the key management overhead? Perhaps the data exists on a platform that has native access control built into it. Perhaps the business partners that need access to the data already have authentication credentials on the platform and a simple access control list is the answer. The moral of the story here is do not get distracted by the latest hot security technology with cryptography written all over it. Do not overlook a simple, cost effective solution that has been available since the implementation of the original application. Always be on the lookout for the best security control. Do not be fooled by the used car encryption salesman.

Data Integrity

Integrity is a valuable cryptographic principle that is often overlooked because it is overshadowed by the marketing of encryption and confidentiality. Security professionals that truly understand cryptography realize that data integrity is just as important as data confidentiality. They also realize that encryption is not the security silver bullet because data integrity is lacking.

Integrity checks can even be used to monitor how well data confidentiality solutions are doing their job. Integrity checks augment data confidentiality solutions by alerting applications when business data has been tampered with due to a possible key compromise. This paper will not dive into the mathematical proofs related to hashing functions, randomness, and check sum collisions. Yet, what is important to know is that integrity checks are critical to prevent malicious modification of business partner data. Major negative business impacts from unauthorized data modification may be illustrated through risk assessment documentation. In this case, an integrity solution should be deployed as a part of the application security controls. This is another example of how important formal risk assessment is in discovering the correct cryptographic security control.

A security analyst cannot recommend and implement the correct risk mitigation controls until they understand the true business case that drives these

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

security requirements. Failure to correctly evaluate business requirements will most likely result in implementation of unnecessary security controls. Examples of this include implementation of encryption solutions even though data integrity is the business requirement or leveraging hashing functions when data confidentiality is needed. Cryptographic hashing functions are just as useful as cryptographic ciphering functions. The two different types of functions provide different security benefits and should be applied appropriately

Client Accountability

Accountability can be the most confusing of the principles. The confusion is due to the abuse or misunderstanding of trust. The concept of using cryptography to provide user or transactional accountability is nothing new. Business applications have been digitally signing documents and transactions for years now. The problem is that a digital signature without the proper supporting trust model is not worth the ones and zeros it consists of.

Defining a valid trust model will probably lead you into philosophical and legal debates with your coworkers and legal department. This is the underlying issue to successful deployment of a public key infrastructure. The mathematical details of asymmetric cryptography will not be explored in this paper but suffice to say that public key cryptography is the heart of cryptographic accountability. There is a lot more to a public key infrastructure than the million dollars worth of technology. There is another million in paperwork. Significant effort goes into the political and legal documentation that is necessary to support a solid public key infrastructure (PKI). It takes a very solid PKI to be the cornerstone of cryptographic accountability.

Again, granular risk assessment and accurate cost benefit analysis is the only way to justify such a cryptographic solution. As stated before with confidentiality and integrity, accountability is another area where business requirements can be misinterpreted. Take enterprise internal secure email as an example business requirement. At first glance a group of security professionals may diagnose the problem as a need for enterprise user messaging accountability via public key infrastructure. After all, there are plenty of industry examples of secure email through public key technology. Vendors of these public key infrastructures can spend entire days mesmerizing potential clients with the wonders of public key technology. PKI sales people tell customers how PKI products will secure enterprise email as well as several other “money saving” features. Many of these claims may very well be true.

Unfortunately, most data security areas of large enterprises underestimate the cost associated with building a trust model based on PKI. Monetary, resource, and time costs are not the only factors that most organizations underestimate. Opportunity cost can be completely ignored. In other words, what other threats and vulnerabilities could be mitigated if more funding was diverted from the PKI into other security efforts. Perhaps risks associated with secure emails are far out weighed by risk associated with an intrusion detection effort or a simplified sign-on effort. Formal risk assessment documentation needs to be filed for each enterprise security effort so cost benefit can be compared across all of them. The idea is to have a general understanding of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

how much cost can be afforded for the implementation of a certain cryptographic security control. It's like balancing a checkbook. Installing a fancy, motion detecting, quick response home security system may not leave enough in the pocket book for a dead bolt on every door.

To finish the secure email example, take a closer look at the business requirements driving the cryptographic solution. The business partners need to prevent unauthorized access to the data contained in the email messages. They also require a level of assurance that the message is from the apparent source and that source is not being impersonated. Thinking outside of the traditional solution box may result in a more cost effective and efficient way to accommodate the business requirements. Issuing certificates to each end user might be the best way to get the cryptographic accountability required. Is it necessary to encrypt the message contents to prevent unauthorized access to the data? If strict procedures are executed for authentication and authorization to the email infrastructure then it may be feasible to simply protect the messages as they transmit through the network. A simple transport layer security implementation could solve the problem, saving time and money along the way. This is just an example of how important it is to analyze both data confidentiality and integrity before the final cryptographic solution design decisions are made.

Client Authentication

Authentication is a practical extension of the cryptographic accountability principle. Once accountability is established it can be leveraged to prove identity to a system or application. This principle also relies heavily on a strong trust model. Authentication is dependent on the policies and procedures surrounding the public key infrastructure that issues the certificates. A system that uses cryptographic authentication must trust the certificate authority registration and distribution process. The system has to assume that proper process has been implemented to ensure appropriate certificate management. If the certificates are managed correctly then the system can be confident that the client presenting a certificate is represented by the information in that certificate.

Probably the most important part of managing the client certificate is authorized access to that certificate. Client certificate access is what makes cryptographic authentication more secure that simple ID and password solutions. The owner of the client certificate should have to present something they know in order to gain access to their certificate. Thus, that client has used something they know (a pass phrase or pin number) to gain access to something they have. The goal is to require more than one factor of authentication. Keep in mind that cryptography is not providing magic security dust here either. Cryptography is used to verify the authenticity of the certificate and its client information. Overall authentication is dependent on the strength of trust model and diligence of access control to private data.

Cryptographic solution discovery is a cost-benefit decision procedure. Cryptography can bring the benefits of confidentiality, integrity, accountability, and/or authentication. The cost of these benefits needs to be compared with the cost of alternative solutions. The cost of any security solution, including

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

cryptographic solutions, must be weighed against the cost of potential security compromise.

Cryptographic Solution Integration

Once a cryptographic solution has been discovered through documented risk assessment and justified through cost-benefit analysis that solution can be integrated into business applications. The documentation produced through cryptographic solution discovery should remove any question about what solution will be integrated. The effort should concentrate on logistical details of solution deployment during cryptographic solution integration.

It may seem like most of the hard work has been accomplished when the security requirements have been documented and a specific cryptographic solution chosen. Unfortunately, there is considerable work required to make the cryptographic solution a seamless part of the business transaction. Solution integration is the return on time and money invested in the solution discovery phase. Security professionals must follow through on the promises made to business partners during the solution discovery phase. This is accomplished by efficiently implementing the selected cryptographic technology.

One of the most effective ways to ensure smooth solution integration is to maintain a group of approved cryptographic solutions that can be reused. Business partners that share an enterprise will reuse much of the same infrastructure as they deploy business applications. When cryptographic solutions are proven they can be leveraged by future efforts in the form of reusable services or patterns.

Reusable Cryptographic Services

Reusable services are the cornerstone of quick hitting cryptographic solutions that can be integrated into business applications with low overhead. These reusable services should exist and interoperate on multiple platforms. The services should also be accessible through different application development models. The reusable services should be based on industry standard algorithms and technologies. Cryptographic reusable services provide a thin layer of abstraction to business applications by hiding the cryptographic implementation details. This will allow the services to stay current with the strongest cryptographic techniques without major changes to business application functionality.

An example service might be a simple component that performs triple DES ciphering. The client interface may simply consist of three parts, an encrypt function, a decrypt function and a key management function. This simple implementation can prove to be a powerful tool for confidentiality of data both at rest and in transit on different platforms. For instance, these basic triple DES functions are supported in the Java development language[5] as well as the Microsoft .Net framework through the C# development language.[6] The same triple DES functionality can be found in IBM's Integrated Cryptographic Services Facility on their mainframe systems. The end result is a group of Application

[5] See "Java Cryptography Extension"
[6] See "System.Security.Cryptography Namespace"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Programmer Interfaces (API) that produces the same cipher text on Windows, UNIX, and zOS.

Industry standard algorithms will interoperate between vendors as long as certain variables are configured the same way. This may require additional research and development of the reusable service but it is well worth the investment in the long run. These APIs can be invaluable when sharing sensitive data across disparate platforms.

Reusable Cryptographic Patterns

Reuse of cryptographic solutions is not limited to application layer technologies. The same concept of reusability can be applied at other layers of the infrastructure. Consider data in transit. Three examples are web browser requests, FTPs, and web services. The data associated with these transactions may require protection based on risk assessment. Perhaps changes to the business application will cost more than the benefit provided by existing reusable cryptographic services. Another option to provide seamless, low overhead solution integration is to leverage cryptographic solution integration patterns. The patterns may not consist of reusable APIs. Solution patterns can document how to implement reusable cryptographic technologies like Secure Sockets Layer, IP Security, and Secure FTP. As new efforts prove out certain cryptographic solutions in certain parts of the enterprise, these implementations should be documented as new cryptographic solution patterns. Integration patterns should call out any implementation issues. Road bumps and mistakes made in past deployments can be prevented in future implementations by having detailed descriptions documented.

Proactive monitoring of cryptographic solution patterns will produce solution trends. By watching solution trends, a security area might actually be able to implement a reusable cryptographic solution before there is high business application demand for it. There is a fine line between predicting the cryptographic future and reacting to cryptographic emergencies. An effective cryptographic technology support team will find the happy medium between these extremes. Do not get caught up in building a cryptographic cure a security "disease" that is not validated through a risk assessment. At the same time, do not wait for a security "forest fire" to create the first cryptographic fire extinguisher. Certain cryptographic solutions may need enhancement beyond their current implementation. This type of proactive work should be done before another cryptographic solution discovery occurs which requires the enhancement. Educated guesses based on cryptographic solution pattern analysis will allow for the creation of just-in-time solutions. The deployment timing of these cryptographic solutions will speed up the overall deployment time of the business applications. Such proactive behavior will help business partners understand how security and cryptography is an enabler, not a roadblock.

Cryptographic Solution Maintenance

The last phase of the cryptographic solution lifecycle is solution maintenance. This stage of the solution lifecycle is as important as discovery and integration combined. Maintenance of a cryptographic solution ensures that

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the time and money investment continue to produce business value. Solution maintenance is a significant factor in the cost benefit analysis that occurs when comparing security solutions. The cost of cryptographic solution maintenance can be easily underestimated.

Key management is one of the reasons that the cost of solution maintenance is consistently underestimated. Many security professionals and business partners do not understand the resource requirements for strong key management. Whether dealing with symmetric shared keys or public key certificates, there is a set of core management functions.[7] Examples of these management functions include key registration, generation, distribution, storage, revocation, expiration, and recovery.

The key registration task can consume support resources because this is the initial point of contact a client has with the cryptographic solution. The first step in using any cryptographic solution (other than integrity hashing) is to acquire the appropriate key. Much of the security inherent to a cryptographic solution relies on accurate key registration. Registration is the point at which a client identity is bound to cryptographic key material. With out proper key registration, client identity impersonation can occur and the cryptographic solution is broken before the key is even used.

There are two major factors of any cryptographic solution trust model. First, clients must trust the authority issuing keys does thorough key registration to prevent impersonation. Second, clients trust that keys are delivered securely to key storage. That key storage refers to both the client's key storage and any key storage of the authority. Hence, key distribution is another very important part of managing a cryptographic solution. Some management features may be built into cryptographic technologies that are purchased from vendors. Do not assume third party products will solve all key management problems. Make sure all key management functions are appropriately covered.[8] Placement of cryptographic keys could make or break a solution over time. Key storage is a critical function of key management and should be monitored to prevent key compromise. A client certificate is only as useful as the level of protection the client provides for its storage. If a client is careless with their certificate, it may be compromised with out their knowing.[9]

The only way to minimize negative impacts to business during a key compromise situation is to have a solid key revocation process. Key revocation has the same importance as key registration when it comes to preventing malicious attacks on a cryptographic solution. Business value of a cryptographic technology is significantly lower if key revocation process is missing.

Finally, keys need to be managed so cipher text can be recovered in the future. Key history is important to business partner data that has been protected via encryption. Strong encryption solutions have adequate key expiration periods that keep the data safe. Encryption key expiration means the old keys must be

---

[7] See Barker, Elaine. "General Key Management Guidance"
[8] See Barker, Curt. "Key Management Lifecycle"
[9] See "Digital Certificate Management: Navigating Your Success"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

properly archived to decrypt old data. Cryptographic key recovery procedures will ensure accurate key history.

Key management is not the only aspect of a cryptographic solution that can cause the solution to weaken over time. Strength of the cryptographic algorithms themselves will loose their security value as technology advances. Older cryptographic algorithms will be broken and key lengths become obsolete. At some point cryptographic solutions must migrate to keep up with the latest cryptographic technology. Performance and availability also factor into the end of solution lifecycle. Cryptographic solutions may become inefficient compared to newer technology. Speed of cryptographic operations as well as cipher text size should be considered.

Summary

Cryptography is not a magical security serum. The need for investment in cryptographic solutions must be backed by formal risk assessment. Risk assessments are only valid if an enterprise standard for data classification exists. Once the security analysis is complete, business partners must determine how deep they want to dig into their pockets to protect their data. Security professionals can ease some of the cost by having strategic cryptographic solutions readily available for integration. Finally, cryptographic solutions are a living technology. Each one will come to the end of its lifecycle. At that time, the solution will be replaced with a new and more secure cryptographic technology.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

Schneier, Bruce. “Risk, Complexity, and Network Security” April 2001.
URL: http://www.counterpane.com/presentation1.pdf

“The Standard of Good Practice for Information Security”
Information Security Forum. March 2003.
URL: http://www.isfsecuritystandard.com/index_ie.htm

“Information Security Risk Assessment Practices of Leading Organizations”
United States General Accounting Office. November 1999.
URL: http://www.gao.gov/special.pubs/ai00033.pdf

Parker, Donn B. Fighting Computer Crime New York: John Wiley & Sons, Inc, 1998. 27-55, 369-382

“Java Cryptography Extension”
Sun Microsystems, Inc. July 2003.
URL: http://java.sun.com/products/jce/index-14.html

“System.Security.Cryptography Namespace”
MSDN. 2003
URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpref/html/frlrfSystemSecurityCryptography.asp

Barker, Elaine. “General Key Management Guidance” November 2001.
URL: http://csrc.nist.gov/CryptoToolkit/kms/section5%20notes%20(b-w).pdf

Barker, Curt. “Key Management Lifecycle” November 2001.
URL: http://csrc.nist.gov/CryptoToolkit/kms/lifecycle%20slides%20(b-w).pdf

“Digital Certificate Management: Navigating Your Success”
RSA Professional Services. 2003.
URL: http://www.rsasecurity.com/services/guides/DCMNV_GD_0503.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced