Attacks and Security

Hanmankar Sneha Rao[1] Romil Dodhiwala[2]
[1,2]Department of Information Technology
[1,2]Atharva College of Engineering

Abstract— In order to ensure protection to a system, in this paper it is discussed on introduction of control system and other methodologies to regulate privacy policies , but often it is subjected to privacy issues, safety risks, loss of data , intervention and malicious attacks, spy , intrusions. Most of the cases security is compromised as the programs are complicated, expensive. Thus, once vulnerability is detected, the attacker may launch shots and affect the overall system leading to irreparable, unrecoverable damages in few cases. This paper, discusses the need of security, issues due to unauthorized access its effects, inadequate security and requirements and current scenario.

Key words: Attacks, Security

I. INTRODUCTION

The Information Technology (IT) world has been dealing with the security problem for approximately two decades. Many organizations have been involved with this issue. "British Standard 7799", first published in February1995, is a code of practice for information security management and a specification for an Information Security Management System (ISMS). BSI 7799 has become ISO/IEC 17799, a standard code of practice, and a comprehensive catalogue of security practices. Many intellectual successes concerned to security have been there, notable among them are the subject/object access matrix model , access control lists, multilevel security using information flow and the star-property, public key cryptography, and cryptographic protocols. Although these successes, security of the hundreds of millions of deployed computer systems is terrible: a determined and competent, attacker could destroy or steal most of the information on almost any of these systems. The easiest way to break into a system is to bribe an insider. This short paper, however, is limited to computer systems.

As the digital infrastructure is increasingly getting complex there is growing difficulty in achieving security exponentially. Web applications are subjected to plethora attacks such as cross site scripting, cookie theft, browser hijacking, self-propagating worms. Thus there is a need of secure web application, need of considerate SDLC secure programs

People live with such poor security; suffer loss in real world systems. The reason is that security is not about perfect defenses against determined attackers. Instead, it's about value, locks, and punishment.

The purpose of locks is not to provide absolute security, but to prevent casual intrusion by raising the threshold for a break-in, but perfect defenses simply cost too much. Furthermore, computer security has been regarded as an offshoot of communication security, which is based on cryptography. Since cryptography can be nearly perfect, it's natural to think that computer security can be as well but it ignores two critical facts:

- Secure systems are complicated, hence imperfect.
- Security gets in the way of other things you want.

Software is complicated, and it's essential to make it perfect. Even worse, security is set up by establishing user accounts and passwords, access control lists on resources, and trust relationships between organizations. In a world of legacy hardware and software, Networked computers, mobile code, and constantly changing relationships between organizations, setup gets complicated. Hybrid networks continue to form in the industrialized world. However, today the connection of devices using Ethernet technology is increasingly being adopted. Consequently, interfacing of industrial equipment is much easier, but there is now significantly less isolation and natural security protection. In order to understand the threats inherent in networking these computer systems, an awareness of networking basics is required. Communications over Ethernet use TCP/IP to identify nodes and ports to identify processes running on these nodes. Company networks, or intranets, are strung together using hubs, switches and routers.

This paper tries bring together the comparative study in brimming the security policies , making it more firm against varied type of attacks, loopholes, limitations and discuss the subjects involved in the different approaches.

This paper is structured as follows: Section 2 gives literature survey of different policies that have been put forth in the recent research papers. Section 3 is the comparative study of the suggested developments. Section 4 presents the overview of related work, other options and finally concludes the discussion.

In the next section we are going to discuss the suggestions put forth in following papers.

II. LITERATURE REVIEW

Most Personal computers (PC) can be "hacked" by intrusion readily available tools that identify vulnerable programs running on the target PC. An open port is one that has a listening application running on the machine. An example of this is a service called "NetBIOS", or Network Basic Input Output System. It is an Application Programming Interface (API) that allows client software access to LAN resources. NetBIOS can be used to either tie up (Denial of Service or DoS) or access a computer's resources. Security is compromised and loosened because systems are complicated, and therefore both the code and the setup

have bugs that an attacker can exploit, but it is not the heart of the problem. If there are some major security catastrophes, buyers will change their priorities and systems will become more secure. Short of that, the best we can do is to drastically simplify the parts of systems that have to do with security:

- Users need to have at most three categories for authorization: me, my group or company, and the world.
- Administrators need to write policies that control security.
- Everyone needs a uniform way to do end-to-end authentication and authorization across the entire Internet.

Since people would rather have features than security, most of these things are unlikely to happen. In reality security depends more on police than on locks, so detecting attacks, recovering from them, and punishing the bad guys are more important than prevention.

A. Security Vulnerabilities Of Today's Industrial Control Networks

In the paper [1], methods are presented to reduce, determine vulnerabilities by conducting a thorough assessment of process control network, evaluate risks, procedural counter measures to tackle with them. The ISA Security Life Cycle Model is a fifteen-step process that covers all areas of security management. The main focus of the assessment procedure can be found in step 2 and 3 of the ISA Security model namely to "Assess and Define Existing System" and "Conduct Risk Assessment and Gap Analysis".

Producing a human assessment, device inventory and network diagram is the first step. Development of sensitive assessment tools that can gather the required information are then entered into a database, analyzed and then compared to industry. Assessment involves surveying key employees in the operation of security of the control network. General understanding of security policies is to protect from attacks. Study of current security system architecture, remote connection of the control system devices. This information is then transferred to project database. Inventory of network controlled devices must be developed to complete assessment of database. Vulnerability Assessment scanning tools, widely used by IT administrators, determine if devices attached to the network are correctly configured and patched. Device assessment investigates the network devices. In the project database, data is analyzes, report is created outline the areas of both compliance and concern. Recommendations out of the analysis are identified and the gap is filled with proposed solutions. To provide plant floor security we implant security policies, network architecture, and system hardening. Network Architecture-it consists of the basic network diagram consisting of network connectivity and configuration data. Device assessment involves identifying the device connections.

Protective measures involves system hardening that means tightening the system security to avoid the attacks by hackers, viruses by removing unnecessary open ports.

Remote connections-remote access software is used to connect remote users to the process control machine, this involves use of passwords and data encryption. This involves a key fob that displays a new 6-digit code that changes every sixty seconds. This code is combined with the password to authenticate the user to the system. Furthermore, some form of central logging and administration of these connections should be implemented.

In the next section we briefly outline the ways of adopting security policy, mechanism is planned and assurances also discuss the flaws that were proposed by Butler W. Lampson Microsoft in the Computer Security in the Real World

B. Internet-Wide End-to-End Authentication and Authorization-

Instead of constant efforts to provide secrecy, integrity, and availability, implemented by access attacks take place endangering computer systems.

1) Policy: Specifying Security

People working under a domain may define their needs for security under 4 major headings

- Secrecy
- Integrity
- Availability
- Accountability

The most important dangers to information having loosened security is vandalism or sabotage. Policy for security is usually levied from the policy for security systems that do not involves computers. Military, defenses are concerned with integrity, secrecy, industries and organizations with accountability, integrity and telephone companies with availability. A secrecy policy has both positive and negative aspects Thus it is primarily understood that only authorized employees should have access to the information others should not have.

2) Mechanism: Implementing Security

One man's policy is another man's mechanism. Confidential information and the set of properly authorized employees must be described precisely. The implementation of security has two parts: the code and the setup or configuration. The code is the programs in the trusted computing base. The setup is all the data that controls the operations of these programs: access control lists, group memberships, user passwords or encryption keys, etc.

The job of a security implementation is to defend against vulnerabilities i.e.to provide

- Isolation. It provides the best security; it is impractical for all but a few applications.
- Code signing and firewalls do this.
- Sandboxing typically involves access control on resources to define the holes in the sandbox. Programs accessible from the sandbox must be paranoid
- Catch the bad guys and prosecute them. Auditing and police do this.

Auditing is necessary to ensure that no unintended access where made, it is used for maintaining the accountability of the users.

The well-known *access control* model provides the framework for these strategies. It consists of guard controls which are usually encapsulated in objects. Here in the paper proposed is access model which provides framework for security policies. It consists of guard who controls the access to a particular resource for a request made which are usually encapsulated in objects. Thus the guard decides whether to allow the source perform operation or not. The guard is separated from the object to keep the configuration simple. Another model is sometimes used when secrecy in the face of bad programs is a primary concern: the *information flow control* model [6, 13]. This is roughly a dual of the access control model, in which the guard decides whether information can flow to a principal.

3) Assurance: Making Security Work

To make security work the answer is based on the idea of a *trusted computing base* (TCB), the collection of hardware, software, and setup information on which the security of a system depends.

- It may act as a firewall allowing access to web but not to other internet services, inward access, browser code, hardware.

The idea of a TCB is closely related to the end-to-end just as reliability depends only on the ends, security depends only on the TCB.

In both cases, performance and availability isn't guaranteed. In general, it's not easy to figure out what is in the TCB for a given security policy. A good way to make defects in the TCB less harmful is to use *defense in depth*, redundant mechanisms for security. TCB is all the *setup* or configuration information, the knobs and switches that tell the software what to do. Although set up is simpler than codes but still complicated, usually done by less skilled people, code written once, but setups are different for every installation. It is usually voluminous, obscure and incomplete at its best. Developers need a type-safe language like Java; this will eliminate a lot of bugs.

4) End-To-End Access Control

Secure distributed systems need a way to handle authentication and authorization uniformly throughout the Internet. In this section we first explain how security is done locally today, and then describe the principles that underlie a uniform end-to-end scheme.

a) Local Access Control

Most existing systems do authentication and authorization locally and group membership, and a local database of authorization information, usually in the form of an access control list (ACL) on each resource. In these systems access control works like this:

- It's assumed that the channel on which the user communicates with the system is secure,
- The system has a local database of user names and passwords. Usually it stores an internal security identifier (SID) for each user and group as well.
- The user authenticates the channel by sending a password response to the system. This is called "logging in". After verifying, the system creates a process for the user, attaches it to the channel, and assigns the user and group SIDs.
- Each resource object has an ACL that is a list of SIDs along with the access each one is permitted. Each system in the domain has a secure channel to the controller, implemented by a shared key to encrypts messages between the two; this key is set up when the system joins the domain. To authenticate the user to another system in the domain, the login system can ask the controller to forward the authentication to the target system. Authentication to another domain works the same way, except that there is another level of indirection through the target domain's controller. A shared key between the two domains secures this channel. A further extension organizes the domains in a tree. Unless the domains trust each other completely, each one should have its own space of SIDs and should only be trusted to assign its own SIDs to a user.

b) Distributed Access Control

Distributed systems involve different organizations and are managed differently. To do access control cleanly in such a system we need a way to treat uniformly all the items of information that contribute to the decision to grant or deny access. Authenticated session keys. User passwords or public keys. Delegations from one system to another Group memberships. ACL entries. We want to do a number of things with this information:

- Keep track of how secure channels are authenticated, whether by passwords, smart cards, or systems.
- Handle authorization via ACLs.
- Record the reasons for an access control decision so that it can be audited later.

c) Chains of responsibility

There is a chain of responsibility running from the request at one end to the resource at the other.

C. Black list-Using Web Crawler

Web is a open platform where everyday many users create web pages at a daunting pace. Attackers are relentlessly hunting for such vulnerable hosts, inexperienced people who can be exploited and be leveraged to store malicious web pages and then accumulate them in the malicious meshes to trap the users. Thus to protect the users it becomes necessary to take these web pages-

- Blacklist- It prevents users from accessing these malicious web pages. It has emerged as a popular defense tool and gain support of all major browsers and antivirus vendors. This is a 3 step process-Firstly the URLs are collected using crawlers, quickly inspected with a fast filter and finally examined in depth using specialized analyzer. The number of pages it may return might be too large for in depth analysis. This in turn requires a prefilter to discard pages that are very

likely to be legitimate. These prefilters examine the state, properties of the webpage URLs. It uses static or dynamic analysis techniques to examine HTML content of a page as well as its active elements. It may also look for changes to the persistent state of the OS once a page has been loaded. This approach to improve the efficiency of the searching process of malicious webpage uses a tool called ËVIL SEED.

– EVIL SEED- It is similar to blacklist. Evil seed is a 3 step process –firstly crawl to collect URLs, apply fast prefilters, use precise but slow oracle to classify the remaining pages. It improves the webcrawl phase. This is guided search. It analyzes them, thus leading to find more such likely malicious pages. This is advantageous for search engines. Thus, applying the EVILSEED, protecting users of the engines becomes easier. The cyber criminals search for such vulnerable patterns of the web pages and exploit them by injecting malicious codes into their pages using toolkit to create attack pages by linking many pages to a single malicious page. There are dataset tools available to the malicious URLs, as search engines indexed large portions of web that keeps the web up to date by using good crawler information structure.

1) Evilseed Architecture

The core of this system is the set of gadgets. These gadgets consume as feed of the malicious webpage and produce queries for the search engines then forward to the analysis infrastructure. The goal of a gadget is to leverage a set of known, malicious web pages to guide the search for additional, malicious content on the web. Gadgets find candidate pages that are likely to be malicious based on the pages likely that are contained in the seed. Seed is a set of malicious pages that are to the gadgets. Queries to the search engine can be simple search for words or related terms. Oracle consists of 3 components Google safe browsing blacklist, We pawet, custom built tool to detect site that host fake AV tools.

– Google safe browsing blacklist creates and makes available a "constantly updated blacklist of suspected phishing and malware pages."
– We pawet is a client honey pot. It uses anomaly based technique to detect drive by download attacks.
– AV host – it is a detector to webpage it hosts fake antivirus software, this informs uses about the security of their computers and deceives them into downloading rogue security software.

Guided search approach is tool effective search for malicious pages is validate and does in an efficient manner by use of 2 key metrics-1) Toxicity 2) Expansion.

D. Computer Security and Privacy- in Multiprogrammed, Time Sharing Systems

With computer systems came the advent of sharing resources, networking, this leads to leakage of information, risk of espionage attacks to penetrate the computer systems containing confidential, classified information by the competitors. Thus here an overview of the technological aspects to the problems faced and possible approaches to safeguard systems are discussed.

Privacy is defined as isolation, seclusion, or freedom from unauthorized oversight or observation. Thus we will have close observation of the vulnerabilities of highly important system their configuration that may become a point for leakage of information. Thus paper tries to bring to the notice the ways in which the information can be divulged in multisharing systems-

– Hardware configuration of a system consists of central processor attached to files and communication links for networking. These files contains different levels of information of sensitivity, central processor is a combination of hardware and software components. These may fail in cases and may leak to improper destinations. Since the processor consists of the high speed electronic circuits, large electromagnetic energy will be radiated, conceivably leading to eave dropping third property. Software failures will lead to disabled access control, routing information, memory bound control.

By making use of wiretapping method, cross talks the information can be stealed from the lines of communication links. Thus the users of the system, the central processor must make certain in identifying with whom to converse, to identify, verify, configure, authenticate the user.

Succeeding discussions are put forward as –

1) It needs to be noted that privacy problem is to some extent prevailed wherever sharing structures, resources takes place.
2) A program is not executed without interruption, central as storages and other levels of external peripherals. Thus unless a computer is completely stripped off the programs, this means clearing or removing access to all levels of storage – privacy infractions may take place.

Thus to control user access in resource sharing one time passwords can be used to identify and authenticate the users.

1) To have serious legal liabilities for unauthorized leaking of confidential information. In file access and protection not all users are authorized
2) To access all files, hence there must be some combinations of hardware and software to control access to the online classification files in conformation with security levels.
3) Having a certifying authority. It is easy to demonstrate that a large computer programs have huge number of internal paths, that means existence of error conditions.
4) Monitor programs for internal scheduling and multiprogramming , time sharing, batch operated machines are likely to be extensive and complex, thus we aborted to certify that monitor programs are properly programmed and checked out.

E. Client Side and Server Side Defenses

The paper[7] discusses the end-to end argument that the client and server must collaborate to achieve security goals, to eliminate common security exploits, and to secure the emerging class of rich, cross domain Web applications referred to as Web 2.0. Thus Mutation-Event Transforms:

An easy-to-use client-side mechanism that can be used that requires only straightforward changes to existing Web browsers.

Script injection are by far the most prominent and is used in cross-site scripting [9] and Web application worms. A script injection vulnerability may be present whenever a Web application includes data of uncertain origin in its Web pages;

Measures needs to be taken by both server and client side but the corresponding server-side checks are difficult to perform and, in practice, incomplete in ways that enable attacks. However for web developments tools and methodologies are bought for server side security along with this the server must correctly model complex, dynamic client activities such as string manipulation, and take into account all possible client features and bugs. This entails server consideration of a myriad different tags, encodings, and operators for comments and quoting.

At the client side security enforcement through a new client mechanism: Mutation-Event Transforms, or METs. At runtime, and during initial loading, these MET functions are invoked by the client on each Web page modification to ensure the page always conforms to the security policy. *Mutation events* are defined in the proposed Document

Object Model [8], level-2, as events caused by any action that modifies the document structure. METs are similar to, but simpler than, these standards proposals. METs are also more expressive since they operate on extended data that include both the standard DOM tree model and the abstract syntax trees (ASTs) of executable scripts.

From the paper [5] discussions put forth are as- Web applications have quickly become the most dominant way to provide access to online services. In this paper, some common aspects of client side attacks against web applications and present two simple techniques that can be used by web applications to enable secure input are discussed. The main advantage of our solutions is that they do not require any installation or configuration on the user's machine.

Client side attacks takes place in three phases-it involves installing the malware at the users computer , the malware then monitors clients interaction, once a detects security critical attempts it tries divulgence of the information.

Web attacks have been ranging from simple phishing to sophisticated attacks involving installation of Trojan horses which are also called as drive by attacks. Thus it becomes necessary to ensure security to the user of the web application running on an untrusted platform. Although the communication between the web client and the web applications are encrypted using Transport Layer Security (TLS) to thwart sniffing and man-in-the-middle attacks, the web client is the weakest point in the chain of communication where Trojan horse can install itself as a browser plugin and then easily access, control, and manipulate all sensitive information that flows through the browser. Numbers of solutions have been proposed to date to enable secure input on untrusted platforms for web-based applications. The majorities of these solutions are hardware based and require integrated or external peripheral devices such as smart-card readers or mobile phones. Such hardware-based solutions have several disadvantages. Solutions to this posed in- Secure Input for Web Applications [10] is that they do not require any installation or configuration on the user's machine. Additionally, in order to evaluate the feasibility of proposed techniques for mainstream deployment, studies are conducted for ensuring their usability.

F. TAN

Transaction numbers are mostly used during online banking transactions. These are randomly generated numbers .They have one time use, so only knowing the users name and password is not enough for attacker and attacker has no access to TAN list. Unfortunately, TAN-based schemes are easily defeated when an attacker performs a client-side attack. Furthermore, such schemes are also vulnerable to phishing attempts in which victims are prompted to provide one (or more) TAN numbers on the phishing page. The problem with regular transactions numbers is that there is no relationship between the data that is sent to the web application and the TANs. Thus, when the bank requests a certain TAN, malicious code can replace the user's input without invalidating this transaction number. To mitigate this weakness and to enforce integrity of the transmitted information, we propose to bind the information that the user wants to send to our confirmation token.

Note that when using confirmation tokens, our focus is not the protection of the confidentiality, but the integrity of this sensitive information. Another possibility to circumvent our schemes is trying to guess the right confirmation token.

G. Captcha

Graphical input is used by some banks and other institutions to prevent eavesdropping of passwords or PINs. Instead of using the keyboard to enter sensitive information, an image of a keypad is displayed, and the user enters data by clicking on the corresponding places in the image. The basic idea of the second solution is to extend graphical input with CAPTCHAs [12]. A CAPTCHA, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, is used in computing to determine whether or not the user is human. Hence, a CAPTCHA test needs to be solvable by humans, but not solvable for computer applications. CAPTCHAs are widely employed for protecting online services against automated (mis)use by malicious programs or scripts. An important characteristic of a CAPTCHA is that it has to be resistant to attacks. That is, it should not be possible for an algorithm to automatically solve the CAPTCHA.

Graphical CAPTCHAs, specifically, need to be resistant to optical character recognition [13]. OCR is used to translate images of handwritten or typewritten text into machine editable text. To defeat OCR, CAPTCHAs generally use background clutter (e.g., thin lines, colors, etc.), a large range of fonts, and image transformations. Such properties have been shown to make OCR analysis difficult. Usually, the algorithm used to create a CAPTCHA is made public CAPTCHA algorithms [11] are still considered resistant against OCR and are currently being widely used by companies such as Yahoo and Google.

III. COMPARATIVE STUDY

It can be generalized from many discussions prevailed from the significant research papers and may agree upon having the following setup—

- Being preventive rather than being curative.-user authentication.
- Establishing secure connection, adopting full proof security policies, abiding by strict rules and regulations for cyber security.
- Spot and remove the threats , raise the alarm.-certifying the hardware and software.
- Encipherment of the information using secured keys.
- Use of FTP for file sharing across firewalls . Use of Captcha for protecting online services against automated malicious programs and scripts.
- Enforce more research in the area of different security measures.
- Carry out periodic IT security checks, audit trails, improve security infrastructure,
- GOVT. may appoint CISO for security administration. In EVIL SEED approach it is founded that attackers might prevent crawlers for searching malicious pages and can even try attacking the detection technique such as oracle. Thus we need to rethink over performance, scalability, evasion, proper gadget selection.

This paper reviews the different views offered to build a concrete security policy and make it reliable for its users. Thus there are many ideas that can be used for security assessments, by using different proposed techniques, implementing policies, introducing IDS to study behavior of the attacks, optimize performance. One of the important technique for security information is enciphering by using keys that are made available only to authorized users, but problem is in communicating with these keys. Strategies are involved securing multimode computers using enciphering is a topic under research and also finding techniques of enciphering and deciphering is a subject for research.

IV. CONCLUSION

With the advancement there is always need for research improvement. Thus to each threat finding new solutions is needed at a faster rate. It is posed that true computer security is impractical. This is due to wrong perception and improper failure analysis programs. There is a need to provide the security to the systems to defend various cyber-attacks, computer viruses, many techniques have been proposed which includes cryptography, firewalls, IDS, among which IDS has been more promising for defending complex and dynamic intrusions and behavior. SQL injection is an old approach but still popular amongst the attackers. In an attempt to prevent script injection, most Web application servers try to carefully filter out scripts from untrusted data. As cyber security policy is evolving it needs to be regularly updated/refined in line with technological trends and security challenges posed by such technology directions. Cyber security needs to be dynamic in nature and have necessary depth to detect, stop and prevent attacks. Security needs to be built-in from the conceptual design stage itself when it comes to developing and deploying critical information infrastructure, as opposed to having security as an afterthought. The effectiveness of cyber defense lies in the proactive nature of security counter measures as well as in ensuring resilience and continuity of operations, despite the possibilities of successful attacks. Thus it can be concluded that with growing technologies, problems too grow and to this problems solutions are there and these needs to be found and bought to notice to provide security.

ACKNOWLEDGEMENT

Our sincere thanks to the technology that allowed us in doing this short review by providing relevant materials from different authors research papers. We would like to thank Mr. Sunil Rane sir for conducting this conference and giving us opportunity to present this. We would like to express my heart-felt gratitude towards our teachers, parents and all those who encouraged us to accomplish and supported us in our work.

REFERENCES

[1] A. Creery, P.Eng.P.E.,E.J.Byres,P.Eng.Industrial Cyber Security for Power System and SCADA Networks. Paper No. PCIC-200DV45
[2] Butler W. Lampson1Microsoft on Computer Security in the Real World
[3] Luca Invernizzi,Christopher Kruegel,Paolo Milani Comparetti,Stefano Benvenuti on EVILSEED: A Guided Approach to Finding MaliciousWeb Pages
[4] Willis H. Ware on Security and privacy in computer Systems– APRIL 1967
[5] Martin Szydlowski, Christopher Kruegel, Engin Kirda on Secure Input for Web Applications
[6] Department of Information Technology Ministry of Communications and Information Technology on National Cyber Security Policy
[7] U´ lfar Erlingsson,Benjamin Livshits,Microsoft ResearchYinglian Xie òn End-to-end Web Application Security.
[8] T. Pixley. DOM level 2 events specification. http://www. w3.org/TR/DOM-Level-2-Events, 2000.
[9] CGI Security. The cross-site scripting FAQ. http://www. cgisecurity.net/articles/xss-faq.shtml.
[10] N. Chou, R. Ledesma, Y. Teraguchi, and J. C. Mitchell. Client-side defense against web-based identity theft. In Proceedings of the Network and Distributed Systems Security (NDSS), 2004.
[11] S. Hocevar. PWNtcha - Captcha Decoder. http://sam. zoy.org/pwntcha.
[12] S.Mori, C. Y. Suen, and K. Yamamoto. Historical review of OCR research and development. Document image analysis,pages 244–273,1995.
[13] CarnegieMellonUniversity. The CAPTCHA Project. http://www.captcha.net