Evolution of Information Security Technologies

Created by Dan Hitchcock
Security Architect, Microsoft Information Security
October 7, 2005

Abstract

The intent of this document is to provide a succinct, high-level view of the changing control landscape in the practice of Information Security. Previous state is covered briefly, with focus primarily on present-to-long-term state (i.e. next 5-7 years). This document is intended for consumption by business decision makers, architects, and system/software developers in the Information Security space.

Scope

The trends discussed herein are applicable to any digital information-bearing organization, but most relevant to private enterprises with requirements to interact with external entities, wherein there is a reasonable expectation that the enterprise's data will reside, at times, on networks and/or hosts outside of the enterprise's span of direct control. As a counterexample, a military installation with a network of computers operating in an underground bunker with state-of-the-art, highly scrutiny, highly redundant physical security controls, and no external connectivity, may have minimal need for specific host or data security controls, and place a much higher reliance on the network itself than any enterprise with external connectivity can justify. Such physical and logical control scenarios are rare in private enterprise.

The Evolution Graph

The graph below depicts anticipated trends in three major control categories: Host, Network, and Data. The y-axis (low/medium/high) represents (*) *utility,* which is defined here as the relative availability of tools and technologies, combined with their effectiveness at mitigating information security risks. The x-axis denotes time.

It is important to note that the graph is *both descriptive and normative*. In other words, the trends depicted are consistent with industry and attack trends, but the longer-term states are *ideal conditions* that can only be achieved through the combined efforts of the information technology and development communities.

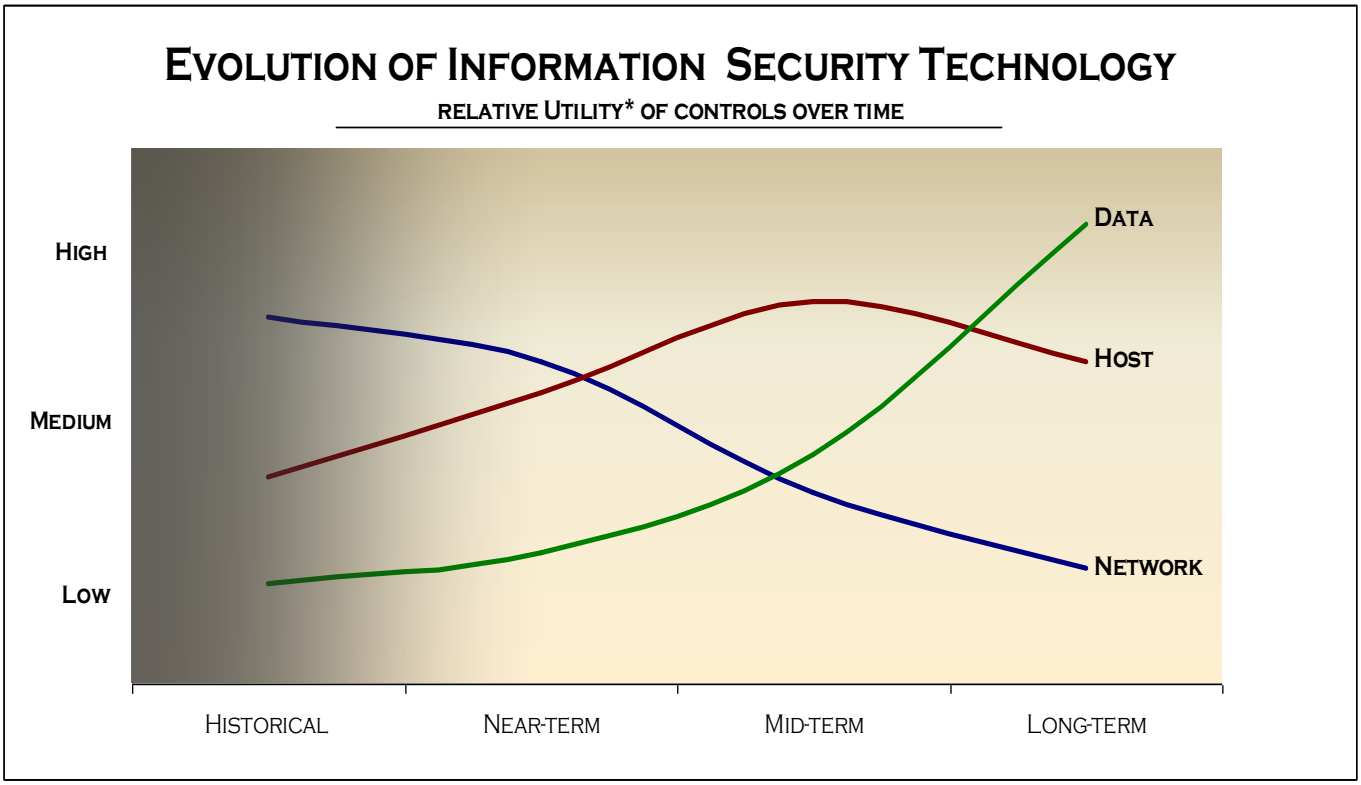

Figure 1 - Relative Utility of Security Controls over Time

Definitions

The terms "network," "host," and "data" above were chosen for their high "recognition value." In other words, these high-level categories make the trends (above) and technologies (below) instantly consumable for a wide audience. In truth, these terms are used merely as representations of three key categories, as defined below:

HOST refers to the systems responsible for the housing of digital assets. HOSTS petition access to NETWORKS and DATA as instructed (either directly or indirectly) by a human. They are the endpoint for access to digital assets from other petitioners. A personal computer running Windows and Internet Explorer, being operated by a human, is an example of a HOST. A "Smart Phone" accessing mail via Outlook Mobile Access is a HOST. A high-end, mutliprocessor server in a datacenter is a HOST. A laptop in a lead suitcase is a HOST. A Storage Area Network (SAN) is also a HOST.

NETWORK refers to all systems, devices, technologies, and equipment responsible for transporting data between HOSTS. A router is NETWORK. Cat-5 and fiber-optic cabling are NETWORK, as are WiFi RF spectrum, phone lines and phone switches, and GPS signaling. A network-based firewall appliance is NETWORK.

DATA refers to the actual bits-and-bytes that represent human-created and/or human relevant information. All digital assets consist wholly of DATA. A Word document on a hard drive or in a computer's memory is DATA. An analog phone conversation being transmitted over copper is DATA. The result of a SQL Server query as displayed on a computer workstation is DATA.

Technology Trends and Timeframes

The Evolution Graph above depicts a few key notions:

- The graph shows three distinct periods of dominance, or "ages," as represented by the highest of the three lines on the graph in a given time period. We are currently in the "Age of Network Security; the "Age of Host Security" and the "Age of Data Security" lie ahead.
- In the present and near-term, network-based security controls retain the highest utility of the three control categories.
- None of the control categories ever go to zero-utility, though their *relative* utility shifts dramatically over time.
- Data security controls must ultimately have the highest utility, and network security controls the lowest utility.

Network Trends

NETWORK has traditionally represented the key control against attacks and breaches. The first "firewalls," which appeared in the late 1980's, were "packet filters," or router-based access control lists. The first commercial firewall was a bastion host/application proxy-based product from DEC, based on their own internal firewall. Raptor Eagle followed shortly thereafter, joined by FWTK (Firewall Toolkit, which later became Gauntlet) in 1993, and Check Point's Firewall-1 in 1994. The market is now replete with a wide variety of firewall technologies, and the network's role has more recently expanded to include intrusion detection and prevention technologies (commercially, at least - network-based intrusion detection's roots span back more than two decades). In the present, the network is very frequently looked to *first* as a point of security control – though other approaches are recognized, a security engineer or consultant is quick to ask, "where are the firewalls and IDS systems?"

The relative maturity of network-based security technologies has two key ramifications: first, they are effective in their realm; second, their strengths and limitations are very well-understood by both security practitioners and attackers, and, more recently, business decision-makers. Of even greater impact is the ever-widening adoption of "untrustworthy" networks, most notably the Internet, by corporate enterprise for legitimate business purposes. The traditional paradigm of a "crispy outside and a chewy inside," describing a well-firewalled enterprise, is increasingly invalid, as the demarcation between "outside" and "inside" is dissolved by business scenarios such as "telecommuting" and increasingly network-dependent partner and vendor interactions. *As the hosts that carry an enterprise's data are increasingly found on networks not under the direct control of the enterprise itself*[1]*, reliance on network-based controls becomes increasingly unjustified*. The best network-based firewall and intrusion detection controls in an enterprise cannot mitigate attacks against their systems when those systems move to foreign networks.

Whatever forms the "network" may take over the long term, its most essential role will continue to be that of transport, i.e. ensuring appropriate delivery of traffic. From a security perspective, the role of the network in the long-term is simply to maintain the availability of the security control plane. Administrators should expect that the network will ensure delivery/denial-of-service protection for

[1] Common examples include the Internet, hotels, other corporate networks, public guest access networks, or virtualized "private" carriers sharing transport, driven by business scenarios such as mobile workforces, branch office connectivity, data-enabled mobile devices, etc.

that subset of traffic that ensures the security of a network – for example, audit streams, or policy delivery mechanisms like Group Policy.[2]

Host Trends

Hosts (and, for the sake of this discussion, the applications that execute thereon[3]) have historically taken the role of authorizing access for requestors, most often at the application layer. Telnet/SSH, Microsoft File and Print Sharing, and your online bank all utilize this approach. The host has shouldered very little of the burden for either protecting itself from the network, or interacting with data to ensure data security (beyond the simple access restrictions available through mechanisms like NTFS). More recent activity has showed the industry's increased awareness of the host's role in both. On the network side, host firewalls and intrusion detection/prevention packages have become much more prevalent, with increasing power to prevent illicit behavior from affecting the integrity of the host, and host-based IPSec authentication is starting to gain ground as an enterprise host protection strategy. Emerging technologies such as Trusted Platform Model (TPM) show an increased awareness of the host's role in securing credentials and keys relevant to data access. The utility of HOST as a security control is headed for its peak; the mid-term will see the pre-eminence of host-based controls over those provided by NETWORK and DATA. Key technologies contributing to the higher utility of HOST as the control point include enhanced ability to enforce least-privilege lower-layer access at the host (firewall/IPSec), improved boot/on-box authorization protection via Secure Startup and Full-Volume Encryption, and TPM. As the curve depicts, HOST will enjoy a "heyday" as the highest-utility control, as reliance on NETWORK controls decreases, and prior to the later high-utility phase of DATA. HOST controls will sustain a relatively high level of utility into the long-term; they inherently represent a control point closer to the asset itself (i.e. the data) than does NETWORK, and many DATA controls will have some interdependent reliance on the HOST. The trend depicted in the long-term, wherein DATA surpassed HOST in terms of utility, is representative of the fact that the "hosts on unknown networks" theme is repeated at this level – in other words, similar pressures such as "anywhere access" for employees and vendors, and increased business partner interaction, mean that DATA will increasingly reside on HOSTS outside the control of the data-owning organization. In this scenario, HOST controls alone clearly cannot be relied upon to provide data confidentiality and integrity.

Data Trends

The roots of data protection can be traced back thousands of years (see David Kahn's "The Codebreakers"). As in ancient times, the modern approach to data protection relies almost exclusively upon ciphers, often referred to in the security industry as cryptography. Present-day processing power enables the protection of data using cryptographic keys and algorithms that far exceed the complexity of the manually-processed ciphers of the early Egyptians, Assyrians, and Greeks. The objective, however, remains the same: to produce "ciphertext" with a very low probability of being deciphered (or "decrypted") by an unintended recipient within the useful lifetime of the information, but which is readily deciphered by the intended recipient. The aim is simple when thus written, but the implementation thereof has been difficult since the beginning, hampered by the classic challenges of key distribution and resilience to attack of the cryptographic

[2] This effort may produce the side-effect of ensuring *data availability*, which is of tremendous import to the business, but which is actually contrary to a pure security program – where the data itself is the asset, available data is the least secure data.
[3] An argument can be made for applications as a separate entity from host, network, and data, and there is also a compelling case for making applications a subset of DATA (i.e. data has no function in the absence of an application to present it). These are acknowledged; there is also a clear argument for applications as part of the HOST taxonomy (i.e. aside from the hardware, the HOST as we know it is essentially a collection of applications, from kernel to user). In the present context, applications will be discussed as a subset of the HOST taxonomy.

algorithm (or the implementation thereof). The advent of public key cryptography, commonly attributed to Whitfield Diffie and Martin Hellman in 1976, provided a quantum leap in the practicality of key distribution, but nearly 30 years later, encryption remains more the exception than the rule in private enterprise. The *adoption* has been hampered by significant usability and performance barriers, for both the individual consumer and the corporate enterprise. Current encryption/rights management solutions such as EFS and Information Rights Management as implemented in Microsoft Office, along with public-domain solutions such as the venerable PGP, have made some progress in this arena, but often support only specific scenarios such as mail or particular document types. Solutions to date struggle to provide a functional and user-acceptable solution that satisfies individual user, corporate user, and/or cross-enterprise use cases. As an example, the question, "how do I send information to friends or colleagues securely?" has many answers, is scenario-dependent, and the answers are often not readily within the reach of those who most need them.

Current and anticipated trends point to an increasing requirement for data-based security. In addition to the logic presented above around data *location* (that is, data on untrusted hosts, which are, in turn, on untrusted networks), both foreign and domestic legislation is driving increasingly strict regulations regarding data security. In the current environment, some the most commonly-referenced pieces of legislation driving towards data protection are:

- California Senate Bill 1386 (SB1386)
- Gramm-Leach-Bliley Act (GLB)
- European Union Privacy Directive (EUPD)
- Health Insurance Portability and Accountability Act (HIPPA)
- Sarbanes-Oxley Act (SOX)

A solid story around network- and host-based security controls is core, and remains well-justified in the world of 2005, but absent a data protection story, an enterprise that remains dependent on network and host controls is increasingly deficient, from both a risk and regulatory compliance perspective. Figure 2 (below) mentions some of the technological improvements that will be required in the Age of Data – the solutions impact hosts, applications, and even hardware, as the data is dependent on all of these components to be useful to people. The drive to such technologies is not optional, nor a theoretical "wish list" – the question is merely whether the industry will move that direction quickly enough to keep pace with current attack and regulatory trends. The alternative – to permit data protection technologies to flag in their progress – is to continue to expose consumers and enterprises to the increasingly painful consequences of inadequate data protection.

Technology Timeframes

The matrix below outlines some of the technologies expected to prevail in each of the three categories (network, host, and data) in the near-, mid-, and long-term. In the near-term, the examples are often named specifically, as we know with some confidence what the technologies will be within the next year or two. In the long-term, of course, the technologies are more conceptual, and in many cases, have yet to be born.

	NEAR-TERM	MID-TERM	LONG-TERM
	Example key components	Example key components	Example key components
Network	➢ Enterprise-wide network device configuration management ➢ Broad deployment of access control lists/firewall rules (layer 3/4 access control) ➢ Intrusion Detection ➢ Event Correlation of network data ➢ Denial of Service (DoS) protection ➢ Layer 2 access differentiation (e.g. 802.1x)	➢ DoS Protection ➢ Some deployment of access control lists/firewall rules ➢ Event Correlation of network and host data ➢ Layer 2 access differentiation (e.g. 802.1x)	➢ DoS Protection (subordinate technologies like 802.1x for integrity of QoS marking)
Host	➢ Patch Management ➢ Basic Anti-malware (anti - virus, anti-spyware) ➢ Base security state verification (antivirus, firewall on/off) ➢ IPSec domain isolation ➢ Introduction of Network Access Protection (NAP)	➢ Host Security State: ➢ Enterprise Management of host security - AV, Firewall, (Application Segregation/IPSec+Selective Authentication) ➢ IPSec host/application authentication/isolation ➢ Network Access Protection (NAP) ➢ Advanced anti-malware (add, e.g., behavior blocking) ➢ Intrusion Detection/Prevention ➢ Event correlation of network and host data ➢ Trusted Platform Model (TPM)	➢ Pervasive NAP + strong user authentication as sole "edge strategy" (implementation potentially shared between end-host and bastion devices) ➢ Event correlation of all security data (i.e. HOST security data) ➢ "trusted host" model to complement strong data-inherent protections
Data	➢ EFS ➢ Limited Rights Management (i.e. Office 12) ➢ IPSec/SSL transport encryption	➢ Extension of reach of data protection mechanisms (industry standards, mobile/removable devices) ➢ Volume encryption/secure startup (protection of local account store data)	➢ Pervasive data rights management/protection, portable across disparate business relationships, platforms, file types, file systems, and datastreams ➢ Data effectively demands protections and assurances from hardware/hosts/applications prior to revealing itself ➢ Application as credential for data access (trusted applications)

Figure 2 - Sample Technology Elements in Major Control Categories over Time

A note regarding "business utility"

It is worth reiterating that the relative utility/reliance for the three technology buckets described in this paper focuses solely on *utility as a security control.* It is clear that each component – network, host, and data – have a unique and significant role in enabling enterprises to do business. Though their relative utility as security controls will shift, as described herein, over time, the three components will continue to work co-operatively in accomplishing business goals. This is expected to remain true beyond any visible time horizon.

Conclusions

The next five to seven years promise to bring radical changes, with accompanying opportunities, for the information security technology industry. We are moving from what we may term an "Age of Network Security," wherein the network dominates the control landscape, to an "Age of Host Security," in which the host provides the highest-utility security controls. Finally is the "Age of Data Security" – the "age" in which data controls have matured adequately to provide the highest utility of the three control types.

The notion that the data is the asset of greatest interest is certainly not new to the attacker – the data has, ultimately, always been the target of the most successful, prolific, and damaging attacks.

The "call to arms," then, goes out to the key players in the game:

- **To the home and enterprise consumer:** to demand usable and effective tools to secure their information;
- **To the Information Technology industry:** to demand the same on behalf of their user community, and "vote with their dollars" for solutions that provide the best protection of their data; and
- **To the software development community**: to anticipate and respond to this demand by delivering strategic solutions in line with the timeframes presented above

References

Firewalls and Internet Security, the Second Hundred (Internet) Years
by Frederic Avolio, Avolio Consulting

http://www.microsoft.com/windowsvista/basics/security.mspx

SANS Whitepaper: History of Encryption, Volume 2

Kahn: David Kahn, ``The Codebreakers'', Macmillan, 1967.

Acknowledgements

The author would like to sincerely thank the following individuals who provided significant feedback and review in bringing this document to its final form:

Reviewers
Scott Hogan – Microsoft IT Technology Integration Planning
Matthew Lehman – Microsoft Information Security
Price Oden – Microsoft Information Security

Contributors
Gregg Atkins
Geoff Brock
Kellie Larkin
Konstantin Matev
Cam McCleery
Bill Murray
Pete Narmita
Nick Payton
Jason Popp
Paul Rich
Arjuna Shunn
Rama Shunn
Ryan Vatne
Lee Walker