

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Secure Software Engineering in Higher Education and Professional Societies

**Samuel T. Redwine, Jr.
James Madison University**

**Software Assurance
Object Management Group
February 15, 2006**

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Overview

- **Secure Software Assurance**
- **Higher Education Activities**
- **Professional Society Activities**
 - Organizations
 - Publications
 - Events
- **Conclusion**

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Secure Software Assurance

- Assurance
- Justified Confidence
- Assurance Case
- Uses of Assurance Case
- Body of Knowledge

Assurance

- “Assurance” is used in several ways, but underlying concept is to reduce uncertainty
- To rationally decide to use software in dangerous situation one needs
 - The software
 - Justified confidence in it

Justified Confidence

- To have one's uncertainty reduced so have justified confidence in a security claim need convincing
 - Evidence
 - Arguments that tie evidence to claim
- Implies valid evidence and arguments

Together these make the “assurance case”

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Uses of Assurance Case

- **Planned assurance case helps determine development plan and activities**
- **For developer: assurance case contents (so far) need to be adequate at each step**
 - Especially release
- **Assurance case helps decide purchase and use**

Secure Software Assurance BOK

- **Body of knowledge document out for review (until Feb. 21st)**
 - At buildsecurityin website under Additional Resources
 - (<https://buildsecurityin.us-cert.gov/portalresources/>)
- **Identifies knowledge and gives references**
- **Approximately 225 pages**
- **To be issued in March**
- **Government, industry, and academic involvement**

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Higher Education Status

- Depending on how one counts one can identify between two and twenty-two institutions that teach secure software engineering
- Few regular software security courses or programs offered
- Secure Software Assurance body of knowledge out for review

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Higher Education Activities

- **Naval Post Graduate School**
 - Number of Masters theses
- **James Madison University**
 - Secure Software Engineering Masters
- **Carnegie Mellon University**
 - CyLab
 - Computer Science Department
 - Software Engineering Institute
- **Northeastern University**
 - Engineering Secure Software

Example Single Topic Courses

- **Purdue**
 - Secure Programming
- **George Mason University**
 - Secure Programming
- **Princeton**
 - Secure Internet Programming
- **Columbia**
 - Programming-heavy Network Security

Textbooks

- **Only one of the major Software Engineering textbooks treats security**
 - **Sommerville 7th edition treats critical systems (and safety) at length and security briefly but explicitly in this context**
- **None of the many Software Quality Assurance texts I have examined treat security in more than passing**

Software security books:

- **Gasser 1988 last introductory text to emphasize high security**
- **Few professional books go much beyond programming**

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background.

Funding for Curricula

- **Microsoft has given a number of modest awards to improve education in Trustworthy Computing and Software Engineering**
- **Federal funding has been quite modest**

Professional Society Activities

- **Organizations**
 - ACM Risks Forum
 - IEEE CS TCSE Committee on Secure Software Engineering
 - NDIA committee on software assurance
- **Publications**
 - ACM Trans. Info and System Security
 - IEEE Trans. Dependability and Security
 - IEEE Security and Privacy magazine

Events

- **IEEE International Symposium on Secure Software Engineering March 13-15 in Arlington VA**
- **Software Engineering for Secure Systems Workshop**
- **Workshop on Secure Software Engineering Education and Training**

Also: DHS Software Assurance Forum, NIST Workshops on tools and metrics, and NDIA Software Assurance events

Professional Examinations

- **Canadian Council of Professional Engineers** has an elective **Software Engineering** examination on **Security/Safety**
- **British Computer Society** exams mention security under networking and distributed systems topics (not SwE)
- **IEEE Computer Society Certified Software Development Professional** exam does not currently cover security
 - **SWEBOK Guide** should add “soon”

Conclusion

- **Must have Software *and* Justified Confidence**
- **Higher education efforts limited but growing**
- **Professional society publications and events exist**
- **Secure Software Assurance body of knowledge out for review**