T-110.5230 Special Course in Practical Security of Information Systems

Introduction to the course
Topic selection

22.1.2009

Outline

- Basic course information
- Student introductions & pairing up
- Topic selection (+ some old topics)
- Other issues

Basic course information

Basic course information

- T-110.5230 Special Course in Practical Security of Information Systems
  - 4 credits, post-graduate level
- Course language = English
  - Lectures, slides, web
  - Student presentation in English
- Course staff
  - Sami Vaarala (lecturer), Antti Nuopponen (assistant)
- Contact information
  - Web (noppa): **https://noppa.tkk.fi/noppa/kurssi/t-110.5230/**
  - E-mail: **t-110.5230@tml.hut.fi**
- All course information is on the course web page
  - Student group and topic related pages are not public (e.g. indexed by Google) but available to Noppa users
  - Confidential topics are handled outside Noppa entirely (more about this later)

Basic course information

- Learning goal
  - Security through attack and defense in practice
  - Systematic information search, **practical exploits**, documentation
  - Heavily practice oriented – planning and executing attacks
- Course deliverables
  - Paper TOC and references
  - Attack plans
  - **3 vulnerability reports**
  - **Paper** (8-10 pages)
  - **Presentation**
  - + Assorted peer reviews
- Course work is done in pairs
  - In special cases 1 or 3 persons

Basic course information

- Schedule (see the course web page)
  - Two lectures after this one + presentations
  - Course work begins after next lecture, and ends in presentations (in second half of April)
  - Before presentations, there are several smaller deadlines
  - Because the course is practice oriented, it is not possible to “cram up” during the last week – hence multiple checkpoints
- Grading
  - Based on all course work deliverables
    - Especially “polished deliverables”: paper, presentation, and vulnerability reports
  - All deliverables affect grading, but rule of thumb:
    - “Base grade” based on topic difficulty: easy=1, medium=3, difficult=5
    - A modifier (plus or minus) based on how well topic has been executed
    - Example: medium topic, well executed, can be 4 or even 5
  - We'll give “base grade” feedback when we get your attack plans

Sending course deliverables

- All deliverables in PDF format
  - PDF must be compatible with Acrobat Reader
  - Paper must be produced using LaTeX (templates on course web page)
    - Template based on NetSec 2004 paper template
    - See e.g. NetSec web page and newsgroups for LaTeX tips
- Submission using e-mail by midnight (24:00)
  - Compress all files into **one ZIP file**
  - Send the ZIP file as an e-mail attachment
- Late submission = impact on grading
  - If you're going to be late, notify us in advance if possible
    - If you have a valid reason, no impact on grading (e.g. family emergency)
  - Deadline extensions – only for unforeseen, valid reasons

Student introductions & pairing up

Student introductions & pairing up

- Student introductions
  - Help in pairing up and avoiding topic conflicts
  - => **Let's do that now!**
- Please describe
  - Who are you ?
  - Why are you interested in the course ?
  - What types of topics are you interested in ?
  - Do you already have a pair ?
- If you don't have a pair
  - Stay behind after the lecture and find a pair
  - **You should have a pair after the lecture (finding one later can be difficult)**
  - If you don't find a pair after lecture, please come talk to us

Topic selection

Central criteria for a good topic

- Topic must include **actual attack work**
  - Purely theoretical work is not enough, unlike in most courses
- Successful attack should **cause some compromise**
  - If you succeed, some **(security relevant) harm** should be done
  - You need to define your security assumptions and relate the attack to these
- Successful attack should be **possible but not self-evident**
  - If successful attack is clearly not possible, the topic is useless
  - If successful attack is automatically guaranteed, the topic is **usually** useless (more discussion on this on following slides)
  - A failed attack does not cause a negative grade impact, if the effort was good
- Attacks **can be implemented** within course scope
  - 2 people and 4 ECTS credits of work (including paper work)
- Topic should be **challenging** for student capabilities
  - Requires a stretch but not beyond course scope
  - Choose a topic which challenges you and makes it interesting

Other considerations

- Own topic is best, if you can find one
  - Try to find a topic that hasn't been extensively covered yet
- Grading may be affected by an easy or “old” topic
  - If old topic (say 802.11 security), try to find a novel perspective
    => more interesting and better grade possible
- Can you actually find three vulnerabilities related to topic?
  - Combination attack may result in more realistic exploits
  - To ensure you know what you're doing, we require attack plans
- Do you have access to the equipment you need ?
  - Remember – The course does not provide these
  - Permissions from property / asset owners
  - Novel or custom built hardware is fine
- Overlap with other course participants
  - Rule of thumb – max. 2 pairs per topic
  - Usually not an issue

Other considerations

- Company-sponsored topics
  - A company may provide a product for vulnerability testing
  - If you know interested parties, let us know
- Confidential topics
  - Your topic relates to your company or other contact who wants to remain anonymous (for example)
    - Come talk to us after the lecture if your topic might be confidential
  - Special arrangements: e.g. deliverables returned in paper format
    - You'll present your paper, no need to reveal e.g. company name(s)
    - The paper or vulnerabilities will not be available to other students
- Hardware, software, testing environment, permissions
  - You need to get all these yourself !
  - You may use the laboratory network
  - Vmware, User Mode Linux, Xen, Qemu, KVM, or other virtualization ?

Common questions re: topic

- Can an existing vulnerability be a topic ?
  - **Yes** – topics do not have be truly novel, but it is preferable to find some new angle to the topic, for instance:
    - You extend the attack in some manner
    - You apply the attack in situations where it hasn't been applied before
    - You combine multiple known attacks together into an interesting combined attack
  - If the attack is difficult to carry out (e.g. biometric spoofing), then even a previously known but difficult attack may be OK as is
    - There is considerable difficulty and related risk of not succeeding
    - Examples: implement a recently discovered theoretical (e.g. cryptographic) vulnerability, reverse-engineer a non-public exploit, repeat a known challenging attack (side channel attacks, optimized brute forcing, etc)
- Can existing tools be used ?
  - Existing tools **should** be used whenever possible
  - However, they reduce the amount of practical work done
  - => Ensure that even with the use of existing tools, there is enough practical work (programming etc) to fulfill course target effort (2 x 4 ECTS credits)
- If unsure, please ask through course e-mail

Topic reservation

- You should come up with topics this week
  - Email course staff if you're unsure about a topic or just can't find one
- Reservation during next lecture
  - List of reserved topics
  - Conflicts will need to be worked out
  - Backup topics – you should have a backup topic in case your primary topic is too popular or otherwise not acceptable
- Conflict resolution
  - We'll work it out peacefully next lecture
  - If all else fails, random choice

Rough topic areas

- Protocols
- Protocol implementations
- Hardware
- Operating systems and core services
- Application software
- Products (e.g. networking)
- Web technology
- Misc

Protocols

- Cryptographic protocols – SSH, IPsec (IKEv1/v2), TLS
- Authentication protocols
- Peer-to-peer protocols
- Databases – LDAP, Active Directory, SQL
- Grand old Internet protocols – DNS, HTTP, FTP, etc.
- Mobility protocols – HIP, Mobile IPv4, Mobile IPv6
- Routing protocols – RIP, OSPF, BGP
- Link level protocols – Bluetooth, 802.11

Protocol implementations

- Look at the implementation of basically any important or interesting protocol
- Both server and client software is OK
- You may compare multiple implementations of the same protocol (e.g. IPsec in Windows XP and other implementations)
- You're almost certain to find security issues :-)

Hardware

- Printers, digital cameras, scanners, etc
- Tamper-proof (or rather, resistant) devices – smart cards, USB tokens ...
- Electromagnetic leaks, timing attacks
- Dismantling smart cards or other hardware devices
- Hardware man-in-the-middle attacks

Operating systems & core services

- Microsoft platforms – XP/2003, Windows Mobile
- UNIX platforms – Linux, *BSD, Solaris, ...
- Mobile platforms – Symbian, Windows Mobile
- Virtualization technologies – Vmware, Xen, User Mode Linux, Qemu, etc
- System services – Authentication models, disk encryption, etc

Applications

- P2P clients and servers
- Audio and video players, codec libraries
  - Try to produce media files that exploit vulnerabilities in player software
  - Digital TV decoders
- Mail clients, web browsers
- Software vulnerabilities in widely used or critical applications

Web

- HTTP, CGI backends (mod_perl, mod_php, etc)
- Java, JavaScript, ActiveX
- Web browsers and servers
- Flash

Miscellaneous

- Connection hijacking
  - ARP spoofing + TCP spoofing, man-in-the-middle attacks
- Cracking cryptographic primitives or constructs
  - Distributed brute forcing, etc.
- Admin security tools – libsafe, samhain, etc.
- Attack tools, toolkits, rootkits, etc.
- Social engineering
- Biometric authentication spoofing

Some topics from previous years

- DES 40-bit Key Recovery Software Implementation and Results
- Security flaws in SSH-1.2.17
- Denial of Service Attacks
- Network Attacks on IPsec
- Rootkits revealed
- Quality of Third Party Networks Services at Company X
- Hijacking a TCP/IP connection using an ARP attack
- WLAN Vulnerabilities
- Social Engineering Continued
- Attacks of GPRS
- Security of USB tokens
- Attacking predictable IPsec ESP initialization vectors
- IPv6 enabled Mobile Router Security

Some topics from previous years

- The Internal Network of an Office Building
- Fooling Fingerprint Scanners
- Attacks on Kerberos V in a Windows 2000 Environment
- Penetrating embedded personal firewalls with trojans
- Game Server Vulnerability Exploits in DoS attacks
- Xerox 7132
- UPnP Protocol
- Message Stream Encryption (MSE)
- AES side channel attacks
- BSD rootkit
- Cross site scripting
- Security analysis of cadred.org
- Xen hypervisor

Some topics from previous years

- Attacking Kerberos 5 Vulnerabilities
- Attacks against the Clavister firewall
- Attacking the Microsoft Fingerprint Authentication System
- PhpBB
- OpenVPN
- RFID
- Faking WLAN hotspots
- Eavesdropping and taking control of Symbian phones
- DHCP
- Cache timing attacks on AES (Bernstein attack)
- IPV6 stateless autoconfiguration
- Testing Axapta application security
- Bluetooth

Some topics from previous years

- P2P client security
- BitTorrent networks
- Windows file sharing & SMB protocol
- Wireless keyboard sniffing
- Flow control vulnerabilities in web based applications
- Attacking electronic documents and digital signatures
- Linux firewall security
- DoS against CRL distribution point by compromising NTP service
- Vulnerabilities of game network implementations
- ICQ vulnerabilities
- Feeding malformed media files to popular media players
- VoIP vulnerabilities

Other issues

Legal issues

- The course deals with practical exploits
  - For instance, people have explored how Trojan horses work
- You are responsible for the legality of what you do on the course
  - HUT or the course (staff) is not responsible for what you do
  - In particular, you're responsible for ensuring no harm is done to other people's equipment, network, etc.
  - Get permissions for whatever networks or equipment you will be hacking
- Finnish law applies (of course)
  - We (or HUT) cannot make judgments on what is legal and what isn't, we don't have the necessary training
  - Digital Rights Management (DRM) has been a problematic topic since beginning of 2006 :-((organized discussion is now probably illegal)

Paper publication

- Best papers may be submitted as conference papers
  - Papers typically need a substantial amount of editing and re-scoping before they are ready for submission
  - 3 papers accepted to Australian Information Warfare and Security Conference (AIWSC '03) from the course in year 2003
- The process depends on the paper, case-by-case basis
  - We'll ask the authors of best papers whether they are interested in submission
- Keep this in mind as an alternative
  - Valuable experience, if you haven't published before
- Of course, you're free to proceed on your own, independent of the course
  - This is not directly related to course work or grading

Summary

- Your effort => 4 (ECTS) credits
  - Vulnerability reports, paper & presentation + supporting submissions
- Next steps – before next lecture
  - Make sure you have a pair to work with (if not, stay after lecture)
  - Topic selection begins after this lecture
    - Look up topics, brainstorm for your own topics
    - Select primary and backup topic
    - Discuss topics in the newsgroup if you think there may be overlap
  - Next lecture: topic reservation, writing process, other issues
  - After that, mostly deadlines (maybe one interim lecture) before presentations
- Questions ?
- See you **Thursday 29.1.2009 T4 16-18**