This is a writing assignment of how to improve the security posture of a given organizational scenario. A ‘security posture’ is established when precautions are taken to ensure against theft, espionage, etc.; and is the protection of data to ensure that only authorized personnel have access to computer files.[[1]](#footnote-1) It also defines a company’s approach to all of its security issues, to include both technical and nontechnical elements (such as policies, procedures, and controls) that address internal and external threats.[[2]](#footnote-2) It builds upon a multilevel approach with layers of security, for both, physical and virtual access to the computer network. Physical access is controlled by security guards, restricted access to rooms, authentication, authorization, and accounting. Technologies of cardkey systems and biometrics have made security more effective, efficient and convenient. Virtual access is controlled with a defense system of firewalls, network intrusion detection systems, and ‘all-in-one’ network security appliances to create a solid perimeter to keep attackers out.[[3]](#footnote-3)

A second layer of protection would be the encryption of valuable data, which makes the ‘intellectual property’ content unreadable until it is decrypted. Even if an attacker penetrates the defenses and steals the files, they cannot read the data because they do not have the means to decrypt the data. The most effective precaution is policy and practice to diligently encrypt the data in files in the first place. When data is stored and transported on portable devices, such as laptops, handheld devices, and USB flash drives and taken out of the security of the local network perimeter of the office, then the importance of encryption and the risks of attack increases for that data. Those devices can be lost or stolen and the casual use of free Wi-Fi hotspots are not safe environments for networking. The encryption/decryption process is called cryptography and as a last line of defense, does a number of good things:   
 1) Protects confidentiality of the information by ensuring only authorized parties can view it;

2) Protects the integrity of the information by ensuring the data cannot be altered;

3) Ensures availability of the data to authorized individuals who have been given the key;

4) Verify the authenticity of the sender and the encrypted data.

5) Enforce nonrepudiation to prove a user performed an action and prevents fraudulent denial.

Eventually, security will be a priority and typically, a business should have one or more IT professionals to make a team to focus on their security issues. A security policy should be adopted to follow the best practices for routine precautions and incidence response procedures. All security issues should be addressed, including the management of critical data ownership, access and responsibilities. The IT team can share security control by a separation of duties and job rotation. The overlapping authority assures management of continued access to critical systems, afforded by administrative passwords for the core network router and firewall, network switches, the corporate virtual private network, the Human Resource system, the e-mail server, and the Windows Active Directory. Critical data, such as data in database files, security certificates, and private keys can be protected by the strongest security of computers built for security with components of the Hardware Security Module (HSM).

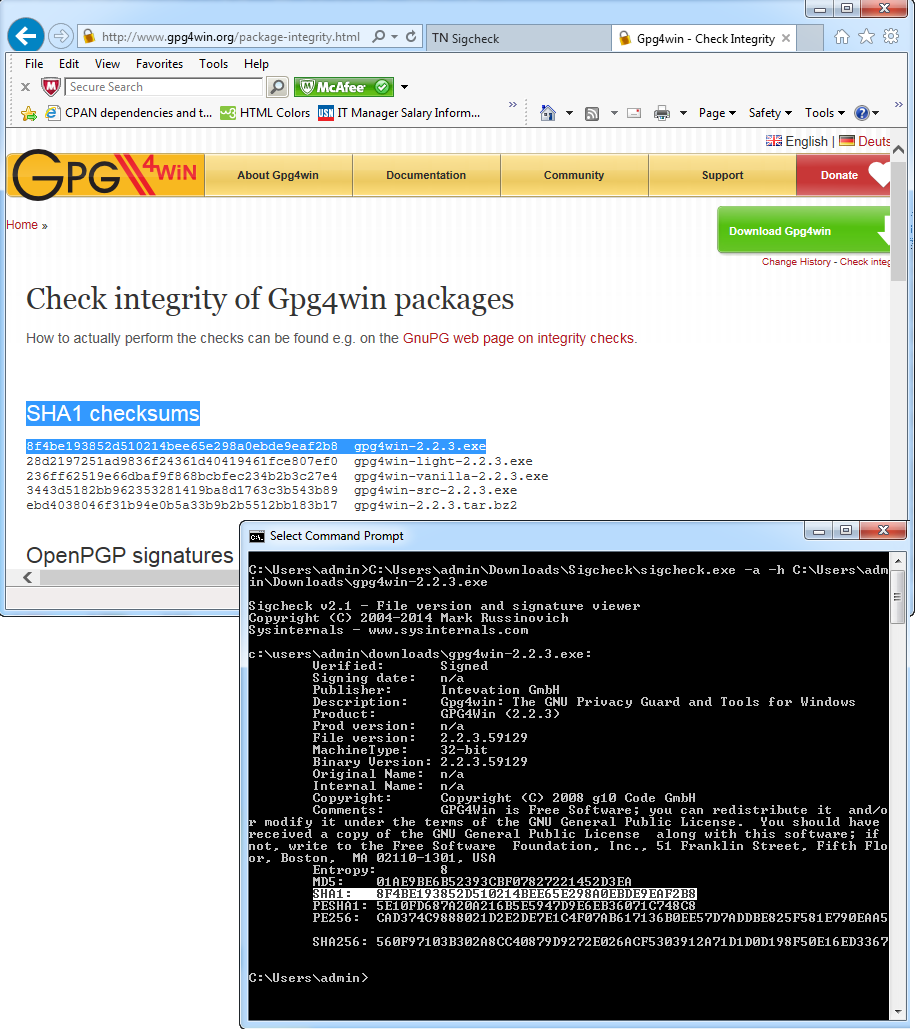
The integrity of data is only as reliable or ‘secure’ as the integrity of the computers and the integrity of the networks. There is always a tradeoff between the level of security and the level of convenience; they are inversely proportional. Critical data should be stored on a secure network server where access is controlled and it ensures the data is safeguarded with a backup copy stored to a remote site. Besides controlling access with several security appliances and multiple firewall devices, each computer workstation and company-issued mobile device should have security measures configured so they cannot be tampered with. The configurations should typically set user-access to be ‘least-privileged’ until otherwise authorized. Computers should be protected, starting with physical access and at the lowest level of password-protection of the BIOS settings and restrict booting from the hard-drive. Then have controlled-access with login accounts, authorized through network servers, running Microsoft® Active Directory™ on a domain controller. Also protect the network at the OSI’s network layer with a setup for IPsec.[[4]](#footnote-4)

Standalone computer operations should be made impossible. Local storage of critical data should only be allowed when stored in locked safes or approved security-cabinets. Via the network, all workstations will receive automatic software updates and scheduled, automated scanning for malicious software (malware), conducted without user intervention or interference.

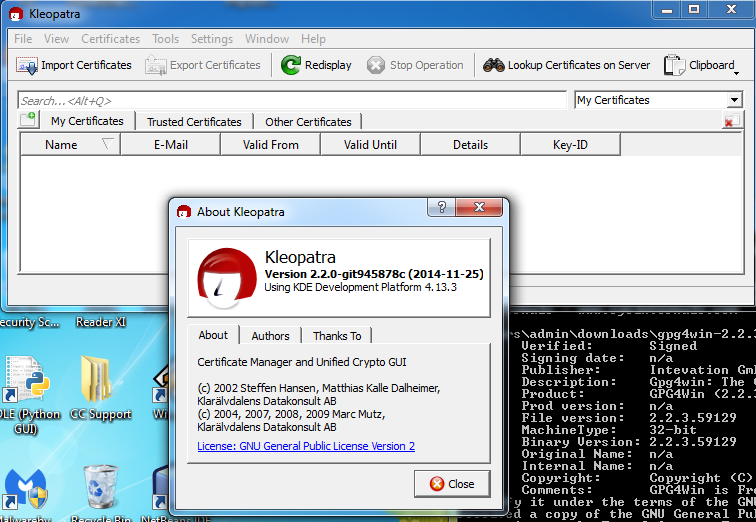
The installation of software applications will be restricted to IT personnel and they will install software only after the product has been verified to be unaltered by comparing the MD5 hash signature from the software publisher (and not from a mirrored-site). “I was aware of this precaution; usually warned by software publishers to do this step between the software product file download and the software program installation.” But I never have until now. I thought it was widespread and common but it became an involved procedure that was only made possible by the Lab Manual of this course. Before installing, the MD5 hash of the downloaded software can be determined with the software, called Sigcheck™.[[5]](#footnote-5) At Command DOS prompt, type:

sigcheck –a –h {*full name of the file*}

The source of the file was downloaded file shows the SHA1 Checksum and it matches what the Sigcheck software found from what I actually downloaded.[[6]](#footnote-6) Pretty good, huh?!



The Gpg4win software installed this Kleopatra, Certificate Manager and Unified Crypto GUI. There are probably a lot, to still learn, about the products that are on the market.



The network administrator can create a template of customized groups and security settings, called a Security Template. This is used as a baseline to return to, after changes made while experimenting with different security scenarios and solutions. [[7]](#footnote-7)

It is necessary to transmit sensitive data in the course of business transactions. Business partners establish direct lines of communication to suppliers, distributors, and customers, via Electronic Data Interchange (EDI), which has been around 40 years but advances in security technology has allowed the use of the Internet for securely transferring sensitive data. These enterprise-systems provide direct connections to ensure authenticity and availability of the data.

Businesses everywhere heavily rely on Electronic Mail (email) to transmit information and transfer files with sensitive data. These email systems, like Yahoo, Gmail, and even Hotmail use hashing to ensure the integrity of the attached file with a Class 1 digital certificate. But hashing is not encryption. Those files should first be encrypted, then the encrypted copy is the file attached to the email message. The processes of sending encrypted files and decrypting received can be facilitated by various methods. Symmetric encryption can protect the confidentiality of an e-mail message. Asymmetric encryption can verify the authenticity of the sender and enforce nonrepudiation, such as the popular Pretty Good Privacy (PGP) encryption.[[8]](#footnote-8)

The best solution for businesses to share their sensitive business information is to use an established third-party entity that all parties can trust. A ‘chain of trust’ can be established with the trust of the third-party. Established trusted authorities such as DigiCert®, RapidSSL®, Comodo®, Symantec Group®, Go Daddy Group®, GlobalSign®, and GeoTrust® issue ‘digital certificates’ that are digitally signed for authentication; they are called a Certificate Authority (CA).[[9]](#footnote-9) The Public Key Infrastructure (PKI) is used in a Distributed Trust Model of a CA with Intermediate CAs and be compatible to the bridge model that would be provide a trust with major business partners and government agencies. Certificates are registered by a Registration Authority (RA), and certificates are stored in a Certificate Repository (CR) and certificates are revoked from a Certificate Revocation List (CRL). To quote one source, DigiCert, the cost of a Standard (Class 2) digital certificate is generally $140-175 / year, Extended Validation (Class 3) digital certificate is generally $295 / year, Class 2 digital certificate is generally $ / year.[[10]](#footnote-10)

At the consumer end, businesses should perform Web browser management and have a Certificate Policy (CP)[[11]](#footnote-11) for the management of digital certificates and have a Certificate Practice Statement (CPS)[[12]](#footnote-12) to process applying, registering, and revoking. There is the tremendous ongoing tasks of managing digital certificates during the digital life cycle of creation, suspension, revocation, and expiration. Key handling procedures include the escrow, expiration, renewal, revocation, recovery, suspension, and destruction of digital keys. Key management can be assured by the method M of N Control of key parts. This is done with multiple pairs of dual keys, separated and shared by different groups of people. One pair of keys are used for encryption with the public key backed up off-site, and the second pair of keys are used for digital signatures with no backup of the public key. Company personnel would have Class 2 digital certificates. For web servers, have Class 3 digital certificates. All would be dual-key certificates. The extremely critical systems use dual-sided certificates and authenticate the other party. If the business is the publisher of software then the business should be interested software signing Extended Validation (Class 3) digital certificates. Business transactions between companies require Class 4 digital certificates.

The software developers, like myself, are concerned with the encryption, transmission, and storage of account passwords, especially with web-based application software.[[13]](#footnote-13) The user password is created by the user by typing it into a textbox of a web form. In its original form it is called cleartext and is never shown or stored. The typing of the password is concealed by a mask of dots. Upon pressing the form submit button, the password is handled as plaintext (unencrypted) within the restricted memory of the running software. The software program will encrypt the password with a unique seed, called a salt, which strengthens the encryption. The encrypted password is called ciphertext. But the ciphertext will be hashed before it is stored or transmitted. The Cryptographic Hash Function is not a Password Hash function. [[14]](#footnote-14) The one-way hash is irreversible but it will match a comparison to another encryption of the same password; for authentication. The hash is typically sha256[[15]](#footnote-15) and the encryption/hash process is usually repeated four iterations; and the final result is called the digest. Here is a sample of Perl code for password encryption.

function encryptPassword() {

$VAR{plaintext} = $FORM{password};

$VAR{salt} = substr($VAR{plaintext}, 0, 2);

$VAR{ciphertext} = crypt($VAR{plaintext}, $VAR{salt});

$VAR{digest} = sha256\_hex($VAR{ciphertext});

password = asdf  
Encrypted password = asZvhAtTX.i7g  
SHA256 hashing of encrypted password, called the digest =

e4951b5267f3b7369f03a3c5987733aead692128ba059ccbef6edf2401a39d7e

The digest will be stored in the database for future reference and to authenticate logins later. It may be possible to decrypt the password if you know how it was encrypted.[[16]](#footnote-16)

1. security posture | English definition dictionary | Reverso, online at <http://dictionary.reverso.net/english-definition/security%20posture> [↑](#footnote-ref-1)
2. security posture – Termwiki, online at <http://www.termwiki.com/EN/security_posture> [↑](#footnote-ref-2)
3. SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, 4TH Edition, Mark Ciampa, Ph.D, © 2012 Course Technology, Cengage Learning. [↑](#footnote-ref-3)
4. How to setup IPSec for Linux, OpenBSD and PGPNet at [www.linuxsecurity.com/resource\_files/cryptography/ipsec-howto/HOWTO.html](http://www.linuxsecurity.com/resource_files/cryptography/ipsec-howto/HOWTO.html) [↑](#footnote-ref-4)
5. Microsoft® Windows™ Sysinternals program: Sigcheck™, downloaded from <https://technet.microsoft.com/en-us/sysinternals/bb897441.aspx> [↑](#footnote-ref-5)
6. Gpg4win - Check Integrity at [www.gpg4win.org/package-integrity.html](http://www.gpg4win.org/package-integrity.html) [↑](#footnote-ref-6)
7. LAB MANUAL FOR SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, 4TH Edition, Dean Farwood. © 2012 Course Technology, Cengage Learning. [↑](#footnote-ref-7)
8. Gpg4win - Secure email and file encryption with GnuPG for Windows at [www.gpg4win.org](http://www.gpg4win.org/),

   WHERE TO GET PGP (Pretty Good Privacy) at [www.cryptography.org/getpgp.htm](http://www.cryptography.org/getpgp.htm), [www.symantec.com/encryption/](http://www.symantec.com/encryption/), <web.mit.edu/network/WhatsNewWin.html>, [www.pgpi.org/](http://www.pgpi.org/) [↑](#footnote-ref-8)
9. Public key certificate - Wikipedia, the free encyclopedia at <http://en.wikipedia.org/wiki/Public_key_certificate> [↑](#footnote-ref-9)
10. SSL Digital Certificate Authority - Encryption & Authentication at <https://www.digicert.com/> [↑](#footnote-ref-10)
11. DigiCert Certificate Policy at <https://www.digicert.com/docs/cps/DigiCert_CP_v406-May-14-2014.pdf> [↑](#footnote-ref-11)
12. DigiCert Certificate Policy at <https://www.digicert.com/docs/cps/DigiCert_CPS_v405-May-2-2013.pdf> [↑](#footnote-ref-12)
13. Storing Passwords Securely at <http://throwingfire.com/storing-passwords-securely/> [↑](#footnote-ref-13)
14. Storing Passwords Securely at <http://throwingfire.com/storing-passwords-securely/> [↑](#footnote-ref-14)
15. SHA-256 hash calculator. Online SHA-256 hash generator. Mining Bitcoin at <http://www.xorbin.com/tools/sha256-hash-calculator> [↑](#footnote-ref-15)
16. perl - How to decrypt hash stored by bcrypt - Stack Overflow at <http://stackoverflow.com/questions/18084595/how-to-decrypt-hash-stored-by-bcrypt> [↑](#footnote-ref-16)