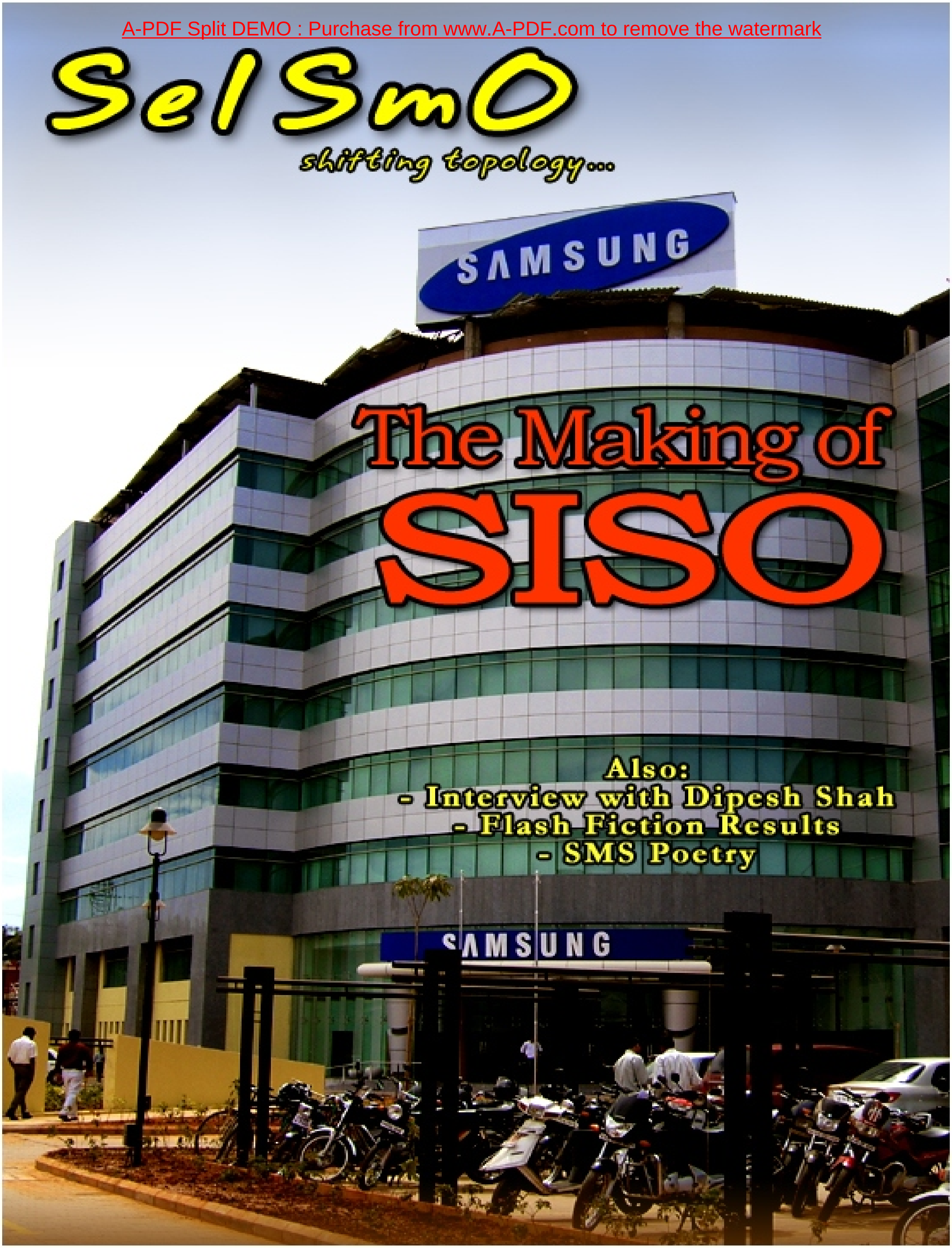
Volume 1, Issue 2, Feb'06

SelSmO

shifting topology...



The Making of SISO

Also:
- Interview with Dipesh Shah
- Flash Fiction Results
- SMS Poetry

SAMSUNG

SelSmo

Shifting Topology

INSIDE THIS ISSUE

Dear SISO-ite,

It is customary to thank everyone for the "overwhelming" response to our call for articles! But let us be frank here! The response to any of our calls was certainly not overwhelming! Though the number of articles was less, their quality was high! We were amazed to see the literary talent of a few SISO-ites!

To respond to the call made by you in our survey, we have reduced the number of pages! So, we could not accommodate all the articles we received. Congratulations to those whose writings are published! And to those whose articles are not published, there is no reason to feel bad. The articles are always in our archives & would find their way in the future editions! By the way, do not forget to send more articles!

This issue has a special cover story on "Making of SISO" to celebrate 10 years of existence of our company! Other "Don't miss it" items include an interview with Dipesh, Flash Fiction, Short Stories, Poetries & two "short & crisp" technical articles! And then there is a Quiz & a section on Books - these are sections we plan to have regularly in every edition.

Your views on Bagmane Tech Park sent as SMS entries have been put across the magazine!

Here are the prize winners!
Best Article: Uday Trivedi - Praying our Heart out (Selected by Editorial Team)
Best Flash Fiction: Raghunandan (Selected by external reviewers!)

Happy Reading! Do send in your comments to sisojournal@siso.com

Best Regards
Editorial Team

System Security -An analysis

~Mohanlal Jangir

With fast growing networking and automation, the security threats have grown commensurately. The security threats differ in their nature and can vary from password cracking to data access to system instability and many more. This article addresses system security from Physical, Network and DoS point of view with some real-life examples.

1. Physical Security

This section deals with some of the possible attacks, a hacker can inflict on system, given the physical access. Primary attack in case of physical access is password cracking which paves path for any kind of attack.

1.1. BIOS password

This attack is most talked, rarely done and easy to execute because a hacker needs nothing but a screw driver to open the CPU case. BIOS password can be disabled by powering-off and powering-on the BIOS chip. This can be accomplished by changing jumper (with 3 pins adjacent to battery) setting of BIOS chip from slot 1-2 to 2-3 or from 2-3 to 1-2 (if initially it is at 2-3). Turn on the system and turn off after some time. Revert the jumper settings to original one and next reboot does not prompt for BIOS password.

> *The security threats differ in their nature and can vary from password cracking to data access to system instability and many more.*

1.2. Single Booting

This attack is particular to servers running Linux (It's not a bug in Linux but a feature of Linux. It's up to you how do you define it). A Linux machine can be run in different run-levels ranging from 0 to 6. The run-level 1 provides a feature where user is dropped to Linux super-user shell without any password. The following paragraphs describe how Linux can be booted in run-level 1 with two widely used boot loaders, LILO and GRUB.

LILO – This is a very common attack and very popular among students specially. Pressing CTRL-X before booting drops user to LILO prompt. Command 'Linux 1' or 'Linux single' boots the Linux in run-level 1.

GRUB – The same attack can be done with GRUB boot loader although procedure is different as described below:

A. Select the Linux kernel version you want to boot and type 'e' (to edit)

B. Select the line starting with 'kernel' and again type 'e' to edit this line.

C. At the end of line, append 'single' and press enter to finish editing

D. Type 'b' (to boot)

This drops the user to run-level 1 exactly like LILO case. Many administrators protect these attacks by boot-loader password but this effort is almost futile as we see in the next section which bypasses even the boot loader.

1.3. Bootable Disk

This attack can bypass initial booting mechanism with help of a bootable disk. Take a bootable Redhat Linux disk (for example) and boot the system. Mount the system file system at some directory path (say /mnt/rescue) and chroot to that directory (with 'chroot /mnt/rescue' command). At this point of time it really doesn't matter which operating system is loaded on the system. For Linux, it's matter of issuing 'passwd' command to change the super-user password. For Windows, mount the Windows partition as MSDOS or NTFS file system (whichever is applicable in your case) and you need a registry editor which can read and write to Windows registries (what regedit does on windows). One such registry editor is available at http://home.eunet.no/~pnordahl/ntpasswd/

This approach is easy to execute and works for any operating system as long as you have read and write support of target machine file system and you know where the passwords are stored (It doesn't matter what form they are stored in).

Looking at above three sections, we can safely conclude that it's almost impossible to prevent a hacker from damaging the system given the physical access. In the worst case, no one can prevent the attacker by smashing the system with a hammer ;-) The only way to prevent these attacks is to prevent unauthorized admission, and that's the reason all important servers are always kept in strong locked rooms.

2. Network Security

This is the arena where a shrewd system administrator makes difference from a naive one. Although the horizons of network loopholes and protections are unlimited, we restrict our attention to some very common and widely used protocols which are vulnerable to security threats.

2.1. Protocols sending password in clear-text

Many commonly used protocols provide a user-name and password authentication mechanism like telnet, ftp, http etc. But the user-name and password are sent in clear-text which can be tapped by any packet sniffing tool on network (One such tools is available at http://www.ethereal.com/). These tools on one hand provide a lot of help to software developers, but at the same time give a key to hackers also. To see a live example, just run ethereal tool in promiscuous mode with filter 'http.request.method contains "POST"' and you will get user-name and password of all the SISO employees who logged on to HRIS during capture time.

Note: I personally don't advice to do this. If you want to experiment, capture your own packets in non-promiscuous mode because theft in your own house in not a crime ;-)

2.2. Password-less protocols (rcp, tftp)

There are many protocols which either don't support password mechanism (i.e. Tftp) or can be made to work in password-less mode (i.e rcp, rsh, rlogin etc). This security hole may lead to unauthorized data access or total system break down (Think what an 'rsh –l root rm –rf /etc' can do). A good system administrator must always keep such services disabled.

2.3. Firewall breach attack

One very popular firewall breach attack is called SYN/FIN attack. This attack was very popular until TCP stacks fixed a bug very recently (and many haven't yet). The major reason behind this was vague standard defined in RFC 793. According to the RFC, a TCP packet carrying SYN bit alone is used for connection establishment initiation. But this RFC does not define behavior of packets having SYN bit with other possible combinations (except SYN and ACK). This fact was exploited by many hackers for establishing a connection behind firewall. The firewalls relied on the fact that packet having SYN bit alone from illegitimate peer must be discarded. But liberal firewalls let packets with SYN/FIN bit pass through. The TCP implementation didn't understand SYN/FIN bit combination exactly and again liberal implementations let connection established considering SYN bit present. Although seems improbable, this bug was present in almost all TCP implementation regardless of the vendor.

Many implementations now discard SYN/FIN packets blindly but this introduces incompatibility with a new TCP version called T/TCP (RFC 1379).

2.4. IPSec, SSL and secure protocols

The numbers of security methods are tantamount to security holes. Again for the sake of space we keep ourselves limited to a paragraph.

The various dimensions of

SMS Poetry

Run from pillar to post for a
spkr phone weekly . Late by
10 minutes,call started in
chairs absence.Call over
after 1 hour, ear-peace lost
by desk phone use

security are authentication, encryption, data integrity etc. Most of the time authentication and data integration are considered two flips of same coin assuming no one else other than legitimate user knows the secrete key (like your Citibank password). The encryption is provided by some well known encryption algorithms.

SSL (Secure Socket Layer) and TLS (Transport Layer Security) provide secure API(s) to applications. This requires change in applications. On the other hand, IPSec (IP Security) works on IP layer and is controlled by administrator policy. It is completely transparent to applications and therefore any application (including legacy ones) can use security features. That's the reason IPSec is entering into every walk and has a very good prospect.

3. Denial of Service

The attacks falling in this category do not aim to access data or crack passwords but creates such environment that system keeps on doing unnecessary processing and legitimate users can't avail expected services. There are much more types of DoS attacks possible than what this article describes. The article attempts to give a glimpse of some of very popular and common DoS attacks.

SMS Poetry

Dust and dirt circle in the air
from dawn to dusk in this
Bagmane TPO. I am
pessimistic to hope that we
will not carry home this after
February

3.1. SYN flooding

This attack is also attributed to a flaw in TCP specification. On receiving SYN packet, the host sends a SYN/ACK packet (half-open connection state) and waits for ACK packet to arrive to change the connection from half-open to established state. During SYN flooding attack, the attacker sends only SYN packets and never sends ACK packets, causing so much of half-open connections at the victim host, bringing it to the knees. Many implementations try to mitigate this attack by using SYN-cache or SYN-cookies.

3.2. Fragments storm

The fact that IP stack has to wait for fragments' reassembly until all fragments arrive, make system vulnerable to fragment storms. The attacker keeps on sending fragments but never sends all fragments. This causes many chains of fragments at victim host waiting for remaining fragments to arrive. The timeout value (of discarding fragments) may vary from 15 seconds to 255 seconds, which gives enough time to attacker to eat up system memory.

3.3. Ping of Death

ICMP packets serve control as well as informative purpose. The later category includes ping and node information query packets which are responded back by peer. Attackers can send an enormous number of such packets. This has led to complete degradation of many servers. Even an ordinary Linux-box can infuse millions of packets within a minute and congest the network (For example try "ping –f –b 107.108.72.255"). Taking a precaution against this, many hosts have stopped replying to ICMP informative packets (For example, try pinging www.microsoft.com).

The DoS attacks are many and each attack bears a different attribute. Because of this face, defending them is a severe challenge to system administrators. With the telecom networks moving towards packet switched networks the threat has become more acute and dangerous. This is one of the reasons, all telecom corporate prefer to have single point entry systems like SBC (Session Border Controller) where security is handled completely and network topology is kept hidden by NAT.

Mohalal Jangir is working as Lead Engineer is TND. He earlier worked network protocols such as Ipv6, IPSec and embedded systems. He is a keen lover of Linux and likes to work on device drivers, wireless networks and network security. He holds masters degree in Computer Technology from IIT DELHI. ■

SMS Poetry

...have lake view, Good!
SISO should contribute to
maintaining the lake.
Regarding facilities, let them
come up first!