

NATIONAL
INFRASTRUCTURE
PROTECTION
CENTER

HIGHLIGHTS

Formerly known as *Critical Infrastructure Developments*

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.



Issue 1 - 01
January 18, 2001

Editors: Linda Garrison
Martin Grand

-
- ! **Intrusion Techniques:** Networked printers are prime targets for denial of service attacks and root access intrusion attempts
 - ! **Domain Name Security:** Service and Registration Vulnerabilities
 - ! **Harnessing the Internet and Making Election History**
 - ! **Localization Facilitates Foreigners' Access to Hacker Tools**
-

This issue has an overall classification of "Unclassified."

Analytical commentary within is identified in **bold** text.

We welcome your comments and suggestions for improving this product. For more information, or to provide comments, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202) 324-0334 or (202) 324-0353.

Intrusion Techniques: Networked printers are prime targets for denial of service attacks and root access intrusion attempts

Networks are only as strong as their weakest link, and printers are often overlooked when assessing and implementing network security measures.

Vulnerabilities associated with widely used name-brand networked printers (NPs) may allow intruders to perform denial-of-service (DoS) attacks, and possibly gain root access to network administrative services if left undetected. While some of these vulnerabilities have been well documented, it is important to raise awareness of these easily avoidable vulnerabilities.

As NPs conform to compatibility and ease-of-administration demands, a number of harmful vulnerabilities have appeared.

- \$ There are a number of networked printers that allow users the ability to remotely administer them via an assigned Internet Protocol (IP) address (i.e., 100.101.103.1) via the Hyper Text Transfer Protocol (HTTP) port 80.
- \$ Password protection for the administrative functions of the NP is an option usually left open by default. An intruder could map out the target network, use the IP and port address information from the mapping, and enter the IP address of the networked printer into a standard web browser. If the printer is not password protected, the intruder would then have immediate access to the printer administrative services.
- \$ More importantly, some NPs' password challenges can be overcome by entering a simple query into the URL line of a web browser that would then reply with a plain text version of the password. If the intruder were to gain access to the NP, they would do so unchallenged and most likely, unnoticed due to the open access of HTTP port 80.
- \$ Furthermore, a powerful extensive programming language, PostScript, controls the majority of NPs' graphical outputs. An intruder's ability to manipulate the PostScript of print jobs and/or use the FTP and Telnet services of the NP also pose serious ramifications if compromised.

The abilities of intruders to gain illegal root administrative access and to successfully employ DoS attacks against networks continue to rise at an alarming rate. The same awareness and attention that are given to vital systems on the network should also be applied to networked printers. Best practices to deter NP based intrusions or DoS attempts would be to disable the HTTP services located on the NP, to select passwords with mixed alphanumeric characters, and to configure NPs into the firewall filters. Awareness of NP vulnerabilities, and the concurrent implementation of recommended best practices, are essential to combat potentially damaging network attacks.

Domain Name Security: Service and Registration Vulnerabilities

Internet users rely on names to access on-line resources, making the Domain Name Service (DNS) a vital part of the Internet, as we know it. The software package commonly used to provide DNS has been the target of numerous attacks, highlighting the importance of system administrators keeping current with patches and upgrades.

DNS provides for translation of alphabetic names to the numerical addresses used to identify Internet hosts, thereby enabling users to access Internet resources by means of easily intelligible names like <www.nipc.gov> instead of difficult-to-remember Internet Protocol (IP) numbers. When a user requests a website by name, a query is sent to a nearby name server (a server running a specialized software package that performs DNS translations), which asks what IP address the name corresponds to. If the first name server does not have a listing for that name, it relays the request to another name server higher in the DNS hierarchy until it finds a server that can provide a translation.

Most DNS installations do not incorporate strong authentication, making it possible for malicious parties to insert false directory data into the DNS hierarchy. If an intruder can manipulate an organization's DNS, the intruder could then maliciously divert on-line traffic; e.g., a user trying to access <www.nipc.gov> may be sent not to the real NIPC website, but to a phony site with false information. DNS attacks can also be carried out for other malicious purposes, such as stealing data, harvesting account information, or denying Internet service.

Another security concern lies in the domain name registration process. Central registrars maintain listings of domain names, their owners, and the name servers that provide DNS lookups. If an organization moves to a different Internet Service Provider or makes changes to its servers, it may change its DNS settings. In many cases, it does this by sending a simple e-mail request to the registrar and then confirming the desired changes in a follow-up e-mail message. If a malicious third party can forge e-mail from an organization, the former may be able to effect unauthorized changes in its domain name registration, thereby mounting an effective denial-of-service attack. This vulnerability was illustrated in an incident earlier this year in which a number of institutions found their domains hijacked. Early one weekend, an unknown party forged e-mail messages to a domain name registrar requesting that the domains of a number of universities, commercial enterprises, and nonprofit associations be redirected to a New Jersey provider of on-line services. The operator of the New Jersey site noticed the fraudulent domain transfers and took corrective action. However, it took several days for the erroneous DNS listings to be rectified. Some of the institutions victimized in this attack experienced significant disruptions in Internet connectivity.

In response to this risk, some domain name registrars have implemented optional authentication procedures for DNS modification requests. Such requests are often required to be accompanied by a secret password or digitally signed by the domain's registered owner. However, domain owners should be aware, that in many cases these authentication options are not enabled by default and will need to be requested by the customer.

DNS, like numerous other Internet protocols, lacks security commensurate with its importance. Although, it will likely be some time before more secure DNS implementations are widely deployed, there are technical initiatives underway to improve its security through authentication and data integrity checks. In addition, the emergence of new registrars in the domain name registration market complicates the registration process. It is possible that this will result in enhanced security emerging as a selling point among some of the competing agents. Organizations need to be aware of the risks surrounding DNS, and should actively investigate options for securing both the service as well as the process.

Harnessing the Internet and Making Election History

During March 7-11, 2000, Arizona voters who had previously obtained a special personal identification number (PIN) cast "e-votes" (also referred to as i-votes or on-line votes) from diverse locations across the state participating in the nation's first legally binding election for public office involving on-line balloting.

While Arizona conducted the first legally binding on-line election for public office, many states are evaluating on-line election procedures and issues. On January 24, 2000, registered Republicans living in remote locations of three districts in northeastern Alaska used the Internet to cast votes in the state's Republican

HIGHLIGHTS 1 – 01

January 18, 2001

straw poll. In February 2000, voters in Thurston County, Washington, cast votes on-line in a mock presidential primary conducted simultaneously with the state's actual primary election. The Department of Defense is also planning a pilot test for a small number of service members stationed overseas during the fall 2000 elections. There are several security issues specific to Internet voting that must be dealt with in any e-voting system.

Media reports of security issues in the 2000 Arizona on-line election

While a strong case can be made for on-line capabilities to support the election process, some media reports of the initial on-line experiences indicate problems were encountered. However, those reports minimized concerns about security and indicated that problems could be addressed by both technical and procedural approaches.

The Voting Integrity Project's report "Is Internet Voting Safe?" dated July 10, 2000, identified a number of security issues in the 2000 Arizona on-line election as follows: Because there were no proven security lapses, the vendor in that election - Election.com claimed complete success. This gives the public and election officials a false sense of security about Internet Voting. However, the following security vulnerabilities were present in that election:

- The election run by Election.com under contract to the Arizona Democratic Party was a system not certified or supervised by election officials.
- The election was vulnerable to a denial of service attack such as those that brought down Yahoo, CNN, Ebay, and other giant web portals earlier this year. This was implicitly acknowledged by Election.com when they chose (in advance) to suspend Internet voting for the final day of the election. Such an attack could have stopped the Internet voting entirely.
- The election was vulnerable to virus/Trojan horse and remote control software attacks against voters' PC's. Such a vulnerability could have allowed a single person, acting alone, to circulate a virus (similar to the recent "I Love You" or "Love Bug" virus) that could have substituted the virus writer's vote for that of thousands of legitimate voters, and do so entirely undetected, from virtually anywhere in the world.
- Voter authentication was minimal and could have been easily defeated.
- Election.com issued the PIN's and had access to the ballots, thus leaving the election vulnerable to insider violation.
- Several Macintosh computers, and all computers using older Netscape browsers, were unsupported.
- An unexplained one-hour total outage.
- There has been a lack of information about important features of this election and the protocols critical to ensuring its integrity.

Security: A unique context in on-line elections

Security has a larger context beyond the specific technical and procedural items noted in the general media reports. First, on-line voting results in a shift of control from election officials to election vendors because of the technical expertise required. Second, state and federal laws have not evolved to address the on-line voting environment. Third, the potential for automated attacks on the voting process increases. Finally, voting from remote locations represents a further shift of responsibility for maintenance of the voting infrastructure from the election officials and vendor, to the voter or third party-provider of the venue such as employer, hotel, military installation, school, etc.

The security problems and concerns mentioned above appear to be relatively minor in scope and are similar to concerns regarding various forms of e-commerce, since many e-commerce methodologies, approaches, and products are also utilized in i-voting technology. Solving these problems will draw upon well-established principles, practices, and experience developed from integrating technology and complex business processes in mission critical functions. However, security requirements for an on-line election must be higher than for e-commerce because the stakes are higher.

Localization Facilitates Foreigners' Access to Hacker Tools

An aspiring hacker in the United States will have little difficulty in finding attack scripts, hacking tools, and hacking instruction guides; such materials may be freely downloaded from hundreds of Internet sites. However, for the foreign counterpart not fluent in English, access to such information is currently more difficult.

Most on-line material related to hacking is written in English. While English is one of the most widely spoken languages today, only a fraction of the world's population has a mastery of the language advanced enough to understand complex English-language technical material. These facts have effectively precluded large portions of the global Internet population from gaining access to hacking tools and information. However, recent trends in the global computer underground seem to be moving toward the removal of this language-based barrier. Increasingly, hackers across the globe are gaining access to materials in their own languages. Although the following sections highlight some recent developments in the Russian-language computer underground, this phenomenon is not limited to one region or linguistic group.

Localized How-to Guidance

Foreign hacking activity is facilitated by the dissemination of hacking how-to guides or instructional material in the local language. One example of this is in a glossy print publication targeted squarely at the Russian-language computer underground. The publishers provided a brief, yet detailed, how-to guide on the procedures that even an inexperienced Linux user could use to break into vulnerable servers on the Internet.

The article explained how to scan for FTP servers, suggesting that users may try scanning a range of IP addresses "somewhere in far-off New Zealand or Australia." The article then demonstrated how to identify hosts running a vulnerable version of the wu-ftpd FTP server. Explaining which exploit would allow the intruder to gain root access to the vulnerable host, the article walked the user through the process of running the exploit, and guided them in downloading and installing a root kit on the compromised host to enable future unauthorized access. The article concluded with an explanation of how to remove evidence of the intrusion by wiping the host's log files. Throughout, the author provided the exact keystrokes to type at a Linux command line to effect the break-in; along with precise URLs for the files needed to complete the attack. In short, the article provided everything a budding young Russian-speaking hacker would need to break into a vulnerable site anywhere on the globe.

Localized Tool Documentation

Non-English-speaking hackers may also be aided by publication of localized documentation for software tools that can be used for malicious purposes. For example, Nessus, is a freely available remote security scanner, that has found an enthusiastic following throughout the security community. Nessus may be used by system administrators to secure their networks, or by potential intruders to identify vulnerable targets.

Fairly complete Nessus documentation has been available in German for some time, but was recently introduced to another, potentially larger foreign audience. In August 2000, a hacker called “deathor” posted an article about the Nessus security scanner on a Russian hacking site. The author acquainted the Russian-speaking audience with the Nessus package and explained its powerful scanning capabilities. He also provided detailed instructions on how to acquire and install the software, as well as how to use it to carry out several types of remote scans for security vulnerabilities. “Deathor’s” Nessus article quickly became the most popular article on the website.

Localized Tools

Finally, the production of completely localized tools that make any knowledge of the English language unnecessary will aid foreign hackers. A textbook example of this involving the tool Nmap has also appeared in the Russian-speaking world. Nmap is a stealth port scanner and network mapper. It’s author points out on the utility’s home page that it is well suited to a range of activity, including “network security auditing, general Internet exploration, and hacking.” Freely available on the Internet, Nmap—like Nessus—has gained broad popularity in the security community.

On 31 July 2000, a Russian national, publicly announced the availability of RuNmap, a completely Russified version of Nmap. The Russian had made a beta version of the utility for Unix available for immediate download from a website. This site also hosted complete Russian-language documentation for the tool and announced that there were plans to release a version of RuNmap for Windows. (Work on this project was reportedly well underway.)

The on-line community is no longer made up of a small group of academic elites. The publication of localized materials worldwide provides a boost to local on-line populations, who may be tempted to utilize this knowledge for malicious purposes. We can anticipate that new foreign users, many in countries with poorly developed computer crime laws, will gain access to powerful hacking tools with instructions for use in their native tongues. Localization will contribute to negative tendencies in the Internet’s security environment, and will be an additional factor system and network administrators and managers should consider in protecting their electronic infrastructures.