Title: **Information and System Security**

Lecturer: **Martin Rehak**

Team: **Tomas Pevny, Michal Svoboda, (Karel Bartos, Martin Grill)**

Textbook: Ross Anderson, Security Engineering 2nd/1st edition (major part available online), chapter numbers refer to second edition

Goal: The goal of the course is to give the students a basic gasp of information/system security problems and solutions. Rather than teaching specific current technologies and vulnerabilities/threats, we will introduce general problems, formalize them if appropriate and illustrate them with a wide range of examples, both with current and legacy technologies. We put emphasis on problems that will be encountered by most programmers and developers through their careers.

Principles:

- Course modeled after the Cambridge University courses, which defined the universally adopted and widely recommended textbook: Security Engineering.
- Includes about 25% of our original content in our domains of expertise, which will be covered by additional materials.
- About 75% of the course covers the areas with direct research contribution or significant professional expertise of the lecturer and team members.

Team background (relevant to course topics):

- **Martin Rehak:** ***network security, network intrusion detection, trust modeling*** – PhD thesis, active original research, impacted, cited publications, industrialization
- Secure mobile systems, location-based services, mobile banking systems; ***protocols, cryptography, secure systems development, smartcards, distributed systems security*** - professional experience with Schlumberger (Gemalto)
- **Tomas Pevny**: ***steganography, information hiding, steganalysis*** – PhD thesis (SUNY), original research, numerous impacted, cited publications, postdoc (CNRS)
- **Michal Svoboda**: ***secure systems administration, host security, multi-level security*** (SE Linux) – professional system administration experience in highly secure environment (pharmaceuticals), currently PhD student/researcher, research in network security
- **Martin Grill, Karel Bartos**: ***network security*** research – co-authors of the CAMNEP system, publications, PhD students

Themes/Lectures:

1. **Introduction, Security models, threat models (Anderson, Ch.1)**
    a. Security properties: confidentiality, integrity, non-repudiation, availability, …
    b. Methods: Authorization, Authentication, ciphering, replication…
    c. Attacker/threat models: sophistication, resources, time

   d. Assumptions
   e. Security by obscurity vs. guaranteed system properties

2. **Protocols and Access Control (I) (Anderson, Ch. 3)**
   a. Importance of protocol, assumptions
   b. Why protocols, their properties
   c. Attack surface, Attacks on protocols
   d. API
3. **Cryptography (I) (Anderson, Ch. 5)**
   a. Ciphering basics and terms - invertibility, key, plaintext, ciphertext...
   b. Block/Stream ciphers
   c. Vernam
   d. DES, AES
   e. Cipher modes, practicalities, side-channel attacks
4. **Cryptography (II) (Anderson, Ch. 5)**
   a. Asymmetric cryptography (DH,EG,RSA)
   b. Cryptographic hash functions
   c. Electronic signatures
   d. Certificates
   e. WEP failures, A4/A8 failures
5. **Protocols and Access Control (II) (Anderson, Ch. ¾, GSM/3GPPS spec,…)**
   a. Kerberos
   b. Protocols for authorization, authentication, integrity, non-repudiation
   c. GSM login, UMTS3G login
   d. Banking, electronic transactions
6. **Protocols and Access Control (III) (Anderson, Ch. 3/4/6)**
   a. SSL, MITM attacks, phishing
   b. Key distribution, key distribution in wireless networks
   c. Access control
   d. Rights management - satellite broadcasts use-case
7. **Multi-Level Security (Anderson, Ch. 8)**
   a. Bell-La Padua model
   b. Technical solutions and implementations
   c. Networking in MLS
   d. Data pumps
   e. SE Linux, security policies, access controls, policies and modifiers…
8. **Multi-Lateral Security, Inference Security, Privacy (Anderson, Ch. 9)**
   a. Census data security
   b. Workplace home pairs as a practical example
   c. Location based services security
   d. Social network mining
9. **Steganography, Information hiding, covert channels (TBD)**
   a. Steganography introduction and motivation

b. Current problems
c. Steganography
d. Steganalysis

10. **Economic Considerations (Anderson, Ch.7)**
    a. Game theory
    b. Electronic marketplaces
    c. Botnet economic model, e-crime economic models
    d. Reputation systems, their strengths, attacks-on, misuse
11. **Network Security (I) (Northcutt: Inside Network Perimeter Security)**
    a. Threat analysis
    b. Attacks (vulnerabilities: e.g. buffer overflows, weak passwords,)
    c. Transmission vectors,
    d. Rootkits, malware
12. **Network Security (II)(Northcutt: Network Intrusion Detection: An Analyst's Handbook)**
    a. Host security
    b. Firewalls, network policies, routers, VPN, tunnels
    c. Network monitoring, Intrusion detection
13. **Monitoring and Attacks on Monitoring (Anderson, Ch.12)**
    a. Importance of monitoring
    b. Monitoring phases: observation, data processing, recognition, decision, feedback action
    c. Attacks on sensors
    d. Attacks on cognition, misleading, confusion,…
    e. Disinformation

Labs:

Labs will concentrate on a limited number of topics, selected on the basis of being representative of the domain, feasible for the students and practically applicable through their careers. While the lectures will remain on a high level of generality, labs will tackle specific instances of the theoretical problems discussed during the lectures.

1. System Analysis, security properties of a specific system, threat model [**1/2 labs**]
2. Crypto/protocols: [**4/5 labs**]
    a. SSL session setup (bit-by bit) , vulnerabilities, key management, certificates
    b. Protocols: eavesdropping in GSM/3G networks, MITM attacks, API security, access control
3. Multi-level security: practical setup of SELinux, testing, BLP model implementation, resilience to attacks and single application vulnerabilities [**3 labs**]
4. Selection of labs [**4 labs**]:
    a. Steganography
    b. Network security