Caught between Security and Time Pressure?
An Empirical Investigation of Operator's Perspective on Security Misconfigurations
Outline

1. Security Misconfigurations
2. Empirical Approach
3. Preliminary Findings
4. Conclusion
Security Misconfigurations

- Simple errors in deploying an internet service that lead to security issues:
  - Publication of secrets/passwords
  - Missing/disabled authentication
  - ...
Examples

- Running your MongoDB on the Internet
Examples

- Running your MongoDB on the Internet
- Having your TR-069 publicly reachable
Examples

- Running your MongoDB on the Internet
- Having your TR-069 publicly reachable
- Storing your AES key next to your encrypted backups
Who, what, why?

- Who misconfigures?
- What gets misconfigured (easily)?
- Why does it get misconfigured?
Who, what, why?

- Who misconfigures?
- What gets misconfigured (easily)?
- Why does it get misconfigured?

How to prevent misconfigurations?
Asking Operators

- Research on Security & Usability mainly focusses on end-users
- Asking people is hard
- Asking the right questions is even harder
  Think: “Please buy a bottle of milk; if they have eggs, bring a dozen.”
The Usual Approach

1. Explore the issue
2. Do small focus groups with target audience
3. Do structured interviews with target audience
4. Build a questionnaire to get quantitative insights
The Sysadmin Approach

- Go to the local sysadmin regulars’ table and talk to them
The Sysadmin Approach

- Go to the local sysadmin regulars’ table and talk to them
- Install an IRC client
The Sysadmin Approach

- Go to the local sysadmin regulars’ table and talk to them
- Install an IRC client
- 5 Interviews and 1 focus group with 5 participants...
  - Did you ever encounter security misconfigurations?
  - What do you think: Why do they occur?
  - Did a security misconfiguration incident change anything about this?
What happened?

- Beloved Defaults
What happened?

- Beloved Defaults
- Misleading Conventions
What happened?

- Beloved Defaults
- Misleading Conventions
- Troublesome Accidents
What happened?

- Beloved Defaults
- Misleading Conventions
- Troublesome Accidents
- The Lost, Forgotten and Abandoned
Why did it happen?

- Lack of Experience
Why did it happen?

- Lack of **Experience**
- Non-existing / unspecified / too strict / too loose / too complicated **Processes**
Why did it happen?

- Lack of **Experience**
- Non-existing / unspecified / too strict / too loose / too complicated **Processes**
- Betrayed **Faith in Suppliers**
Why did it happen?

- Lack of **Experience**
- Non-existing / unspecified / too strict / too loose / too complicated **Processes**
- Betrayed **Faith in Suppliers**
- Backfiring **Legacy Support**
Why did it happen?

- Lack of Experience
- Non-existing / unspecified / too strict / too loose / too complicated Processes
- Betrayed Faith in Suppliers
- Backfiring Legacy Support
- Unwise Budgeting
How to prevent this?

- Provide for **Experience**
- Voice to management in case of deficient **Processes**
- Challenge **Faith in Suppliers** (Make them listen to you, OPS!)
- Ditch **Legacy Support**
- **Budget** wisely
Conclusion

- Misconfigurations happen.
- Knowing *how* allows for detecting measures to prevent security incidents.
- We’re not ready…

Questionnaire coming soon to an operations mailing list near you!
Conclusion

- Misconfigurations happen.
- Knowing *how* allows for detecting measures to prevent security incidents.
- We’re not ready…

**Questionnaire coming soon to an operations mailing list near you!**
Conclusion

- Misconfigurations happen.
- Knowing *how* allows for detecting measures to prevent security incidents.
- We’re not ready…

Questionnaire coming soon to an operations mailing list near you!