Foundations of Security: A short course
Bertinoro International Spring School

Joshua D. Guttman*

This course presents a personal view of central problems and techniques in the foundations of security for distributed systems. Although there are many other formalisms and implementation methods, the instinct and insight to specify and analyze security is shared. This schedule in pdf form is here: `http://web.cs.wpi.edu/~guttman/biss/schedule.pdf`

The projects for the class are now available at `projects.pdf`. They are due 8 July by email to my address. Please include the string "[biss]" in the subject line of your email.

Monday *17.30:* How to break a protocol.

18.30: Protocol proofs via strand spaces.

Slides, 1: `http://web.cs.wpi.edu/~guttman/biss/break_in_bertinoro.pdf`
Slides, 2: `http://web.cs.wpi.edu/~guttman/biss/strands.pdf`
`http://web.cs.wpi.edu/~guttman/pubs/jcs_strand_spaces.pdf`

Tuesday *11.30:* Protocols and their shapes; CPSA.

Slides: `http://web.cs.wpi.edu/~guttman/biss/shapes.pdf`
CPSA examples: `http://web.cs.wpi.edu/~guttman/biss/cpsa_examples.tgz` `http://web.cs.wpi.edu/~guttman/pubs/shapes_surveying.pdf`

12.30: The anatomy of TLS

Slides: `http://web.cs.wpi.edu/~guttman/biss/tls_anatomized.pdf`
`http://www.cs.ox.ac.uk/gavin.lowe/Papers/TLSpaper.pdf`

Wednesday *9.00:* The goals of protocols

Slides: `http://web.cs.wpi.edu/~guttman/biss/protocol_goals.pdf`
`http://web.cs.wpi.edu/~guttman/pubs/goals_and_transformations_xtended.pdf`

10.00: Protocol transformation

Slides: `http://web.cs.wpi.edu/~guttman/biss/6mar13_transformation.pdf`
`http://web.cs.wpi.edu/~guttman/pubs/goals_and_transformations_xtended.pdf`

*Partially supported by the US National Science Foundation under grant 1116557.
Worcester Polytechnic Institute, guttman@wpi.edu. 4–8 March, 2013.

17.30: Separability: composition and sessions

Slides: http://web.cs.wpi.edu/~guttman/biss/paths_and_normalcy.pdf
http://web.cs.wpi.edu/~guttman/biss/disjoint.pdf
http://web.cs.wpi.edu/~guttman/biss/sessions_8mar13.pdf
http://web.cs.wpi.edu/~guttman/pubs/disjoint.pdf
http://www.loria.fr/~cortier/Papiers/FMSD09.pdf
http://cs.bham.ac.uk/~mdr/slides/pdf/08-guessing.pdf
http://hal.inria.fr/docs/00/14/31/16/PDF/RR-6166.pdf
http://web.cs.wpi.edu/~guttman/pubs/CG13_short.pdf

18.30: Protocols with state

Slides: http://web.cs.wpi.edu/~guttman/biss/state_envelope.pdf
http://web.cs.wpi.edu/~guttman/pubs/fair_exchange.pdf

Thursday *15.00:* Trust management

Slides: http://web.cs.wpi.edu/~guttman/biss/authorization_trust_mgt.pdf
http://web.cs.wpi.edu/~guttman/cs564/papers/rt_li_mitchell_winsborough.pdf
http://web.cs.wpi.edu/~guttman/cs564/papers/binder.pdf
http://research.microsoft.com/en-us/um/people/blampson/45-AuthenticationTheoryAndPractice/Acrobat.pdf

16.00 Programming with cryptographic protocols

Slides: http://web.cs.wpi.edu/~guttman/biss/trust_engineering.pdf or in native advi format,
http://web.cs.wpi.edu/~guttman/biss/trust_engineering.dvi
http://web.cs.wpi.edu/~guttman/pubs/trust_mgt_in_strand_spaces.pdf
http://web.cs.wpi.edu/~guttman/pubs/pcp_final.pdf

Friday *10.00:* Separability: session-based protocols

Slides: http://web.cs.wpi.edu/~guttman/biss/sessions_8mar13.pdf
http://web.cs.wpi.edu/~guttman/pubs/CG13_short.pdf

11.30: Cryptographic definitions, constructions and proofs; Crypto interpretation of protocols

Slides: http://web.cs.wpi.edu/~guttman/biss/elements.pdf
Katz and Lindell, *An Introduction to Modern Cryptography*, Chapman and Hall, Boca Raton, 2008. Chapters 3, 4, 10, 12.
http://web.cs.wpi.edu/~guttman/cs564/papers/bellare_rogaway93.pdf
http://web.cs.wpi.edu/~guttman/cs564/papers/abadi_rogaway.pdf
http://web.cs.wpi.edu/~guttman/cs564/papers/MicciancioWarinschi.pdf

12.30: Authenticated Diffie-Hellman protocols

Slides: http://web.cs.wpi.edu/~guttman/biss/dh.pdf