GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

The Present and Coming Security Threat of Internet Appliances

Christopher J. Holm
10 January, 2001

The PC and Internet revolutions each brought with them significant new challenges for technology, computing, and the society that they support. Even though the technology professions have risen to the challenges of distributed computing and are fortifying best practices to deal with each of them, a new wave of threats fast approaches – some would argue that it has already reached our shores, though its full force has not yet been felt. Empowered by communications and computing technologies, the advancement of Internet and web-enabled devices, known collectively as Internet Appliances (IAs), bring with them some familiar security challenges our profession is still learning to grapple from the last waves.

Depending on your viewpoint, the fact that mobile devices and communications are integrating might, or might not be, a good thing. What is undeniable is that they *are* converging, *right now*, under our very noses. And although the power of this synthesis is displayed openly in the media every day, what is not nearly so well-understood is the impact of these technologies on businesses and individuals. Particularly, the pervasive use of powerful applications on phones, faxes, Personal Digital Assistants (PDAs), handheld / wearable computers, TVs, and other young or yet-to-be-conceived devices will drive the need for pervasive and effective layered security measures for these technologies. One thing is for sure: it's not just securing PCs and servers anymore.

In this work, I will outline a framework for dealing with the security threats presented by IAs, drawing upon the standards emerging from the fields of industry and personal creativity. Luckily, the same concepts that applied to PC and Internet security are valid in the realm of IAs; it is merely the implementation of the technology that differs. Since this is a discussion mostly about technology threats, it might be inappropriate for me to delve deeply into the fields of privacy, trust, or digital rights management, although they are inextricably bound to and impacted by IAs.

As technology security professionals, we are all familiar with developing strategies and policies to deal with technical solutions, manage these solutions' deployment, and monitor the security events surrounding them. But at what levels should we apply these concepts? And further, how do these concepts apply to Internet Appliances? A wide array of experience and training have formed a model for describing technology security at the application, data management, platform, network, and physical levels. Although I cannot claim credit for inventing this model, I will use it to describe IA technology and the threats it presents to us. At every level of this model we should strive to implement strategy and policy, technical solutions, deployment management, and event monitoring in our organizations.

Physical Level

The simplest idea of which to conceive is that of physically securing devices with powerful access potential. Doubtless, many in our industry know at least one person or the story of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

someone who has once lost their PalmPilot, or forgotten their cell phone in another city on a long business trip. Of course, these losses are usually high-impact and high-stress for that individual, especially because these tools usually "control" that person's life. Calendars, contact lists, personal financial plans, business memos, and other personal data are "gone" in an instant, sometimes including the ability to use that information at all. Whether or not they recover their digital instrument or not, the damage is done. Add in the potential for that device as an IA and the impact of loss goes even higher, especially if there are no controls for accessing, changing, or destroying information stored on the Net or corporate information system. Whether it can be changed or not, even knowing where or what kind of data the victim accesses can be harmful and dangerous in the hands of a less-than-honest discoverer. Furthermore, with the convenience of lightweight applications that store the logins and passwords required for other security levels, the only real assurance a device user may have is to know that initial access is difficult to obtain. As an example, the Palm V PDA has a lock-out feature that requires the correct password to be entered before the operating system starts. So it is imperative that some similar and practical measures be taken to secure IAs at a physical level. The following are some of practical methods to utilize:

Loss Preparedness – Users need to be especially aware of the location of IAs, both for personal and corporate reasons. When an IA is lost or missing, a good policy would provide that corporate IS personnel are advised, so that they can begin to lock-down impacted accounts or monitor for malicious activity. Additionally, an individual's Internet user accounts should also be disabled as quickly as possible, or the passwords changed before any real harm or theft affects their personal affairs or property.

Lock-out - Because this feature may not normally be enabled on most IAs by default, an essential part of any personal or corporate security policy would be the enablement of a lock-out password, within advised password strength parameters.

Safe Beaming & Sharing – Users of IAs should be aware of the "promiscuous" modes of their IAs, some of which leave themselves open to "beaming" at their infrared ports. Although both the Palm Pilot and most other PDAs request confirmation prior to downloading programs and files, it's only a matter of time before the right Worm comes along to convince users of this potentially dangerous channel. Perhaps the only practical way to protect against this is to cover the IR port until needed. Savvy IA manufacturers will begin to incorporate this into their designs.

Shoulder-Surfing Zones – As nearly all users of desktop and laptop PCs already know, sensitive information can be gained fairly easily simply by watching a person's activity near a computer. IAs are no different – and can be stolen more quickly and effectively than a desktop, server, or laptop. Users should be aware of their surroundings (airports, hotel lobbies, training centers, etc.) and take appropriate precautions to reduce their exposure to prying eyes and fingers.

Network Level

Because of its relative newness and rampant technology change, this level of security for IAs is wide-open for abuse and misuse. Fortunately, some of the earliest vendors of IA networking

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

have taken a strong technical lead, learning from some of the naiveté and exploits of our recent hard-wired Internet history. For example, the OmniSky mobile networking service appears to have combined several time-proven technologies to create a reasonably secure and efficient network. OmniSky's client modems use standard TCP/IP protocols, but encapsulates them with Elliptic-Curve Cryptography (ECC) for the Palm OS on the wireless-end, and further encrypts transmissions to the Internet using the RSA algorithm on the wired-end of their networks for web-clipping applications. Windows CE devices support RSA encryption at the device level, but the algorithm is less efficient and consumes more power this way. Using these methods, the IP address of the IA is never broadcast in the clear. Furthermore, IA authentication is completed using several Public Key Cryptography techniques, associating the device's address with a hard-coded private key pair. It is by this method that OmniSky ensures that their client devices are authenticated on their wired and routed network, also guaranteeing that OmniSky customers are appropriately billed. Because of these layers of network security, IAs using its service are more vulnerable to physical, platform, and application-level hazards than they are at the Network level.

Similarly, the BlueTooth wireless radio standard is emerging for other types of wireless devices and IAs. The BlueTooth Special Interest Group (SIG) has decreed that compliant devices by manufacturers must make at least 1600 radio frequency hops per second, and automatically adjust their transmission power levels to accommodate for the proximity of the device with which it is networking.

OmniSky's example of technology is a good one because of its trust not in one be-all-end-all proprietary technology, but because of it's combination of layers of network security. Certainly OmniSky will not be the only vendor to come forward with this technique, nor should they. Likewise, the BlueTooth standard is rapidly being adopted by many companies seeking to integrate IAs and other devices, like telephones. The accelerating use of IA technologies will need to follow similar paths if network-level security is to be trusted for these devices.

Transmission Encryption – Vendors, users, and managers of corporately-deployed IAs need to ensure that effective cryptography systems are in place for their mobile appliances. ECC has emerged as an effective solution because of it's relative "lightness" for the weaker processors of IAs. As time goes on, these processor strengths will continue to rise, so eventually a stronger system may be needed. For more radio-based systems, frequency hopping may be the ultimate solution, but it is likely that higher-end applications will need additional cryptographic techniques in the future to ensure the highest security.

Authentication – IAs need to be authenticated, much the same as NICs use MAC addresses for address resolution. Some method of device authentication should be required, but IA devices should likewise require authentication from their network routers and transmitters. Otherwise, the door is open to "downstream" transmission mischief and the veritable launchpads that hundreds of wireless devices portend for a network.

Routing – Secure routing techniques should be emplaced by companies and vendors for all hard-wired and potential future wireless routers, including edge and core routing techniques developed for today's Internet. Keep in mind that the hard-wired network should be physically

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

secured except to trusted administrators; if you can't trust the security of the wired network, you can't trust the wireless one, either.

Platform Level

Just as the PC revolution saw the concurrent rise of computing power and powerful operating systems, so will the next wave of IAs. Already, several strong contenders are in the running for IAs, including the Palm OS and Microsoft Windows CE. With an early lead, the Palm OS got its start from the quick adoption of Palm Pilot PDAs, eventually spinning off from 3Com to form their own subsidiary company. Now the Palm OS is licensed separately to several manufacturers, such as Handspring, similarly to the licensing scheme Microsoft Windows CE to Compaq, HP, and others. Both the form and function of these two platforms are radically different, but they both allow mobile device users to perform many of the same activities.

While the Windows CE operating system runs many familiar technologies in a lightweight version, the Palm OS was designed for personal information management from the beginning. As a consequence, Palm OS IAs tend to be more lightweight, with custom-written programs taking advantage of streamlined programming and limited device options. Conversely, CE devices require more powerful hardware (like the Compaq Pocket PC) with a wider variety of peripheral mixes, and offer familiar versions of PC office software such as Microsoft Excel. It is not my place to say which OS is more suited to the nature of IA devices, because regardless of their functionality, the security needs of emerging lightweight platforms are the same.

Required Services – The operating systems of IAs, similar to their client and server cousins, need to cautiously allow only those services to run that are required by the applications the user has opened. Because they are lighter-weight, IAs will generally tend to not have extraneous applications and services running, but as processing power and memory proliferate, unnecessary services will require more discipline to lock down. Managing these OSs may be foreign territory for both corporate and enthusiast users, but there are distinct parallels between securing IAs and securing both PCs and servers. Certainly best practices will emerge as device deployment continues.

System Management / Access Controls – Just as servers and PCs have configuration settings, IAs will need to be manageable in similar ways. The Palm OS has a hardware abstraction layer and kernel that define the interaction between hardware and software operation, and Windows CE has settings similar to its Registry keys for NT. Unfortunately, since IAs on the market have no hard drive, the ability to audit and store configuration settings on these devices is next to impossible, short of long-term RAM or written logs. Although there are many fewer events to keep track of for an IA, relative to a server, managing many IAs for corporate deployment many demand the ability to configure and track this information. Finally, if IAs are to be shared among people or groups, the ability to maintain separate user accounts, along with varying levels of permissions, will become a necessity. When it does, so will the requirement for user authentication; whether the method of choice is a password or biometric remains to be seen.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Data Management Level
This area of concern is the most difficult to appreciate at the current date, because of the limited storage capability of most IAs. In the client-server world, we would consider this to be the realm of databases. However, as mentioned earlier, most PDAs and other devices today use flash memory for their processing. There has been development work on corporate "wireless" database systems, but in actuality the mobile device merely communicates with a database server, which actually stores database records and other information. The primary example is SQL Server 2000 for Windows CE, a scaled-down multi-platform version of the server-based RDBMS bearing Microsoft's mark. Most other data management is performed at the application level of these devices, with data being stored in flash memory or on other hard-wired systems. As long as this is the case, many of the same rules apply for IAs as for other client-server based systems.

Access Controls – Both for applications and for users, data management design will need to continue to focus on the appropriate level of access control to the plethora of information in corporate personal database systems. These systems should, for now at least, be treated as an extension of the access rights already available from PCs. Similarly, they should be encrypted at the file & disk level whenever performance allows, and protected from all the hard-wire threats familiar to today's database security designs.

Application Level
The application level presents one of the most challenging threats to security for IAs. The first PDA viruses have already been unleashed, and the first IA worms cannot be far behind. The most popular application for IAs is email, with Internet browsing a not-so-distant second place. With all the known threats to these types of applications, it is the growth of Internet applets and macros that will threaten IAs the most in the near future, precisely because they may tend to be inherently trusted by these popular and potent messaging and surfing programs. The threat of application-level vulnerabilities is merely multiplied by the many devices that are now finding themselves Internet application-equipped: digital cameras, GPS, telephones, etc.

Viruses, Worms, & Trojan Horses – These will be difficult to stop at the IA device level until processing power and memory allows for more active monitoring. Until then, the major anti-virus vendors have releases for the already-present viruses and corruptive programs, which reside at the desktop level for PDA synchronization. Still, "beaming" and downloading provide channels for these intrusive programs to attack IAs, and most effective defense for now may be an educated user. As messaging and browsing programs become more powerful on IAs, watch for this threat to increase.

Data Leaks – All applications give out information about themselves and their systems over the network in order to get properly formatted and configured information. As any administrator of a web server knows, publicly known vulnerabilities are relatively easy to attack until a patch or fix is applied. And should the network or physical levels of security be compromised, application-level access provides an intruder or eavesdropper with loads of data, with quick and harmful consequences. Since most IA programs today do their own data management (without a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

local database), the application level provides perhaps the richest trove of information that could be intercepted, duplicated, or analyzed by a would-be or current attacker.

Conclusion

While the challenge is before us, all is certainly not lost. The wealth of knowledge the technology community has amassed over the last decade is staggering, with many parallels between the hard-wired world of client-server and Internet platform computing, and that of Internet Appliances. Luckily, we are watching as these mobile devices grow up before our eyes, knowing that many of the same concepts that threatened us in the last decade of PCs and the Internet will re-emerge in a familiar form. Preparedness and awareness is the key to keeping alive the promise and performance of Internet Appliances in the future.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Palm, Inc. "Handbook for the Palm V Organizer"
File: http://www/palm.com/support/handbooks/palm5.pdf (January 4, 2001)

Bluetooth SIG. "Bluetooth Security FAQ."
URL: http://www.bluetooth.com/bluetoothguide/faq/5.asp (January 5, 2001)

OmniSky Corporation. "OmniSky Security White Paper" Revision 1.0. April 17, 2000.
URL: http://www.omnisky.com/support/security.jhtml (January 5, 2001)

Palm, Inc. "Palm OS: A Flexible Architecture for Innovative Solutions."
URL: http://www.palmos.com/platform/architecture.html (January 5, 2001)

Microsoft, Inc. "Microsoft Windows CE 3.0 Datasheet." September 1, 2000.
URL: http://microsoft.com/windows/embedded/ce/guide/datasheets/ce30datasheet.asp (January 4, 2001)

Microsoft, Inc. "System Requirements, Installing SQL Server CE" September 1, 2000.
URL: http://microsoft.com/sql/productinfo/cesysreq.htm (January 4, 2001)

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: April 26th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS