ABSTRACT

The protection of Critical Infrastructures (CIs) has become one of the most cutting-edge research areas in recent years. There has been considerable effort and expenditure since 9/11 on the protection of ‘Critical National Infrastructure’ against different attacks. This is because information is out of control of the owner. The traditional device-centric security systems are not efficient enough and information telecommunications services require security measures in three domains: information storage, processing and transmission.

We present the fundamental model components of critical control systems which manage most critical infrastructures. We address some of the security solutions to modern critical control systems followed by protection solutions that can be deployed to mitigate attacks exploiting these vulnerabilities.

KEYWORDS

Critical infrastructure; Security; ICT; Model

1 INTRODUCTION

For the past decades, the use and development of Information and Communication Technology (ICT) has improved the efficiency and flexibility in providing services and many organizations are increasingly relying on ICT which evidently handle the critical part of the organization’s core function. ICT can be defined as the convergence of telecommunications and computing’ [1] Due to the increased in speed and efficiency increasingly on electronic possesses where critical business services have migrated to technology that depends on internet services. [2] concluded that ICT benefits lie in the astonishing speed. For instance, teleconferencing in lieu of flights, digitization of goods and service, on a website in for of a catalogue to customers are ways ICT has changed businesses.

Enterprises and government agencies recognize that their internet services delivery assets must deliver value for money while keeping pace with the ever-increasing need for on demand information services. As ICT gains in popularity, information migrated off the premises is exposed to more threats that ever before. This is because information is out of control of the owner. The traditional device-centric security systems are not efficient enough and information telecommunications services required security measures in three known domains; data storage, processing and transmission. Data stored in the clouds and in storage devices requires a mechanism to protect it; data in transit need to be protected either at the service or transmission level while data
being processed needs to be protected during the processing stage.

With dominant presence of communication technology many critical pieces of organizational in fracture now rely heavily on complex interconnected communication systems which include interdependencies among physical and human component in infrastructure seem to be very strong and complex. Complex systems include but not limited to public and private infrastructures which contains nation. [3] argues that no complex system could exist solely physical or technical without human system could exist solely physical or technical without human factor(s). Human factors such as decision making influences the continuing operations and maintenance of any complex system. This paper presents the analysis of potential threats associated to critical information infrastructure (CI) through ICT services and proposes an on-demand security conceptual model. We firstly identify various threats relating to business CI. Out proposed method used a mathematical model with security policies.

The paper is structured as follows; Section II discusses background of CI and its associated threats. Section III describes our On-demand security conceptual model. Section IV proposed a solution to CIP threat using our method with security features. A summary in Section IV concludes the paper.

1.2 Background Of Critical Infrastructure Protection

Critical infrastructures (CIs) are technical systems that are important for our smoothing running of our day to day life CI comprises, but not limited to finances, energy, food supply, health; water, transport, telecommunication, education etc [4]. Each of these infrastructures on a greater or lesser extent rely heavily on critical information infrastructures for proper functioning and communication. These CIs are increasingly connected to the internet to provide benefits like; cost reduction, where large systems can be remotely managed over the public network, increase capability – by providing sufficient computing resources for infrastructure hardware with less capability power; improved efficiency and transaction speed.

However, the technology that underpins these capabilities may contain vulnerabilities that can be exploited Cyber threats pose a high risk on a nation’s complex information systems and cyber-based critical infrastructures. These threats have escalated in recent years and have become more sophisticated. Threats can extend through the interdependent infrastructures while posing unexpected and increasingly serious failures on essential services. Interdependence and interconnection of CIs [5], make them vulnerable to cyber attacks. Aim of many cyber attacks is to manipulate CIs. Attacking CIs can be performed in various ways, while distributed denial of services attack (DDoS) has become more prevalent in today’s cyber attack. For example, disruption within any communications technology that supports businesses could ripple up from the individual business and sector level to affect the national economy or incident that caused a major failure in CIs, such as the oil and gas, power or health sectors, could affect other sectors nationwide.

There are a number of documented security incidents where critical infrastructure control systems were adversely impacted. In the past, several Supervisory Control And Data Acquisition (SCADA) attacks have posed direct threats to businesses, health and safety. Of recent, several US back were attacked using distributed denial of service attack via wire payment to steal millions of dollars [6]. Similarly, Worcester attack of 1997 where a telephone network that services the airport, fire department and nuclear power plant was blocked [7]. Moreover, attack on businesses with multiple key dependencies and interdependencies could have a major impact
on the global economy, for example, Dow Jones computer glitch scenario that halts NASDAQ, while stock exchange abroad subsequently drops in value [8]. A persistent attack could impact the infrastructure that will be critical to public safety, national or economic security. In the realm of ICT Critical Infrastructure Protection (CIP) that contains Government sensitive data, such as Cyberspace, which depends on an interdependent network of critical physical and information infrastructures, if managed without a well-defined vision and strategy could prove costly and the effect might damage the ability of the government to protect the nation.

Various methods of cyber defense have been proposed.

### 1.3 On Demand Security Conceptual Model

We propose a method which uses mathematical model with necessary security policies, Figure 1. illustrates how a conceptual security model can be achieved in an ICT based telecommunications service environment using on demand security model.

![Figure 1. An on demand Security Conceptual Model for ICT-base telecommunications services](image)

Assume vectors as the security unit set. Let be $\bar{A}_1$, the security unit set of the transmission security domain $\bar{A}_2$, the security unit set of the processing security domain and $\bar{A}_3$ the security unit set of the storage security domain. $\bar{A}_1$, $\bar{A}_2$, and $\bar{A}_3$ are the subsets of $\bar{A}$; that is

$$\bar{A}_1 \subset \bar{A}, \bar{A}_2 \subset \bar{A}, \bar{A}_3 \subset \bar{A}$$  \hspace{1cm} (1)

Where $\vec{i}_1$, $\vec{i}_2$, and $\vec{i}_3$ and are the security parameter vectors of the security unit sets of the above three domains. The expression of these security parameter vectors is $\vec{i}_1 (x_1, x_2, x_3)$, where $x_1$ is service type, $x_2$ is site where the data is located and $x_3$ is the level of security.

On demand security for ICT based telecommunications service is computed as:
\[
\vec{A}_1 \times \vec{j}_1 \oplus \vec{A}_2 \times \vec{j}_2 \oplus \vec{A}_3 \times \vec{j}_3; \tag{2}
\]

Where equation 2 is the integration of the security solutions of three domains, and \( \oplus \) are the connectors.

The security units in \( \vec{A}_i \) are the security functions such as encryption, authentication and integration that were already realized by the ICT platform during the Research and Development R&D stage. \( \vec{j}_i \) are the security assessment models that should be implemented by Security Operation Center (SOC). In our proposed model, a security needs to configure 2 parameters namely: security location (\( x_2 \)) and service type (\( x_1 \)). The users configure the last parameter called the security requirement for a service (\( x_1 \)). These parameters are only Relevant to the service platform. Once a service and an ICT platform has been decided, \( x_1 \) and \( x_2 \) are determined and kept static, while \( x_3 \) is determined by the user requirements.

There are four benefits of this security domain division model. These includes:

- Only 3 types of parameters need to be configured, that is \( x_1, x_2, x_3 \). This made input of parameters manageable and configurable.

- Each security domain constructs its own policy model depending on its own security unit characteristics. Changes of \( \vec{j}_1 \) are independent from \( \vec{j}_2 \), and \( \vec{j}_3 \) that is \( \vec{j}_1, \vec{j}_2 \) and \( \vec{j}_3 \) are thoroughly decoupled. This simplifies the policy models and means they can be easily and accurately implemented.

- Only implementation of security unit technologies needs to be considered while execution is delegated to the policy model. In this way the development of security modules involved is made easier. Existing network, services, and storage can be used simply by adding a configuration interface open to the policy model.

- The execution result can be feedback to a charging center so that on-demand security of security as a service can be provided.

Fig. 2 below illustrates that application of the model in an ICT-based telecommunications service scenario. Alice, Bob, and George are employees at the same company. Alice is staying in a hotel during a business trip, and Bob and George are both in the office. Alice initiates a video call with Bob and a text conversation with George to discuss the market strategy for next year (which requires high level confidentiality). The cloud-based conference server chooses the appropriate security mechanism for Alice, Bob and George by acquiring the location indicator (can be determined from IP Address), service type indicator, and the security assurance level that Alice, George and Bob set beforehand.

The conference server chooses a stronger authentication mechanism for Alice because she is in a less secure environment than Bob and George. For Alice, authentication using a password and USB key is necessary, while for Bob and George, only a password is required. Considering the confidential nature of their meeting and the high security assurance level selected by all of them, at least 256 bits or stronger encryption key and Advanced Encryption Standard (AES) [10] encryption algorithm is needed. Data integrity protection is not applicable for communication between Alice and Bob so that high real-time performance can be achieved, but it should be applied between Bob and George to avoid the texts being tampered with. The security unit set in this case is the security capabilities supported by the cloud-based conference system.
A. Proposed Security On Stored Information
Consider a intermediate, in which it verifies account, resulting in a sequence of mappings between three connectivity above in figure (2). It starts with detail

Account (mid, name, year, information transmission, IP address) where mid means account identifier. The designer decides that only 3-account’ should be present in the IP database; we edit the table obtaining the following account and mapping:

\[
\text{ThreeClientsAccounts} (\text{Mid, name, year})
\]

\[
\pi_{\text{mid, name, year}} (\sigma_{\text{Verifying}} = 3 (\text{Accounts})) \subseteq \text{ThreeClientsAccounts}
\]  

(3)

To improve data and information transmission, we then splits the ThreeClientsAccounts into two groups, resulting in a new account and mapping

Names (mid, name)  Years (mid, year)

\[
\pi_{\text{mid, name, year}} (\sigma_{\text{Verifying}} = 3 (\text{Accounts})) \subseteq \text{Names} \triangleleft \text{Years}
\]

(4)

The intermediate map (3) and (4) to verify account from different clients

\[
\pi_{\text{mid, name}} (\sigma_{\text{Verifying}} = 3 (\text{Accounts})) \subseteq \text{Names}
\]  

\[
\pi_{\text{mid, year}} (\sigma_{\text{Verifying}} = 3 (\text{Accounts})) \subseteq \text{Years}
\]

With the mapping we can verify the data from accounts and reformulate authorizations to client with IP in the database by verifying what we trust.

B. Proposed Security Information On Processing and Transmision
Two common examples of hash functions are the Secure Hash Algorithm (SHA), commonly SHA-1, and Message-Digest algorithm 5 (MD5). SHA-1 is used in many common security applications including SSL, TLS, S/MIME and IPSec. MD5 is generally used to create a digital fingerprint for verifying file integrity [8].

So symmetric is fast, but exchanging keys is a problem; and asymmetric has more security services, but it’s slow. The solution: Combine them in a hybrid system. This is what is done in the digital-certificate-based crypto systems that are in common use for e-mail, IM and SSL Web traffic. The basic idea is to use an
asymmetric system, as is done with Diffie-Hellman key exchange, to exchange a symmetric key to do the bulk of the data encryption. The popular examples of hashing functions [9] found to be used in different places are HMAC, MD5, SHA-1.

We present our approach with correlation to figure (2) above for information processing and transformation between three parties (Alice, in Hotel, Bob, in office and George, in office) that cryptographic system use hash functions. A hash function \( H \) maps a long text \( P \) into a shorter text \( H(P) \). For instance, \( P \) might be 1000 bits long and \( H(P) \) only 160 bits long. Thus, \( H(.) \) is many-to-one function: Many to different texts \( P \) result in the same \( H(P) \).

A Hash function must be difficult (computationally) to pseudo-invert. That is, given \( M \) it is very difficult to construct a text \( p \) such that \( H(p') = M \). Depending of the application, the additional properties may be required:

**Property 1:** Given both \( P \) and \( H(P) \) it is difficult to construct \( p' \neq p \) such that \( H(p') = H(P) \). This condition is stronger than the previously one because knowing both \( p \) and \( H(P) \) may make it easier to construct \( p' \) than if only \( H(P) \) in known.

**Property 2:** It is difficult to construct two texts \( p \) and \( p' \neq p \) such that \( H(p) = H(p') \)

**Property 3:** Given \( P \) but not knowing a string \( K \) it’s difficult to find \( p' \neq p \) Such that \( H(k \circ p) = H(k \circ p') \).

In this notation, \( k \circ . \) means the concatenation of two strings \( K \) and \( P \), that is, the bits of \( K \) followed by the bits of \( P \). ( For Instance,10011 \( \circ 011101 = 10011011101 \.)

Our discussion of security on information transmission above indicates which properties are required of \( H \). Hash functions are primarily used to generate fixed-length output data that acts as a shortened reference to the original data. This is useful when the output data is too cumbersome to use in its entirety. One practical use is a data structure called a hash table where the data is stored associatively. Searching for a person’s name in a list is slow, but the hashed value can be used to store a reference to the original data and retrieve constant time (barring collisions).

2 CONCLUSION

The world has changed. Governments are actively acquiring cyber-weapons, and this means that adequate means of protection are needed in response. Still, despite the fact that key information infrastructure is extremely important; there exists today no means to properly safeguard it. The solution proposed stresses upon applying hashing techniques not only in prevention stage in the form of data storage and information authentication, but also in different stages of processing and transmission. The efforts can be made in the direction of improving hash functions to avoid collisions, using stronger hash keys by making them dependent on additional parameters like biometric credentials, passwords, IP addresses etc. The hash techniques can also be tried for keeping the link status of the network. The paper also proposed the conceptual model with at least four overall advantages to security domain division.

3 REFERENCES


R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.


B. Arun, Security in Ad-hoc Networks, Computer Science Department. University of Kentucky, Sited on September 2013 from people.du.ac.in/~vmadan/resources/research/Hashing_PaperDoc.doc