HealthManagement
Promoting Management and Leadership

Volume 5 / Issue 5 / 2010 - Features

Security Considerations For Mobile Communications

Author

Louis Leahy

Inventor,

Armorlog TM VPCSML TM

Smart phones and personal digital assistants (PDA) are fast replacing the desktop, laptop and notebook computers as the primary access device of digital network users. In some developing economies that rely on mobile phones primarily for communications they are already the dominant device.

An Ever-Growing Threat

The plethora of programmes that can now be instantly downloaded to these devices presents an ever-growing threat to organisations seeking to comply with their obligations to keep network assets secure and patient data private. Some of what is discussed here regarding Authentication topology is newly developed technology that is not yet in common use. However, some proactive experts are actively studying these matters.

There are also a myriad of threats in existence at various layers in digital networks and communications. However, these are beyond the scope of this article.

Here we address the common garden-variety scams that are used to dupe users in to revealing network access to attackers. I would suggest however that if proper end to end encryption is used on networks much of that risk could also be eliminated. Again, there appear to be many enlightened industry figures pushing for standards.

No Simple Solutions

There are no simple solutions for network protection, only an ever increasing number of steps that need to be taken to try to ensure the organisations obligations are met. Firstly I will address authentication which I think is the primary issue that needs to be attended to. Then I will address application testing and lastly, I will outline the other aspects of protection that are worthy of consideration; if used in conjunction with an enhanced authentication topology and application testing, they will go a long way toward deterring the current crop of attacks.

'Foolishness' is no Legal Excuse

It is network owners who primarily need to address their methodology for authentication as a first step. At a basic level the system should protect the user from being tricked into revealing their network access credentials.

Currently, simple scams involve telephoning users and pretending to be from their IT departments and talking them into loading software or changing settings on their device to allow the attacker access or simply asking for their access credentials to the network concerned. Many IT professionals argue that people are foolish if they fall for these traps.

That may be true but the issue is that the ever increasing legal compliance obligations do not make provision for the stupidity or otherwise of an organisations' members – be they employees, associates or volunteers. Personally, I think that this approach is a poor excuse for defective services and products being sold to organisations. The level of sophistication of network attacks is getting so good that even seasoned power users or IT professionals could be tricked.

Some systems are, in fact, so poorly designed as to allow an attacker to reset the access credentials to a set of their choosing.

Experts also Vulnerable

There was a recent case of a test of government department members run by its own hierarchy and to which the members failed dismally. They were warned of an upcoming departmental inspection of their computers and that they should provide their access details so the computers could be checked before the inspection to ensure they were not breaking any rules. Something like 35 percent of the participants fell for the scam.

These were well-trained people with access to sensitive network assets. I give this example not to embarrass anyone but to simply demonstrate that anyone who suggests networks can be protected by observation is really perpetuating a flawed security architecture.

Designing Robust Authentication Routines

Programming routines for authentication need to be designed so that it is made difficult for the user to be tricked into revealing their credentials.

In addition to phishing scams is a huge library of software used to attack networks to secure the user name and password details. Consequently, I recommend credentials should not be in the public domain (this includes the user name). Nor should the logon address – this would make it difficult for an attacker to know which user logs on where and as a result makes it more difficult to launch an attack.

At present, most companies tell everyone where their users logon. In addition, their user name is often in the public domain, since it will be their actual name, email address, network operating system username, or a username pseudonym – used, for example, in a social networking site. Such a structure means that only one item is required for an attacker to identify to get network access.

It is important that a network authentication system compels the user to use credentials that have not been used elsewhere to prevent weakening security through duplication. This can be achieved by forcing the use of an extended set of graphics keys outside the traditional key sets.

Deterring Malware

Furthermore, in order to deter malware, it is important that the underlying number sequence is proprietary to the organisation and not a system in common use. It is also preferable that the device be used as a pointing device and that any keyboard interaction by way of keyed input be disable during authentication to prevent logging of credentials by malware (keyboard logging) or timing attacks.

Equally important in the design of the authentication topology is the need to deploy time outs and lockouts to prevent sustained attacks to guess the user name and password. The design deployed should be such that the user is not inconvenienced by the use of the lockouts. If the correct design is instigated it is possible to frustrate hacking attempts without annoying the user by having him or her locked out of their account for no apparent reason from their perspective.

Vulnerability Test and Certification

In addition to the above generic steps, which we advocate as part of our technology, we believe other methodologies also need to be taken by network owners. Many of these are already common practice. However, we believe they all need to be put in place to provide the necessary level of protection for organisations to meet their obligations for protecting data and assets.

Firstly it is important that any applications that are to be used on the network or on devices used to access the network have been tested and certified for vulnerabilities. There are now companies online that test at binary level.

This means testing is now more thorough and can be automated, which keeps the cost relatively low for developers.

However while this is primarily the responsibility of the software vendor, the network owner needs to ensure that policies and procedures are in place to ensure that the certification has been undertaken for any products introduced to its network so as to limit known vulnerabilities in code.

The Specific Challenge of Mobile Devices and Diverse OS

Virus and malware scanning is yet to be fully developed for mobile devices. However, it is a necessary component to mitigate risk of attacks.

One of the barriers to implementation by vendors is the increasing number of operating systems to contend with. Obviously these should also be deployed on the network together with appropriate intrusion detection software. There is also a major issue for network owners having to contend

with differing access standards of various cellular network providers for the devices.

It may therefore be necessary for the organisation to have policies limiting the scope of supported devices and cellular networks, to keep costs in check. There are also considerations as to whether approved cellular networks are complying with provisions that mirror those required by the organisation to meet its obligations for data protection and privacy.

Certificate or token arrangements can also significantly improve network security. The main factors for consideration are the costs of implementation and maintenance for a user base.

Costs for licensing are dropping as more vendors come into the market. Costs, in fact, appear to have dropped by up to 90 percent overall compared to some years ago.

Nevertheless, as always, there is the caveat of quality verses price and the trade off there to be taken into consideration. There also are single sign on arrangements. However, I would caution against the use of any purely automated access process that does not challenge a user trying to access a network. This has specific dangers as the risk of unauthorised access from a compromised client device, undetected for an indefinite period, greatly increases the scope of anyone alleging breaches in an attempt to bring a class action.

Monitoring Data Traffic

Firewall management and data traffic monitoring are critical to successful network security management. A key concept that should be implemented is two way port management: networks often block incoming traffic on ports; however, all outgoing ports are open. This means that if a rogue piece of software is installed, it may not be picked up if it uses a port that is not being monitored.

Thus, it is important that ports which are not being monitored are disabled.

This poses many headaches for network administrators when it comes to getting applications to work for users, and consequently there is a reluctance to run tight controls.

It is true that many attacks are now on the most popular port types, such as port 80 used for computer browser software. Nevertheless, we would insist that it is important to limit the risk of undetected infiltrations occurring for extended periods, given the reasons outlined above.

At the moment, there also are a range of software options under development for managing the output from protection mechanisms to highlight areas of possible risk and assist the network administrator. As more vendors roll out such solutions, competitive forces will decrease costs.

The Need for Standards

As mentioned previously, encryption is clearly a good way to protect network assets. There are various facets here, including data encryption on storage devices and encryption of communications and connections between devices. Encryption is considered to be more effective if the encryption occurs without the receiver knowing the senders encryption method. However, as there are ongoing difficulties with standards, these issues are subject to difficulties in implementation. In addition, the absence of end-to-end standards means that there also are risks that the data may become unencrypted depending, for example, on the routing of traffic.

Updates: The Inherent Vulnerability

One area of security which is getting a lot of media attention (with good reason) is that of keeping software on computers up to date. This is a dangerous issue. I believe that it is only a matter of time before attackers start to exploit automatic updates as a way to trick users into installing malware.

Once again, fortunately, new vendors are coming on to the market with software to monitor a network computer or user device and automatically update any components that are required. I think this is a really useful development: by controlling the update process via one application, the risk of a rogue process masquerading as a legitimate update is greatly reduced.

This would also relieve general users of the responsibility of trying to decipher complex technical processes and determine if something is real or not. Once again, this is a return to my original premise that users should not be required to resort to observation in order to try to keep networks safe. That is a job for professionals, and the responsibility of the owners of a network.

Published on : Thu, 30 Dec 2010