VT23, EP2520/FEP3250
Building Networked Systems Security (BNSS)
Project

Panos Papadimitratos

Networked Systems Security Group
www.eecs.kth.se/nss

January 20, 2023

Contents

1 Project Description

1.1 Overview

You are part of a network security experts team, specialising in design and implementation of secure networked systems. You come across 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 company needs, propose a suitable design, implement and test your solution, and make a convincing presentation & demo to ACME.

1.2 Practicalities

The project structure, which unfolds in three phases, is outlined next. The ACME call for proposals is in Sec. 2.

All documents and progress (submissions and feedback) will be handled via KTH Canvas, BNSS, Assignments.

All deadlines refer to midnight, End of Day (EoD), Stockholm time (GMT+1).

All page counts for the deliverables assume: page size A4; font size 10; single-spaced text; single-column layout, reasonably narrow margins (1 inch); space-efficient inclusion of group members' information.

Hint: It can be highly beneficial to start considering - as early as possible in your design phase - potential implementation approaches, start familiarising yourselves with the networking environment and tools you are likely to use.

1.3 Project Structure

1.3.1 Solution Design (Phase 1) (*Deadline: Feb. 15, 2023*)

Please start by studying ACME's needs, discussing within the team possible solutions, and do the necessary research and reading. Then, please submit a preliminary write-up and receive feedback. Please continue your work, submit a technical report, peer-review another report, receive feedback, finalise your design and submit your revised report. More specifically:

- **Initial requirement analysis** (*Deadline: Feb. 3, 2023*) (*max. 1 page*)

  Please discuss your understanding of the project scope and objectives, along with your preliminary action plan.

- **Requirement analysis & design** (*Deadline: Feb. 13, 2023*) (*max. 3 pages*)

  Please write a technical report that contains:

  - Your analysis of the ACME needs and precision of the related security requirements for your solution.

    - Your system design, addressing all security requirements; including a figure of the networked system topology. Please specify software/tools to be deployed (at each (virtual) machine or other device).

- **Peer review** (*Deadline: Feb. 15, 2023*) (*max. 0.75 page*)

  Please read the report of another team and provide feedback, with concise technical justification for each point made. Please identify strong points and please comment on apparent weaknesses.

- **Finalized analysis & design** (*Deadline: Feb. 17, 2023*) (*max. 4 pages*)

  Based on all feedback, please revise and expand your report.

    - Please reconsider your design. Please explain briefly in an appendix how you took feedback into account.
    - Please update your technical report, conveying technical strengths and relevance of your proposed system design.

1.3.2 Implementation (Phase 2) (*Deadline: Mar. 12, 2023*)

Please devote all your efforts to the implementation of your finalised design and the preparation of a final report with all implementation information. More specifically:

- Please fine-tune your decisions on tools; implement and verify your solution.
- Please reflect how the functionality and the security of your solution can be demonstrated; consider specific use cases.
- Please provide a finalised **report** with all implementation information (*max. 5 pages*). Please update and extend your Phase 1 final report.
- Please use appendices for technical details, adding *max. 3 pages* to your above-mentioned 5-page report. Please pay attention to readability.
- Please provide a ReadMe file for a non-expert user of your system; *max. 2 pages*.
- Please submit a single `.pdf` **Phase 2 document** (report, appendices and ReadMe) (*max. 10 pages in total*).

1.3.3 Presentation & Demo (Phase 3) (*Deadline: Mar. 17, 2023*)

At this final phase, please make an appointment with ACME during week 11, notably *March 15-17, 2023*, to present your work. The audience will be the ACME (aka teaching) team and an opposing team.

You will have the opportunity to oppose a team too. The schedule and the opposing teams will be announced *March 13, 2023, noon*.

- **Final presentation and demonstration**
    - Please prepare a slide-show presentation, to pitch your solution (*max. 10 slides*).
    - Please be ready to run a few use cases that reveal the scope and merits of your design.
    - Please be prepared to perform reasonable customisations on the spot or show-case and explain details.

    - Please make sure that each team member has a good command of the solution and the demonstrated system and that she or he is ready to answer questions. You can of course have experts on different parts. Please be prepared to answer all questions about your system, justify your design and implementation decisions, and reason on related hypotheses.

- **Opposition**

  Each final presentation & demo slot includes two teams, taking turns as presenting and opposing team. The opposing team has access to the presenting team's final report and can prepare friendly but technically incisive questions.

- **Final remarks** (*max. 0.75*)

  After the final presentation, each team puts together some final brief remarks.

  a. As presenting team: reflecting on the main points raised by the ACME and the opposing teams; if needed, adding thoughts on how to address any residual issues.

  b. As opposing team: reflecting on the presented project and your final technical assessment (also briefly commenting on how effective the demonstration was).

- **Final submission** (*Deadline: Mar. 17, 2023*)

  Please submit your final presentation slide-show, your final remarks, and an updated Phase 2 document if needed (in case there were any updates or fixes after the Phase 2 deadline).

Important note: In order to pass the course, you will have to successfully complete all three phases. It is imperative to follow correctly all instructions for all assignments, e.g., group formation, uploads.

2 ACME Scandinavia “Call for secure IT environment proposals”

2.1 ACME Secure Network

ACME Scandinavia provides consulting services since 1990. Its headquarters are in Stockholm and a new branch 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 this spring. All proposals must be ready and undergo review of a working, documented system, demonstrated by *March 17, 2023*.

2.1.1 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. ACME regularly sends experienced employees from Stockholm to its London office. Each employee carries a company laptop computer when visiting London. ACME’s laptops are equipped with Wi-Fi cards. A secure web server is needed in our headquarters in Stockholm.

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 (share) files with each other in a secure manner.

We also require that employees use their phones for 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.

Moreover, after the covid-19 pandemic, but also in the context of our global expansion, we want our employees able to securely work from home or while they travel. They would need access to our networked resources remotely, using their work laptops, with the exception of some highly sensitive operations that could be performed only in Stockholm or London.

Our employees have typical working hours when working at their base, be it in Stockholm or London. When working from home, it is likely to ’spread’ their hours. When visiting our branch, it is often the case to extend their working hours. While traveling, their work patterns can vary significantly.

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 a requirement: to enable users to obtain credentials from this x-PKI. Options and details will be communicated by the ACME team during Phase 2. One interesting feature is to have both ‘traditional’ credentials (certificates) or anonymized ones with a short(er) life-time (usually termed “pseudonyms”).

2.1.2 Security Requirements

ACME has the following security requirements for the new network:

- **Employee Authentication:** We want to be able to authenticate our employees. Each one should have a digital identity verified by digital certificates issued by our own infrastructure. Each employee should also have a device that can be used for 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 server in Stockholm. Only ACME 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. Remote access should be handled very carefully. Logging of network traffic and requests to our web server is vital. Employee-to-employee communication should also be secured.
- **Confidentiality and anonymity:** 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. Less critical web servers should be accessible by employees in other circumstances, e.g., from their homes with their personal laptops. All communications between any server and a user should be encrypted and authenticated. While travelling, our employees may need to hide from curious observers that they connect to our network or that they securely exchange files with each other.
- **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:** We understand that there is always a possibility that attackers try to infiltrate our corporate network(s); it is critical for us to be alerted whenever an attack is launched against our infrastructure. We are also particularly concerned with *clogging* Denial of Service (DoS) attacks against our infrastructure. Having read about Domain Name System (DNS), we also want to be sure our domains cannot be exploited or our employees mislead when browsing the Internet. Last but not least, we need to be able to handle swiftly cases with employee equipment stolen or employee credentials compromised.

2.2 Infrastructure for Demo

Please implement your demo solution with the following infrastructure:

- Servers (Virtual Machines on your own laptops): One can install VMs using Oracle VM VirtualBox: `https://www.virtualbox.org/manual/ch01.html`. You will also have the option to request and get a couple of VMs in our infrastructure.
- 2 Wireless Router(s) provided (can be flashed, e.g., to OpenWrt), used to connect laptops and smartphones to Stockholm or London network.
- 2 smartphones: we provide Android smartphones but you can use your own phones too.
- 2 Ethernet switches and a dozen Ethernet cables.
- 4 USB-to-Ethernet connectors.

If you need additional equipment, please contact ACME as soon as possible and motivate your proposal.

2.3 Expectations

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.