Security in E-Learning

Edgar R. Weippl
weippl@acm.org
www.e-learning-security.org

Motivation

- Situation - Reliability
  - Increased dependence on systems reduces fault tolerance
  - Just in time delivery systems
- Machines were built for maximum extensibility
- Technology built by geeks for geeks
- Computers can, by design, run any code

Target Audience

- **Authors** creating e-learning content
- **Teachers** using e-learning systems.
- **Managers** responsible for the selection and maintenance of e-learning programs
- Security Checklist

Authors

- Why is security relevant when creating content?
- Which kind of threats are there?
- Which assets should I protect?
- How can I protect the aforementioned assets?
- Are there ways to impede illegal use through smart design?
- How much additional effort will be required?

Teachers

- Why is security relevant when using e-learning?
- Which kind of threats are there?
- Which assets should I protect?
- Does standardization (of e.g. exams) undermine the freedom of academia?

Teachers

- How can I determine the level of risk exposure of my exam questions?
- How can I make my lecture „secure“? Will it have a negative impact on my “honest” students?
- How much additional effort will be required?

Managers

- Which organizational issues are relevant to security?
- How is security influenced by
  - infrastructure
  - buildings and floor layouts,
  - organizational workflows
    e.g. how are exam results handled to eventually affect grades?

Managers

- How can a manager make a good case for security so that teachers, authors and students will support him?
- How much additional effort will be required?

Contents

- Introduction to Security and Dependability
- Content Authors
- Teachers
- Managers
- Security Risk Analysis

Contents

- Techniques to protect digital content
- Privacy
- Feedback and Assessment of Students, Authors and Teachers
- Security Checklist

The Basics

The Basics - Security

- Secrecy
- Integrity
- Availability

Basic Terms

- **Secrecy** Users may obtain access only to those objects, for which they have received authorization
- **Integrity** means that only authorized people are permitted to modify data (or programs). Secrecy of data is closely connected to the integrity of programs of operating systems.

Basic Terms

- **Availability**
  A system is operational and functional; loss of availability is a.k.a denial-of-service

The Basics - Dependability

- Availability
- Reliability
- Safety
- Integrity
- Maintainability

The Basics - Dependability

- Reliability
  refers to the continuity of correct service.
- Safety
  the absence of catastrophic consequences on the user(s) and the environment
- Maintainability
  the ability to undergo modifications and repairs

Secondary Attributes

- **Non-repudiation**
  Users are not able to deny (plausibly) to have carried out operations

Identification & Authentication

- Without reliable authentication systems security cannot be achieved.
- What You Know - Passwords
- What You Have - Keys, Cards
- What You Are - Biometrics
- What You Do - Signature

Passwords

- Use this sentence to get a great password!

Uts,tgagp!

Learn how to type

Uts,tgap←←agp!qfta←←←←

What you have

- RFID cards - keys for rooms
- Smart cards
  - Excellent security when correctly used
  - Best combined with public key cryptography
  - In Austria used for e-government (currently first field users)

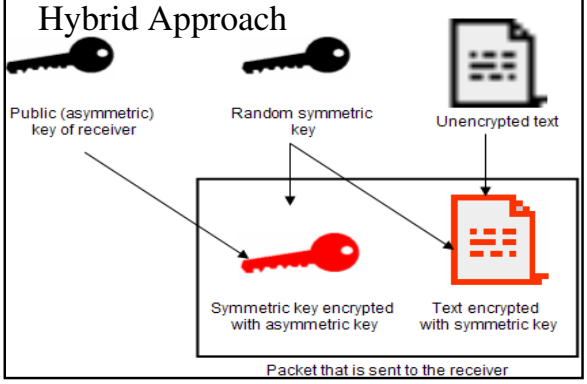
Biometrics

- User acceptance problems
- Not very reliable
- Useful for in combination with e.g. cards, to check that they are not passed on.

PKI – Key Management

- How are keys produced? (Trojans)
- Who generates keys and where? (Trojans)
- Where are keys stored? (public computers)
- When and how do keys become invalid?

Hybrid Approach



Authors

Authors

- Why is security relevant when creating content?
- Which assets should I protect?
- How can I protect the aforementioned assets?
- Are there ways to impede illegal use through smart design?
- How much additional effort will be required?

Why is security relevant when creating content?

- Readers expect integrity of the content.
- Readers want to read without being watched.
- Protection against unauthorized use.
- Protection against unauthorized modification.
- Protection against loss / DoS.

Which assets should I protect?

- Texts
- Images
- Audio / Video
- Interactive Examples / Applications
- Interaction between real people

How Can I Protect Texts?

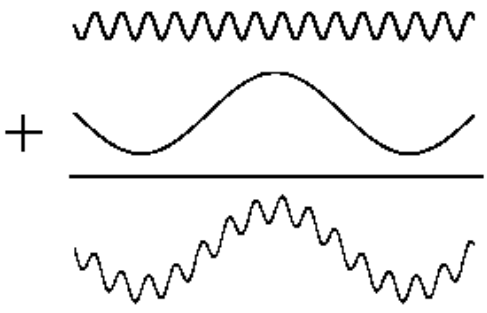
- Cryptolope™ (IBM) or similar concepts
- Non-standard browsers

- Do not design so that the real value is the text

How Can I Protect Images?

- Watermarking offers mostly protection of the copyright but not copy protection.
- Make „batch copying“ more difficult
- Use visible watermarks

How Can I Protect Audio/Video?



How Can I Protect Applications?

- Offline Registration Numbers
- Online Authorization
- Dongles
  - images from www.keylok.com
  - www.microcosm.biz

Are there ways to impede illegal use through smart design?

- Focus on the real value, which will most probably be interaction.
- Interaction is easier to protect.
- Protection of executable programs.
- **Interaction between people cannot be copied.**

How much additional effort will be required?

- Risk Analysis will require days, not weeks.
- Implementation will not be more work once users are trained and the workflow has been established.

Teachers

Teachers

- Why is security relevant when using e-learning?
- Which kind of threats are there?
- Which assets should I protect?
- Does standardization (of e.g. exams) undermine the freedom of academia?

Teachers

- How can I determine the level of risk exposure of my exam questions?
- How can I make my lecture „secure“? Will it have a negative impact on my “honest” students?
- How much additional effort will be required

Why is security relevant when using e-learning?

- Lecture notes
- Exams
- Grades and other confidential information
- Electronic communication with students

Which kind of threats are there?

- Secrecy
  - e.g. grades & information about students
- Integrity
  - e.g. students' answers on exams
- Availability
  - e.g. examination systems
- Non-repudiation
  - e.g. handing in of exams

Which kind of threats are there?

- Reliability
  - Automatic grading
- Maintainability
  - Who can modify the platform – access to source code?
- Do not underestimate the additional effort required to maintain large installations
  - Personal use
  - Department wide
  - University wide

Which assets should I protect?

- Bulletin Boards
- Teaching Material
- Email
- ...any form of interaction and communication

Freedom of Academia

- Does standardization (of e.g. exams) undermine the freedom of academia?
- Industrialization of educational process
- Faculty in the mass production of content?
- Focus on interaction – the real value

Exams

- How can I determine the level of risk exposure of my exam questions?
- Constantly monitor for suspicious results
- Create dynamic questions whenever possible
- Use at least some free text answers

“Securing” Lectures

- How can I make my lecture „secure“?
- Will it have a negative impact on my “honest” students?
- Think about these issues when setting up e-learning classes

“Securing” Lectures

- Specify how Bulletin Boards are backed up (or not) and when and how the content is deleted.
- Encourage the use of pseudonyms.
- For confidential/important information use encrypted/signed email or confirm personally

“Securing” Lectures

- Delete Emails after a specified period
- Denial-of-Service is frustrating for students. Provide
  - instant help for real-time activities such as chats (phone number)
  - and help within a day for all other issues
- Run checksums on the content to ensure integrity.

Managers

Managers

- Which organization issues are relevant to security?
- How is security influenced by
  - infrastructure
  - buildings and floor layouts,
  - organizational workflows (e.g. how are exam results handled to eventually affect grades?)

Managers

- How can a manager make a good case for security so that teachers, authors and students will support him?
- How much additional effort will be required?

Which organization issues are relevant to security?

- Communication processes (e.g. exam results)
- Physical access (e.g. hardware, printed information, backups)
- Processes in cases of emergency (fire alarms, …)

How is security influenced

- by infrastructure
- buildings and floor layouts,
- organizational workflows

Motivation

- How can a manager make a good case for security so that teachers, authors and students will support him?
- Inform about risks and what each individual person might lose.
- Organize a fast, efficient and effective security risk analysis.

How much additional effort will be required?

- None that does not payoff
- Risk Analysis takes several days for a typical (small) research project.

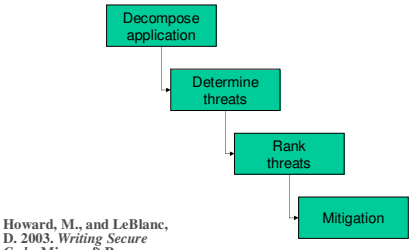
E-Learning a New Critical System?

- How much downtime are you / students willing to accept?
- Continuity in support
  - Student admins not well suited
  - Simpe systems! (Moodle?)
- Vendor lock in
  - Do not use elaborate content unless you know what you are doing

Which kind of threats are there?

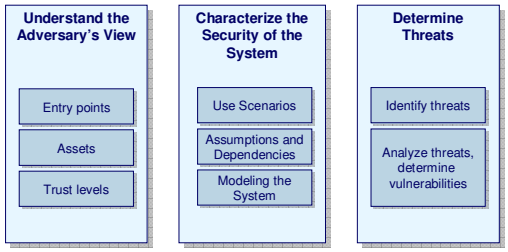
- Do not underestimate the additional effort required to maintain large installations
  - Personal use
  - Department wide
  - University wide

Threat Modeling



Howard, M., and LeBlanc, D. 2003. *Writing Secure Code*, Microsoft Press

Thread Modeling



Swiderski, F., and Snyder, W. 2004. *Threat Modeling*, Microsoft Press

Security Checklist

- Learn – take training, read guidance, help educate users
- Connect – participate in the community, subscribe security newsletters
- Manage risk – implement security and risk management process

Security Checklist

- Integrate – adapt defense-in-depth security approach
- Implement – operating system, learning platform
- Standardization – maintenance, patches, …

Resources

- Guidance and training
  - Security Guidance Center
    - http://www.microsoft.com/security/guidance/default.mspx
  - E-Learning Clinics
    - https://www.microsoftelearning.com/security/
  - Moodle
    - http://security.moodle.org (Developers)
    - http://www.moodle.org
  - NIST
    - http://www.nist.org

Resources

- Community engagement
  - Newsletters
    - http://www.microsoft.com/technet/security/secnews/newsletter.htm
  - Webcasts and chats
    - http://www.microsoft.com/seminar/events/security.mspx

Resources

- Newsletter Bruce Schneier
  - To subscribe, visit http://www.schneier.com/crypto-gram.html
- Risks Newsletter
  - Issues is archived at http://www.risks.org
  - The current issue can be found at http://www.csl.sri.com/users/risko/risks.txt

The 7 most important facts

- Perform a security risk analysis for each and every project
- Use simple tools and procedures – non-compliance is the greatest risk
- Test your tools and procedures
- Evaluate additional risks introduced by risk control measures (e.g. backups – secrecy, cryptography – availability)

The 7 most important facts

- Use the security checklist (and update it)
- Educate your colleagues and students about security basics
- Think about the impact that any action has on security issues!

Security in E-Learning

Upcoming book published by Springer, NY addressing

- Teachers
- Authors
- Managers
- Students

that use e-learning systems

It's not over yet!

www.e-learning-security.org

- Slides
- In-depth Content

- Case Study of the current situation concerning security in e-learning

Thanks for Attending the Tutorial