Final Report – Applied Cryptography

Compilation & Security Model for ACME Insurance Company X

Author: Chad Nelley

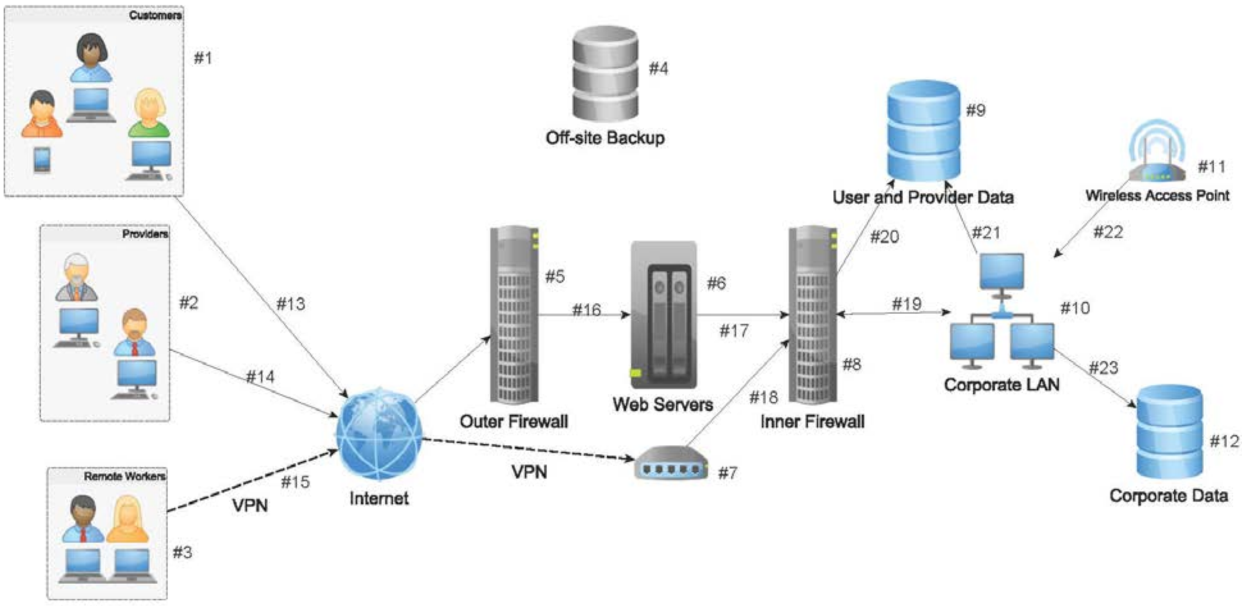
Date of Report: April 25, 2016

Executive Summary

Information and data integrity are core to the day-to-day operational survival of ACME Insurance X. In order for ACME to remain vital and profitable for our shareholders, customers, vendors and employees it is critical that we build a security posture that reflects our commitment to information and data integrity. Whether data is idle behind our firewalls or in transit between customers, vendors or employees we must put security at the forefront of our thinking and design. This report will attempt to lay out a security network and posture that incorporates physical security measures, data security measures, electronic security measures, policy and procedural application and enforcement of security best practices for the organization.

Architecture & Network Diagram

Below, in an effort to illustrate our security network and architecture, is a compilation of the network topography with specific network and data security call outs listed in high level order or function. This report will attempt to call out specific areas where traditional hardware and software solutions can be implemented throughout the diagram. A specific focus throughout this report will be on the implementation of various Cryptography solutions and implements that will augment our security posture as it relates to data at rest and in transit. Encryption and cryptographic technologies are paramount to augmenting hardened network, server and endpoint solutions. Below is a graphical look at our current network topography:



The image above represents the architecture for the ACME Insurance X. Each component and interface is labeled with a corresponding number. Below I have outlined the security measures we will take in regards to each labeled element in the environment. Further in this report I will speak to the specific implementation of Cryptography elements to ensure secure data flow within and external to this environment.

Components

#1 Customers: While we can’t control how data comes to us from customers, we can control what we do with it and how we protect it once it arrives in our environment. Once data arrives and is stored we will apply encryption to that data.

#2 Providers: While we can’t control how data comes to us from providers, unless we have established contractual parameters, we can control what we do with it and how we protect it once it arrives in our environment. Once data arrives and is stored we would want to apply encryption to that data. Further, would recommend that in the courting and vetting process of any provider/vendor relationships we establish contractual obligations that state how data is to be handled at rest and in transmission.

#3 Remote Workers: Full end point protection with central administration capabilities to include an RSA quality encryption solution that covers every component of the remote workers environment/system. I of course would recommend the ESET Antivirus End Point solution managed by RA in conjunction with the ESET Deslock encryption solution for all drives and data.

#4 Off-Site Backup: Full encryption of data stores and back-up environment

#5 Outer Firewall: Limited access port availability configuration. Port 80 to allow web traffic. All other non-relevant ports closed to external traffic.

#6 Web Servers: Fully Patched and updated with latest antimalware solutions riding along. Additionally we will add PKI through trusted CA’s and we will ensure HTTPS is configured for all web pages that reference any PII or transactional elements.

#7 VPN: Configure VPN with Strong VPN standards that include a strong 128bit or better CA and user Certs as well as strong User and TA keys. Configure VPN device according to instructions provided with device toggling advanced settings and customize the settings to best suit the VPN criteria required.

#8 Inner Firewall: Configured to only allow verified VPN traffic into the internal domain. Also would implement IDS/IPS on this firewall, along with a continuous monitoring solution as to actively monitor network behavior beyond the initial penetrations test findings. Also, not listed here in the diagram, are any “honey pot” servers to attract nefarious actors who might find their way into the DMZ. Would consider adding these as potential “traps” for bad actors to gain insight to whom is trying to infiltrate.

#9 User and Provider Data: Once in our environment, data to be encrypted for storage and transport beyond internal network.

#10 Corporate LAN: Implement Cisco LAN Controller configuration best practices across the LAN environment. To comprehensive to cover here in a timely fashion, but some of the configuration elements regarding security would include: 802.1x Authentication; Enable Secure Web Access; Secure SSH/Telnet; Peer-to-Peer Blocking; Disable Aironet IE; CCKM Timestamp Validation; etc, etc. Also, implement specific subnets for specific groups/users as identified from Group Policies established CISO/CIO/CTO office.

#11 Wireless Access Point: Configured with WPA2

#12 Corporate Data: Corporate Data to be encrypted for distribution beyond internal network

Interfaces

#13 Customers to Outer Firewall: For access to secure account information located on Web Servers behind the first firewall, would implement authentication and login access controls for account access.

#14 Providers to Outer Firewall: For access to secure account information located on Web Servers behind the first firewall, would implement authentication and login access controls for account access.

#15 Remote Workers to VPN: Set up Access lists and configure Cisco PIX VPN appliance accordingly. Ensure all access lists conform to and associate with group policies and create specific tunnel groups that map back to the group policies. Ensure groups/users map and have access to only the subnets that are germane to their daily work.

#16 Outer Firewall to Web Servers: Enable ports 25/80/443

#17 Web Servers to Inner Firewall: Enable ports 443/987/20/21/3389

#18 VPN to Inner Firewall: Enable port 1723

#19 Inner Firewall to Corporate LAN: Enable ports 25/80/443/987

#20 Inner Firewall to User and Provider Data: Configured for No Access

#21 Corporate LAN to User and Provider Data: Block Cypher/Encryption Enabled access: 128bit/256+bit keys (Internal access/VPN approved access only)

#22 Wireless Access Point to Corporate LAN: WPA2

#23 Corporate LAN to Corporate Data: Block Cypher/Encryption Enabled access: 128bit/256+bit keys (Internal access/VPN approved access only)

Additional Controls Not listed in Diagram

1. Network Access Controls
2. Mobile NAC
3. Intrusion Detection Appliance/Controls
4. Intrusion Prevention Appliance/Controls
5. Implementation of a Network Behavioral Analytics Solution (ex. Flowscape by Cyberflow Analytics)
6. Active Patching/Updating of all End Point and Server OS' in environment
7. Active and repetitive User Education

Addition of RSA Encryption & Key Length

1. Add RSA Encryption Standards with a minimum 2048 key length for all customer/patient interactions at the website data entry login page.
2. Add RSA Encryption Standards with a minimum 4096 key length for all employee, vendor and provider interactions at login page.

This diagram and summary of measures demonstrates our approach and security posture for the organization from a high level. Policies have been developed to guide and enforce appropriate access controls at all levels of the organization and IT procedures have been established to ensure that best practices are followed in the monitoring and maintenance of the environment.

Security Threats & Risks

As part of our early assessment we have identified the following risks associated with the day-to-day operations of our environment. They are as follows:

- Competitive Espionage
- Insider Threat
- Data Leakage
- Physical Access/Breaches
- Technical/Network Access Breaches
- Malware & End Point Exploitation
- Data Integrity, DRM and Business Continuity

Security Strategy

The IT Group at ACME Insurance X has formulated a specific set of strategies that we have deployed in the build out and maintenance plan of the above Infrastructure. Those include:

- A Physical Security Plan
- A Network Security Plan
- A User Access Plan
- A Data Security Plan
- A Disaster Recovery Plan
- A Communications Plan
- A rigorous Set of Policies and Procedures
- A Business Continuity Plan

Each of these specific plan documents will be made available for Executive review as part of the best practices library for the environment design outlined above. This document will serve as one of the primary components of the broader Data Security Plan as here-in we will outline specific use of Cryptography and Encryption technologies.

Information Security Overview

As part of the broader strategic plan we will also be putting together specific strategies for securing data and information across the ACME Insurance X organization. At the core of these plans will be data encryption and data integrity strategies and tactics. These strategies will be outlined in the Data security measures section of this document below. Essentially we will be employing/deploying the following practices:

- Definitions of consistent and integrated methodologies for the design, development and implementation of Data Security techniques and tactics
- Detection of Data Security exploit attempts and resolution/remediation of weaknesses
- Provisioning flexible, yet secure data architectures
- “Security by Design” in the Information and Data lifecycle
- Encryption of data in transit and at rest
- Back-up and Disaster Recovery policies and procedures
- Information Assurance Audits & SOP’s

- Application of Standards on Data Handling and transmission
- Information classification

Data Security Measures

- Implementation of PKI
- RSA Encryption Technologies
- Application of the Kerberos Server

Implementation of PKI

As part of our PKI strategy & design we will incorporate a PKI policy that includes the following key elements:

- A trusted and industry prevalent certificate authority
- A trusted and prevalent registration authority
- A certificate database which will store all certificate requests and executes certificate issuance and revocation.
- A certificate store which will reside on a local host to be used as the certificate repository and the place to store any private keys associated with issued certificates

Our approach to PKI will be as follows:

Security in communications with PK techniques depends on whether the user of a public key correctly knows who the key's owner is. A PKI provides a way for public key users to know who owns a key pair. A trusted third party (TTP), the certification authority (CA), creates a digitally signed document, a public key certificate or certificate, that includes the name of the key pair's owner and the public key. The certificate includes other information related to the owner, the PKI, and the uses the CA intended for the certificate.

The PKI manages certificates. The PKI issues certificates when requested according to prescribed processes and procedures that ensure the owner of the key pair is correctly identified. The owner of the public key contained in a certificate is also known as the subscriber. The PKI also provides a convenient storage solution for users to obtain copies of certificates belonging to an individual and, therefore, obtain the individual's public key from the certificate. A user who obtains a public key from a certificate and depends on the association between the owner's name and the public key and on other information in the certificate is known as the relying party.

Determination and trust of the CA is highly critical in the application of PKI. For our environment, I would recommend a highly trusted CA to administer certificates. A few of highly known, high integrity commercial CA's to look at for our web server environment might be Symantec, Comodo or GoDaddy. For CA's that are servicing the OS mix internal to our network, we might want to look to vendor or OS recommended CA's for information protection.

For purposes of our environment, we will recommend and implement Digicert who was not listed above as one of the top 3 highly trusted CA's and here are the primary reasons why:

1. Digicert's primary business model is Digital Certificates

2. DigiCert assisted in the development of the Extended Validation Certificate, which provides enhanced identity verification of certificate holders.
3. DigiCert also worked in conjunction with Microsoft to develop and promote the use of subject alternate names in SSL certificates, for use with Microsoft Exchange Server.
4. DigiCert is the largest public CA that does not issue "domain validated", "low assurance", or "instant" SSL certificates either directly or through a subsidiary brand. It primarily sells Organization Validation (OV) and Enhanced Validation (EV) SSL certificates

As to how Certificates will be managed, distributed, issued, revoked and protected; With regard to digitally issued certificates specifically for protecting data that is transmitted via our web servers, we will employ Digicert's certificates in accordance with our Access Control and Data Integrity policies. Our IT staff will ensure proper processes are followed in implementing the digital certificates and maintaining their integrity in accordance with our standard operating procedures with regard to web server maintenance, patching and general upkeep.

We believe that this addition will serve to enhance our security posture in general, however we understand there are still significant risks should the Digicert solution become compromised. Hence we will have at the ready a second and third source that we can quickly deploy in the event Digicert should suffer an event that would put our architecture at risk. Furthermore, we intend to negotiate options and contractual "out clauses" in the event Digicert's technology is ever deemed unacceptable for our application.

RSA Encryption Technologies

We will look to add RSA Encryption functionality to key points of entry for both customers/patients and for providers/vendors and employees. We will recommend two separate keys – One for Patients and customers at a 2046 key length for strong encryption with minimal overhead and speed of use to get to data. For employees, vendors and service providers, we will recommend implementation of a 4096 key length RSA implementation.

Key assumptions:

1. Customers and Patient data and access, will be a less likely source of breach vector. Bad actors will most likely attempt to infiltrate and exploit vendor, employee and provider access privileges rather than one-off customer/patient access privileges. For purposes of providing a fast hand shake and good (limited latency) customer experience, the 2046 key length should provide strong data security without impacting the customer experience.
2. Because bad actors will target the vector that provides the deepest level of access to obtain the broadest access to information – they will likely target unsuspecting employees, vendors and service providers that instead of having access to one record, may have access to several if not all records. In this case, in the access conduit for these operatives, I would employ a 4096 key length to ensure that encryption key breakage is as difficult as possible at this stage.

In this model we believe it is imperative to provide at least a strong minimum level of protection to the lowest common denominator and provide strong assurance to customers that their data is protected and secured behind industry leading technologies. Further, I think the reasonable expectation of employees, vendors and providers is that data security is more crucial to business continuity, than is speed and convenience in this particular case, so if there is a latency or lag at the handshake stage, this should be an accepted “cost” of the proper secure solution.

We believe this approach will also signal to bad actors that they are going to have to find another vector to exploit in order to obtain access. In other words, hey this house has an alarm system, but that one across the street doesn’t. Maybe that other house is the better target.

Application of the Kerberos Server

In the current diagram of our network for the ACME insurance X, we have outlined, network security, physical security, data and application layer security, cryptographic and encryption security, perimeter security, DMZ security and have touched on policy related to enforcing secure methodologies across the environment. We have not specifically talked about client-server authentication. Here is where we would implement the Kerberos solution. Assuming that the environment is a windows based environment, Kerberos would be the standard “out-of-the-box” client-server authentication protocol of our entire environment.

As to where we would implement this solution in the environment – any point at which there is a client-server inter-relationship and access requirement or exchange element. For instance, when internal or external employees are accessing key network services – upon first interaction, username and password credentials would be required to gain access – these credentials would be validated and confirmed via the Kerberos function at the server level to authenticate appropriately.

With regards to a reliable key distribution server and its augmentation to satisfy critical controls that I’ve identified in module 3 – I believe Kerberos would serve to augment the NAC and Mobile NAC controls that were part of the module 3 network topography enhancement.

With regards to how Kerberos works – in short; A client authenticates itself to the Authentication Server which forwards the username to a KDC (Key Distribution Center). The KDC issues a “ticket” known as a TGT which is time stamped, encrypted and associated to the client machine. This TGT serves as “clearance” for the client system and serves as the authentication requirement. Typically there is a 4 step protocol process associated with Kerberos authentication:

1. User Client Based Logon
2. Client Authentication
3. Client Service Authorization
4. Client Service Request

In building this into the environment, the System Admin/Network Admin will need to open port 88 on the firewall appliance for UDP access and authentication to occur for remote users.

Kerberos implementation is fairly standard these days and I guess I had initially assumed in Assignment 3 that it would be part of the NAC and Mobile NAC implementation. While I am by no means a network or computer systems admin by trade, I know that in the last 15-20 years or so, Kerberos has been fairly standard as since the roll out of Windows 2000 it has been used as Windows default authentication method and many Unix and Unix-like operating systems have been including Kerberos authentication tools as part of their standard deployment packages.

Cryptography, Encryption and Cipher Blocks Application

In reviewing the configuration document that has been provided I believe the best and most effective places to implement Cypher Blocks and/or Encryption technology would first be at the data stores behind the firewall. Assuming that data that comes into the environment is captured and stored behind the firewall. In this instance, Corporate Data, User and Provider Data as well as Offsite Backup would all be recommended for AES/RSA level encryption/cipher blocks with a minimum of 128bit keying, but recommended 256+ bit keying on anything that would potentially recirculate out of the environment through day-to-day business or customer interaction.

Some of my initial assumptions with regard to the environment:

- Strong User Authentication Practices are in place
- Strong Policies and Procedures have been established regarding Access Control
- Strong Group Policies in place and monitored/audited on a regular basis
- Strong procedures are in place and regularly reviewed and enforced to ensure the environment is operating as it should and that operators are acting as they should
- Strong IDS/IPS is in place and these output logs are regularly reviewed by IT security staff and the IT leadership has an active disaster/breach plan at the ready
- All endpoints for remote workers and insiders are running a Top Tier AV solution
- All Servers and Endpoints have been and are regularly kept updated with the latest security patches
- Webservers are utilizing HTTPS for all data interactions beyond public marketing materials and messaging

Some of the initial assumptions around the “people” in the equation:

- With regards to Employees – Assumption is that they have been rigorously background checked at hire and since hire have received regular updated training around HIPAA requirements, basic cyber hygiene and standard operating procedures.
- With regard to Provider Operatives – Assumption is that there are strong contractual agreements in place between providers and entity, that specifically call out how data is to be handled, transported and stored – and that each employee of the Provider companies that have access to critical data have been made aware of the policies and procedures related to 3rd party data handling.
- With regards to customers – Assumption is that customers are inherent “risks”, in that they could be or could not be informed on our policies with regards to data handling and general cyber hygiene. Assumption is that they have scrolled through (without reading) our privacy and data handling policies made available on our website, and have merely “checked the box” at the end of the read acknowledging that they have seen/read and agree to our policies as such. I assume also, that in the spirit of “doing the right thing” by our customers that we have made available some basic information and training about the risks associated with their PII and have given them some basic cyber hygiene tips to consider when they are interfacing with us throughout the customer lifecycle. I’m assuming we have a webpage set up for them that an account manager directs them to when they become a customer of ours.

In this model, with the assumptions listed, we believe we have set up a secure environment, with appropriate gates and appropriate data protection measures, that leverage Cryptography technologies and solutions where best applicable and in the most cost effective manner.

Logon & Authentication of Users

One of the most fundamental elements of the ACME Insurance X organization's security strategy is verifying the identity of clients and granting them appropriate access to system resources based on their identity. By creating an authentication strategy for the ACME we will work to prevent attackers and malicious actors from accessing and tampering with sensitive information, consuming computing power or other system resources, and/or impersonating users in order to send misleading or incorrect information. In pursuit of this objective, we will work to develop an appropriate Authentication strategy by following the below 5 steps:

- Create a foundation for Authentication through Group, Administrative and User Access Policies
- Secure the Authentication Process
- Extend the Authentication Framework
- Enact & Enable Supplemental Authentication Strategies
- Educate Users

Further, we will follow best practices related to the following Authentication parameters:

- Central Administration of Accounts
- Single Sign-on Environment
- Accounts in AD (Computer and Service based)
- Certification
- Audit Authentication
- Kerberos Authentication Protocol

Summary & Conclusion

As we look to implement and maintain the infrastructure above for ACME Insurance X we will look to apply physical layer, data layer (in transit and at rest) and network layer security measures that will serve to harden our environment. The fact of the matter is that regardless of how many controls we put in place, we will never be able to guarantee 100% impervious security. We believe these measures will serve to better protect our network and data structures, and hence, give us the best opportunity to isolate, monitor and thwart potential breaches of data via network, systems or data hacking.