Prüfungsprotokoll EDV2

WiSe 2016/17
mündliche Prüfung
TU Berlin

Prüfer: Lars Örgel
Beisitzerin: mir unbekannt

Allgemeines

Lars hatte in der Prüfung einen Zettel vor sich liegen, auf dem ca. 40 Fragen notiert waren. Diese sind nach Themen sortiert und dienen ihm wahrscheinlich als Leitfaden. Er fängt zu einem Thema immer leicht an und schaut dann, wie weit er "in die Tiefe" kommt. Er fragte keine Shell-Befehle ab, außer zum Binden/Linken von dynamischen und statischen Bibliotheken (aber das war eher die Ausnahme. Am Ende der Prüfung meinte er, dass er ja keine Shell-Befehle abfrage...).
Die Prüfung würde, so Lars, wenn man gut durchkomme, 45mins dauern. Bei mir hat sie knapp eine Stunde gedauert, weil er mit einigen meiner Antworten unzufrieden war und deshalb selbst erklärt hat. Er fragt schon mehr ab als 1:1 in den Skripten steht. Das wäre ja langweilig, so Lars.

Rechneraufbau

Das vier-Schichten-Modell des Rechneraufbaus anzeichnen, wie er es immer an der Tafel hatte. Kernel-Funktionen erklären. Was machen Bibliotheken (Bibs) etc.? Insgesamt recht wenige Fragen dazu, ca. 5min.

Bibliotheken

Welche Bibs gibt es, was sind ihre Aufgaben? Vor- und Nachteile von dynamischen vs. statische Bibs. etc. Dann: Er habe im Netz in einem Forum die Frage gelesen, ob eine statische in eine dynamische Bib. umgewandelt werden könne (ohne den Quelltext zu besitzen, also nur auf Basis der Bereits übersetzten Bibliothek *statlib.a*). Ich sollte auf die Forum-Frage antworten: Nein, weil statische Bibs absolute und dynamische Bibs relative Adressen benutzen. Hierzu unbedingt die Bibliotheken-Hausaufgabe (HA03) ansehen (alle anderen Hausaufgaben natürlich auch! Er fragt ähnlich und sagt z.B., aber das kam doch in der HA X dran etc.). Statische Bibs werden mit `gcc -ar` und dynamische Bibs mit `gcc -fPIC` erzeugt. Die Flagge `-fPIC` steht für *position independent code*. Wenn man also nur den bereits kompilierten Code der statischen Bibliothek hat, kann man die Adressbezüge nicht mehr ändern und es gibt (laut Lars) auch kein Programm, das dies könnte.
Er fragte außerdem, wie statisch gebundene Bibs *statlib.a* aussehen. In ihnen sind z.B. 10 *object-files* enthalten...

Internet

Vier-Schichten-Modell vom TCP/IP-Schichtenmodell zeichnen. Dann fragte er viel zu Ethernet und dessen Sicherheit. Z.B.: Angenommen, eine Person würde sich mit ihrem Laptop und einem LAN-Kabel mit eine Buchse verbinden, also innerhalb des CFD-Netzwerks eine Verbindung herstellen - könnte diese Person allen Traffic mitschneiden? Antwort: Je nach dem, ob ein HUB oder ein SWITCH verwendet wird. Ein HUB (veraltet) leitet allen Traffic an alle weiter. Während also zwei von 50 Rechnern miteinander kommunizieren, müssen alle anderen 48 die Klappe halten. Daher kann bei Verwenundg eines HUBs jeder zuhören. Und Ethernet ist nicht verschlüsselt (standardmäßig ist im Internet NICHTS verschlüsselt! Diesen Satz will er immer und immer wieder hören). Ein SWITCH hingegen kann den Traffic gezielt vom Absender an den Empfänger (und nur an den Empfänger) leiten, daher kann C nicht die Kommunikation zwischen A und B mitschneiden. Was machen die anderen drei Schichten des TCP/IP-Schichtenmodells? Er fragte, wann TCP und wann UDP verwendet wird. Außerdem, wie und von wem entschieden wird, wann TCP und wann UDP verwendet wird. Das sind natürlich die darüber liegenden Protokolle wie SMTP, HTTP, POP3/IMTP, FTP etc. Fast alle verwenden TCP (auch das File Transfer Protocol!), weil man doch eine hohe Sicherheit möchte. UDP ist eher für Anwendungen innerhalb eines Netzes zuständig, also z.B. um meine Daten bei Anmeldung am Poolrechner auf diesen zu laden.

Verschlüsselung

Drei Grundziele der Kryptografie nennen: Vertraulichkeit (sym. Verschlüsselung), Authentizität (asym. Verschlüsselung) und Integrität (Hash-Funktionen) und welche Verschlüsselungsverfahren diese Ziele umsetzen. Viel Wert legte er immer auf die Schwachstelle der Internetsicherheit. Er lies mich z.B. durchüberlegen, wo de Schwachstelle bei den Zertifikaten zur asym. Verschlüsselung liegen. Wenn eine Person das Zertifikat von Amazon klaue und es gleichzeitig schafft, in mein DNS einzudringen um meinen Traffic zu ihm umzulenken: Kann sie mir dann erfolgreich vorgaukeln, dass sie Amazon sei? Auch unter der Prämisse, das das Zertifikat gültig ist und dass der Browser denkt, er kommuniziere mit der richtigen Person (ausreichende Infos hierzu stehen ja im Zertifikat drin)? Nein, denn er hat ja nicht den privaten Schlüssel von Amazon, sondern nur den öffentlichen. Es bringt ihm also nichts, unsere Kommunikation mitzuschneiden.
Wenn einer andern Person plötzlich 2000€ von der Kreditkarte fehlen, wie kann das zustande gekommen sein? Ihr wurde nicht die Kreditkarte geklaut und sie hat ganz brav immer nur absolut sichere Internetverbindungen benutzt, um mit ihrer Kreditkarte Einkäufe online zu bezahlen. Vermutlich hat also der Empfänger der Zahlungsdaten, also ein Online-Shop, der ja diese Daten im Klartext braucht um die Zahlung zu tätigen, meine Daten irgendwie (*vermutlich* unfreiwillig) weitergegeben (bei ihm wurde erfolgreich eingebrochen/er wurde gehackt). Hier wieder: Das Internet ist prinzipiell *nicht* sicher. “Wer damit nicht leben kann, darf es nicht benutzen”, so Lars.