Practical and Comparable Security for RFID

Dr Gerhard Hancke

gerhard.hancke@rhul.ac.uk

Smart Card Centre

Information Security Group

Royal Holloway
University of London

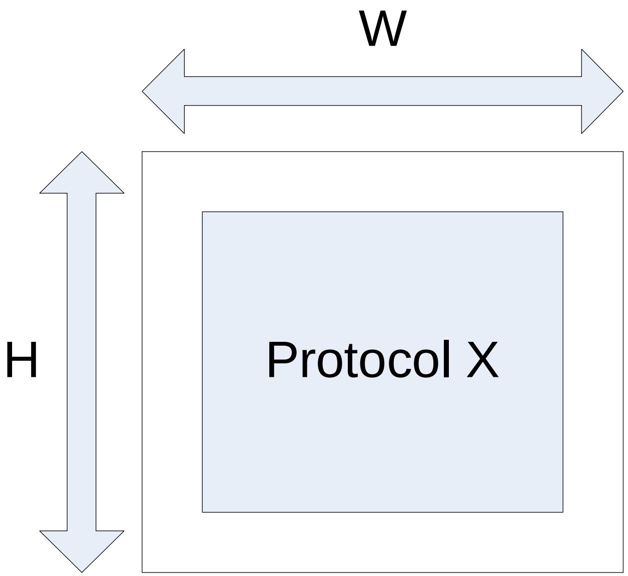
To start off….

- There is a large and ever growing body of work with regards to RFID security protocols
  - Diverse methodology and perception of key issues involved

- Why is ‘practical’ important?
  - Ideally research should solve real world problems
  - An idea does not solve the problem if its not implemented
  - If it is not practical it will not be implemented

- Why is ‘comparable’ important?
  - A measure of the current ‘state of the art’
  - Places new work in perspective
  - Provable advancement of the field

What is ‘practical’?



- We can implement this protocol within a given set of constraints (considered realistic with current technology)
- Identify and define/quantify constraints
  - Demonstrate that implementation is possible

What is ‘comparable’?

≤

- Under the same conditions mine is better than yours
- Use a number of metrics to generate a measure of the protocol’s performance
  - Compare the performance of the new protocol to the performance of previous protocols

Confusion

- Problems…
  - Many application scenarios and functional requirements
  - Not all RFID technology is created equal
  - Different design goals
- What metrics should be used for comparison?
- What constraints are considered to be practical?

Who is in charge?

- Who decides what is practical or how to compare?
  - Industry? Possibly some influence…
  - Standards? Not really…
  - Paper authors on an ad-hoc basis? Frequently…☺

- Is it possible to come up with an authoritative framework for evaluating RFID security protocols?
  - There are already frameworks for subsets of the RFID field
  - A general framework would require a group of knowledgeable people with diverse expertise in:

    protocols, primitives, models, hardware, systems, etc.

Difficulties

- Not possible to cover all technology, applications, etc.
  - Will probably need to focus on selected aspects

- The framework would need to be dynamic
  - Related aspects might change
  - Periodic updates and revisions needed
  - Backwards compatible?

- Might just get ignored
  - No one actively uses it → does not serve purpose
  - Depends on how ‘authoritative’ the framework is, i.e. who is involved, etc.
  - Still serve as a technical guideline/white paper

Potentials benefits

- Easier to judge quality and contribution of research
  - Comparison to the state of the art
  - More clarity on the ‘this is practical’ argument
- Better classification of related research results
  - Easy to identify related work
  - This could assist knowledge transfer to commercial world
  - Consistent vocabulary for technical concepts
- Possibility of shaping future research trends
  - Steer research in direction of certain applications
  - Provide a target to aim at – weak areas will attract more work
- Quality assurance?
  - Clear method, trusted tests → ‘Good’ results?

Framework Contents (1)

- Classification for comparison
  - Operating environment/functional requirements
  - Infrastructure
  - Token technology
  - Security primitives
  - Security services
  - ???

- Metrics for comparison
  - Attacks/threats addressed (attack success probability for each)
  - Resources required (memory, logic, power)
  - Communication (exchanges, bits transmitted)
  - Protocol execution time
  - ???

Framework Contents (2)

- Practical values for evaluating metrics
  - Used for calculating the metrics of comparison
  - Based on current technology, selected research results
  - Primitive processing time, resources to implement
  - Memory available for required nonces, message buffers, etc
  - Communication bit rate, setup time
  - Power for communication and processing
  - ???

- Practical constraints
  - Set upper limits on capability of the systems based on design choices during classification
  - Based on current technology

How can a framework be applied in practice?

- Simply formalise aspects and standardise terminology
  - Provide a list of system elements to consider
  - Define/explain each element
  - Let the user combine elements in any way
  - Is this an improvement?
- Dependent selections
  - Each element has some attached conditions
  - Set design rules based on choices already made
  - Initial choices limits influence later elements
  - This could get complicated – needs a clear process….
- Provide 'profiles'
  - Fixed environment, different achievable goals
  - The user has no choice but to stay within this profile
  - Limited number of profiles inhabit progress?

Conclusion/Comments

- Such a framework is only an idea….
  - Would require some co-ordinated effort to be comprehensive
  - Build on existing work or start from the beginning?
- Would require a group of people with diverse expertise
  - Lots of input/ideas….
  - Strong review/feedback process
  - Authority results from the number/quality of participants
- Various needs….
  - Formalised definitions of all system aspects/elements
  - Metric and performance models
  - Accurate practical values to calculate performance
  - Practical limits/constraints
  - Design rules or ‘profiles’

Thank you!

Any questions?

Gerhard Hancke

gerhard.hancke@rhul.ac.uk