

INTERNET SECURITY BASICS

TUTORIAL PRESENTATION

Robert Bruen

Massachusetts Institute of Technology

As more colleges connect to the Internet, more colleges are faced with the security problems created by global access. The security problem is not new, but it can be somewhat confusing and overwhelming if one lacks the experience. The problem itself is growing and changing because more people are trying to breach security, as well as new software bringing new avenues for attack.

This tutorial will cover the basic areas to provide an outline for the college trying to protect itself. There is no guarantee for security, but being prepared is a better approach than ignoring it. Security is obviously a far larger topic than the 75 minutes allotted for this tutorial, but after the presentation, attendees will have been exposed to the fundamentals and will have pointers to further resources.

The topics range from knowing what it means to what can be done.

OUTLINE

1. Definitions, description, issues, basic concepts, jargon and the extent of the problem of security and the internet.
 - Intruders, viruses, and worms.
 - Inside the organizations.
 - Special problems in academia.
 - Privacy.
 - How do they do it?

2. Technical explanations:
 - Authentication
 - Firewall
 - Public Keys
 - Cryptography

3. Managing security.
 - Commonsense.
 - Web pages.
 - PGP.
4. Policy making.
 - Issues.
 - Setting a policy.
 - Creating problems.
 - Key escrow.
5. Resources.
 - Bibliography.
 - Home pages.
 - Software.
 - Glossary.

Short Bio: Robert Bruen is the Manager of Computing and Networking for the Lab for Nuclear Science at MIT. He has a PhD in Higher Education Administration from Boston College, MS in Computer Science from Boston University, MS in Library Science from Simmons College and a BA in Philosophy & Religion from Northeastern University. He has worked at MIT for 13 years.