Building Networked Systems Security (BNSS)

MSc: 2520, PhD: 3250

Project

Instructor: Panos Papadimitratos (*papadim@kth.se*)
Networked Systems Security Group
www.ee.kth.se/nss

February 6, 2015

1 Project Description

1.1 Overview

You are part of a network security experts team, specializing in design and implementation of secure networked systems. You come across the interest of ACME Scandinavia, based in Stockholm. ACME wishes to securely extend their headquarters IT environment to their new branch office in London and enhance their employees access to the company IT resources. This sounds like an excellent opportunity for your team. What you are after is to propose and implement a viable and highly secure solution that meets ACME's requirements. You must understand the needs of the company, propose a suitable design, implement and test your solution, and eventually make a convincing presentation to ACME.

It can be highly beneficial to start considering - as early as possible in your design phase - potential implementation approaches, start familiarizing yourselves with the networking environment and 'playing' with alternative tools (that you deem likely to use).

The project structure, which unfolds in three phases, is outlined next. The ACME call for proposals is in Sec. 2. All documents and progress shall be communicated via KTH Social groups. All deadlines refer to midnight GMT+1. All page counts for the report(s) assume: font size: 10; single-spaced text; single-column layout, reasonable narrow margins.

1.2 Project Structure

Phase 1: Solution Design: You start by studying ACME's needs, discussing within the team possible solutions, and do the necessary research and reading. Once you have your solution laid out, you put it in a tech report. Then, you pass it to another team and you get another tech report to review. The teaching team will also comment on all designs. Your reviewed approach should be accompanied by a concise explanation why and how your proposal is expected to work. More specifically:

- **Requirement Analysis and System Design**: You are expected to write a technical report (max. 3 pages) that contains: *(Deadline: February 18, 2015)*:
  - Analysis of the ACME needs and precision of the related security requirements for your solution.
  - Outline of your design, in order to address the specified security requirements.
- **Peer-Review** : Receive report(s) from other team(s) and provide feedback (max. 0.75 page per received report). Please identify strong points and comment on what you find possibly as weakness, justifying technically your assessment. Please point out suggestions for improvement in your review. *(Deadline: February 20, 2014)*:

- **Finalization of Analysis and System Design**: Revise your report submitted on Feb. 18, according to the feedback. The total size of your report should not exceed 4 pages. *(Deadline: February 24, 2014)*:
  - Reconsider your design based on the feedback you received.
  - Briefly explain in an appendix how you did this.
  - Finalize your design.
  - Update your technical report accordingly.

Phase 2: Implementation of your solution Devote your efforts fully to the implementation of your finalized solution. This phase should conclude by *(deadline: March 15, 2014).*

More specifically, during this phase you will:

- Finalize/fine-tune your decisions on tools you will use.
- Implement and verify your solution.
- Provide detailed documentation of the whole implementation phase.
- During the process, continuously reflect on how the functionality and the security of your solution can be demonstrated; consider specific use cases.

Phase 3: Reporting, Presentation, Demonstration: Once finished with your implementation, you update and extend your "Analysis and Design" report into a final report and make an appointment to show it to ACME by *(Deadline: March 22, 2014).* The demonstration appointment with ACME can happen already during week 11, but at the latest during week 12 - notably Mon.-Wed. March 23-25, 2015. Demonstrations at an early stage are encouraged (if this does not affect the quality of your solution and presentation).

- Extend your report to a maximum of 5 pages (but use wisely appendices for additional material that fits there).
- Be ready to run use cases specified by the teaching teams.
- Prepare a short presentation, to pitch your solution (max. 10 slides).

Important note: In order to pass the course you will have to successfully complete all three phases.

2 ACME Scandinavia, Call for Secure IT environment

ACME Secure Network Implementation

ACME Scandinavia provides consulting services since 1990. Its headquarters are in Stockholm and a new brunch has been now operating in the greater London area. ACME is looking forward to building a new secure network infrastructure in order to seamlessly connect its London branch to Stockholm. We are looking for cutting edge technology and highly secure solutions proposed by security experts within the following weeks. All proposals should be ready and undergo demonstration by March 25, 2015 the very latest.

Analysis:

The current ACME network infrastructure cannot accommodate the London expansion seamlessly. In fact, we are keen on creating a new secure network from scratch. We ask you to setup a secure web-server in our headquarters in Stockholm. ACME regularly sends experienced employees from Stockholm to its London offices. Each employee carries a company laptop computer when visiting London. ACME's laptops are equipped with Wi-Fi cards.

Visiting employees usually work extra hours, while the rest usually follow an 8 hours schedule and rarely work more. Laptops are necessary for the visiting employees in London because there are no extra desktop computers available in London. Using their laptops, they should access the Stockholm network.

Our employees also have mobile devices provided by ACME. We require that employees connect to the corporate network with their devices and, in addition, exchange files with each other in a secure manner.

We also require that employees use their phones for a two-factor authentication to access the data from the secure web-server when not using their cryptographic credentials; e.g., when accessing the server from a machine other than their corporate laptop.

The security solution you are asked to implement should be scalable and compatible with a currently experimental credential management system ("*x-PKI*") currently deployed by ACME. Note that while you are developing your solution, if offered the project, this can be brought to you as an additional requirement: to enable users obtain credentials from this x-PKI; this might be motivated by privacy protection concerns.

Security Requirements ACME has the following security requirements for the new network:

- **Employee Authentication:** We want to be able to authenticate our users/employees. Each employee should have a digital identity verified by digital certificates issued by our own infrastructure. They should also have a device that can be used in the two factor authentication as a proof of possession.

- **Secure connectivity:** Secure connectivity is a major concern. Visiting employees in London should be able to connect to our web servers in Stockholm. Only ACME's employees should be able to access our infrastructure. Only computers with addresses from the Stockholm headquarters or the London branch should be able to connect to our internal network. Computers outside these two network should be denied access. Logging of network traffic and requests to our web server is vital.

- **Confidentiality:** Information exchanged between the branch and the headquarters should be hidden from third parties. The main web server containing critical corporate data should be accessed only by trusted users, i.e., employees at London's branch and Stockholm's headquarters but also employees from their homes with their personal laptops. All communications between the server and a user should be encrypted and authenticated.

- **Secure Wireless Access:** Visiting employees in London should be able to connect to Stockholm using their laptop computers and a Wi-Fi connection. Authorization and authentication should be done via the wireless network.

- **Secure File Exchange:** The *confidentiality*, the *integrity* and the *authenticity* of the file exchange process (between the employees' mobile phones) should be guaranteed. Furthermore we require that only ACME employees should be able to exchange files.

- **Other Security:** Since we understand that there is always a possibility that attackers try infiltrating to our corporate network(s), it is critical for us to be alerted whenever an attack is launched against our infrastructure.

Infrastructure for Demo:

Due to strict budget constraints you are to implement your demo solution by utilizing the following infrastructure:

- 4 Virtual Machines
- 1(2) Wireless Router(s)
- 1(2) Smart phone(s)

Points for discussion: Beyond the demo constraints, ACME expects a convincing presentation of your assessment of the security requirements, how your solution meets them, and how your system interfaces with our company policies. We are open to all proposals, even those exceeding our base requirements; technical elements, especially if costs and overheads increase, should be justified.