

## Q3 2007: THE STATE OF CYBER-SECURITY VULNERABILITIES

Rather than attempt to tackle the related policy issues in this limited space, given our view from the digital ventures world, we choose to focus on *two critical factors* that govern the current state of cyber-security, and allow this statement to be used by those more focused on the related policy matters. These factors have differing but related effects on three areas of great public policy concern: [1] personal information privacy; [2] digital commerce and business continuity; and [3] critical infrastructure security especially in the context of homeland security.

Both factors share a root cause of wide reliance on commodity operating systems and other infrastructure software (“*commodity platform technology*” or “*CPT*”) that have proven to have a pervasive characteristic of continuing security vulnerabilities.

**Factor #1:** The first factor is the state of threat against commonly deployed systems used for typical purposes including personal computing, server computing, and datacenter infrastructure. A great many of these systems rely on CPT, with the result that a large number of them are compromised or vulnerable in similar ways, often referred to as the “*monoculture problem*.” The current state of threat has two characteristics: [1] variety of mechanism, and [2] motivation of adversary. Variety is characterized by the continually evolving variety and sophistication of attacks, of uses of compromised systems, and sophistication of stealth mechanisms to hide both. The motivation of adversary can be summed up in a phrase: *criminal enterprise*. Sophisticated adversaries are part of an ecosystem of increasingly organized crime wherein compromised systems are commandeered as tools for theft and fraud for financial gain, particularly the deployment and management of “botnets” for use in phishing, DDoS attacks, and propagation of malware for financial fraud. Both the variety and motivation are indicated by the ever expanding jargon of malware: *polymorphism, blended attacks, rootkits, keyloggers, sub-virts, bots, and botnets*, to name a few. It has become an arms race to address. And we for one have no trouble properly labeling this “*Cyber Terrorism*.”

**Factor #2:** The second factor is the increasing mismatch between CPT’s primary benefits – ease of modification to run arbitrary software – and the needs of systems built on CPT. An increasing variety of *fixed-function systems are built on CPT for convenience*, despite the fact that flexibility and easy modification are not desirable (*quick examples include bank ATM machines, parking lot pay*

*kiosks, and digital voting machines*). At the other end of the spectrum are PCs for which easy modification is an end-user benefit, but where the flexibility also enables the variety and sophistication of malware.

**Impact on PII:** For personal information privacy, one measure of effect is shown by estimates of the proportion of personal computers that are currently compromised: a variety of estimates vary around 20% +/- 10%. *These systems are fundamentally incapable of protecting personal information*, and are often used as tools in attacks to compromise other systems. Given the large proportion, and the large absolute number of systems, this situation must be regarded as a fixture of the landscape for the foreseeable future.

**Impact on Business Continuity:** Similar consequences apply for digital commerce and e-business. Although such business systems are sometimes more amenable to detection and correction of compromise, they *continue to be undermined by the combination of the continuing stream of vulnerability discovery, and the availability of botnets of compromised personal computers available for use in concerted attacks* on business systems with data of monetary value to attackers.

**Impact on Critical Infrastructure:** For critical infrastructure (CI) systems the consequences apply in a similar way but with two variations. [1] First, *the impact of attack can include public safety, basic service availability, etc.* [2] Second, the flexibility of CPT is often not at all needed for special purpose systems (e.g. *control systems for hydro-electric dams, nuclear reactors, power grids, chemical plants, etc.*) These are often fixed-function or special purpose systems that have more recently “entered the monoculture” of CPT for cost and convenience of development and management, rather than an intrinsic need for CPT features.

Across the range of privacy, e-commerce, and homeland security, these same two factors contribute to an increasingly entrenched “installed base” of compromised and stealthed systems, managed and used by criminal adversaries, and available for use in further attacks for cyber-crime or possible cyber-terror. We believe the policy implications should be clear from this overview; however, we observe one of the more obvious: Consideration must be given to the continued allowance of commodity platform technology as the foundation for function-specific applications such as in the case of digital voting equipment or any critical infrastructure management utilities.

---

**NT+D Ventures – Digital Ventures Advisory**  
John Sebes | 415.203.8020 | [john.sebes@ntd-llc.com](mailto:john.sebes@ntd-llc.com)  
Greg Miller | 415.381.1414 | [gam@ntd-llc.com](mailto:gam@ntd-llc.com)