

How Hacking Effects Everyone's Life and How to Protect Yourself from Hackers

Hampton University
January 22, 2009

Daniel J. Ryan, *JD*
National Defense University

Professor Daniel J. Ryan



Legal Stuff

- This presentation is designed to provide authoritative information with regard to the subject matter covered. The information is provided for your information only and should not be relied upon as legal advice. This presentation makes no warranties, express or implied, based on the information it contains. Nothing in this presentation constitutes the establishment of an attorney-client relationship between you and Daniel J. Ryan, Esquire. Please remember that laws may differ substantially in individual situations or in different states, so you should never rely on legal or other materials from this or any other slide presentation without first seeking advice about your particular situation from an attorney licensed to practice in the appropriate jurisdiction. Nothing contained in this presentation should be construed to constitute a recommendation or endorsement of any company or firm, product, or service.

We Face New Choices



© 2001 STAHLER—CINCINNATI POST

Professor Daniel J. Ryan

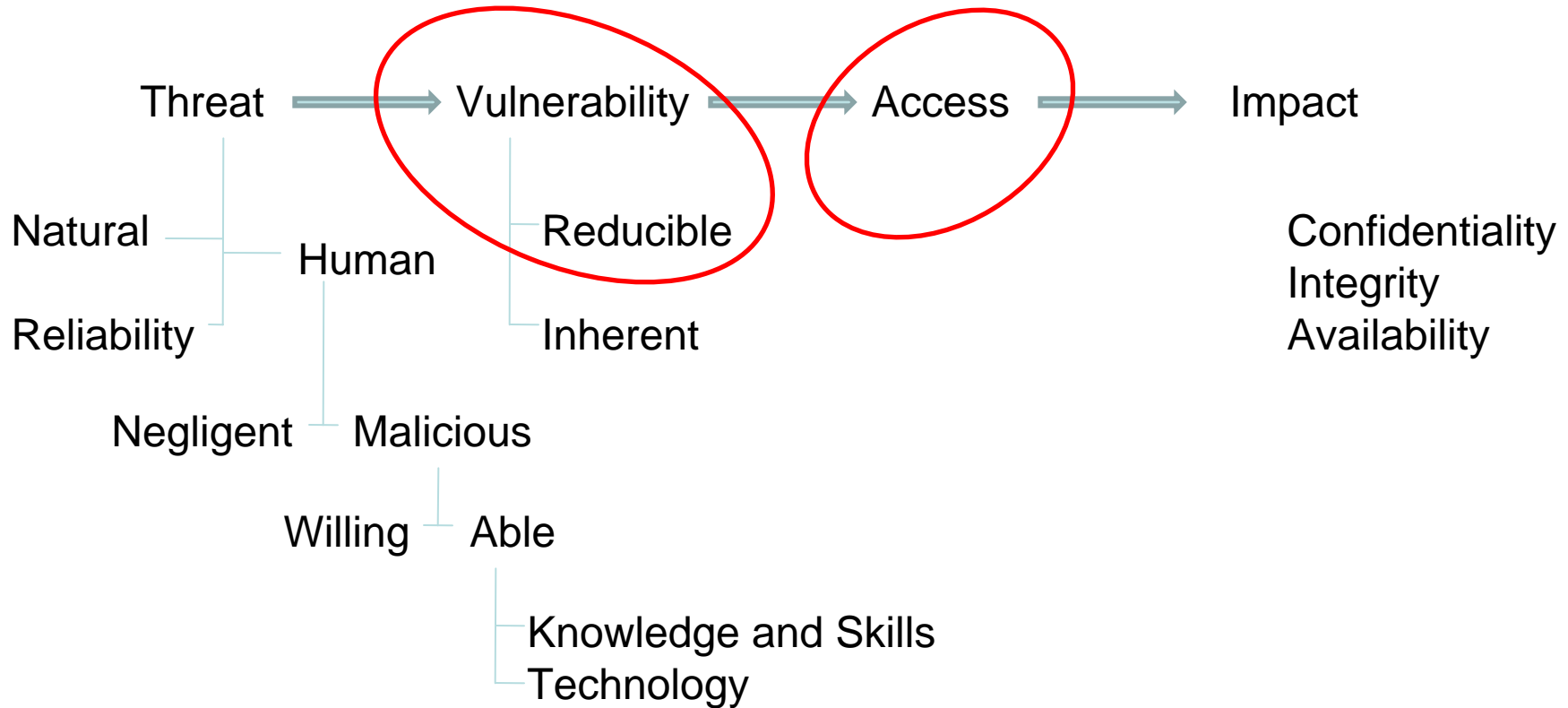
Threats

- ◆ A *threat* is any agency, malicious or otherwise, that can have an undesirable effect on the assets and resources associated with a computer system or network
 - Natural Disasters
 - System and component failures
 - Accidents and mistakes
 - Organizations or individuals who both intend us harm and have the capability to accomplish their intentions
 - Computer hackers, criminals, industrial or state-sponsored spies, enemy armed forces, terrorists, psychotics, drug lords or saboteurs

Malicious Threats

- Confidentiality
 - Theft of secrets
 - National security threats
 - Trade secrets
- Integrity
 - Identity theft
- Availability
 - Denial of service
 - Destruction of assets
- Malicious code
- Masquerading
- Social engineering
 - Phishing
- Covert channels
- Van Eyck radiation
- Poisoned pages
- Clickjacking
- Botnets

The Threat Model



Protecting Yourself, Your Family and Your Organization

Professor Daniel J. Ryan



If We Had World Enough and Time . . .

- In a perfect world, starting from scratch and with infinite time and resources:
 - Benchmark system capabilities, enterprise operations, policies and procedures
 - Perform a vulnerability assessment, taking into account standard operating procedures and any countermeasures
 - Create an enterprise vision for security:
 - What should be protected?
 - How long should it be protected?
 - How strongly should it be protected?
 - Implement a comprehensive risk management program
 - Protect, detect and correct

Raising the Bar

- But!
 - this isn't the perfect world, and you're not starting from scratch, and you don't have infinite resources
- You need cheap, simple and effective security
 - A short list of things that you can do right now
 - That are effective -- these really work!
 - That are inexpensive
- Why?
 - To deter all but the most dedicated of opponents
 - Buy time to put a more comprehensive security program in place

Review Your Security Policies, Practices and Procedures

- What information assets and systems need protection? How much protection do they need? How long must protection be continued?
- Good information security is more than computer and network security. It requires a balanced mix of security practices and procedures.

Have Good Passwords

- Self-chosen passwords are inadequate
 - Many are easily guessed
 - Any word in the dictionary is recoverable
 - Hackers can recover most self-chosen passwords in a few minutes
- Complex passwords are better
 - Combinations of symbols and cases
 - Need to be changed regularly
 - Still vulnerable to sniffers
- One-time passwords are best
 - Token-based (time-synchronized or challenge-response)



Use Good Antiviral Products

- Insist on having good antiviral software on all workstations and servers
- Update your antiviral software frequently
- Teach your people about the dangers of bringing in software from home
- Test all media off-line before letting them be put into a workstation connected to the network
- You may need to use more than one antiviral product

Implement a Patch Management Program

- CERTs maintain lists of known vulnerabilities
- CERTs supply patches to close known vulnerabilities
- A robust patch management program ensures that you are not vulnerable to known attacks

Use Good Cryptography

- Very good cryptographic systems are available
 - Symmetric systems like Rijndael (AES), triple DES or IDEA
 - Require secure key management
 - Public key systems
 - Require trusted Certificate Authorities
- Long keys are essential
 - Single DES key spaces exhausted in 79 hours with an investment of less than US\$ 250,000
 - 168-bit key lengths now exportable from the United States

Have Good Firewalls

- Firewalls protect information as it enters and leaves your organization
 - Firewalls are not sufficient protection by themselves
 - Cryptography is needed to protect your communications with the outside world
 - Auditing and good security practices are needed to protect you from insiders
- Firewalls range from unsophisticated packet filters to complex rule-based systems, so choose the level you need based on sound risk management

Have a Good Backup System

- Backup your information systems frequently
- Store your backups securely offsite
- Remember that you don't need to save everything forever

- If you are in a time-critical industry, you may need to have a mirror site (beta site) capable of assuming operational responsibility in an emergency



Audit and Monitor the Use of Your Systems and Networks

- Make sure your employees know that they have no expectation of privacy when they use your systems
- Enable auditing on your systems and networks
- Have a system that helps you analyze the audit logs
 - Immediate alerts on security-relevant activities
 - Statistical analyses to establish norms
 - Alerts on variations from norms



Have a (Good) Training and Awareness Program

- Training and awareness is needed at all levels of the organization
- Training and awareness is your best line of defense against
 - Introduction of viruses and other malicious code
 - Penetration by fraud (“social engineering”)
- Training and awareness must be repeated
 - Remind people who have already taken it once
 - Keep awareness level high
 - Train new people
 - Maintain expectations of actions and duty

Test Your Security Frequently

- Analyze your systems for vulnerabilities
 - War-dial your facilities to detect unauthorized modems
 - Use SATAN or other testing products
- Test the security features of your systems and networks
 - Ensure that the latest patches have been incorporated
- Perform penetration testing
 - Technical penetrations
 - Social engineering
- Use outside experts for testing



Have Contingency Plans In Place

- When the crisis is occurring, it's too late to start planning how to handle it
- Have a properly trained and equipped CERT team standing by
- Have strategic alliances already developed
 - Lobbyists
 - Public relations
 - Security experts
- Make sure your people know what they have to and need to do
- Practice, practice, practice

Elements of a Comprehensive Security Program

- ✓ Review your security policies, practices and procedures
- ✓ Have good passwords
- ✓ Use good antiviral products
- ✓ Implement a Patch Management Program
- ✓ Use good cryptography
- ✓ Have good firewalls
- ✓ Have a good backup system
- ✓ Audit and monitor the use of your systems
- ✓ Have a good training and awareness program
- ✓ Have contingency plans in place
- ✓ Test your security frequently

Remember: Good security doesn't have to be expensive!

Thank you!

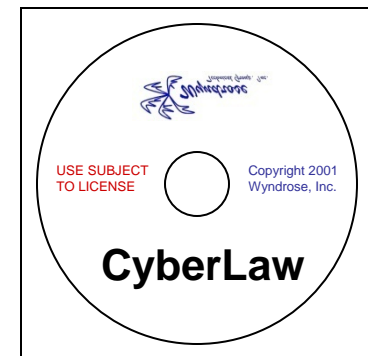
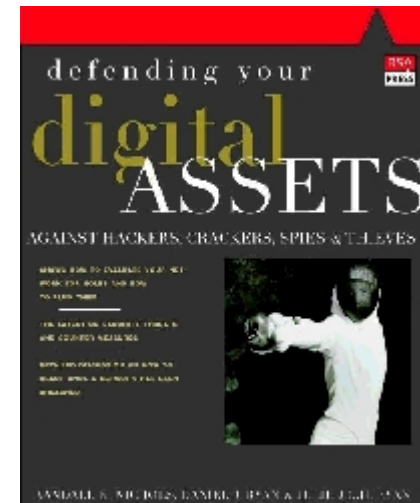
Daniel J. Ryan
Professor Systems Management

Information Resources Management College

National Defense University

202-685-2843

ryand@ndu.edu



Professor Daniel J. Ryan

