EITC/IS/CSSF Computer Systems Security Fundamentals

Primary supportive curriculum reading materials

Cryptography

- Applied Cryptography by Bruce Schneier. John Wiley & Sons, 1996. ISBN 0-471-11709-9.
- Handbook of Applied Cryptography by Menezes, van Oorschot, and Vanstone.
- Introduction to Cryptography by Johannes Buchmann. Springer, 2004. ISBN 978-0-387-21156-5.
- Cryptographic libraries:
    - KeyCzar by Google.
    - GPGME by GnuPG.
    - OpenSSL.
    - NaCl: Networking and Cryptography library by Tanja Lange and Daniel J. Bernstein.

Control hijacking attacks

- Smashing The Stack For Fun And Profit, Aleph One.
- Bypassing non-executable-stack during exploitation using return-to-libc by c0ntex.
- Basic Integer Overflows, blexim.
- The C programming language (second edition) by Kernighan and Ritchie. Prentice Hall, Inc., 1988. ISBN 0-13-110362-8.
- Intel Memory Protection Extensions.
- Intel Programmer's Reference Manual (combined volumes), May 2018.
- Intel 80386 Programmer's Reference Manual, 1987.
  Alternatively, in PDF format.
  Much shorter than the full current Intel architecture manuals below, but often sufficient.
- Intel Architecture Software Developer Manuals.

Web security

- Browser Security Handbook, Michael Zalewski, Google.
- Browser attack vectors.
- Google Caja (capabilities for Javascript).

- Google Native Client allows web applications to safely run x86 code in browsers.
- Myspace.com - Intricate Script Injection Vulnerability, Justin Lavoie, 2006.
- The Security Architecture of the Chromium Browser by Adam Barth, Collin Jackson, Charles Reis, and the Google Chrome Team.
- Why Phishing Works by Rachna Dhamija, J. D. Tygar, and Marti Hearst.

OS security

- Secure Programming for Linux and Unix HOWTO, David Wheeler.
- setuid demystified by Hao Chen, David Wagner, and Drew Dean.
- Some thoughts on security after ten years of qmail 1.0 by Daniel J. Bernstein.
- Wedge: Splitting Applications into Reduced-Privilege Compartments by Andrea Bittau, Petr Marchenko, Mark Handley, and Brad Karp.
- KeyKOS source code.

Exploiting hardware bugs

- Bug Attacks on RSA, by Eli Biham, Yaniv Carmeli, and Adi Shamir.
- Using Memory Errors to Attack a Virtual Machine by Sudhakar Govindavajhala and Andrew Appel.

Mobile devices security

- iOS security