Mittuniversitetet
MID SWEDEN UNIVERSITY

Den fullständiga studiehandledningen för DT012G Informationssäkerhet och riskanalys

Daniel Bosk, Lennart Franked och Carina Bengtsson*

studyguide.tex 696 2013-02-25 08:50:01Z danbos

Innehåll

1 Mål

Kursen behandlar informationssäkerhet utifrån användar-, teknik- och organisationsperspektiv. Du får praktisk erfarenhet och en grundläggande begreppsbild inom området. Kursen ger dig kunskap om olika risker samt åtgärder och arbetssätt för att förebygga dessa. Även juridiska aspekter tas upp.

Mer specifikt ska du efter genomgången kurs uppfylla följande mål:

- Att du ska ha erfarenhet av hur utformandet av lösenord påverkar enkelheten att knäcka dem.
- Att du ska kunna redogöra för olika tillvägagångssätt för att komma åt lösenordsskyddade resurser utan att ha tillgång till själva lösenordet.
- Att du ska få en uppfattning om *advanced persistent threats* (APT) och vad detta kan innebära.

Kapitel 1	Kapitel 8
Kapitel 2	Kapitel 13
Kapitel 3	Kapitel 14
Kapitel 4	Kapitel 15
Kapitel 7	

Tabell 1: Läsanvisningar för [1].

- Att du tillsammans med andra ska diskutera och reflektera över olika aspekter av säkert användande av lösenord.
- Att du ska ta del av forskning kring hur olika lösenordspolicyer påverkar användares val av lösenord och vilken typ av policy som ger säkra lösenord som är enkla att komma ihåg och ändå motstå attacker.
- Att du ska kunna analysera hot mot informationssäkerheten och ge förslag på skydd mot dessa hot.
- Att du ska kunna tillämpa MSB:s metodstöd för att analysera, utvärdera och ge förslag på förbättringar för informationssäkerheten i en organisation.

2 Litteratur

I detta avsnitt presenteras det material ni för att kunna genomföra denna kurs. Det första ni behöver är Anderssons bok *Security Engineering* [1; 2], denna bok [1] finns tillgänglig gratis om man inte vill köpa den senaste utgåvan [2]. Kursen är anpassad för att den äldre upplagan ska kunna användas, men den senaste upplagan rekommenderas då den är 7 år nyare och har väsentligen mer innehåll.

Förutom den ovan nämnda boken kommer vi att använda oss utav information och dokument som går att hitta på Myndigheten för samhällsskydd och beredskaps (MSB:s) webbplats informationssäkerhet.se[1]. Huvuddelen av kursen kommer att fokusera på detta material [8; 15; 13; 19; 14; 4; 5; 20; 17; 16; 12; 10; 7; 21; 6; 11; 18; 9; 3].

MSB har även webbplatsen CERT-SE [26] som har en del intressant referensmaterial och säkerhetsnyheter.

3 Läsanvisningar

Du bör börja med att läsa [1; 2] för att ha möjliga attackvektorer i åtanke när du läser om processer och modeller i MSB:s material.

De delar som ska läsas i [1], alternativt [2], ska läsas översiktligt. Vi kommer inte att begära några detaljkunskaper utan ni behöver vara bekanta med innehållet för övriga delar av kursen. För vilka delar av [1] som ska läsas se tabell 1. För vilka delar av [2] som ska läsas se tabell 1.

[1] Se `http://www.informationssakerhet.se`.

Kapitel 1	Kapitel 9
Kapitel 2	Kapitel 15
Kapitel 3	Kapitel 16
Kapitel 4	Kapitel 17
Kapitel 8	

Tabell 2: Läsanvisningar för [2].

3.1 Laboration 0: Lösenordsknäckning och *advanced persistent threats*

Innan du genomför denna laboration ska du ha läst kapitel 2 *Usability and Psychology* i Anderson [2][2] i sin helhet. Följande avsnitt ska läsas noggrant:

- 2.2 *Attacks Based on Psychology*,
- 2.4 *Passwords*, och
- 2.5 *System Issues*.

Övriga avsnitt kan läsas översiktligt. Du bör också ha läst kompendiet av Bosk [22] i sin helhet.

Du ska även läsa artikeln av Fisher [23] som behandlar hur attacken mot RSA genomfördes i början av 2011 samt artikeln av Juels och Yen [24] som diskuterar *advanced persistent threats*.

3.2 Seminarium 0: Lösenordspolicyer

För att delta på seminariet krävs att du läst artikeln av Kommanduri m.fl. [25] där författarna undersökt olika lösenordspolicyer och hur användarna skapat lösenord utifrån dessa.

3.3 Föreläsning om metodstödet del 1

Inför denna föreläsning ska du ha läst igenom dokumenten *Introduktion till metodstödet* [8], *Säkra ledningens engagemang* [15], *Projektplanering* [13], *Verksamhetsanalys* [19] och *Riskanalys* [14].

3.4 Promemoria 0: Ledningssystem för informationssäkerhet (LIS)

Du ska inför skrivningen av detta PM ha läst dokumenten

- *Introduktion till metodstödet* [8],
- *Säkra ledningens engagemang* [15], och
- *Projektplanering* [13].

[2]Detta kapitel från den andra utgåvan finns att hämta gratis från bokens hemsida, `http://www.cl.cam.ac.uk/~rja14/book.html`.

3.5 Föreläsning om metodstödet del 2

Inför denna föreläsning ska du ha läst igenom övriga dokument i MSB:s metodstöd [4; 20; 17; 16; 12; 10; 7; 21; 6; 11; 18; 9; 3].

3.6 Promemoria 1 och seminarium 1: Verksamhets- och riskanalys

Du ska inför denna promemoria ha läst dokumenten

- *Verksamhetsanalys* [19], och
- *Riskanalys* [14]

i MSB:s metodstöd.

4 Förslag på schema

För att underlätta läsningen av kursen ges i detta avsnitt ett förslag på schema. Det är naturligtvis valfritt att följa detta schema sånär som på deadlines för kursens uppgifter. Detta schema är anpassat med dessa deadlines i åtanke. Du finner det i tabell 3 på nästa sida.

Referenser

[1] Anderson, Ross J. *Security engineering : a guide to building dependable distributed systems*. Wiley, New York, 2001. ISBN 0-471-38922-6. URL `http://www.cl.cam.ac.uk/~rja14/book.html`.

[2] Anderson, Ross J. *Security engineering : a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2 utgåvan, 2008. ISBN 978-0-470-06852-6 (hbk.).

[3] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Fortsatt arbete. URL `http://www.informationssakerhet.se`. dec 2011.

[4] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Gapanalys, dec 2011. URL `http://www.informationssakerhet.se`.

[5] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Gapanalys – checklistan, dec 2011. URL `http://www.informationssakerhet.se`.

[6] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Granska, dec 2011. URL `http://www.informationssakerhet.se`.

Kursvecka	**Arbete**
1	Kapitel 1 och 2 i [2].
2	Påbörja laboration L0. [25].
3	Seminarium S0. [8; 15; 13].
4	[19].
5	[14].
6	[4]. Promemoria PM0.
7	[20; 17; 16]. [12; 10; 7]. [21; 6].
8	[11; 18]. [9; 3].
9	Kapitel 3 och 4 i [2].
10	Kapitel 8 och 9 i [2].
11	Kapitel 15 i [2].
12	Kapitel 16 i [2].
13	Kapitel 17 i [2].
15	Promemoria PM1 och seminarium S1.
16	Projekt.
17	Projekt.
18	Projekt.
19	Projekt.
20	Projektinlämning.

Tabell 3: Ett schemaförslag anpassat efter kursens deadlines och en studietakt på kvartsfart.

[7] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Införa, dec 2011. URL `http://www.informationssakerhet.se`.

[8] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Introduktion till metodstödet, dec 2011. URL `http://www.informationssakerhet.se`.

[9] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Kommunicera förbättringar. URL `http://www.informationssakerhet.se`. dec 2011.

[10] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Konstruera och anskaffa, dec 2011. URL `http://www.informationssakerhet.se`.

[11] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Ledningens genomgång, dec 2011. URL `http://www.informationssakerhet.se`.

[12] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Planera genomförande, dec 2011. URL `http://www.informationssakerhet.se`.

[13] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Projektplanering, dec 2011. URL `http://www.informationssakerhet.se`.

[14] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Riskanalys, dec 2011. URL `http://www.informationssakerhet.se`.

[15] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Säkra ledningens engagemang, dec 2011. URL `http://www.informationssakerhet.se`.

[16] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Utforma policy och styrdokument, dec 2011. URL `http://www.informationssakerhet.se`.

[17] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Utforma säkerhetsprocesser, dec 2011. URL `http://www.informationssakerhet.se`.

[18] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Utveckla LIS och skyddet. URL `http://www.informationssakerhet.se`. dec 2011.

[19] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Verksamhetsanalys, dec 2011. URL `http://www.informationssakerhet.se`.

[20] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Välja säkerhetsåtgärder, dec 2011. URL `http://www.informationssakerhet.se`.

[21] Andersson, Helena, Andersson, Jan-Olof, Björck, Fredrik, Eriksson, Martin, Eriksson, Rebecca, Lundberg, Robert, Patrickson, Michael, och Starkerud, Kristina. Övervaka, dec 2011. URL `http://www.informationssakerhet.se`.

[22] Bosk, Daniel. Grundläggande lösenordsanalys. URL `http://ver.miun.se/courses/infosak/compendii/pwdanalysis.pdf`. 2013.

[23] Fisher, Dennis. RSA: SecurID attack was phishing via an Excel spreadsheet. URL `https://threatpost.com/en_us/blogs/rsa-securid-attack-was-phishing-excel-spreadsheet-040111`. Publicerad den 1 april 2011.

[24] Juels, Ari och Yen, Ting-Fang. Sherlock Holmes and The Case of the Advanced Persistent Threat. I: *LEET*, 2012. URL `https://www.rsa.com/rsalabs/staff/bios/ajuels/publications/SherlockHolmes.pdf`.

[25] Kommanduri, Saranga, Shay, Richard, Kelley, Patrick Gage, Mazurek, Michelle L., Bauer, Lujo, Nicolas, Christin, Cranor, Lorrie Faith, och Egelman, Serge. Of passwords and people: Measuring the effect of password-composition policies. I: *CHI*, 2011. URL `http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf`.

[26] Myndigheten för samhällsskydd och beredskap. CERT-SE. URL `https://www.cert.se`.