Computers & Security (2005) **24**, 599–603

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Timing is everything

Nathan Friess, Ryan Vogt, John Aycock*

Department of Computer Science, University of Calgary, 2500 University Drive N.W., Calgary, Alberta, Canada

KEYWORDS
Human factors;
Vulnerabilities;
Patching;
Time;
Holidays

Abstract Social engineering attacks are well-known to prey on human weaknesses. Besides these weaknesses, humans insist on eating, sleeping, and partaking in non-work activities. On a global scale, work schedules combined with IT policies leave large windows of vulnerability — but how large? We examine calendar data through the year 2010 and locate the longest vulnerability windows which could be exploited by well-timed attacks by malicious software. The same data can be analyzed to solve a related problem: determining the best times to release software patches.
© 2005 Elsevier Ltd. All rights reserved.

Introduction

Vulnerabilities in code are one attack vector that worms can use to infect machines. For instance, the Slammer worm exploited some buffer overflow vulnerabilities in the Microsoft SQL server (Ször and Perriot, 2003). The ''best'' time for a worm release, from an attacker's point of view, would typically be the time when the worm can infect most machines. A software maintainer, on the other hand, would want to announce a patch for a code vulnerability when most machines can be fixed. When knowledge of a vulnerability is taken into account, four cases result:

1. An attacker knows about a vulnerability prior to its public announcement. The information might have been discovered by the attacker's own analysis of the vulnerable software, or by other means, like monitoring full-disclosure mailing lists.
2. A software maintainer is aware of an unannounced vulnerability, but has not yet released a patch for it. The vulnerability may have been found by an internal code audit, or perhaps by an outside security researcher who privately disclosed the problem to the maintainer.
3. An attacker has no prior knowledge of an exploit. The attacker learns of the vulnerability from the software maintainer announcing the vulnerability directly, or announcing it indirectly by releasing a patch. A worm exploiting the vulnerability can infect more machines immediately after the vulnerability's disclosure (Nazario et al., 2004).

* Corresponding author.
E-mail addresses: friessn@cpsc.ucalgary.ca (N. Friess), vogt@cpsc.ucalgary.ca (R. Vogt), aycock@cpsc.ucalgary.ca (J. Aycock).

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.09.007

4. An unannounced software vulnerability is being actively exploited, and the software's maintainer must make a patch available. The cat is out of the bag, as it were, and the rapid release and deployment of a patch is essential.

In the latter two cases, the attacker and the software maintainer fare best by acting immediately. There is no choice. The first two cases are different, though: the attacker can choose an optimal time to exploit the vulnerability; the maintainer can choose the best time to release a patch. The timing is a problem, because it involves humans.

Humans are well-known to be one of the worst problems in computer security. Humans can be tricked with social engineering attacks, choose weak passwords, mount insider attacks, even offer up their passwords in exchange for chocolate (BBC News, 2004). However, the work patterns of humans and the impact these patterns have on computer security have not been extensively studied.

People do not always apply patches with religious fervor. Studies have shown that vulnerable machines persist long after a security patch is available (Arbaugh et al., 2000), and that the rate of patching and repair tails off with time (Provos and Honeyman, 2001; Rescorla, 2003). Granted, there are often good reasons for this: applying patches consumes people's time, which is rarely in great supply to begin with. Patches can themselves be faulty, and applying them may cause more problems than they solve (Beattie et al., 2002).

Some recent operating system releases have the capability to automatically apply patches as soon as they are available, without human intervention. Such auto-patching reduces the impact of the problem we describe, but does not eliminate it. Not everyone uses recent operating systems, nor do they all enable auto-patching. In practice, automatic patching may be avoided, or forbidden by company policy, for fear that a patch may break systems. Also, not all applications in a system may have the capability to automatically patch themselves, or a vulnerability may lie in a more dedicated device like a router.

What if a best-case scenario is considered? Say that patches are not flawed, that people apply patches as soon as possible. With worms exploiting vulnerabilities in Internet-connected computers worldwide, it is still entirely conceivable that globally, computers are more vulnerable at some points in time. The reason: people do not work continuously, and even in the best-case scenario, it will be atypical for patches to be applied outside of normal work hours. Human factors must be considered.

To the best of our knowledge, no one has ever looked at how work hours worldwide can conspire to create larger-than-normal windows of vulnerability, when patching is unlikely to occur. In what follows, we look for these global vulnerability windows, so that defenders can be apprised of them, and the timing of patch releases can be well-selected.

Methodology

We compiled a database with the following information for each country of interest, for a six-year span from 2005 through 2010:

- the time zone(s) that the country spans;
- the normal business hours for each day of the week;
- the dates when the country observes daylight savings time (DST), if at all; and
- the dates of national holidays.

These data were used to find times when none of the countries in the database had normal business hours. The basic assumption we made is that, outside of business hours, the overall level of computer support in a country diminishes. Updates are less likely to be applied during these times, regardless of whether the updates are software patches, anti-virus updates, or configuration changes to firewalls or intrusion-prevention systems. There is some empirical evidence to suggest that this may be the case (Rescorla, 2003).

One item added to each country's database entry was its approximate number of Internet-connected hosts. There is a huge gap between the number of computers in highly-connected countries and the number of computers in less-connected, less-populated, less-wealthy countries. Our database was constrained to consider only the top 50 countries in terms of the number of Internet hosts they possess, based on data from the CIA World Factbook (Central Intelligence Agency, 2004) that was current when we did this work — any countries below this ''top 50'' point would clearly be considered statistical noise.

The key idea behind our analysis algorithm is to use both the normal business hours and national holidays of each country to find time spans of interest to an attacker. Since most of the countries in our study are distributed in different time zones, it was necessary to take each nation's time zone into account. We conduct our analysis in Universal Coordinated Time (UTC), but as a nation's vulnerability is dependent on local business hours and

Download English Version:

https://daneshyari.com/en/article/10341416

Download Persian Version:

https://daneshyari.com/article/10341416

Daneshyari.com