ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 253 – 258 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

Resistant Protocol To Resist Large-Scale Online Password Guessing Attacks

Mohd Muzaffaaruddin Arshad,
Student M.Tech (CSE),
Nizam Institute of Engg & Tech,
Deshmukhi Village, Nalgonda Dist.
muzafferuddin21@gmail.com

Ayesha Siddiqua,
Head of the Department (CSE),
Green Fort Engineering College,
Bandlaguda, Hyderabad.
ayesha19in@gmail.com

Ishrath Nousheen
Student M.Tech (CSE),
Nizam Institute of Engg & Tech,
Deshmukhi Village Nalgonda Dist
ishrathnouseen@yahoo.com

ABSTRACT:

Passwords, passphrases and security codes are used in virtually every interaction between users and information systems. Unfortunately, with such a central role in security, easily guessed passwords are often the weakest link. They grant attackers access to system resources; and bring them significantly closer to being able to access other accounts, nearby machines, and perhaps even administrative privileges. The purpose of this research is to introduce the concept and methodology, follow it by some real-life examples, and scare organizations into implementing stronger password policies. Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. We proposes a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts to as low as a single attempt per username, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT.

Key words: online password attack, password guessing resistant protocol, security policies & password strengths.

----------♦♦♦♦----------

1 INTRODUCTION

Passwords are sequences of symbols usually associated with a user name. The combination provides a mechanism for identification and authentication of a particular user. If all was right with the world, they would be more or less unique and grant privileges only to the account's owner (or other intended user). Alas, the world is not all right.

Attackers have several venues of guessing passwords and overcoming this obstacle. Fairly low on the difficulty scale, we have attacks against default passwords. These are established by the vendor and built into many applications and operating systems, allowing attackers an almost effortless point of entry. The vulnerability exists because overworked, uninformed, or lazy administrators fail to change them; and crackers maintain large databases. Exploits of this nature are easy to implement and either succeed or fail within a matter of seconds (or probably longer if the target device must be identified first, for an example database of default passwords) [9].

1.2 Organization

Section 2 discusses related work on prevention techniques for online password attacks. Section 3 presents the PGRP login protocol. Section 4 discuss about security analysis that memorized password. Section 5, we evaluate risk assessment hackatism. Section concludes.

2 RELATED WORKS

Although online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. Account locking is a customary mechanism to prevent an adversary from attempting multiple passwords for a particular username. Although locking is generally temporary, the adversary can mount a DoS attack by making enough failed login attempts to lock a particular account. Delaying server response after receiving user credentials, whether the password is correct or incorrect, prevents the adversary from attempting a large number of passwords in a reasonable amount of time for a particular username. However, for adversaries with access to a large number of machines (e.g., a botnet), this mechanism is ineffective. Similarly, prevention techniques that rely on requesting the user machine to perform extra nontrivial computation prior to replying to the entered credentials are not effective with such adversaries.

3. PASSWORDS GUESSING RESISTANT PROTOCOL

3.1 Goals And Overview

3.1.1 Goals: Our Goals For PGRP Include The Following:

1. Applicability to web and text logins: PGRP is not limited to web-only login (unlike proposals solely relying on browser cookies), as it uses IP address and/or other

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 253 – 258 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

methods to identify a remote machine in addition to optionally using cookies. By using text-based ATTs (e.g., textcaptcha.com), SSH login can be adapted to use PGRP.

2. Through automated programs, brute force mechanisms, and low paid workers (e.g., Amazon Mechanical Turk). Incidents of attackers using IP addresses of known machines and cookie theft for targeted password guessing are also assumed to be minimal.

3. Traditional password-based authentication is not suitable for any untrusted environment (e.g., a key logger may record all keystrokes, including passwords in a system, and forward those to a remote attacker). We do not prevent existing such attacks in untrusted environments, and thus essentially assume any machines that legitimate users use for login are trustworthy.

4. The data integrity of cookies must be protected (e.g., by a MAC using a key known only to the login server)

3.1.2 Overview

The general idea behind PGRP is that except for the following two cases, all remote hosts must correctly answer an ATT challenge prior to being informed whether access is granted or the login attempt is unsuccessful:

1) When the number of failed login attempts for a given username is very small; and

2) When the remote host has successfully logged in using the same username in the past (however, such a host must pass an ATT challenge if it generates more failed login attempts than a prespecified threshold). In contrast to previous protocols, PGRP uses either IP addresses, cookies, or both to identify machines from which users have been successfully authenticated.

2.2 Web Cookies Versus IP Addresses

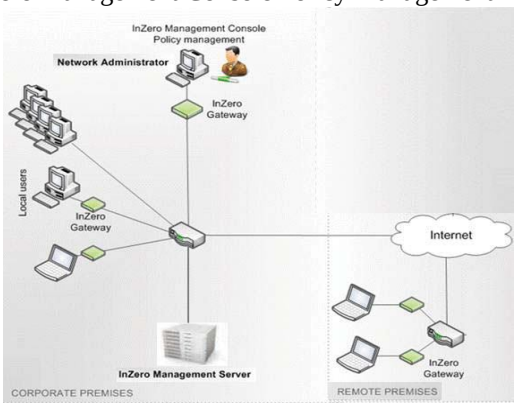
2.2.1 Inzero System FIPS 140-2 Security Policy

This document describes the non-proprietary security policy for the InZero® Gateway XB2CUSB3.1 Series Cryptographic Module, subsequently referred to as *FIPS module*, *Gateway module*, *module*, or *Gateway*. InZero also sells a standard (not FIPS capable) InZero Gateway XB2CUSB3.1 device with different firmware and a similar enclosure. The FIPS module can be identified by the firmware version and presence of four tamper evident seals and an opacity shield covering the air vents. The rest of this document pertains only to the FIPS module[17].

2.2.2 Inzero Security Platform Architecture

The InZero Security Platform provides centralized management for multiple Gateways. The following figure shows the components of the InZero Security Platform for a small security domain. Network administrators install the InZero Management Console software on their PCs and use the Management Console software to configure Gateways, Policies, and Virtual Private Networks (VPNs). These administrative settings are stored on an InZero Management Server, which makes the settings available for Gateways to download.

Fig:1
Inzero Management Console Policy Management



2.2.2.1 Module Overview

The Gateway module protects against classes of malware attacks (known and unknown) and controls User and application network activity. It provides the following

Table: 1
Authentication Mechanism

Authentication Mechanism	Assumptions	Strength of Mechanism	To Increase Strength
Password-based (Operator)	• Six random lowercase characters (User)	1 in 26^6 (one in 308 million is stronger than one per million)	• Use longer password • Use mixed case, numeric and punctuation
Certificate-based	• Minimum RSA key size of 1024 bits provides 80 bits strength	1 in 2^{80} (one in a 2^{80} is stronger than one per million)	• Use 2048-bit keys (112 bits strength)

Services: Hardware-enforced Application Sandbox provides a safe environment for opening dangerous content

• Firewall provides Network Access Control and limits propagation of malware

• Mail and web proxy services filter network data according to policy

• File conversion mechanism creates a sanitized copy of a malicious file

• Flexible management solutions (standalone, member of domain).

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 253 – 258 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

Fig: 2 Gateway Modules

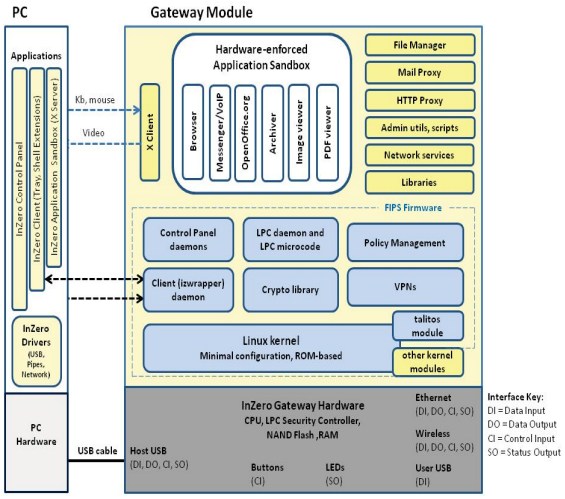


Table: 2 Types of Authentications

Role	Type of Authentication	Authentication Data
CO	Role-based	Password (8 or more characters, minimum strength **Good**)
User	Identity-based	Password settings configured by Network Administrator: • Minimum password length. Section 4.1 (Secure Operation) explains that the module must be configured for a minimum User password length of 6 characters. • Minimum password strength **Good** (Recommended) • Password lifetime restrictions (optional) • Lockout mechanism to deter password guessing (optional)

2.2.2.2 Authentication

The Gateway module performs authentication for the following operator roles. Passwords may be up to 31 characters long and use mixed-case alphabetic, numeric, and non-alphanumeric ASCII characters. The PC's client software displays a graphical login prompt, reads the password (displaying a round dot for each character typed), and transfers the credentials to the module's USB interface for authentication. When the module is powered off and subsequently powered on, the results of previous authentications are not retained and the module requires the operator to be re-authenticated. Table presents the minimum strength results for password and certificate-based authentication mechanisms using random authentication credentials:

2.3 9 Password Security Policies For SMBs

2.3.1 Use Complex Passwords

Whether you've been flying by the seat of your pants or are a full-fledged security wonk, go back to the basics. "Those are things that everyone tends to slack on," Slain said, because ignoring the obvious steps is easy to do. The first of those steps: Use complex passwords. That means a case-sensitive combination of letters, numbers, and special characters--at least eight in total. Because "complex" can sometimes mean "easy to forget," Slain suggests using memorable phrases broken up by spaces, special characters, and/or numbers. "Those can create pretty robust passwords that are a lot easier to remember," Slain said[16].

2.3.2 Don't Reuse Passwords

This one's a must, yet it remains a common danger. Employees that use the same password across multiple systems--often both professional and personal--to keep things simple can turn a minor, isolated issue into a major security breach. Slain points to the recent Zappos case that exposed external customer passwords as an example. Unique passwords help stop the bleeding much faster if a password is leaked or stolen--otherwise access to a Twitter account can suddenly turn into bank accounts, health information, customer databases, and other sensitive areas.

2.3.3 Change Passwords Regularly

It's the last piece of the holy trinity: Change your virtual locks regularly to further minimize risks. Slain recommends updating credentials at least every 60 days; better yet, do it every 30.

2.3.4 Double-Down On Email Accounts

Slain thinks too many SMBs get lazy with their email passwords, leading to larger-scale problems "Those are the holy grail for thieves," he said, particularly for online applications that use the ubiquitous "Forgot Password" feature. When a hacker gains control of employee email credentials, it can turn into an all-you-can-eat data buffet--particular if that those credentials were re-used across other systems. Email breaches can also lead to increased spear phishing and social engineering risks. Treat email with a similar level of caution as bank and other high-risk accounts.

2.3.5 Restrict Application Settings

Particularly for online and mobile applications, it's a good idea to modify security and privacy settings to the most locked-down options. Be leery of new applications and consider using a secondary email address outside of the corporate system when testing or signing up for new online tools.

2.3.6 Consider A Password Wallet

One password pitfall common inside SMB offices is found in password sharing among workgroups and team members. This can lead to weak security habits, both of the analog (Post-it Notes on the monitor, yelling passwords

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 253 – 258 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

over the cubicle wall) and digital variety (passwords shared via email, IM, and related means).

2.3.7 Use A Device-Lock Apps

The mobile era has compounded the potential security threats inherent in password breaches. A lost or stolen device, for starters, can become a nightmare for the unprepared SMB. Begin by requiring--or at least strongly encouraging--staff to use a device-lock feature or app. set it to time out automatically at one minute or less of inactivity.

2.3.8 Don't Jailbreak Or Root Phones

This one's likely to be a particular concern for SMBs that encourage employees to bring their own device to work. Users that jailbreak their iPhone or root their Android device could be bringing increased security risks onto the corporate network. Consider a policy restriction that bans such devices for company use.

3.3.9 Fully Exit Apps

Slain recommends users sign out and exit business apps when not in use rather than leaving them running in the background. That's a step that sounds easy but sometimes involves more than just closing it, depending on the phone and its operating system. iPhone users, Slain points out, must double-click the bottom button, find the app in a list, tap its icon, and then tap the minus sign that appears.

3 SECURITY ANALYSIS

4.1 Memorization and Guessing

In *The Memorability and Security of Passwords*, Jeff Yan et al. examine the effect of advice given to users about a good choice of password. They found that passwords based on thinking of a phrase and taking the first letter of each word are just as memorable as naively selected passwords, and just as hard to crack as randomly generated passwords. Combining two *unrelated* words is another good method. Having a personally designed "algorithm" for generating obscure passwords is another good method. However, asking users to remember a password consisting of a "mix of uppercase and lowercase characters" is similar to asking them to remember a sequence of bits: hard to remember, and only a little bit harder to crack (e.g. only 128 times harder to crack for 7-letter passwords, less if the user simply capitalizes one of the letters)[10].

4.2 Password Longevity

“Password aging" is a feature of some operating systems which forces users to change passwords frequently (e.g., quarterly, monthly or even more often). Such policies usually provoke user protest and foot-dragging at best and hostility at worst. There is often an increase in the people who note down the password and leave it where it can easily be found, as well as helpdesk calls to reset a forgotten password.

4.3 Website Password Systems

Passwords are used on websites to authenticate users and are usually maintained on the Web server, meaning the browser on a remote system sends a password to the server (by HTTP POST), the server checks the password and sends back the relevant content (or an access denied message). This process eliminates the possibility of local reverse engineering as the code used to authenticate the password does not reside on the local machine. Transmission of the password, via the browser, in plaintext means it can be intercepted along its journey to the server. Many web authentication systems use SSL to establish an encrypted session between the browser and the server, and are usually the underlying meaning of claims to have a "secure Web site". This is done automatically by the browser and increases integrity of the session, assuming neither end has been compromised and that the SSL/TLS implementations used are high quality ones.[9]

4.4 Password Cracking

In cryptanalysis and computer security, **password cracking** is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Another common approach is to say that you have "forgotten" the password and then change it. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk, but involves system administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crack able passwords.

4.5 Easy To Remember, Hard To Guess

In "The Memorability and Security of Passwords", Jeff Yan et al. examine the effect of advice given to users about a good choice of password. They found that passwords based on thinking of a phrase and taking the first letter of each word are just as memorable as naively selected passwords, and just as hard to crack as randomly generated passwords. Combining two unrelated words is another good method. Having a personally designed "algorithm" for generating obscure passwords is another good method. However, asking users to remember a password consisting of a “mix of uppercase and lowercase characters” is similar to asking them to remember a sequence of bits: hard to remember, and only a little bit harder to crack (e.g. only 128 times harder to crack for 7-

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 253 – 258 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

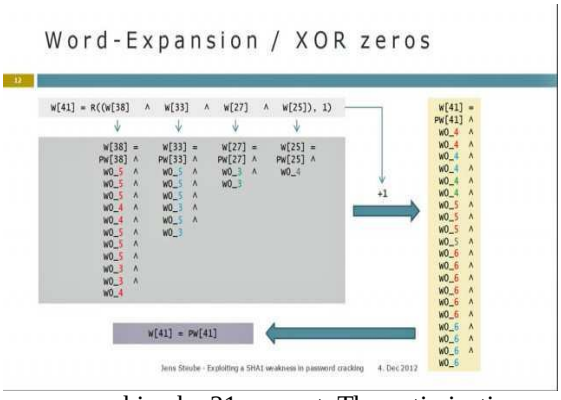
letter passwords, less if the user simply capitalizes one of the letters).

5 RISK ASSESSMENTS, SECURITY AND HACKCTIVISM

5.1 New attack makes some password cracking faster, easier than ever

A researcher has devised a method that reduces the time and resources required to crack passwords that are protected by the SHA1 cryptographic algorithm. The optimization, presented on Tuesday at the Passwords^12 conference in Oslo, Norway, can speed up password

Fig: 3 Word Expansions

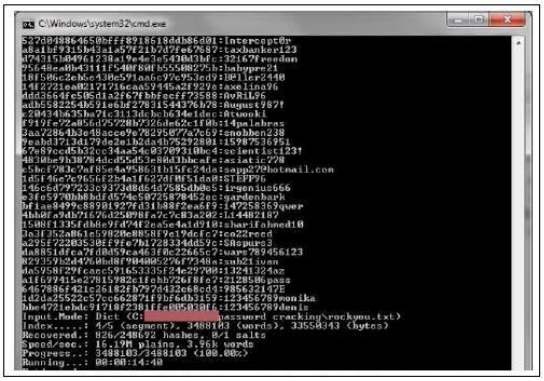


cracking by 21 percent. The optimization works by reducing the number of steps required to calculate SHA1 hashes, which are used to cryptographically represent strings of text so passwords aren't stored as plain text. Such one-way hashes—for example 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 to represent "password" (minus the quotes) and e38ad214943daad1d64c102faec29de4afe9da3d for "password1"—can't be mathematically unscrambled. "This technique reduces the computational cost of testing candidate passwords when one is given the SHA1 hash of an unknown password," Jean-Philippe Aumasson, a Switzerland-based cryptography expert, wrote in an e-mail to Ars. "In mathematical terms, it does so by avoiding redundant operations—that is, operations that have to be performed regardless of the password tested." Aumasson is the main designer of BLAKE, one of five finalist hash functions in the competition to designate the SHA3 algorithm[18], [19].

5.2 *Guild Wars 2* officials say password attack, blocked accounts, generate 8,500 requests (correction)

A password-cracking campaign against players of the popular game *Guild Wars 2*, combined with account log-in problems, generated more than 8,500 support requests over the weekend, company officials said, adding that the account take-over attacks were in part aided by compromised credentials siphoned from an unknown fan site that was recently hacked. Officials with *Guild Wars 2* developer Arena Net recently began the practice of proactively e-mailing customers when someone logs into an account from a new location. They're also advising users to choose long, random passwords that are unique to their accounts and to check e-mail only from trusted devices.

Fig 4: Password Attack



The compromised sites include an unidentified *Guild Wars* related fan site that Arena Net officials said recently warned of a breach of its account database. "That's important, but just one of many apparent breaches of other games and web sites that hackers have been collecting email addresses and passwords from," they added. The warnings come amid a wealth of anecdotal evidence pointing to an ongoing campaign, possibly by an employee of Norway-based security firm Norman ASA recounted receiving an e-mail warning that someone used her details to attempt to log in to her *Guild Wars 2* account just one day after it was created. "It's been just over a week since the game launched, and I've now had 10 e-mails detailing attempts to access my account from China," the unnamed Norman employee wrote. "I live in Europe[20].

6 CONCLUSION

A system's cryptographic protocol also plays a roll in security (or lack thereof). For instance, UNIX machines might rely on crypt, a one-way hashing algorithm based on a modified DES algorithm, to transform passwords into cipher text. Since crypt, algorithms such as MD5 were found to provide a more secure and attack-resistant representation of passwords; yet many systems have not upgraded. Online password guessing attacks on password-only systems have been observed for decades.

Present-day attackers targeting such systems are empowered by having control of thousand to million-node botnets. In previous ATT-based login protocols, there exists a security usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. Our empirical

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 253 – 258 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

experiments on two data sets (of one-year duration) gathered from operational network environments show that while PGRP is apparently more effective in preventing password guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users even if no cookies are available. However, we reiterate that no user testing of PGRP has been conducted so far.

7 ACKNOWLEDGMENT

We would like to thank Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot for their suggestions on early versions of this work. We thank the reviewers for their comments and suggestions for improving this work. The authors would like to thank the editor and reviewers for their insightful and constructive comments.

REFERENCES

[1] Revisiting Defenses against Large-Scale Online Password Guessing Attacks by Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, JANUARY/FEBRUARY 2012.

[2] Revisiting Defenses against Large-Scale Online Password Guessing Attacks by Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, FEBRUARY-13 2011.

(Book style)

[3] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 162-175, 2010.

[4] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldszmidt, and T. Wobber, "How Dynamic Are IP Addresses?" SIGCOMM Computer Comm. Rev., vol. 37, no. 4, pp. 301-312, 2007.

[5] J. Yan and A.S.E. Ahmad, "A Low-Cost Attack on a Microsoft CAPTCHA," Proc. ACM Computer and Comm. Security (CCS '08), pp. 543-554, Oct. 2008.

[6] J. Yan and A.S.E. Ahmad, "Usability of CAPTCHAs or Usability Issues in CAPTCHA Design," Proc. Symp. Usable Privacy and Security (SOUPS '08), pp. 44-52, July 2008.

[7]DEPENDABLE AND SECURE COMPUTING, DOI bookmark http://doi.ieeecomputersociety.org/10.1109/TDSC.2011.24

[8] J. Nielsen, "Stop Password Masking," http://www.useit.com/ alert box/passwords.html, June 2009.

[9] Password Guessing by B. Michael Hale. http://all.net/CID/Attack/papers/PasswordGuessing2.html

[10] New feature in version 11.28: Security Policy - cPanel Forums http://forums.cpanel.net/f5/new-feature-version-11-28-security-policy-...

[11] Security Policy and smarter mail password length - Parallels Forums http://forum.parallels.com/showthread.php?t=261438

[12] Password Memorizing and guessing - Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Password#Memorization_and_guessing

[13] Password cracking - Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Password_Guessing

[14] Oh great: New attack makes some password cracking faster, easier than... http://arstechnica.com/security/2012/12/oh-great-new-attack-makes-so...

[15] Digital Library at www.computer.org/publications/dlib.

[16] 9 Password Security Policies for SMBs - Smb - Security - http://www.informationweek.com/smb/security/9-password-security-po...

[17] InZero® Systems 2010-2012

[18] Access control - Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Access_control

[19] Change the Password Policy - SBS 2011 http://social.technet.microsoft.com/Forums/en-US/smallbusinessserver/...

[20] Guild Wars 2 officials say password attack, blocked accounts, generates... http://arstechnica.com/security/2012/09/guild-wars-2-password-attack-...

[21] New feature in version 11.28: Security Policy - cPanel Forums http://forums.cpanel.net/f5/new-feature-version-11-28-security-policy-...