

DTEK8026 Organizational level information security - Learning journal

UNIVERSITY OF TURKU

Department of Information technology

Computer science

17.3.2009

Vesa Nieminen

Contents

Introduction.....	1
1 weekly report 1	2
1.1 About the lecture.....	2
1.2 The spam situation of the world.....	2
1.3 Article 1: 'How Good Are Our Weapons in the Spam Wars?'.....	3
1.4 Questions:.....	4
1.5 Appendix: Spam table.....	5
2 Weekly report 2.....	6
2.1 About the lecture.....	6
2.2 Metric-driven method for security risk assessment and decision making.....	6
2.3 In 2007, the total salary costs at the University of Turku were 118,435,000 eur,	7
2.4 Compare the formula you derived above to the formulas provided in the last link.....	8
3 Weekly report 3.....	9
3.1 General thoughts on the topic (no lecture this week).....	9
3.2 Summary.....	9
3.3 The "four waves" of information security.....	10
3.4 What will be the fifth wave of information security?.....	11
4 Weekly report 4.....	12
4.1 About the lecture (IT Governance).....	12
4.2 Discuss your comprehension of IT security as part of governance frameworks.....	13
4.3 In practice, what kind of governance would you implement?.....	13
5 Weekly report 5.....	14
5.1 About the lecture.....	14
5.2 Compare notes on the printer/copier/fax security issues gathered by team members.....	14
5.3 Discuss the biometric attack vectors and defences.....	15
6 Weekly report 6.....	17
6.1 About the lecture.....	17
6.2 Discuss the Geneva approach.....	17
6.3 Discuss the futuristic vision of an ubiquitous health care and monitoring infrastructure.....	18
7 Weekly report 7.....	20
7.1 About the lecture.....	20

7.2	About the article / research paper.....	20
7.3	Discuss the survey results in general.....	21
7.4	Discuss the phenomenons described from section 8.2.2. onwards.....	21
8	Compensatory work.....	23
8.1	How poor management causes IT failure.....	23
	Conclusion.....	25
	Attachment.....	26

Introduction

This is my learning journal for the course “Organizational level information security” where we (the students) had the assignment of keeping track of our progress throughout the whole period. In addition to that we had group meetings with team 3 members each week where we discussed the topic at hand to make our learning experience easier, more efficient, and more fun. At least that's my interpretation of the whole deal.

Team 3 consisted of 7 persons: Juha, Lasse, Lauri, Santtu, Saul, Rauli, and Vesa. I've known Juha since I was a kid but all the other people were new acquaintances for me, and quite pleasant ones at that I might add.

Group meetings were held at the following times:

- 1st 23.01.09 12 – 13 (me as the chairman)
- 2nd 29.01.09 12 – 13
- 3rd 06.02.09 14 – 15
- 4th 12.02.09 13 – 14
- 5th 19.02.09 13 – 14
- 6th 26.02.09 13 – 14
- 7th 05.03.09 13 – 14

All of the meetings took place in the ICT library's biggest group work room, which I had found to be a good location previously in another course.

1 weekly report 1

1.1 About the lecture

The topic for this week's lecture was 'Email system security and spam countermeasures in a large organization'. The lecturer first talked about security issues and spam generally and then for the last 30 minutes went on to describe anti-spam techniques more specifically. I found the lecture to be quite interesting and as a topic it fit well into this course. Everybody uses email these days so the topic applies to everyone. On the technical level this lecture introduced me to various different anti-spam techniques that I was not aware of before.

1.2 The spam situation of the world

In short the situation is quite bad. In the lecture Eino Tuominen showed statistics that argue that 95% of all email sent in the world today is spam. If that were true and we would have no anti-spam techniques in use it would mean that for every 20 messages you received only one of them is “real” email that you might care about. Thankfully that is not the actual situation. Instead we have (more or less) effective systems in use that limit the spam that we receive on a day to day basis. For example, when using the utu email address, every once in a while some spam might sneak into your mail but even that is quite a rare occurrence.

A worse case situation of an anti-spam system is when a legitimate email is considered as spam, called false positive. For important emails this is a crucial matter. You would not want to miss an email about financial grants or acceptance email to a university for example and as these things have happened before they are a real concern (some cases have been highlighted in the U.S.). Eino commented that utu IT administration has built their system in such a way that false positives should not happen. A user would rather get a couple of spam messages than miss an important one.

During our group work meeting we discussed a bit about the statistic websites whose urls were

provided for us. Spamhaus turned out to be a more useful statistics site because it gave a more user-friendly view into what's going on with the world of spam at any given moment.

The statistics themselves turned out to be very similar in our group although we had looked at them at different times and days. The top five worst spam origin countries in the world are: USA, China, Russian Federation, United Kingdom, and South Korea (See Appendix on pg 3.).

On Spamhaus's website there are instructions how a person can set up an effective spam filtering system that should catch 99.6% of all the spam that an email server is receiving. That means that for every 300 spam messages only one gets through the filter.

During our group work meeting we also discussed the accuracy of the data from these anti-spam statistic services and we came to the conclusion that the data is probably not exactly the situation in the world but gives a good idea estimate.

For SpamCop the data is gathered from users but Spamhaus has their own systems that they use to detect and identify spam.

1.3 Article 1: 'How Good Are Our Weapons in the Spam Wars?'

Firstly as a philosophy student I want to make a simple comment on the article's title. When oneself is fundamentally at war against something or someone there is little chance to fix the issue. Warring implies resisting and therefore the object is likely to merely persist. A sounder approach would be to accept the issue and seek for a way without conflict. :)

Now with that out of the way I'll make a few comments on the article itself.

I found the article to have a nice and structured way of presenting the case about what spam fighting techniques exist today. Also the content was good as I now have a better understanding of ways to control spam.

Legal ways to protect oneself of spam are explained to be very ineffective because the criminals can just move to a safe haven's where laws don't apply or they can find a loophole in the current laws because they are set in a lax way so as not to go in the way of free speech.

The most insightful (and simple) idea presented in the article in my opinion was: "To actually

reduce the volume of spam, a negative feedback loop is needed in the system.”. What that means is that the email system has to be changed in such a way that the costs for the spammer to do spamming are higher when more spam is being sent. This is of course very basic but I can see that as being in the core of the whole spam issue.

1.4 Questions:

- Spam generation is analyzed as a system. What benefits are there in such an analysis method?
 - It allows for a better understanding of the whole problem and for ways to explore different control methods and to categorize them (eg. sender client, sender server, receiving server, receiving client)
- What seem to be the most effective anti-spam techniques?
 - The combination of blacklisting, whitelisting, and greylisting is reported at least in one occasion to reduce spam by 88%, so that's quite effective. Greylisting has its problems though as it relies on rate throttling ie. delaying the receipt of a message. It can delay 98% of spam but also 40-50% of valid email.
 - Payment based spam control seem quite good as they require a financial, “intellectual”, or computational costs that move the costs more to the sender client end. If spamming actually costs money for you then you are less likely to do it.
 - Information-hiding-based spam control would be very effective but some complex solutions require a total change to the email system.
 - Authentication-based spam control is also effective as it can be used to make the spammers accountable of their doings.
 - Over all the most effective anti-spam techniques are the ones that act directly on the sender server or client.
 -
- What kind of spam seems to be the most difficult to avoid?
 - I did not find anything particular on this question from the article so I'll just comment that the most difficult type of spam to avoid in my opinion are those that use randomization to make a single spam mail look heuristically nothing like another from

the same batch.

1.5 Appendix: Spam table

1	United States	1462
2	China	454
3	Russian Federation	300
4	United Kingdom	210
5	South Korea	202

5 worst spam networks of the day (23.01.09) 11:00

1	sistemnet.com.tr	46
2	hostfresh.com	35
3	gilat.net	31
4	cnuninet.com	30
5	vsnlinternation.al.com	29

5 worst spamvertizers networks of the day (23.01.09) 11:00

1	Canadian Pharmacy A long time running pharmacy spam operation. Uses botnet spam techniques to send tens-of-millions of spams per day. Probably uses many affiliates all over the world to spam but is probably based in Eastern Europe and hosts sites on botnets and on Chines	United States
2	Leo Kuvayev / BadCow Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green"	Russian Federation
3	HerbalKing Massive affiliate spam program for snakeoil Body Part Enhancement scams. Also does replica luxury goods, phama and porn. Spams via botnets, bulletproof hosting offshore and even sometimes uses fast flux hosting.	India
4	Vincent Chan / yoric.net Vincent Chan and his Chinese partners have been sending spam for years. They mainly do pharmacy, and are able to send out huge amounts daily. The use a vast amount of compromised machines, for sending, hosting and proxy hijacking.	Hong Kong
5	AlexBlood / Alexander Mosh / AlekseyB / AlexPolyakov So many Alex & Alexey spamming! AlexBlood tied to Pilot Holding & bbasafehosting.com long ago, then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring, also pharma, mortgage, and more. May work with Kuvayev and Yambo.	

2 Weekly report 2

2.1 About the lecture

This week's lecture was about “Information security administration in a large organization”. Mats Kommonen started the lecture quite philosophically by stating that “The computer is a soulless apparatus that executes single commands that a human being has set for it”. I thought it was interesting way to begin and I suspect the reason was to create some distance to the technical side and to emphasize the human side of security administration. In the end it is always a human task to uphold the security.

The main thing I got from the lecture was about risk assessment. In it you make estimates for certain organizational costs so that you can know in advance how much money is useful to spend on something. That is of course a very rational way to approach the topic.

Mats gave an example of risk assessment where he began calculating the costs if supposedly the power-point presentation for the lecture was ruined by him stomping on his USB-memory stick before it. The USB-memory stick itself is not that costly, Mats estimated it to be about 14 euros, but the resulting failure to give a proper lecture could potentially be.

Another example was that of university of Turku's employee's salaries. If the salaries are 1000e/min and the internet connection does not work it is useful to be able to measure how much money to spend on making sure that the connection does work.

2.2 Metric-driven method for security risk assessment and decision making

- Does the article present a feasible and realistic approach for managers?
 - It does, because it allows for modeling and to measure certain characteristics of security that would otherwise possibly go unnoticed. The data that the model is based on has to be organization-specific to be really meaningful, otherwise they're just guesses based on industry averages. If organizations just blindly follow with compliance to certain standards it does not necessarily do anything positive for the ROI.
- Would you use this kind of approach? Why, or why not?
 - Yes. For a large organization it does make sense to take things into account more but that entails that real organization-specific metrics have to be measured. For a small start up company this might not make total sense as the costs to do systematic appraising of different security components might be too high.
- How would you improve the approach?
 - As is said in the article: “You can't manage what you can't measure”, so I would scrap all the details that are too fuzzy for any specific organization and just keep the ones that can be measured with some certainty.
- What are the key benefits and drawbacks of the approach?
 - This approach helps with managing security and putting effort where it is needed, but it takes time and effort to do it of course

2.3 In 2007, the total salary costs at the University of Turku were 118,435,000 eur, ...

- In the group, make (simple) calculations of how much such shortages would cost annually.
 - Altogether we ended up with the yearly sum of 167 500e, that's 40 085e for teachers, 41 907e for research staff, and 85 514e for other staff (secretaries and other administrative positions).
- Derive a formula for the cost using formula 1 in the second article (Böhme et al.) as a starting point.

- $ALE = SLE \times ARO = 501\,500e$
- What could the university achieve with the money that would be saved if no blackouts would occur?
 - Buy new IT infrastructure and computers for instance

2.4 Compare the formula you derived above to the formulas provided in the last link

- Do you think the result you reached above would be more precise if you used the more complex formulas?
 - Only if the data is correct. With just more complex formulas you cannot gain anything. It might not be possible to get the data anywhere in which case it would be quite pointless to make it any more complex.
- Would the difference be so big that you, as a manager, would instruct your risk assessment employee to use the more complex formulas instead of deriving a simple approximation?
 - Possibly yes, but only on a case by case manner.

3 Weekly report 3

3.1 General thoughts on the topic (no lecture this week)

I've never thought about information security (IS) before as something that has come in waves. In the two articles we read this week professor von Solms did exactly that by defining and, for the last two, explaining them in detail.

It makes sense to think of the whole process as something that grows over time. It would have been hard for a person to come up with the whole concept of what IS should be in the beginning of IT or even during the 80'ies or 90'ies or if IS is even now what it really should be. There are of course these cases such as Alan Turing, Edsger Dijkstra, Donald Knuth, Fred Brooks or even Alan Kay in the field of IT who seem to have had the ability to pave way for the future but these are of course the exception to the rule and not the norm.

3.2 Summary

So, according to von Solms, the process of IS has come in four different waves. During the first wave people thought about IS as something that can be solved technically. If you have file based permissions and passwords for people's user accounts that's enough, because no one can access your files unless they have the required permissions and know the password, right? Yeah, right :)

Second wave can be described as things that have to do with managing the IS situation in a company. Due to IT being more wide spread and having to do with business critical processes there was a need to make sure that everything worked more or less nicely. IS managers were appointed and policies, procedures were created to handle the situation. Also awareness began to grow that IS is perhaps not just about technical issues but also about people, and perhaps even more so.

Third wave (institutionalization) introduced de facto processes that later grew into real standards and the standards allowed for certifications for companies who needed them. Companies sometimes began to refuse partnership with other companies if their IS was not up to par with their own. Metrics were invented to measure the IS aspects in a company so that a proper feedback loop could be used for managers. The previous awareness about IS issues regarding the people were started to get addressed by making IS policies etc to become natural day to day activities in a company. Also during this time von Solms made the prediction of what the fourth wave could possibly be like (which later turned out to be false and quite naive).

The fourth wave von Solms calls, in his second article, IS governance. This wave deals with IS as the “whole package” meaning that it's taken very seriously and is painstakingly tuned to work with the daily work cycle of the company. The main thing is to make the different aspects of IS (policies, people, etc) work together in such a way that the company's electronic assets are maintained at all times, meaning that the confidentiality, integrity, and availability are made absolute premium.

3.3 *The "four waves" of information security*

- Do you agree with the author's views on the waves of information security development over the past decades?
 - Although I wrote that I haven't thought of IS before as waves or anything like that I do accept the von Solms point of view. It gives a nice dissection of the whole IS business. I don't know how this view goes together with real facts but it's at least interesting to see that the second wave is timed to the period where computer hackers began to grow more infamous (eg. Kevin Mitnick).
- The author predicted one kind of fourth wave in the first article. If his analysis in the second article is accurate, did he predict the future correctly? If not, what kinds of development trends lead to actualization of the wave described in the second article instead of the one visioned in the first article
 - Von Solms did not predict the fourth wave correctly in his first article. He painted a picture of a naively bright future that he calls a commodity wave where the IS has become a solved issue. This of course did not happen.

- Trends that impacted the actual fourth wave, IS governance, are eg. the continual commercial spreading of the internet and numerous new threats that companies will have to deal with.

3.4 What will be the fifth wave of information security?

- Make a prediction to the future, considering current development trends in information security and computer networks, like the much hyped cloud computing paradigm.
- The cloud computing paradigm is something I personally think about as being the way of the future. Imagine starting up an internet company and having initially some limited requirements for bandwidth and processing power for serving your company's web site and making database transactions. At this point you don't have many or even any customers so you'd like your expenses naturally to be kept at a minimum. Now, what happens when the needs for your company increase due to getting more customers? Do you just manually buy more bandwidth and processing power, swap to a new service provider, make a new deal with the existing one, try to set up or optimize the system yourself or what? A better and much easier solution would be to just set the whole thing to be automatic. This is something that cloud computing allows for. Why would anyone care what type of system they have if they'd have the ability and assurance to just leave the whole thing running on its own? When more customers begin to come in to your company's web site (ie. getting more actual monetary transactions) that's when your revenues begin to increase as well and that's exactly when you want to put more power to the "cloud".
- As technology becomes more complicated we the users require easier ways to manage the situation. I predict services like this will become a major selling point in the future and the IS issues dealing with those are next in line in the "fifth wave". That wave could be called "integration" where IS just part of every business and is in part made more easy to govern. Not reducing the role of IS just making it more opaque.

4 Weekly report 4

4.1 About the lecture (IT Governance)

From the get go Jaakko Kuosmanen struck me as a person who knows what he's talking about; he seemed like the incarnation of experience for some reason. Waku is a company that concentrates on developing their client companies' customers' service management (specialized organizational capabilities). They do this by using best practices and standards that support the best practices. Currently they have 16 + 50 employees, of which the latter 50 are “robots”. By robots I believe Jaakko meant AI bots that do some sort of business intelligence that benefit the company in some meaningful way. Nobody asked about that in detail later during the lecture and Jaakko did not talk about it any more so that was kind of left in the dark.

I liked the part of the lecture where Jaakko was talking about how standards are born. When some beneficial new way is introduced in an industry it first becomes a unique competitive advantage that allows the companies using it to go way ahead of the others. After some time the uniqueness wears off, a best practice is formed, and the competitive edge diminishes some what because other companies are starting to use the best practice more widely. Later on the best practice becomes just good practice which is the normal way of doing things (although without it having to be methodologically enforced), and even later it evolves into an actual standard that is widely accepted in the industry. The way how this whole process works is not just something that IT governance has but it is very universal and can be seen in numerous other fields.

There was a funny moment in one point where Jaakko explained the type of training they offer for managers of other firms. Some of those trainings include strategy games such as “the Pyramid of Egypt” (or something like that) where a person is given the task of organizing a huge endeavour and challenged to do his/her best to achieve the task with the minimum resources.

All in all I felt this quite a useful lecture.

4.2 Discuss your comprehension of IT security as part of governance frameworks

- Based on this week's lecture and the articles, is it simpler or more complicated than you thought? Is it worth while? Why or why not?
- IS as part of governance frameworks is a more complicated issue than I initially thought. For example CobiT goes to very fine detail in what should be taken into consideration in an organization. In a previous lecture there was talk about how some governance frameworks deal with firebomb situations etc what to do when something goes very wrong. In some cases this fine level of detail is of course required to make sure that everything really is taken into consideration but I believe this can also get in the way of actually doing things that matter for the business, especially in small companies. Following processes blindly don't achieve anything other than make you less flexible which can result in unnecessary losses.
- This also ties very much into the business aspect of needing certifications to create proper partnerships with other companies. That is one reason why this complicated nature of IS governance can be worth while

4.3 In practice, what kind of governance would you implement?

- Would it be strict adherence to one of the frameworks, a combination of several, or some other solution? Why?
- As was described in the second article CobiT and ISO 17799 are complementary frameworks which can both be implemented at the same time with beneficial results. This is why I would choose to go with them both instead of just one or the other.

5 Weekly report 5

5.1 About the lecture

This weeks lecture was about “Issues in administrative data security and privacy” and the lecturer was Reima Suomi. Reima started his lecture by mentioning an international archive (kansainvälinen arkisto) in the health care sector that is currently being developed here in Turku. He said a pilot project will tested with students first to see how young people are able to adjust to the system. That bit sounded quite interesting but Reima did not go more into detail yet. We're likely to hear more about that in the next week's lecture.

Reima proceeded to talk about him having problems with the word “data” in preparing for the lecture. He said that data security also implies security in the infrastructure itself. Without an infrastructure that supports data security it is not possible to have proper data security at all. Reima also said that data privacy requires data security implementation and is otherwise not possible to achieve.

Because in his lecture Reima mentioned mainly just a lot of different technical means of achieving data security and privacy I got the feeling that he actually believes that technology will solve the IS problems and not proper procedures, processes, and accordance to standards. This is knowledge that I have acquired earlier in the course, so there has definitely been benefits for me. Reima also seemed to have a lot of “mutu”-opinions: “I think denial of service attacks are more of an American thing”. These sorts of sentences don't help much with the authoritativeness of the speaker. In fact I believe they diminish it quite a bit.

5.2 Compare notes on the printer/copier/fax security issues gathered by team members

- What is the most surprising risk?

- As was discussed during the weekly meeting we found the issues having to do with Windows NT operating system to be the most surprising ones. No one had really thought before that some company could be using that particular operating system eg. in a network printer because that exposes the whole printer system to unsolicited usage. I believe the rationale behind this is something along the lines the WLAN hardware providers currently have. The most important thing seems to be that the system is usable right out of the box. It does not matter if the device is secured or not because the average user probably does not care or know about it. As long as it works ASAP, it's good. This is of course a false notion.
- Which one is the most obvious one?
 - Hooking up devices to a network with default passwords and not doing proper system updates before use. You can find the default passwords for multiple devices on the web usually even from the manufacturer's own site.
- Can you think of additional risks associated with the devices, not discovered in the web articles team members found?
 - The data that is sent to the printer could be sniffed by a third party which would lead to a security breach
- As a manager, what would you do to reduce security risks associated with network printers?
 - Enforce a security system that has the minimum feature-set that is required for the network printers. This would mean that the printer device itself should not have additional services enabled. Also I would make sure that the network topography was such that access would be granted through secure channels only.

5.3 Discuss the biometric attack vectors and defences.

- Consider an organization that decides to move from password and passkey based systems to biometric systems for physical access and computer access for increased security. What kinds of biometric authentication systems should be installed to achieve both physical access and computer access?
 - We came to the conclusion during the weekly meeting that an iris authentication with a liveness detection would be good for ensuring that someone requiring physical access

would be properly checked in a convenient way. The downside of this approach is the cost but the upside is that it is quite hard to spoof.

- Fingerprint recognition for computer access is very convenient and at least somewhat secure.
- What seem to be the most effective attack vectors against the systems you chose?
 - Spoofing with fake biometric inputs
- How about securing the transportation and storage of the biometric data needed to operate the system?
 - Physical access should be allowed only for the device that scans the actual biometric object. In this way we can exclude the possibility of on the premises hacking.
 - Secure encryption should be naturally used when transporting any type of information over a network that can be remotely accessed.
- What similarities and differences in the risks are there if someone is able to steal passkey codes for electronic door keys vs. the biometric data used to grant access?
 - For one biometric data is much harder to steal or spoof
 - There is no original source with passkey codes.
 - Biometric data can potentially cause more rejections.

6 Weekly report 6

6.1 About the lecture

I cannot make any comments on the lecture other than what I heard from my course friends because I was sick when the lecture was held. I heard there were some interesting bits about how patient records are kept in Finland from two particular days of each month for statistical purposes. The data is gathered anonymously so that the privacy issues can be kept at a minimum.

6.2 Discuss the Geneva approach

- Focus especially on its extensibility to trans-institutional use. Assume that the University of Turku central hospital would start using the system, and in a few years it would be extended to cover all Finnish hospitals and health care systems. Would the system scale up to this?
 - Using the system in Turku central hospital does not sound so far-fetched because the system seems to work in the Geneva University Hospitals (HUG) with over 2000 beds in total. As an educated guess I would say that's more than what we have here in Turku, so there should be no problems in that regard.
 - Because HUG has been using the system for so long we should learn from what they have done right and what they have done wrong in order to make the installation process as smooth as possible.
 - Technically I don't see problems in using a system like that to cover all Finnish hospitals and health care systems but that's of course the smallest of concerns. What matters more or even most is that the personnel that would use the system are not hindered in any way to do their daily work. As the report on HUG mentioned the most important challenge there was to develop a system that does not encumber operational activities for the care providers. So that's definitely some that needs to be looked at before going ahead with

installation of any new system like that.

- What are the security risks?
 - A system that is more accessible is also more prone to security risk by definition.
 - Because the patient has access to his/her data the way that access is allowed raises a security issue. A third party could use the same way of accessing the patient's data and modify the restrictions for care givers.
- How about privacy risks?
 - In the HUG system there's a way for a physician to bypass the access restrictions by “breaking the glass” when they see a reason for it. This could potentially lead to privacy issues because the physician could abuse the power and gain information to something the patient wouldn't want to allow. The physician could also do a lot of harm by “breaking the glass” of multiple patients at the same time and sell that information to a third party or something.
 - More generally, as was pointed out in the second article, although the system allows one-time access to information, that information is still in the care giver's own head and that could lead to potential abuses of the system.

6.3 Discuss the futuristic vision of an ubiquitous health care and monitoring infrastructure

- How soon could this vision be reality?
 - For me it sounds almost as complicated as flying cars and fusion power plants, so I'd give it about 50 years to become reality. It would require new technological breakthroughs in addition to public acceptance of such a system, both of those take a long time.
- What additional privacy and security concerns can you come up with if such a system would be used?
 - As was pointed out by the example, your health information could be leaked out to your employer before you even noticed it yourself. This raises the question of who should really have access to that type of information first. The example is very close to a totalitarian society like in George Orwell's 1984.

- If a system is allowed to administer drugs into your body automatically then obviously that system needs to be fail-safe in regards to malfunctioning and administering drugs when you don't really need them.
- How about the discussion about security measures?
 - They seem to be formally defined in a clear way for each counterpart: Ubiquitous access, monitoring, care, and sensor data.
 - For every one of those the proposal is to allow the patient to decide what information can be accessed by the care givers other than in the case of consultation where the patient might not be qualified (informed enough) to make a decision by themselves. In such as case only “useful” data is transferred to a temporary repository that the care giver can read.
- Are the suggested measures adequate?
 - These measures seem to take it for granted that the technological solution will work as planned and that there is no abuse of the system. In that sense the measures are not adequate because they concentrate on what is required in a perfect world.
- What else would be needed?
 - A full-scale security policy that looks at the system as a part of larger security framework.
- Would you allow your health to be monitored in the way the article suggests?
 - If I knew beyond a shadow of a doubt that it could be trusted to work the way I want it to work and it helped me live a healthier life without additional complications, then yes.
- Would the Geneva approach scale up to this kind of ubiquitous care and monitoring system in terms of all required security and privacy measures?
 - Possibly. It's hard to say without knowing exactly what would be required of such a system and how the system being used in HUG works like.

7 Weekly report 7

7.1 About the lecture

I've heard Mikko Savela's lecture before in Tietokannat II where he was the guest lecturer back in 2006 and I can remember it being a good one with lots of insightful things about databases and information security. Based on that I was looking forward to the lecture on this course.

To put it short, this lecture was not a disappointment. Mikko began with some basic definitions for safety and security and then went on to a more psychological direction with Maslow's hierarchy of needs. After that he proceeded by talking about risk and asked the question of “what is a risk?” from the audience to which he did not get a reply. After that he made the audience participate by asking how many people thought of a particular situation to be a risk. The crux of the whole thing was that all of the 6 different cases were just parts of a risk and risk itself comprises of 5 different things: factor, event, outcome, effect, and probability.

The best parts about Mikko's lecture was, as in 2006, the real life stories of what has happened. The stories make the teaching more concrete in a way and I think that's definite plus. For example, who should be held responsible (or should anyone?) in a university if a person walks in from the street to the library and smacks another one in the face? Is that something the security officer should supervise?

7.2 About the article / research paper

I have to say that the text in this paper was extremely hard for me to understand. The writer is clearly not a fluent English speaker as he is using sentences like this: “In the SSM changing the focus of security to the individual paradoxically allows an appointment with the broadest global threats described by Krause and Williams” (on pg. 181). That to me sounds very cryptic and takes considerable effort to decipher the meaning of it. I bet that particular sentence is a direct translation

from Finnish to English without taking into account how things are said in English. Here's how I would make it more understandable: "If the focus of security is changed individual-centric in the SSM it results paradoxically in the broadest global threats...". I ended the sentence with three dots because it's still missing some information that the original sentence does not provide.

The paper is filled to the brim with individual sentences that seem to have nothing to do with the surrounding text. The paper also overuses complicated terms, which does not help with readability and understandability one bit.

7.3 *Discuss the survey results in general*

- As a security manager, what sort of tools would you get for your daily work and longer term planning from the results of the survey?
 - I wouldn't use a theoretical tool like strategic security model (SSM) because of all the criticism towards it, although using balanced scorecards would be a neat idea in a security model.
 - Deep leadership model (DLM) also seems to get a share of its criticism. It's described as a very rigid and reactive type of model, so I would not use that one either.
 - Strategic security leadership (SSL) sounds as the only choice that does not come with its baggage of problems. There's not much information about it but it looks to be the right choice. That would mean that the security of an organization would be managed in a very top down way where the organization's strategy, policies, principles, and operations would be supported in that manner.

7.4 *Discuss the phenomenons described from section 8.2.2. onwards*

- Have you encountered any of these phenomenons in your study or work activities?
 - I've personally encountered the optimistic paradox when trying explain in a working place why WPA is the correct choice for a security measure in WLAN routers. The person in charge of the administration just brushed the issue off by saying that WEP is secure enough to use because no one will want to hack in the system in that particular case.

- I'm also sure that I've encountered conservative restoration, silent killers and the human firewall phenomenon but I can't think of an example on the top of my head.
- How relevant are these phenomenons in terms of security management?
 - I think these are the heart of the matter because these sound intuitively to be very common problems. The more common the problem the more relevant the security risk. I can easily imagine some financially inclined people trying to cut costs by using something that is cheap and works ok instead of something that actually works well.
- Is one more important than the others to take into account?
 - Probably conservative restoration phenomenon because that sounds like being the closest one to the feeling of security. What I mean by that is when people say that because something has worked ok thus far it should work ok afterwards as well. That's a false sense of security and very easy to relate and fall victim to.

8 Compensatory work

8.1 How poor management causes IT failure

An organization/company has a number of managers who have the task of giving direction to the organization itself. Without any direction/leadership the organization will drift aimlessly in the possibility space until sooner or later it crashes into something undefinable. With proper direction/leadership the organization's efforts can be harnessed in the best possible way to move towards a common pre-meditated goal.

With those simple premises out of the way its easy to take a swing at the topic in question. IT is not in any special situation when compared to any other field. Granted it is a complex field that is part of industrial infrastructure and provides multiple advantages but it also comes with its disadvantages. These days when IT does not function properly in a company work draws into a halt and huge losses are made. The same will of course happen when there's no electricity or possibly heat/air-conditioning, so IT is really not that special.

What is special though is the attitude people in managerial positions have towards IT. For some reason IT is sometimes regarded as a simple thing that either works or doesn't work, either functions properly or doesn't. It's also regarded as just part of the infrastructure that needs to be more or less just installed. This type of an attitude will of course lead to problems when new IT systems are built or old ones are put into use. Avison et al call it managerial IT unconsciousness when managers lack awareness in the area of IT, which is likely to cause problems later on.

It should be of no surprise when managers who are not really qualified to run software projects are given the leadership role in them that there might be some complications. In the "Managerial IT unconsciousness" article three different business cases are described where this sort of activity resulted in huge losses for each business. Although the companies themselves were different, eg. one in private sector and two in public, there were some common themes that could be identified.

In short the software that was being built was designed to be unnecessarily complex (a clear sign of asking for too much, too soon), the companies lacked in IT governance, and there was an

inexperienced and uninfluential IT staff involved. From the manager's point of view the most distressing issue is the one involving the IT governance, the authority patterns for IT infrastructure, IT use, and project management. What that means is that the senior management in each case did not have adequate monitoring in place, they did not have proper financial, auditing, or contract management, and project planning and control were also sub par.

As a not so surprising result a suggestion can be made that in dealing with large and complex software projects, experienced IT and IS staff is also needed along with proper governance and project management. The articles suggests that governance was merely neglected under the premise that "IT doesn't matter". That seems to tie in with the conservative restoration phenomenon mentioned by Kalevi Mäkinen in his Strategic Security research paper. Also some silent killers are quite probable when one thinks about this one particular quote from Royal Melbourne Institute of Technology's personnel: "The project reports that came through to me and then went on to the council showed that the project was on time, on budget, and meeting its milestones. We all thought that this project was actually going OK". If that's not a flat out lie, that is.

Personally I don't think the whole issue has however only to do with poor management causing IT failures. IT is complex by its very nature and its also quite a new field with inadequate occupation ethics where work can sometimes be done in an improper way just to get the software released earlier. Agile methodologies have been in the rise in companies because they seem to deliver more business value for the companies in the long run although initially they might cost more. With all of these nuances the IT staff and managers need to have people on the payroll that understand the field in broad strokes as well as any IT professional.

Conclusion

I found this course's topic and material interesting and the group meetings enjoyable. I like this type of working where the whole course's final thing is not as all encompassing as a full-blown exam where you really have to prepare carefully and with a lot of time spent on reading, usually in a short period of time. In my opinion this allows for a more leisurely bit by bit learning because there's no need to cram the information in your head in one go at the end. Scholar's of old where such leisurely people and the actual classical meaning for the word scholar is a leisurely gentleman, so I guess that's quite fitting as well.

There's really just one thing I disliked about this course and that's the last paper we were assigned to read, titled "Strategic Security" by Kalevi Mäkinen. As I noted in the weekly report 7 in this journal I disliked the writing quite a bit. The text was tedious to read and to understand and it's not just me because each and everyone in our group voiced similar concerns during week 7 meeting.

If I'd have to sum up all that I've learned during the course in one sentence I'd say: "IS is a complicated and crucial system for businesses these days and as such it requires operators that understand its intricacies in detail without needing to resort to trial and error to find out what's best and what's not."

Some other key points for me are:

- IS is a complex subject that not only deals with IT but with pretty much all the other security issues as well in an organization eg. personnel security. These issues impact each other and therefore the understanding of one requires the understanding of another.
- Frameworks exist that specify best practices for companies that allow other companies to trust each others' IT in a way that minimizes the IS risks. I see this very beneficial for start up companies that don't have the security experience to start with but need to have a basic reference that can be used when the time comes to grow in that respect.

Attachment

MEETING MINUTES

Workshop assignment 1

Place: ICT library

Date and time: 23.01.09 12 - 13

Chairperson: Vesa Nieminen

Chairperson next time: Saul

List of group members present: Lasse, Rauli, Lauri, Saul, Juha, Vesa, Santtu

List of group members not present:

Chairperson opened the meeting at 12:15.

This is the first groupwork meeting. First, get to know each other a bit and then proceed to the discussion items.

- Discuss the spam situation of the world.
 - 95% of spam is the current situation in the world
 - Utu spam filters work quite good. You get the subject line pmx that denotes the likelihood of a particular message being spam
 - It takes a lot of resources to filter spam at the receiving end
 - Captcha is quite difficult to implement for email because it requires a change to the email protocol and then it cannot be used in limited devices
 - False positives are a real problem because they can cause the most damage
 - A good example of this: The email message that Seppo sent about the course titled 'Some practical issues', went to the spam folder for Juha
 - How could that have been solved? Put some poems at the end of the mail :)
 - The situation is alarming. Spam runs businesses. “Koira ruokkii kättä” situation. How do we know that anti-spam companies don't secretly promote spam?
 - Advertizing as an immoral act
- Group members probably looked at the statistics on different days.

- Compare the differences in the data gathered by group members. What similarities and differences are there?
 - They're quite similar: the number of spam issues vary but the order of the lists look the same.
 - Spamcop did not have country based lists, mainly just IP address lists, Spamhaus is more user friendly to get general lists and statistics.
- How accurate do you think the data is?
 - It's probably not totally precise but at least gives a ball-park estimate
- How is the data gathered?
 - Users input data and the system finds out the
- If someone visited the spamadvertised sites, what type of content did the sites have?
 - We did not bother/want to visit the sites
- Discuss the topics of the articles. Group members have probably read different articles. Discuss both topics, especially the following:

○ Article 1: Spam generation is analyzed as a system.

What benefits are there in such an analysis method?

- Categorizing different spam methods thus making the differences clearer

What seem to be the most effective anti-spam techniques?

- Our ideas:
 - Making spamming more expensive for the sender
 - Limit the number of mails to something like 10 per day if you're approved as a trusted
 - Graylisting
 - Additional: Otherinbox.com

What kind of spam seems to be the most difficult to avoid?

- The more diverse the spam the harder it is to detect (eg. Combinations of image spam and text spam)

○ Article 2: Discuss the different image spam techniques.

- Randomizing the image (adding noise)
- Anti-spam:
 - Database of images (the database is taught what is spam and what is not)
 - Vectors are used for comparing similarities between different images
 - Color histogram filter

- Vote (if more than 50% of voters say that it's spam, then it is)

Which one would you use to send effective spam?

- shift, linecolor, fontcolor, fonttype
- crop & dots
 - There's limited data on these so they might not be totally accurate
- alternating images and text

Which technique seems to be the easiest to detect and avoid?

- crop
- shift, dots, url

Can you come up with a new technique for image spamming in addition to those discussed in the article?

- Using google image search to get some randomly selected image and then insert text into that
- Encrypting the spam in such a way that it takes a lot of processing power (steganography?) and then decoding it client side with some malware

Chairperson closed the meeting at 13:27.

Date and time for the next meeting: 29.01.09 12:00