Vertiefungsprüfung Prof. Freiling: VVS1, VVS2, Forensik, Common Failures in Internet Applications, Linux und Verschlüsselung (Buch)

25. August 2005

1 Allgemeines

Vertiefungsprüfung bei Prof. Freiling, Beisitzer war Max Dornseif. Die Prüfungsatmosphäre war sehr locker und angenehm. Bewertet wurde die Prüfung mit 1.0.

2 Ablauf

Ich durfte mir die Reihenfolge, wie auch den Startpunkt der ersten Vorlesung wählen. Ich habe VVS2 in Verbindung mit CHT zum Starten gewählt.

2.1 VVS2

- CHT, was ist das, wofür, wie genau. Ausführlich erklärt.
- Überleitung zu TRB, schwächster Fehlerdetektor (perfekter Fehlerdetektor).
- Algorithmus mit Consensus erläutert.
- Wie kann man zeigen, dass der perfekte auch der schwächste Fehlerdetektor ist? Hier konnte ich nur allgemeine, aber nicht genauer erläutern, wie man aus TRB einen perfekten Failure Detektor bekommen kann. Dies habe ich so auch gesagt und wurde im Nachhinein auch als sehr gut anerkannt.
- Byzantine Protokolle, was ist hier anders. Allgemein erläutert.
- Vorraussetzung? $n > 3t$

Die byzantinischen Protokolle wurden als Überleitung zu VVS1 genutzt.

2.2 VVS1

- Klassifizierung von Angreifern. Teilweise aus der Vorlesung, teilweise mit eigenen Sachen erläutert.
- Maximale Kosten zum Schutz? Mit maximalem Schaden begründet.

Als nächstes kam Linux und Verschlüsselung, auch wenn es sich nicht ganz abgrenzen lässt.

2.3 Linux und Verschlüsselung

- Abgrenzung von SSH und SSL. Kam auf die Layer an, und habe ich auch so erläutert. Ausserdem noch relativ viel, was SSH ist, und wie man es nutzt. Genaue Protokollspezifikationen waren bis auf die Authentifizierung des Servers nicht gefragt.
- Was macht man, wenn ein Dateisystem verschlüsselt ist? Bruteforce, Keylogger. Falls es gemoutet ist? Nicht rebooten *g*

2.4 Common Failures in internet applications

Ab hier hat Max übernommen:

- Cross-Site-Scripting in Verbindung mit HTTP/1.1? HTTP-Header-Response Splitting.

Das war dann schon alles hierzu.

2.5 Forensik

- Fallbeispiel: Markenrechtsverletzung im Internet. Wichtig war dokumentieren, und zwar Beweisbar. Indizien sammeln...
- Festplattenforensik in Bezug auf Daten. Gelöschte Daten sind nicht gelöscht, Daten können an verschiedenen Stellen stehen, die eigentlich dafür gar nicht gedacht sind, etc.

Im Fall von Forensik kann man die Beispiele sehr gut aus der Vorlesung lernen, die genauen Techniken (Filesysteme) waren nicht bis in Detail nötig.