Introduction

The vision of computers as a potential information conduit led to the creation of the Internet in the early 60’s. It was widely anticipated that this new “communications network” would revolutionize the way in which information could be accessed and exchanged. The Internet has far exceeded early expectations while prompting anticipation of even greater things to come as networks and related technologies continue to evolve and become more sophisticated. Advancements in networks, hardware and middleware are accompanied by applications of increased sophistication. It should come as no surprise that security is listed as the top priority of network managers, largely due to the ongoing evolution of networks.

In this paper, we discuss the implementation of security with an emphasis on some of the:
- key existing technologies;
- critical challenges;
- importance to higher education; and
- future considerations.

The scope of this discussion will focus on research and administrative computing at institutions of higher education. We also note that although there are indeed significant distinctions between the goals and needs of security in higher education and industry, we will treat the fundamental issues in a similar context.

Key Security Technologies

Bear Stearns, a leading investment banking, securities and brokerage firm, noted that approximately 80% of the traffic running across LANs in corporate environments is external to the facilities. Equally discerning is the fact that security at the network level is addressed primarily at the surface, i.e., equipment is used simply to monitor and control protocol traffic. The next frontier, "Internet computing", will place even greater demands on security requirements given the resolve for a flexible, platform-independent, language-neutral, loosely-coupled way to link applications across the Internet.

We begin this discussion with the dominant security technologies presently used for authentication, data integrity and confidentiality, including: Kerberos, PKI and Transport security (SSL/TLS).
- Kerberos
  - authenticates users via a secure transaction with a Key Distribution Center (KDC) through the use of symmetric keys;
has the distinct advantage that it provides mutual authentication between the client and server;
has the disadvantages that if used for intersite authentication, it must also be used for intrasite authentication, which may not be practical; and
relies heavily on conventional cryptography.

- Public Key Infrastructure (PKI)
  - authenticates users via the use of certificates with public asymmetric keys;
  - provides trusted and efficient key and public key certificate management, for authentication, non-repudiation, and confidentiality;
  - provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks;
  - disadvantages:
    - relies on trust;
    - users must protect uniqueness of private key;
  - better for key management and a large number of protocols.

- Transport Security (SSL/TLS)
  - encrypts data moving between client-and-server and uses Message Authentication Codes (MACs) for data integrity;
  - used to provide message point-to-point integrity and confidentiality;
  - most widely deployed technology for confidentiality on the Internet
  - performance can be an issue because of potential bottlenecks
  - used primarily to secure HTTP-based Web traffic;
  - security and communication services are entangled;
  - allows non-encrypted, authenticated communication;
  - assumes stream-oriented transport layer protocol underneath.

Implementing Security in Higher Education

Confidentiality, integrity and availability (CIA), the three fundamentals of information security, are relevant in commercial, as well, as academic environments. Academia, by nature, encounters difficulties in addressing these fundamentals because of its resolve to remain an open and flexible environment. Industry, on the other hand, is primarily profit- and project-driven; hence, the bottom line is much easier to evaluate and assess. In industry, the ability to prioritize applications and implement necessary security technologies is driven by the assessment of a project’s cost of failure. We present and briefly discuss some of the relevant issues regarding the implementation of security in higher education, including the:

- delicate balance between freedom and security;
  - Institutions of higher learning, because of their resolve to be an open and flexible environment, experience inherent conflicts due to the delicate balance that must be achieved between information and resource access and security.

- policies governing security implementation are a necessary “evil”;
  - Policies that reflect the different needs (administrative, teaching, and research) of the various areas of the institution must be flexible enough to accommodate special needs, but consistent enough to define standards for operation and conflict resolution.

- chance to enhance research and academic collaborations;
  - Many of the funding agencies, industries, federal laboratories, and even other academic institutions will soon require a minimum security infrastructure in order to even collaborate and do business. As business practices and critical applications are increasingly being moved to the Internet, security will be a necessity and no longer a luxury. Universities must now understand the value of computing as more than a tool of research & development (R&D). Registration, payment of fees, etc. are now handled over the Web—it is simply the way that business will increasingly be done. The fact that sensitive information, such as

---

6 http://ospkibook.sourceforge.net/docs/OSPKI-2.4.6/OSPKI/pkix-concepts.htm
7 http://www.itl.nist.gov/lab/bulletns/archives/july97bull.htm
grades, credit card accounts and personal data is moved via the Internet reinforces the need to assure that security can minimize and when possible prevent attacks.

- reduction of costs;
  - Many institutions seek to reduce costs and support new applications by consolidating resources, e.g., converging voice and data\(^2\).

### Critical Challenges

It is important to acknowledge from the outset that achieving 100% security is not a realistic objective. Efforts should be focused on minimizing and quickly responding to intrusion attacks and subsequent access to critical data and resources\(^8\). A significant step towards making environments more secure involves changing the process by which systems are protected, i.e., moving the focus away from the perimeter of the network to the application. In addition, greater awareness by security professionals of the new technologies and architectures that may improve security\(^10\) in the environments in which their users operate must be a top priority.

Security, not so long ago, was relegated to preserving the integrity of information and resources shared between researchers either at the same facility or within close proximity. Generally, the users were well-acquainted and trust was not an issue because potential threats were most likely to come from an unknown attacker who was not a part of the research group. These attacks were related more to a "test of wills", (i.e., hot shot challenging a vendor's pronouncement of an "impenetrable" fortress) rather than accessing sensitive data and resources for personal gain. Unfortunately, more technically-savvy attackers have accompanied much of the progress in Internet-related technologies, and the scope of attacks has now changed—its all fair game. Technological advancements in mobile devices, wireless, data management, and software have enabled reliable and consistent communication via cell phones, PDAs, laptops and desktops. As a result, the scope and nature of security needs have changed dramatically over the last few years. Mobile devices and wireless technology have had huge impacts.

It is impossible to list all of the challenging issues in the security field because they are too numerous to enumerate. However, we cite some of the most prominent ones with apologies for any not included. Security solutions must:

- link dissimilar and often incompatible local security mechanisms;
  - any hope for success will require a careful integration of proposed solutions with existing local solutions. Security administrators will not run the risk of alienating users with major changes in the solutions that they have worked so hard to implement in spite of any shortcomings.

- account for the inadequacies in current technologies to accommodate the range of resource types;
  - all of the existing solutions have advantages and disadvantages. New techniques must enable the wide variety of languages, platforms, and devices that are now a part of the communication enterprise to function properly.

- provide flexibility and control on sharing relationships;
  - current distributed computing technologies do not adequately provide for sharing beyond traditional client-server relationships, e.g., peer-to-peer is not included in present requirements. Single sign-on (ss0) and code exportability are integral to successful sharing between users and processes.

- incorporate credentials and policies that span multiple organizations;
  - a significant bottleneck is possible if a consistent and coherent agreement on credentials and policies is not firmly established between participating parties. This could be a security administrator's biggest nightmare—i.e., trying to authenticate users and determine what resources acceptable users are authorized to engage, blindly.

---

• be modular, interoperable, comprehensive, and dynamic;
  o solutions must have components that integrate into the overall solution. A modified or improved component must interface with the other parts of the solution. The solution must account for a variety of different conditions but still reflect a “seamless” nature.

• evolve;
  o as technologies change, so must the solutions to account for new factors, complications and requirements.

• provide end-to-end security;
  o a solution must be comprehensive and address all of the requirements from end to end. Otherwise, the overall solution will yield inconsistent and unreliable results.

• support consistent and multiple implementations;
  o the global nature of computing suggests the availability of multiple users with applications having varied requirements and needs. Increasingly, large groups will be taking advantage of the technologies all over the world, and the solution must bear this to be accepted and implemented.

Conclusion

A number of recent models such as the Grid Security Infrastructure (GSI) of the Global Grid Forum, Shibboleth of Internet 2, and WS-Security of Microsoft have recognized the need to develop solutions that allow new approaches to integrate with existing local solutions. Some new technologies such as peer-to-peer (P2P) require removing blocks to traffic on firewalls, which inhibits its widespread acceptance. The GSI model proposes a security architecture for large-scale distributed computations. Shibboleth, WS-Security and GSI represent important architectures that are critical to the new philosophy that brings computing to the Internet, initiatives known as “Internet computing” and Web Services.

Success in the realm of security is measured in terms of minimizing and quickly responding to intrusion attacks and subsequent access to critical data and resources. Security in academia is complicated by the fundamental premise of it being a free and open environment. It is therefore critical to balance access with security in order to provide a flexible, but secure infrastructure. Increasingly, organizations are moving to a baseline architecture that will require certain technologies in place in order to communicate and collaborate. Interoperability is critical to enabling the flexibility that multiple platforms require. A hybrid, cooperative solution will be necessary to be embraced by the wider community.

Related Initiatives

We list a few of the initiatives that are related to security implementation, including:

• Global Grid Forum (GGF): http://www.gridforum.org/
  o The Global Grid Forum (GGF) is a collaborative group of academic, industry, and national laboratory researchers and practitioners working on distributed computing, or "grid" technologies

• National Science Foundation Middleware Initiative (NMI): http://www.nsf-middleware.org/
  o NMI represents an initiative coordinated by NSF to create and deploy advanced network services that simplify access to diverse Internet information and services.


---

10 Please note: Informed after the panel that Shibboleth is back in full swing, see website listed.
Middleware Web Authentication Project is designed to create cross-institutional authentication and authorization services on the Web.

  - WS-Security is used in conjunction with several security models and encryption technologies for the purpose of message integrity and confidentiality and single message authentications.

### Related EDUCAUSE 2002 Sessions

#### Tuesday, October 1
- **Tuesday, October 01, 2002**
  8:30 a.m. - 12:00 p.m.
  - B303: Seminar 02A - Model Approaches to IT Policy Development
  - B305: Seminar 15A - Middleware Planning and Deployment 101: Setting the Stage
  1:00 p.m. - 4:30 p.m.
  - B310: Seminar 01P - Implementing a Campus-Wide Wireless LAN: Considerations and Practices
  - B304: Seminar 02P - Patriot Act: Procedures and Protocols for IT Systems
  - B303: Seminar 10P - Crafting and Implementing An Effective IT Security Plan and Policy
- **Wednesday, October 02, 2002**
  11:40 a.m. - 12:30 p.m.
  - B314: Track 2 - Information Sharing Strategies to Improve IT Security
- **Thursday, October 03, 2002**
  8:10 a.m. - 9:00 a.m.
  - B402: Track 2 - PKI Update: The Higher-Education Bridge
  11:45 a.m. - 12:35 p.m.
  - B302: Track 2 - Developing and Deploying a PKI for Academia
  2:20 p.m. - 3:10 p.m.
  - B304: Track 2 - KISSS: A Path to the Nirvana of Authentication Security
  4:55 p.m. - 6:10 p.m.
  - Exhibit Hall B3: Digital Signatures: Virginia Tech's Pilot Project Results
- **Friday, October 04, 2002**
  9:30 a.m. - 10:20 a.m.
  - B312: Track 2 - Security Awareness: Taking the Medicine and Liking It.