IN5100: Breaking Europay/MasterCard/VISA Card Payment Systems and Other Systems using Tamarin

Peter Ölveczky

October 30, 2023

Pensum

Pensum er (utvalgte deler av) de to artiklene

> David A. Basin, Ralf Sasse, and Jorge Toro-Pozo: *The EMV Standard: Break, Fix, Verify.* In Proc. 42nd IEEE Symposium on Security and Privacy (SP 2021). IEEE, 2021. `https://doi.org/10.1109/SP40001.2021.00037`

og

> David A. Basin, Cas Cremers, Jannik Dreier, and Ralf Sasse: *Tamarin: Verification of Large-Scale, Real-World, Cryptographic Protocols.* In volume 20(3) of IEEE Security & Privacy, 2022. Tilgjengelig via `https://doi.org/10.1109/MSEC.2022.3154689`.

1 Detaljer

I artikkelen *Tamarin: Verification of Large-Scale, Real-World, Cryptographic Protocols* er følgende deler *ikke* pensum:

- (Side 2) "Foundations" fra "A formal treatment of Tamarin's foundations" til og med "..., and convergent user-specified theories with the finite variant property."
- (Side 7) "Scaling to Families of Protocols" fra "We present a final example ..." til "..., ranking Noise protocols by their relative security."

Alt annet i artikkelen er pensum. Man kan *særlig* fokusere på (å besvare) følgende spørsmål:

- Hvilken formalisme brukes til å definere protokoller og "adverseries"?
- Hva slags informasjon inkluderer "tilstandene" i systemet/modellen?
- Hvilke tre store applikasjoner diskuteres i (noe) detalj i artikkelen?
- For hver slik applikasjon:

- Hva slags hoved-problem(er)/feil/mangler fant Tamarin (muligens i tidligere versjoner av systemet, som så ble fikset etter at Tamarin fant problemene)?
- Hvorfor er applikasjonen så kompleks?
- "Lessons learnt"?

Når det gjelder *The EMV Standard: Break, Fix, Verify*, så er denne full av teknikaliteter, som CDA, SDA, osv. Man trenger ikke kunne/forstå slike teknikaliteter. Bare hva som "praktisk" skjer, osv. For eksempel er III.A–D (detaljer) meget kursorisk pensum. Vedlegget ("Appendix") er ikke pensum. Heller ikke tabeller og lignende. Fokuser på praktiske sikkerhetshull, hvordan de ble demonstrert, osv.

Noen spørsmål man bør tenke på/kunne svare godt på er:

- (I) Hva er EMV?
- Hvorfor er det fristende for banker å bruke EMV?
- Hvilken er de store sikkerhetshullene, og hva er deres praktiske konsekvenser? (Samme spørsmål?)
- Hvilke er de tre viktigste ("most relevant") egenskaper en EMV-transaksjon må tilfredstille?
- Hva var hovedfeilene de fant?
- Hva ble "testet ut"/"demonstrert" på riktig?
- Nevn noen "eyhical considerations" forfatterne omtaler i hva de har gjort og ikke gjort.
- (II) Hva slags sikkerhetshull fant Murdoch et al? Hvorfor fant ikke De Ruiter og Poll disse problemene?
- Kan du nevne noen andre kjente sikkerhetsmangler (*før* dette paperet)?
- (III) Hvor "stor" og kompleks er beskrivelsen av EMV?
- Hvilke 4 "faser" består en EMV-transkasjon av?
- (IV) Hvordan ser en "typisk" regel ut i Tamarin?
- Hvordan formaliseres de tre (fire?) viktige egenskapene til en EMV-transaksjon? Prøv å forstå formlene!
- Hva modelleres i Tamarin (IV.C)?
- Hvorfor kan ikke Tamarin gi ut *alle mulige* oppførsler/angrep som bryter mot ønskede sikkerhetskrav?
- (V) Hva slags resultater ga Tamarin-analysen?
- Hva er hoved-resultatene av Tamarin-analysene av EMV Contactless Protocol? Bør man bruke MasterCard eller VISA?

- (VI) Hva slags praktisk "eksperimentering"/"demonstrasjon" av sikkerhetsmanglene gjorde forfatterne? (Setup, etc.)
- Hva er hovedforskjellen på Basin et al's "demonstrasjon" av sikkerhetshullene og den tilsvarende "demonstrasjonen"/"implementasjonen" av et angrep til Galloway og Yunusov i [28]?
- Hva er i praksis "free lunch"-angrepet på side 1777? Demonstrerer Basin et al dette i praksis? Hvorfor tror ikke forfatterne at kriminelle vil gjøre det til sitt levebrød å utnytte denne sikkerhetsmangelen?
- Hvordan kan feilen fikses av VISA? (Intuitivt; forlanger ikke tekniske detaljer.)