- **CWE/SANS Top 25, OWASP Top 10**:
  - i 5 rischi di entrambe indicati sulla pagina del corso nella sezione "Problemi, e soluzioni, di base", da http://cwe.mitre.org/top25/ e https://owasp.org/www-project-top-ten/
- **Buffer Overflow**:
  - nozioni di base, da qualunque tutorial (solo principio base: allocazione di memoria e stringhe), oppure da http://en.wikipedia.org/wiki/Stack_buffer_overflow
- **SQL Injection**:
  - da link sopra delle Top CWE e OWASP, oppure da voce Wikipedia
- **Basi di Crittografia**:
  - http://en.wikipedia.org/wiki/RC4 (solo descrizione delle due parti: KSA e RNG)
- **Attacchi a WiFi (WEP)**:
  - Jesse Walker, "Unsafe at any Key Size" (fino a Sez.3.2)
- **Analisi Statica**:
  - saper descrivere il solo approccio di uno degli strumenti menzionati sulla pagina del corso nella sezione "Tool di analisi statica (o ibrida)"-in particolare, di Boon:
    - saper calcolare e spiegare le traduzioni 'C'->'constraints' presenti a pag.8 delle slide su Boon
- **SPIN e Promela, per Needham Schroeder**: pagine 12-16,19,21 da file in materiale aggiuntivi, e pagine 9-15 di http://www7.in.tum.de/~esparza/Talks/slides-maratea.pdf (riguardo al codice: solo struttura e ruolo dei processi)