



IT Security and the Curse of Complacency

An IRM White Paper by

Matthew Lewis



IT Security and the Curse of Complacency

Introduction

This paper aims to stimulate thought and discussion around the current state of the IT security industry. Fundamentally we aim to dispel the notion that IT security is now less important owing to improvements in attitudes towards security and secure system design. We discuss the 'curse' of complacency in this regard, and the pitfalls associated with perceiving security as a self-deprecating function, as opposed to the ongoing process that it is. We present a snapshot of common perceptions regarding the state of the industry, and how complacency in these areas is harmful to the overall security of any existing or new system. We highlight ideas on how the industry needs to evolve in line with the fast pace of IT development, which brings with it ever-evolving attack vectors that must be identified and understood as part of the security process.

Assumption: Exploits are dead

On a technical level, some would purport that conditions such as buffer and heap overflows are no longer an issue. Advances in operating system security design and stack protection mechanisms does mean that future software will be harder to exploit, but not necessarily impossible. The complacency in this area would be to strike such vulnerabilities off the critical list owing to the difficult nature of their exploitation. As technical implementation advances, so does our understanding of those technical details and ultimately how technical security measures, no matter how complex, may be subverted.

Even the skill-set of the 'script kiddie' has advanced in recent times, while understanding of kernel-level bugs and exploits is now more advanced than ever. For example, the concept of the buffer overflow is no longer nebulous. Coupled with multiple tools that exist to assist in authoring exploits, proof-of-concept exploits can often be written within minutes of finding vulnerabilities. This process has evolved into a fundamental component of the software patching domain. The publication of advisories based on found problems is now reported to software developers quicker and better than ever, which in turn has resulted in a much improved patch turnaround since most major software vendors now realise the severity of critical flaws in their products and what that could mean for customer relations and lost revenue. Ongoing research and responsible disclosure of vulnerabilities to vendors is therefore key in maintaining high-levels of software security levels, and should not be dismissed owing to complexities in modern operating system and software design.

Related to the area of exploitation is the security of legacy systems and software. As technology advances, interest in older technologies dwindles as the new 'bigger and better' versions become attractive as targets of attack. The complacency element here typically surrounds the mentality of *'if it ain't broke, don't fix it'*. While there is nothing necessarily wrong with this attitude from a device productivity perspective, it often renders older technologies incredibly vulnerable since no security appraisals have ever been conducted (or allowed) on those systems. The number of much-used commercial and open source legacy software components that have never been security audited is

likely to be staggering, and therefore presents an untapped resource for motivated attackers seeking new challenges.

Assumption: We're running out of OSI layers to explore

Over the years, hackers and security researchers have explored the security of the OSI network layers from physical link to application level. The trend has been to examine each level in depth, which has resulted in identification of vulnerabilities, and in many cases, appropriate patching. The exploration has then typically advanced to the next OSI level, which at the time of writing has resulted in much concentration and exploration of application-level attacks which includes the likes of SQL injection, session hijacking and Cross-Site-Scripting (XSS). The complacency danger here is to assume that the lower OSI levels are now secure. New IP stacks are still subject to introduction into network devices, while changes are constantly made to existing IP stacks for specific security/functional requirements. Most network devices and embedded systems employing network capabilities are likely to implement bespoke networking code, thereby deriving a large field of exploration of the differing IP stacks and operating systems for attackers and researchers. Exploration of application-level security is paramount and yields a wide attack surface that requires continued research and investigation. However, it is also prudent to continue security audits of network devices at all levels of the OSI model to detect any flaws that may have been introduced as a result of changes in code or design.

Assumption: I won't be Socially Engineered

As technical security has improved, the shift of exploitation predicated on user actions has been significant. The modern-day attacker will typically require a number of satisfied user conditions before a return on the attack-investment is made. Examples include tricking users into clicking on links to malicious websites, perhaps through XSS vectors, or downloading and opening malware that may in turn exploit technical vulnerabilities. It would be complacent therefore to assume that the human operator is sufficiently knowledgeable not to fall foul of such activities - attackers will spend much time and effort in deriving realistic and convincing spoof sites, redirections and e-mails that might sometimes fool even the commonly suspicious among us.

The other major problem in the field of social engineering is our willingness as humans to offer much information about ourselves to the Internet. Social networking sites such as *Facebook* provide a convenient method for attackers to identify specific groups and individuals that perhaps work for an organisation in scope for attack. An attacker might easily infiltrate a social network to obtain technical details or befriend individuals to reveal sensitive information that might result in further access into the target network or organisation. Even if organisational policies exist to prohibit use of such sites during work hours, the average worker is likely to be using such sites in the comfort of their own home after work hours. While on-going user education schemes and maintained policies are key in minimising the risks in this area, it is unlikely that this will ever fully eradicate the threat of social engineering.

Assumption: Software security is handled by APIs

Numerous claims exist of improved security in modern software. The Software Development Life-Cycle is now far shorter owing to feature-rich APIs that makes programming easier and more accessible than ever, and the paradigm shift from coding in assembler where each byte was precious and carefully evaluated to where coding is today is significant. The danger in this area is to put all trust in security components of such APIs, which for some applications could span thousands of lines of code. Without complete source code audits and reviews of these APIs, it would be complacent to assume that their security functions are flawless. Much code in the modern development life-cycle is now pre-written or auto-generated from configuration files and should therefore be carefully evaluated in order to gain at least some level of assurance in their stability and correctness.

Misconception: My software says I'm secure

Graphical User Input (GUI) and software trust can be problematic for security. As GUIs develop with modern operating systems, security-based products that traditionally relied on command-line interaction for configuration are now fully configurable through GUIs – examples include IDS/IPS and firewall configuration. While GUIs can make device configuration far easier, there is typically an enhanced layer of abstraction with the use of a GUI tool that may not relate the significance of the security that is currently under configuration. The 'point-click-save' habit could lead to a number of issues if the specific actions being performed are not fully understood by the system operator.

Similarly, a big danger with GUI tools is the potential misinformation relayed to the user. For example when a GUI presents the user with a message such as 'Your Network is Now Secure', perhaps with a green tick box icon, human nature is to trust such assertions and to move on. The reality of that situation however may be completely different, depending on the context and specific application.

Assumption: Our employees are trustworthy

The magnitude of insider threat is huge. While organisations can spend six-figure sums or more on defending their border gateways, there is still much scope for malicious employees to compromise the security of an organisation in a number of ways. Internal security and lockdown is just as important to minimise the possibility for employees to escalate their privileges across internal networks.

Employee turnover is far greater today than ever, and it is common for contractors and other third parties to join and leave organisations for specific work tasks, which ultimately increases the potential exposure of an organisation's IT and intellectual property. Lack of policy on device connectivity to internal networks can be extremely damaging, paving the way for the introduction of malware into the network, or exfiltration of sensitive corporate data. For example, the ever-increasing logical size of USB memory devices with their simultaneous physical size reduction makes for the perfect mechanism for a malicious employee to copy and remove copious amounts of corporate data, possibly undetected.

Assumption: Our security is outsourced

Outsourcing of technology, software and security is more common now than ever. For example, a large enterprise may purchase physical servers, outsource management of the servers to third parties which in turn may outsource application development to further parties. While the rationale behind such practices may be to allow the relevant experts in their field to perform their relevant duties, this can often result in confusion over actual ownership and responsibility of security. In these situations, security tends to suffer – if efforts are made to apply security controls, there may be too much red tape and bureaucracy involved in configuration change requests that typically push security to the bottom of the agenda. It is complacent therefore to assume that security is actually considered and properly implemented within systems that are managed and maintained by multiple parties. Security should form an integral part of all phases of an IT System Development Life-Cycle. Without proper mandate of secure build standards, secure application development and secure network design, organisations cannot appreciate with any confidence the security posture of their systems.

Assumption: Wireless is now secure

Wireless technologies now form a fundamental component of modern networks, and adoption of wireless technology is likely to continue for some time, particularly due to its application to pervasive computing. The issues with early wireless security such as WEP are well-known and improvements have been made to improve the confidentiality and integrity of wireless networks. Despite these improvements, the inherent risk of convergence with backend or internal networks remains. Wireless interfaces into networks could expose entire corporate networks to the outside world, whether through misconfiguration, or introduction of rogue access points by malicious employees. Opportunistic attacks are far more likely in this area, as attackers may simply need to be within a specific physical locality in order to gain access to sensitive corporate networks. As mentioned earlier, no amount of border control filtering can protect against malicious or incorrectly configured wireless access points directly connected to an internal LAN.

Not only is the network cable becoming redundant owing to wireless technologies. Modern PCs now come equipped with Bluetooth interfaces, which enable traditional cabled input/output devices such as mice, keyboards and printers to be connected without wires or cables. Obviously this presents much scope for the possibility of key logging and data interception without the requirement for physical taps or devices on the victim PCs. The open airwaves are therefore likely to form the future attacker's main playground.

The other main concern in this area surrounds the modern trend and availability of home-working. It is now common for employees to take corporate laptops home and connect via a VPN into corporate networks for this purpose. Without any confidence in how employees are connecting to the Internet and internal corporate networks, organisations cannot know that their networks are safe. Many home users now access the Internet via home wireless access points, which are typically shipped without much, if any, default security configuration. Default credentials on the wireless access point or lack of

security could mean that attackers within the locality may be able to access the home-working devices and data of employees, particularly if the corporate laptop build is not sufficiently hardened.

If attackers are able gain such access, then it is also technically feasible for authenticated VPN sessions into internal corporate networks to be hijacked by the attacker, thereby providing direct, authenticated, and as far as the corporate VPN terminating devices are aware, legitimate access to the internal network. Assuming that the corporate network is secure owing to VPN configuration would therefore be complacent – much future work is required in defining secure build standards for home-working devices, VPN connectivity and guidance on use with non-corporate networks. User awareness of the dangers of incorrect home wireless access point configuration is also needed to minimise the risks in this area.

Assumption: We're secure, we have firewalls

The misconception that firewalls are a solution to border security still exists. Firewalls can be compromised in a number of ways, whether through exploitation of known coding flaws, or through taking advantage of lax rules that may have been configured. A common scenario within the firewall configuration domain relates to the introduction of new systems into a corporate network. Should the systems not work across the organisation, the typical line from senior management to the network administrators is to do whatever it takes to make the system available, particularly if deadlines aren't being met, or the new system is not making the organisation any money due to its downtime. Such a scenario typically results in the proverbial ruleset configuration of '*Allow ANY ANY*'. Even a momentary hole such as this could provide the opportunistic or dedicated hacker that's been probing and scanning a network for months or even years with complete access to an internal network. Even worse is the potential for the temporary solution to be forgotten, thereby permanently exposing the entire organisation owing to the fully allowed ingress and egress traffic.

It is complacent therefore to assume that an organisation is secure if it employs firewall technologies. Only regular audits of firewall rulesets and configurations can provide organisations with some degree of assurance in the security of their networks.

Reality: Moore's law continues

Processing power continues to increase, while its cost decreases. Those security solutions that traditionally relied on computability theory for their protection are fast becoming vulnerable owing to the ability to brute-force and compute quicker, better and cheaper than ever. At the time of writing, recent media reports of a security researcher harnessing the power of a PlayStation 3 to effectively crack passwords is just one example of the accessibility of raw computing power to the average person. It is therefore paramount that the IT security industry maintains pace with such developments, as cryptographic solutions that may be secure today may not be so in the near future.

Assumption: We have policy and compliance

IT security is best delivered through comprehensive policy and compliance. Despite this obvious fact, many organisations do not follow their own IT security policies, or even worse, do not possess an IT security policy or standard to follow. Policies can help organisations to factor security into multiple components of a system, from password lengths and strengths to secure build standards. If an organisation holds a policy, it is complacent therefore to assume that this is followed. Similarly, even if an IT security policy does exist within an organisation and is actually followed, that policy should be subjected to a continued state of refinement and updating, to reflect the changes that are occurring in the IT security world, as exemplified through the various sections of this whitepaper.

Certainly concerted efforts are being made across parts of the industry to make improvements in this area, such as PCI (Payment Card Industry) and DSS (Data Security Standard) compliance. It is important that organisations understand the security of both their own internal data and intellectual property, and any client or personal data that may be held on their networks. Policy and compliance goes some way in helping organisations to achieve this understanding, and should not be overlooked, particularly as IT systems grow and become more complex.

Assumption: Web 2.0 is secure

Web 2.0 promises to enrich the user web experience. The semantics of data is becoming ever more important, and there will be a strong requirement for aggregate applications, particularly parsers and renderers within Web 2.0 that will seek to combine and render web searches and web site information in new ways that are more convenient and applicable to the individual. It would be complacent to assume that Web 2.0 will be more secure, purely due to its numeric version increment. Web 2.0 will bring with it most of the existing vulnerabilities of Web 1.0, in addition to a host of new attack vectors surrounding technologies such as AJAX, and software errors in the range of parsers and renders that will be required to comprise Web 2.0 functionality.

Reality: Future technologies

Future technologies will bring with them multiple challenges for IT security. In this paper we've merely scratched the surface of existing security issues. As a few examples, far more security consideration will be required in the future for biometric and RFID systems for example, particularly in conjunction with national ID schemes such as electronic passports and identity cards. Intelligent software agents will also bring with them a number of security considerations, particularly where those software components will be introducing levels of non-determinism within network management and control owing to artificial intelligence engines that seek to protect networks or systems. Digital Rights Management (DRM) is also set to become an important area for security, whereby maintaining the integrity and ownership of data will be important to many systems. Attackers are likely to spend much time and effort in subverting technical measures that aim to protect digital data. Finally, IT convergence will bring with it multiple security challenges, as we aim to provide end-to-end security through multiple interconnected networks of different technologies and over a combination of wired

and wireless media. It is important that all existing IT security risks are understood as technology advances, as the older vulnerabilities are likely to permeate through the newer technologies that will bring with them new vulnerabilities and threats that need to be identified and mitigated.

Conclusions

This paper aimed to highlight the curse of complacency, and how the IT security industry risks becoming complacent by neglecting the issues described in this document. We remind ourselves of the principle that security is a process and not a solution, and that improved security merely raises the bar in terms of the skill levels required to identify and exploit vulnerabilities. Owing to the issues discussed in this paper, the number of challenges available to attackers and researchers in this field is vast. The other important fact to remember is that none of us are infallible. Complacency and user-error will always find a way, which could ultimately be detrimental to the security of a system or organisation. This fact alone is proof of the value in regular audits and risk management exercises which help organisations to understand their current security posture, and the effectiveness of incident response mechanisms that they choose to implement.

IRM has not become complacent. IRM is engaged with industry and clients on multiple research and consultancy projects to help identify those inherent risks and vulnerabilities that could affect the security of systems and organisations. IRM's wide-ranging research programme helps fuel the technical and risk consultancy teams with current information on the security issues surrounding old and new technologies, which ultimately derives a dedicated team of consultants and researchers ready to embrace the IT security challenges of the 21st Century.

About the Author

Matthew Lewis is a Security Consultant at Information Risk Management Plc (IRM) where he performs a range of consultancy services. Prior to working at IRM, Matthew read the MSc in Computer Science at Oxford University, where he majored in formal methods for system specification and design. He then spent over three years at CESG (the UK Government's Information Assurance arm) researching network security and biometric system vulnerabilities. Matthew has presented at many international conferences on the subject of biometric security and co-administered the UK Biometrics Working Group. In March 2008 Matthew will be presenting his work on a biometric keylogger at Black Hat Europe 2008. He is a CESG CHECK Team Leader, and a member of the British Computer Society.

About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at www.irmplc.com for further information.