Final Thoughts

- I will try to outline the process of definition of a new research area to our laboratory.
- This problem appears in telecommunications, military science and computer science quite often.
- With existing old scientific fields this problem has been solved long ago and people on such fields usually do not appreciate problems of this type.
- Actually they are convinced that the problem is that the people in the new field simply are too poor to make good research.
- Many even go so far as to say: you can make a Ph.D. thesis from anything and point out to some weird examples without looking more carefully to each case. This opinion is far from being correct. Ph.D. can be straightforward, or it can be almost impossibly difficult.

Final Thoughts

- What to do to define a research field?
  - Select the research methods
    - Here one should select carefully because some methods require background which is not easily included to the curriculum. You just cannot pick up some good but very difficult mathematical theory, doing so means that you have to add new courses and get students to them.
    - Must be suitable for academic research, that is, it must be possible to use accepted research methods (modeling, analysis, measurement, statistics, experiments, simulation,...), otherwise it will be extremely hard for somebody to make a Ph.D.
    - If nobody can make a Ph.D. the field should not be in the university and will face problems in the future.

Final Thoughts

- Pick up some central problems
  - One needs good, useful, interesting and hard problems.
  - Not problems that are solved in next few years.
  - The problems must be interesting, relevant and modern. Students and external funding will be needed, the problems must be attractive enough for that.
- Find the existing main results
  - There should be some existing research which can be considered as results of the new area, otherwise you are in trouble and have to invent everything to start with.

Final Thoughts

- Find the publication forums
  - This is often ignored as a new field does not have dedicated journals, conferences etc.
  - Ignoring this problem leads into trouble.
  - This will influence the suitable research methods.
- Find the practical application areas
  - The goal of education people is that they will find work where the education is needed.
  - Ignoring this question is very common. It leads to a situation where a set of people are waiting for a single job in the university. They can find some other work, but it means that the education is largely useless.
- Answering all these questions should be enough.

Final Thoughts

- Let me now use this process in the area of the course: Security of Communication Protocols.
  - Select the research methods
    - we have some candidates:
    - cryptography
    - proving cryptoprotocols secure by some calculation
    - hacking statistics from CERN and some Ph.D. thesis
    - design of security features to protocols
    - any other mathematical theories could be considered, maybe Operations Research could be suitable as it is applied math. with engineering and military applications.

Final Thoughts

- What natural mathematical tools we should not elaborate?
- Not cryptography
  - this requires good mathematical basis, number theory, maybe algebra, complexity theory
  - and theoretical computer science: algorithms
  - there areas do not fit into our curriculum well, in fact the necessary areas of mathematics are not well represented in engineering mathematics, engineering mathematics typically contain areas of Operations Research
  - cryptography has too much secrecy, that is, studying only from public sources may not be enough
  - professorship in this area is in TIK
  - for these reasons we should not develop cryptography as a research field here

Final Thoughts

- It cannot only be practical design of secure protocols either, that is not theoretical enough for continued studies
- What seems possible is to use modeling methods in: Military tactics
  - combat equations (Lanchester-type, red and blue side destroy each other according to some differential equations)
  - circular model of barriers (submarine-ship model, how many submarines are needed to sink certain number of ships if there are places where submarines are destroyed with some probability)
- Epidemiological
  - spreading of viruses
- Time series, filters, prediction, game theory

Final Thoughts

- Empirical research should be included:
  - collect information of security breach incidents and analyze statistically
  - make laboratory tests/games to see how people really behave (like in empirical economics), then model the results in mathematical way
- Design of new mechanisms
  - design, implementation, testing, piloting, comparison
  - this is a typical research method in protocols
  - use formal languages (UML, XML, SDL, ASN.1), it gets a bit more precise, research should be precise.

Final Thoughts

- Find central problems:
  - Briefly: information warfare, protection against hackers
- There are security problems which seem hard to remove:
  - Malicious code (viruses,worms, misbehaving mobile code like agents, scripts etc.)
  - Bugs in software (operating systems, protocols etc.)
  - Insecure usage (poor passwords, unprotected services, old versions etc.)
  - Denial of service of some type is usually possible
  - Public key problems of distributing keys
- Related fields bring new problems:
  - Development of cryptoanalysis
  - Fast speed of change in telecommunications

Final Thoughts

- Find the existing main results:
- The results so far are some security mechanisms. The systems covered have a variety of security mechanisms. (This is not a classification, just some mechanisms mentioned).
- **Controlling/limiting access**
- Firewalls, NAT, chrooting, program access rights,
- **Behavior monitoring**
- In Java sandbox, in antivirus software, alarms/logs if changes
- **Cryptographic methods**
- Encryptation, signature, authentication, PKI, KDC, etc.
- **Stopping information gathering**
- anti-scanner tools
- **Access tickets**
- Kerberos-style, what about AAA?

Final Thoughts

- Find main publication forums:
  - Journals of Operations Research
  - IEEE Transactions of Networking and Journal of Selected Areas have published a few articles of this type
  - Conferences, finds some suitable
- Practical applications
  - Not a problem here, security features in protocols, intruder detection etc.

- So, this looks like a good field. Always do this process if you have to invent how to do research on a too practical field.

Some sample ideas

- What one could do with the problems?
- Bugs in software
- Possibility: create a secure protocol development tool
- TCP/IP applications especially in Unix seem to contain vulnerabilities like buffer overflows. In Kerberos V5 they saw some benefit from formal languages, like ASN.1.
- Could we make a secure protocol development tool which guarantees that there are no holes of some type, like buffer overflows? In a limited sense this should be possible.
- Complete automatic code generation is difficult and probably not possible, so there will be places for bugs. There are too many systems coming up, combining them creates problems.
- Using standard interfaces, preferably APIs, standard cryptographic protocols, modular structure etc. should improve software quality.

Some sample ideas

- Filters to protect against DoS ?
- The most common Denial of Service attacks are attacks trying to fill some resource, like mailbox, congest the network or a server, reserve all connections to a port etc.
- One common protection mechanism is using filters, which act as limiters which by blocking connections or by dropping packets.
- Usually we can create a filter which is not congested by levels of traffic which can be offered and therefore it can protect other network elements.
- The concept of a filter has however the problem that legal traffic will also be filtered, so an attacker can decrease the acceptance ratio of legal traffic simply by injecting more bogus traffic. If the filter moves closer to the attacker, it will not reject so much legal traffic. We get to the idea of active networks DoS defense.
- Active networks are unsafe, but try to make something of the idea.

Some sample ideas

- Provably impossible cryptography
- Making own cryptoalgorithms is not a very good idea, there are many cryptoanalysists with a strong mathematical background and much of the work is not public, so it is unlikely to create anything very good and original.
- It is most probably possible to devise cryptoalgorithms that actually never can be broken, but so far many have been broken.
- The following is just an idea, not very serious either:
- There are provably unsolvable problems, like the word problem on finitely presented groups/semigroups (the groups are infinite, bad).
- One can make for instance a proof method: create a representation 1=word using the finite set of group generators and relations. Nobody but you can prove the statement, no algorithm will be ever found, only brute force calculating as far as they think you calculated. Encryptation is harder to make along this idea.

Some sample ideas

- Postal letter type security service, avoid PKI?
- A registered letter is like encrypted email. You need keys and problems come with key management. A normal letter is not safe, but if a cover is opened, you usually see it.
- Normal letters are good enough for most and easier than registered letters. How to make it in email?
- What about a central server from which you can ask for letterID, key pair. You obtain it and submit to the postal service. Any receiver can ask for the key for the letterID and open the letter. The central server will strike out the key as already given.
- If an attacker asked for the key, he would get it and could read the letter, but you would know that the letter was read by somebody else. Poor service, but notice, that users do not have keys at all.
- Of course, PKI is useful and necessary for many services.

Some sample ideas

- Security needs in future networks
  - like always: privacy and control of access/use this has been the traditional area what security mechanisms try to solve
  - as a new thing, charging services (e-commerce, m-commerce)
  - new services made with security mechanisms

  - I will try to invent some new service using security mechanisms to illustrate the last point.
  - Nobody was very convinced of this idea last year.

Some sample ideas

- Security services for Intelligent URLs
- IN had some nice thoughts with new service scripts made with GUI (Graphical User Interface) as combination of SIBs (Service Independent Building blocks)
- URLs in Web often are unreachable after some time, hindering their usage as e.g. references.
- We could define intelligent URLs which would have properties given by some flags, like permanency (will not disappear, will not need to be updated often), security, locality (always comes form a local server, multiple copies exist), running a CGI-script, hiding real identity etc.
- What could be the security services need and how to make them. We want verifiable authenticity, or just inversely hiding real identity, secure communication, credit card call equivalent, etc. all kind of IN type and new services.

Exam hints

- What are the important things in the course?
- Some security threats, one should know what a hacker does.
- Different security mechanisms.
- Some common security protocols.
- The exam is somewhat more than 1 credit, so I expect that you have studied at least 3 days full time. It is <200 A4 pages of text covering the Internet Security book mostly (916 pages) and some additional parts, like one book from IPSec, another book from SET, NT security from Internet Security book’s CD, some parts from WWW-material and from Maximal Security, some information warfare, mCommerce, IDS stuff.
- This means that the source material is quite large and the lectures are not very detailed (or good). There is some sense in this as by knowing a large number of solutions one can invent new solutions and apply the knowledge.

Exam hints

- Exam protoform
- In order to check if you have read the lecture notes two first questions are
- 1. Explain the main principles of X, or explain briefly 6 acronyms
- 2. Explain the main principles of Y
- where X, Y are any topic covered by a lecture (firewalls, viruses, kerberos, WWW or Java security, SET, IPSEC, IKE, Information warfare etc., simply any main topic)
- 3. How could a hacker attack something in some environment and how to protect against it.
- 4. Similar as 3. Example: how could a hacker capture a TCP connection and how could you protect against it. See HUNT tool, explain how the attack is made and what would stop it. I may ask to explain some well known tools used in the exercises.
- 5. Design (sketch) a security solution for the following scenario.

Exam hints

- And what could be the scenario in 5? Something that I have encountered and which needs a security solution, like VHE offering value added services to customers, or offering QoS classes to customers.
- Explain what are the main threats and how they can be solved, or will they be ignored in the solution.
- So, what the exam tests?
- That the material is studied (1+2). You do not need to write directly from my notes if you know better, but do not write worse than there. It is a short summary, you can prepare it.
- That you understand how attacks are made and how they can be stopped. How an attacker could proceed.
- That you can apply the knowledge for designing security solutions. The design is preliminary as there is little time.