



Achieve Information Security by Preserving the Secrecy and Integrity of Keys

Arxan Best Practices White Paper

The Role of Cryptography and Key Protection

Today cryptography and PKI form the cornerstones of information security. The effectiveness of cryptographic routines depend on the secrecy and integrity of keys.

In this paper, we will discuss prevailing threats to cryptographic keys, a **defense-in-depth approach** to addressing key vulnerabilities and how to prevent compromise of your enterprise's intellectual property and customer confidential information. A number of **security options that address risk mitigation** are also reviewed. Additionally, best practices for key protection, which include application hardening are provided. Lastly, Arxan's TransformIT™ is presented, which **enhances software security** by preventing tampering and hacking attacks on keys that are used within software applications. Hence, TransformIT prevents content, data and revenue lost.



TABLE OF CONTENTS

Information Security and Cryptographic Keys	3
Encryption is the Foundation of Information Security.....	3
Cryptography is Ubiquitous in Information Security.....	3
Defense in Depth is Imperative.....	3
Enterprises Benefit from Key Protection.....	4
Two Classes of Key Vulnerabilities.....	4
In-Depth Threat Analysis - An Example.....	5
Key Protection Options	6
Perimeter Security Measures.....	6
Internal Measures.....	7
Intrinsic Defense-In-Depth Measures.....	7
More Information	8

Information Security and Cryptographic Keys

Encryption is the Foundation of Information Security

Authentication, data encryption, and hashing (or signing) are fundamental tools in the enterprise security arsenal. Information security tools span a wide range of applications, including:

1. Protection of the confidentiality of personal information such as credit card numbers, social security numbers and account numbers, generally using a combination of application authentication, user authentication and data encryption.
2. Protection of intellectual property such as business plan documents, financial details, product plans and research documents against espionage or disclosure. These are typically protected by digital rights management (DRM) systems of some type, combined with user authentication tools.
3. Authentication of clients and encryption of data during remote access, e.g. over Virtual Private Network (VPN) connections
4. Authentication of clients and encryption of data during digital communication, e.g. for Voice Over IP (VoIP) communication
5. Security policy enforcement using tools such as Network Access Control (NAC)
6. Code signing to ensure integrity of software
7. Document signing to ensure integrity and establish authenticity of contracts, research logs and similar documents.

Cryptography is Ubiquitous in Information Security

Cryptography forms the basis of information security infrastructure. Data encryption, network traffic encryption, PKI-based authentication and digital signatures all depend on the underlying confidentiality of secret keys and integrity of public certificate authority keys to function as intended. When keys are compromised, information security systems cannot protect data.

First-tier technologies such as network, data and access security measures are used to protect confidentiality of consumers' personal information and to control financial fraud. However, they are ineffective against insider attacks— which can amount to nearly 60% of all targeted information security attacks. Additionally, today's sophisticated malware requires systems to be comprehensively defended against hacking and compromise.

Specifically, PKI (Public key infrastructure) cryptography is a common application of encryption for information security, and forms the basis for SSL and code signing. Its security is predicated on the confidentiality of server, client and CA private keys, as well as on the integrity of the application's copy of corresponding public keys. When internal attackers pursue application tampering via malware or vulnerability exploits, data becomes susceptible to theft and legitimate systems users become susceptible to phishing or similar attacks.

Defense-in-Depth is Imperative

In recognition of today's evolved threats to sensitive data, several regulations such as SOX, PCI, GLBA and FISMA prescribe a multi-layered security solution. Arxan provides defense-in-depth solution for sensitive enterprise data and applications that is comprised of both key protection and application hardening. Together they provide a comprehensive defense in depth solution for your enterprise's intellectual property and customer confidential information:

- TransformIT provides white box cryptography technology to prevent discovery and unauthorized use of secret keys, and replacement of public keys in information security applications.
- GuardIT® provides binary-based application hardening to defend native and managed code applications against tampering and reverse engineering

Enterprises Benefit from Key Protection

Keys must be fortified in three locations – in escrow, in application functions where they are used, and where they reside at rest.

- Enterprises who build their own security infrastructure in-house can directly leverage Arxan's technology to fortify their systems in depth. Adopters see a strong return on investment through diminished risk, lowered breach management costs and lowered security management costs.

Similarly, vendors of security tools, including anti-malware utilities, secure communication utilities and data management utilities are seeing the value of fortifying their products. The enhanced security offers higher value to customers, establishes a differentiating advantage in a fiercely competitive market and prevents adverse publicity from widespread hacks.

Two Classes of Key Vulnerabilities

The threat landscape continues to become more sophisticated as internal compromise and malware is becoming increasingly covert and elusive. Exploits on cryptographic systems for information security are based on two main classes of key vulnerabilities:

I. Discovery or Disclosure of Private Keys

The security of asymmetric cryptography applications, including PKI systems, is predicated on the private key remaining secret and private. If the private key is discovered, then a whole host of compromises are enabled, such as:

- All private key transactions can be spoofed, hackers can arbitrarily emulate your website. This in turn enables highly sophisticated phishing attacks.
 - All data secured by PKI can be snooped, connections such as https and SSL which should be private and secure now become public to hackers. This places confidential data and proprietary information at risk of theft.
 - Hackers can use your private key to impersonate your corporation or a specific individual to tamper signed documents or sign arbitrary documents. Such attacks would be used to compromise research notes, for example, that may be critical to proving patent priority.
 - Hackers can use your private key to impersonate your corporation when signing arbitrary code. This allows unchecked tampering of your software applications, and distribution of malware under the guise of your legitimate software.
 - Knowledge of the private key enables eavesdropping on remote connections such as VPNs. As a result, hackers can read all data and even get the client to connect to an arbitrary server.

2. Tampering of Public Keys and CA lists.

Public keys are often seen as inviolate and permanently safe. However, a computer application only knows a public key as a string of alphanumeric characters. The application's copy of a public key can be replaced with an arbitrary public key, or a malicious public key can be added to an application's list of trusted certificate authorities. These attacks are particularly relevant to client applications, but are also pertinent to server-side applications due to the threat of insider attacks. Tampering of public keys makes the following exploits possible:

- Certificates can be spoofed, a client will authenticate and connect to an arbitrary server. This in turn causes data loss and can enable phishing attacks.
 - The client's copy of a Certificate Authority (CA)'s public key can be altered and be made to reject connections from the legitimate server. This in turn causes denial of service and or blocks legitimate security updates.
 - A client can be tricked into accepting any arbitrary software as genuine since signatures can be spoofed. This in turn facilitates infection of client systems and corporate networks with malware.

To prevent such exploits, every client utility which uses PKI to authenticate a server, an application or a software update must be fortified against tampering. In particular,

- Root public keys must be stored and used in such a way that they cannot be easily isolated and replaced,
- The system must be tamper evident, so that the application using PKI is immediately made aware that its underlying cryptographic routines may have become unsafe.

In-Depth Threat Analysis - An Example

Secure Sockets Layer (SSL) is one of the most commonly used protocols in information security applications, with applications ranging from e-commerce and m-commerce to VPNs. The principle of challenge-response that underlies SSL also powers other authentication methods such as those used in application-to-application (A2A) authentication.

As an example of how private and public keys are vulnerable to attack, and how such compromise results in theft of confidential data, we present below a security analysis of the SSL protocol. (For comprehensive threat representation, we also include threats to SSL from application tampering) Note that, when any one step is compromised, all subsequent steps stand compromised as well. To securely execute an SSL connection in confidence, all vulnerabilities must be fully mitigated.

Note – this discussion assumes the reader is familiar with the basics of public key cryptography and PKI. A good introduction to the subject is available at:
http://en.wikipedia.org/wiki/Public_key_infrastructure

A Security Analysis of Vulnerabilities in SSL Protocol

SSL security measure	PKI assumption	Vulnerability from private key disclosure	Vulnerability from public key tampering	Other Vulnerabilities from application tampering
Verify credentials of other party via well-formed certificate signed by trusted CA	<ul style="list-style-type: none"> CA private key will only be used to sign legitimate certificates Client application has kosher copy of CA public key to verify certificate chain Client application has access to, and uses, latest revocation list 	<ul style="list-style-type: none"> If the CA private key is known to hacker any arbitrary certificate can be signed An arbitrary revocation list can be created and signed with the compromised CA private key 	<ul style="list-style-type: none"> If application's copy of CA public key is replaced with public key of hacker's choice, hacker can use corresponding private key to construct an arbitrary certificate and have application validate it. Similarly, integrity check on CRL can be compromised 	<ul style="list-style-type: none"> Server credential verification can be entirely bypassed and altered to always succeed
Generate challenge (and similarly, generate session key)	Challenge is random and unpredictable, such that known response cannot be replayed. Key is random and unpredictable, such that full strength of cryptographic protocol is obtained.	N/A	N/A	<ul style="list-style-type: none"> If RNG is weakened, e.g. by constant seeding, predictable challenges and keys result
Server signs challenge with private key, client verifies response	<ul style="list-style-type: none"> Server private key is only known to legitimate server application 	<ul style="list-style-type: none"> Any adversary who knows the private key can pose successfully as the legitimate server 	N/A	N/A
In some cases, client signs challenge with private key, server verifies response	<ul style="list-style-type: none"> Client private key is only known to legitimate server application Client private key is only used to sign challenges with client's consent 	<ul style="list-style-type: none"> Any adversary who knows the private key can pose successfully as the legitimate client 	N/A	<ul style="list-style-type: none"> Adversary can leverage client private key for transactions without client's consent
Client transmits session key, encrypted with server public key. This key is used towards securing subsequent data transmissions	<ul style="list-style-type: none"> Since server private key is only known to legitimate server application, only such an application can infer the session key 	<ul style="list-style-type: none"> Any adversary who knows the private key can eaves drop on the session data exchange 	<ul style="list-style-type: none"> If client is tampered to use bogus public key instead of legitimate public key to encrypt, then hacker who has corresponding private key can pose as server 	N/A

Arxan's TransformIT key transformation technology protects private keys from discovery and public keys from tampering. Arxan also provides application hardening for comprehensive protection of the application and its cryptographic routines.

Key Protection Options

Perimeter Security Measures

Perimeter security measures aim to prevent malware and hackers outside your protected network from gaining control over internal resources and systems. These measures include firewalls, intrusion detection systems, network access control measures, and secure remote access.

External measures provide an effective first line of defense against key discovery and key compromise attacks. External measures cannot protect, however, against zero-day exploits and increasingly sophisticated malware. Insider attacks are, today, the largest class of information security attacks and specifically targets valuable data and IP. **Perimeter security alone is also ineffective in protecting against these attacks. As a result, experts today are recommending that companies focus on securing applications themselves rather than rely solely on perimeter security.**

Internal Measures

Internal measures directly protect the key and key-based application from attack and compromise.

Keys in escrow are generally stored in the clear and protected using physical access procedures, or stored in hardware-based appliances and protected using pass phrases or other means of authentication. In all cases the key is stored in its original, integral form. Access control measures must be balanced against the need to recover keys following hardware or software failure, or loss of computer equipment.

Within applications, keys can be stored on hardware devices, can be hard coded into applications, or may be computed on the fly based on a password and possibly additional cryptographic material or tokens. Hardware based protection is effective, but is expensive to deploy and maintain. Loss of keys through theft of hardware devices is also an issue. Software based protection measures work well while the application is at rest, but the key becomes vulnerable to memory-based attacks at run time.

Additionally, none of these techniques are designed to prevent tampering attacks on public keys. Therefore, an **additional layer of defense-in-depth is required to fully protect your data and applications.**

Intrinsic Defense-In-Depth Measures

Arxan's White Box Cryptography based product, TransformIT, transforms private and public keys to secure them both in deployment and in escrow. These measures work in concert with existing internal and perimeter measures to fortify your enterprise applications, data security software tools and other sensitive applications. The result is, durable, easy defense for your data and intellectual property that is cost-effective and low-impact.

White-box cryptography (WBC) is a technique designed to protect secret keys against discovery and extraction attacks, even when the attacker has total visibility into software implementation and execution. This white box context contrasts sharply with traditional black-box cryptography where attacker is assumed to be external (such as a man in the middle) with no access to the application itself.

Arxan's [TransformIT](#) provides strong, fully tunable white-box cryptography protection for asymmetric cryptography operations, which form the cornerstone of any information security infrastructure. TransformIT breaks down asymmetric key cryptographic operations such that the entire key is never revealed. It then conceals the location of the relevant operations themselves, and further tightly binds the secret keys and cryptographic routines to the overall application (and, optionally, to the hardware).

Arxan's [GuardIT](#) provides strong yet performance-friendly static and dynamic protection for software applications.

More Information

No other security solution on the market provides the patented Guard technology deployed in a “Moving Maze” architecture to provide binary based active protection. Arxan’s unique approach effectively combats the urgent problems of software piracy and tampering without development overhead or heavy runtime penalty. For more information about Arxan and other Arxan products, please contact us at info@arxan.com or visit our website at www.arxan.com.

About Arxan Technologies, Inc.

Arxan Technologies, Inc. (www.arxan.com) is a leading provider of application hardening solutions designed to protect software applications from tampering to minimize risk and maximize profitability. Our advanced software protection solutions secure enterprises, ISVs and digital media providers against unauthorized use, malware insertion, piracy, and reverse engineering of intellectual property. Our products defend, detect and react against to attacks through a threatbased, customizable approach that is proven, easy to use and non-disruptive. Arxan supports a full range of application protection needs from commercial software to military grade assurance. The government relies on Arxan Defense Systems, Inc. a subsidiary of Arxan Technologies, to deliver a best-of-breed anti-tamper solutions to protect critical program information. Founded in 2001, Arxan Technologies has offices in Bethesda, San Francisco, London, New York, Dallas, Boston, Chicago and West Lafayette, Ind.

Notices

Arxan Technologies, Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Arxan Technologies shall not be liable for errors contained herein or for incidental, consequential, or other indirect damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Notice

The version of the Arxan product described in this document is sold under a per user license agreement. Its use, duplication, and disclosure are subject to the restrictions in the license agreement.

Trademarks

Arxan, the Arxan logo, Active Defense for Software, Guard, GuardScript are either registered trademarks or trademarks of Arxan Technologies, Inc. in the United States and/or other countries. Microsoft, Windows, Windows NT and Visual C++ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Portions of the information disclosed herein are protected by U.S. Patent No. 6,941,463; U.S. Patent No. 6,957,341 and Patents Pending.

Copyright

Copyright © 2008 Arxan Technologies, Inc. All rights reserved. No part of this document may be photocopied or reproduced without the prior written consent of Arxan Technologies, Inc.

