IN2120 Informasjonssikkerhet
Høst 2023

Del 13: Informasjon for eksamen

Audun Jøsang
Universitetet i Oslo

Del 1: Generelle begreper for informasjonssikkerhet

- Forstå hva informasjonssikkerhet er
  - Definisjon av informasjonssikkerhet (ISO/IEC 27000) som beskyttelse av KIT
  - Forstå hvordan ulike typer angrep kan skade KIT
- Betydning av, og forskjell mellom sikkerhetskonsepter
  - Forskjell mellom enkel data-autentisering med MAC (Message Authentication Code) og ubenektelig (non-repudiation) data-autentisering med digital signatur
  - Forskjell mellom tilgangsautorisering og tilgangskontroll
- Betydning av og sammenheng mellom viktige begreper:
  - trussel(scenario) som består av trinn, trusselaktør som utfører angrep,
  - angrep (at en trussel blir utført)
  - hendelse, når et angrep fører til brudd på KIT
  - sårbarhet, svakhet som gjør at (trinn i) trusselscenario kan gjennomføres
  - verdi/ressurs, som kan skades gjennom angrep
  - konsekvens, kostnader som følge av hendelse
  - risiko (trussel + sårbarhet + verdi) og risikonivå (sannsynlighet x konsekvens)

Del 2: Systemsikkerhet

- Forstå grunnleggende elementer og prinsipper for et system
- Prosess for fjerning av sårbarheter i programvare (CVE, CVSS)
- Sikkerhet i mikroprosessorer og OS
  - OS privilegienivåer
  - kompromittering av minne med buffer overflow,
  - beskyttelse av minne med ASLR, No-Execute
- Virtualisering
  - Hypervisor, gjeste-OS, verts-OS
  - Type 1 og type 2 virtualiseringsarkitektur
  - Kontainerarkitektur
- Forstå prinsippet for sikker oppstart med UEFI og at TPM kan støtte visse sikkerhetsfunksjoner

Del 3: Kryptografi

- Hash-funksjoner
  - Prinsipper (men ikke bry dere om forskjell mellom sterk og svak kollisjonsresistens) Kjenne de mest kjente hash-funksjonene, og om de regnes som sikre
- Symmetriske krypteringer
  - Parametere (blokk- og nøkkelstørrelse) for AES-chiffer
  - Krypteringsmoduser for block-chiffer: ECB, CTR (Tellermodus) og CBC
- MAC (Message Authentication Code)
- Asymmetriske algoritmer
  - Vite hvilke nøkler (offentlig/privat og Alice/Bob) som brukes i asymmetrisk kryptering og DigSig
  - Forstå hybrid kryptering og hvorfor det ikke gir fremoverhemmelighold
- Diffie-Hellmann (DH) nøkkelutveksling
  - Forstå hvorfor den utvekslede øktnøkkelen er anonym, dvs. uten autentisering
  - Forstå hvordan DH kombinert med DigSig gir øktnøkler som gir fremoverhemmelighold
- Kvantecomputere truer tradisjonell asymmetrisk krypto, men nye algoritmer fins

Del 4: Nøkkelhåndtering og PKI

- Nøkkeldistribusjon, forstå:
  - Utfordering med nøkkeldistribusjon med og uten PKI
  - Krav til beskyttelse (konfidensialitet eller autentisitet/integritet) av ulike typer nøkler (hemmelig, privat/offentlig) for nøkkeldistribusjon
- Sertifikater (for offentlige nøkler) og PKI. Forstå:
  - Prinsipp for sertifikater, innhold i sertifikater, gyldighet, anvendelse
  - Hvordan sertifikater er lenket sammen fra rot til subjekt/server-sertifikat.
  - En PKI-tillitsmodell er den logiske strukturen av hvilken CA-er som signerer et sertifikat
  - Sertifikater gir kun tillit til identitet, og ikke til f.eks. lovlydighet/seriøsitet/kvalitet av nettsteder eller programvare

Del 5: Angrepsvektorer og skadevare

- Kjenne prinsipper for vanlige angrepsvektorer
  - Phishing (ulike varianter), drive-by-angrep, falske nettsider, direkte nettverksangrep med injeksjon, leveransekjedeangrep, skadelige eksterne enheter, offeret blir lurt til (uvitende) å installere skadevare
- Kjenne prinsipper for vanlige former for skadevare
  - virus, trojaner, dataorm, exploit, rootkit, makrovirus, skadelig javaskript, bakdør, bott-program, spionprogram, løsepengevirus, keylogger

Del 6: Pentesting

- Forskjell mellom hacking og etisk hacking (pentesting)
  - Kjenne strafferammen for datainnbrudd med hacking
  - Krav til å kunne gjennomføre (lovlig) pentesting / etisk hacking
- Forskjellige typer pentesting
  - svartboks, hvitboks, gråboks
- Trinn i pentesting
- Teknikker
  - OSINT, phishing, kartlegging, prøve tilganger og tjenester,
  - prøv Sudo, få root-tilgang, passordcracking, booting
  - sjekk om programmer har kjente sårbarheter

Del 7: Brukerautentisering

- Typer autentikatorer
  - 1) noe du vet, 2) noe du er, 3) noe du har + sekundære kanaler
- Passordsikkerhet (noe du vet)
  - hashing, salting
- Enheter(noe du har)
  - OTP-brikker, online-enheter, adgangs- og ID-kort, sekundærkanaler
  - Phishingresistent autentisering med passnøkler (teorioppgave 8)
- Biometriske systemer (noe du er)
  - Feilrater og kvalitetsvurdering
- Rammeverk for autentisering i e-forvaltning
  - Autentiseringsnivåer
  - Kjenne hvilke autentiseringsnivåer som støttes av norske eID-ordninger

Del 8: Identitets- og tilgangshåndtering

- Betydning av entitet / identitet / attributt / digital identitet
- ID-modeller
  - Silomodell / føderert modell
- Sentraliserte / distribuerte føderasjonsmodeller
  - 4 ulike kategorier
  - Vite hvilken kategori ulike kjente ID-føderingser tilhører
- Kjenne prinsippet for OpenID Connect
- Tilgangskontroll
  - Prinsipper/modeller for MAC, DAC, RBAC og ABAC
  - Kjenne prinsipp og scenario for OAuth

Del 9: Kommunikasjonssikkerhet

- Strukturen av internet-stakken
  - Vite på hvilket lag de ulike protokoller hører hjemme.
- TLS (Transport Layer Security)
  - Hvordan TLS 1.3 støtter fremoverhemmelighold.
- IPSec (Internet Protocol Security)
  - Hvordan IPSec benyttes for VPN på IP-laget.
- Sky-VPN
  - TOR
- Applikasjonssikkerhet og OWASP Top 10
  - Trenger ikke kjenne hver risiko i OWASP Top 10, bare at det er en nyttig veileder

Del 10: Nettverkssikkerhet og cyberops

- Brannmur
  - Prinsipper for forskjellige brannmurer
  - Plassering av brannmurer
  - Plassering av tjenester: DMZ eller produksjonsnettverk
- IDS (Intrusion Detection System)
  - Signaturbasert (spesifikke deteksjonsregler) og anomalibasert (maskinlæring)
- SOC og cyberoperasjoner
  - Cyber-Kill-Chain
  - APT
  - MITRE ATT&CK

Del 11: IS-ledelse og Sikkerhetskultur

- Vite hva ISO/IEC 27K-serien handler om
  - 27000, 27001, 27002 og 27005
  - Tittel (omtrent) og formål med hver standard
- NSMs grunnprinsipper for IKT-sikkerhet
  - Hva det er, og hva det kan brukes til
- NIST Cyber Security Framework
  - Hva det er, og hva det kan brukes til
- Elementer i ISMS (Information Security Management System)
  - Ledelsessystem for informasjonssikkereht
- Sikkerhetskultur
  - Elementer som utgjør god/dårlig sikkerhetskultur
  - Hvordan forbedre sikkerhetskultur

Del 12: Risikostyring

- Risikostyringsprosess fra ISO/IEC 27005
  - Kjenne overordnet struktur for risikostyring
  - Kjenne hovedtrinnene i risikovurdering
- Trusselmodellering:
  - Hensikt: avdekke relevante trusselscenarier
- Kvalitativ risikoanalyse
- Håndtering av risikoer
- Prinsipp for ROI (Return on Investment) for sikkerhetstiltak

Eksamen i Silurveien

- 27. november 2023, kl.09:00-13:00.
- Praktisk info rundt digital eksamen i Silurveien 2:

https://www.uio.no/studier/eksamen/inspera/index.html

- Digital eksamen består av en rekke oppgavetyper, f.eks.
  - Velg riktig utsagn / flervalgs svar
  - Flytte ikoner på figur
  - Skriv tekst som svar
  - Fyll ut ord / tall som svar
- Oppgaver fra alle forelesningstemaer, der oppgavene fokuserer på innhold i presentasjoner, oblig-oppgaver og teorioppgaver.
  - Men mange lab-oppgaver og teorioppgaver egner seg ikke som eksamensspørsmål.
- 4 timer arbeidstid
- Lykke til !

Første side på eksamenen

Informasjon om eksamenen

UiO : **Institutt for informatikk**
Det matematisk-naturvitenskapelige fakultet

Avsluttende eksamen i IN2120 Informasjonssikkerhet (Høst 2023).

Dato og tidspunkt: **27. november 2023, kl.9:00 - 13:00 (4 timer).**

Ingen hjelpemidler er tillatt.

Merk følgende:

- Oppgavene i denne eksamenen er gruppert i syv deler. Den første delen dekker grunnleggende aspekter ved informasjonssikkerhet på tvers av pensum, mens de øvrige seks delene er fra utvalgte områder av pensum.
- Det er mulig å oppnå 40 poeng i den første delen av oppgavesettet, og ti poeng for hver av de neste seks delene - totalt 100 poeng (= 100%).
- Man kan navigere frem og tilbake mellom oppgavene.
- Skåring for hver oppgave angis eksplisitt. Det kan gis negative poeng for feil svar/valg, men total poengsum for hele oppgaven er minimum 0 (selv om summen over alle svarene er negativ).
- Vær kortfattet når du skriver tekst som svar på en tekstoppgave. Svaret kan skrives på norsk eller engelsk.
- Les oppgaveteksten nøye og spesielt der du skal fylle inn verdier i en tekstboks.
- I navigasjonslinjen nederst på skjermen indikeres fullførte oppgaver med blå søyler.

Tips! Siden du kan gå frem og tilbake kan det være lurt og først svare på oppgavene du syns er lette, og deretter gå tilbake til vanskelige oppgaver hvis du har tid.

Lykke til, hilsen Audun, Gudmund og Nils!