Being a doctor…
what’s next (for me)?

Alexandre Debant

COURI seminar
Rennes, France

July 12th 2021
Who am I?

1 oct. 2017
Start PhD

1 oct. 2020
End PhD

17 nov. 2020
PhD. defense

PhD. Thesis
Title: Symbolic verification of distance-bounding protocols - application to contactless payment protocols

Supervision: Stéphanie Delaune
Who am I?

Post-doc

Title: Designing and proving the security of electronic-voting protocols

Supervision: Véronique Cortier

Location: Inria Nancy - Grand Est
Outline

What was the main steps of my first year of post-doc?
Outline

What was the main steps of my first year of post-doc?

From an administrative point-of-view

- Looking for a post-doc
- Qualification
- Applications to CR/MCF positions
- ...

1 oct. 2017
Start PhD

1 oct. 2020
End PhD

17 nov. 2020
PhD. defense

1 dec. 2020
Start post-doc

Today
Outline

What was the main steps of my first year of post-doc?

From an administrative point-of-view
- Looking for a post-doc
- Qualification
- Applications to CR/MCF positions
- …

From a scientific point-of-view
- Studying a new topic
- Having more freedom
- A new organisation
- …
My post-doc from an administrative point-of-view
Look for a « good » post-doc

When: when you start writing the manuscript

What: what do I want to do after the phd?
Look for a « good » post-doc

When: when you start writing the manuscript
What: what do I want to do after the phd?  Academia
When: when you start writing the manuscript

What: what do I want to do after the phd?  Academia

A « good » post-doc?
• Find a location you want to visit (better if abroad)
• Find a topic you want to investigate
• Find a « good » supervisor:
  ➡ with whom you can work (e.g. not a ghost)
  ➡ who is not too busy
  ➡ who publishes
When: when you start writing the manuscript

What: what do I want to do after the phd? Academia

A « good » post-doc?
- Find a location you want to visit (better if abroad)
- Find a topic you want to investigate
- Find a « good » supervisor:
  ➤ with whom you can work (e.g. not a ghost)
  ➤ who is not too busy
  ➤ who publishes

Your phd advisor is probably able to give you names!
Apply for the « qualification »

When: November/December (reg.: November 9th, app. form: December 15th)

What: gather all the supporting documents
  ▶ a detailed CV
  ▶ administrative documents about the phd defense (reviews, PV…)
  ▶ a summary of past/current research
  ▶ a summary of the teachings

https://cnu27.univ-lille.fr/qualification-note.html
Apply for a CR/MCF position

1 oct. 2017
Start PhD

1 oct. 2020
End PhD

17 nov. 2020
PhD. defense

1 dec. 2020
Start post-do

Today

When: January-March (eligibility) and April/May (admission interview)

Main steps:

‣ Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
‣ Contact the teams as soon as possible
Apply for a CR/MCF position

When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - which problem(s) I’d like to solve in the next years?
  - why this problem(s) is interesting? Why now? Why me?
Apply for a CR/MCF position

1 oct. 2017
Start PhD

1 oct. 2020
End PhD

17 nov. 2020
PhD defense

1 dec. 2020
Start post-do

Today

When: January-March (eligibility) and April/May (admission interview)

Main steps:

▪ Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
▪ Contact the teams as soon as possible
▪ Develop a research project
  ➢ which problem(s) I’d like to solve in the next years?
  ➢ why this problem(s) is interesting? Why now? Why me?
▪ Develop a teaching project
  ➢ how I’d like to teach (project, MOOC, flipped classroom…)?
  ➢ how can I meet the department expectations?
Apply for a CR/MCF position

When: January-March (eligibility) and April/May (admission interview)

Main steps:
- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - which problem(s) I’d like to solve in the next years?
  - why this problem(s) is interesting? Why now? Why me?
- Develop a teaching project
  - how I’d like to teach (project, MOOC, flipped classroom…)?
  - how can I meet the department expectations?
- Do a presentation
  - a short presentation (15min) but a lot of things to mention!
  - no documentation to explain the expectations…
Apply for a CR/MCF position

When: January-March (eligibility) and April/May (admission interview)

Main steps:

- Identify the open positions: Galaxie and mailing lists (gdr-secu, gdr-im…)
- Contact the teams as soon as possible
- Develop a research project
  - which problem(s) I’d like to solve in the next years?
  - why this problem(s) is interesting? Why now? Why me?
- Develop a teaching project
  - how I’d like to teach (project, MOOC, flipped classroom…)?
  - how can I meet the department expectations?
- Do a presentation
  - a short presentation (15min) but a lot of things to mention!
  - no documentation to explain the expectations…
My post-doc from a scientific point-of-view
A trendy application of security protocols
A trendy application of security protocols but with a complex development
E-voting protocols

Voters

Bulletin board

Server
E-voting protocols
E-voting protocols
E-voting protocols

Bulletin board

Server

tally

Voters

12
What are the expected security guarantees?

➡ Vote privacy
  ➡ no-one should know Alice/Bob votes for
E-voting protocols

What are the expected security guarantees?

➡ Vote privacy
  ▶ no-one should know Alice/Bob votes for

➡ Individual verifiability
  ▶ Alice/Bob can convince themselves that his/her votes are correctly published on the bulletin board
E-voting protocols

What are the expected security guarantees?

➡ Vote privacy
  ▶ no-one should know Alice/Bob votes for

➡ Individual verifiability
  ▶ Alice/Bob can convince themselves that his/her votes are correctly published on the bulletin board

➡ Universal verifiability
  ▶ everyone can check that the result of the election corresponds to the content of the public bulletin-board
E-voting protocols

What are the expected security guarantees?

➡ Vote privacy
  ‣ no-one should know Alice/Bob votes for

➡ Individual verifiability
  ‣ Alice/Bob can convince themselves that his/her votes are correctly published on the bulletin board

➡ Universal verifiability
  ‣ everyone can check that the result of the election corresponds to the content of the public bulletin-board

➡ Accountability
  ‣ if a participant misbehaves then it can be detected and prosecuted
  ‣ however, he can also defend himself and prove his honesty in case of false-accusation
Current work

Belenios protocol

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability
**Belenios protocol**

- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

**Election 1 (important election)**

**Election key** = $p_{k_{el}}$

- $\epsilon = (c_b, \sigma_b, \pi_b)$
- $\epsilon = (c_a, \sigma_a, \pi_a)$

- $c_a \mid c_b$
Current work

**Belenios protocol**
- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An **unreported privacy breach** when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

---

**Election 1 (important election)**
- Election key = \( p_{k_{el}} \)

**Election 2 (small/test election)**
- Election key = \( p_{k_{el}} \)
Current work

Belenios protocol
- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

Election 1 (important election)

Election key \( p_{k_{el}} \)

Election 2 (small/test election)

Election key \( p_{k_{el}} p'_{k_{el}} \)

After v1.13 with an honest server
Current work

Belenios protocol
- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

Themis project
- Industrial project between Idemia and Loria
- Results/contributions:
  - Design a voting machine protocol (with industrial constraints)
  - Symbolic proofs of vote secrecy, verifiability, and accountability
Belenios protocol
- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An unreported privacy breach when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

Themis project
- Industrial project between Idemia and Loria
- Results/contributions:
  - Design a voting machine protocol (with industrial constraints)
  - Symbolic proofs of vote secrecy, verifiability, and accountability

Swiss Post’s e-voting solution
- Industrial protocol developed by Scytl and now Swiss Post (expected to be deployed in 2022)
- Results/contributions:
  - Adapt the symbolic proofs to the new version of the specification
Current work

**Belenios protocol**
- Developed at Loria, +1200 élections en 2020
- Results/contributions:
  - An [unreported privacy breach](#) when considering multiple elections
  - Protocol improvements to weaken the trust assumptions for verifiability

**Themis project**
- Industrial project between Idemia and Loria
- Results/contributions:
  - Design a voting machine protocol (with industrial constraints)
  - Symbolic proofs of vote secrecy, verifiability, and accountability

**Swiss Post’s e-voting solution**
- Industrial protocol developed by Scytl and now Swiss Post (expected to be deployed in 2022)
- Results/contributions:
  - Adapt the symbolic proofs to the new version of the specification
  - We discovered a (critical?) vote privacy flaw…
Conclusion

From an administrative point-of-view

- Do not hesitate to contact the teams
- Do not hesitate to discuss with researchers you trust to get advices
- Do not underestimate the work/time that an application requires!
Conclusion

From an administrative point-of-view

‣ Do not hesitate to contact the teams
‣ Do not hesitate to discuss with researchers you trust to get advices
‣ Do not underestimate the work/time that an application requires!

From a scientific point-of-view

‣ Designing a secure e-voting protocol is complex
‣ Considering multiple elections is necessary!
➡ Much work is still needed to obtain a (reasonably) secure e-voting protocol…
Conclusion

From an administrative point-of-view

‣ Do not hesitate to contact the teams
‣ Do not hesitate to discuss with researchers you trust to get advices
‣ Do not underestimate the work/time that an application requires!

From a scientific point-of-view

‣ Designing a secure e-voting protocol is complex
‣ Considering multiple elections is necessary!
➡ Much work is still needed to obtain a (reasonably) secure e-voting protocol…

Thank you!