Aufgabenstellung für eine schriftliche Ausarbeitung im WPF Kryptographie & sichere Programmierung

Klaus Kusche, 2021

Ziel

- ***Selbständige Suche*** nach und ***Beschäftigung*** mit ***konkreten, aktuellen und/oder historisch bedeutenden Sicherheitsvorfällen***.
- Nachweis der Fähigkeit, solche ***Vorfälle inhaltlich zu analysieren und einzuordnen***, nachzuvollziehen, ihre Bedeutung einzuschätzen usw..

Aufgabenstellung

- Konkrete aktuelle und/oder historisch bekannte/bedeutende *Sicherheitsvorfälle darstellen*, und zwar *mehrere einzeln* und unabhängig voneinander (Fall pro Fall).

  Auch eine *gute / breit gestreute Auswahl der Fälle* macht einen guten Eindruck!

  Beispiele von in Frage kommende Arten von Vorfällen:

  ➔ *Sicherheitslücken* in Software
  - incl. BIOS, intel ME, intel SMM, ...
  - incl. Netzwerk-Software (obwohl diese ausdrücklich nicht Lehrstoff war)
  - insbesondere Krypto-Software!

  ➔ *Hardwarenahe Sicherheitslücken*:
  - Vorfälle durch Seitenkanal-Attacken, HW Reverse Engineering, ...

  ➔ *Schwächen* in *kryptografischer Software*
  - „Krypto-Fails“ und erfolgreiche Attacken auf Krypto-Algorithmen incl. Hash-Algorithmen, kryptographischen Zufallszahlen, ...
  - Defekte Implementierungen an sich sicherer Krypto-Verfahren
  - „Passwort-Fails“: Hart codierte Passwörter & Backdoors, Design-Fehler, keine/zu schwache/falsche Verschlüsselung von Passwörtern, ...
  - Andere Probleme mit Authentifizierungs- und Zugangssystemen, soweit sie in Zusammenhang mit dem Lehrstoff gebracht werden können

  ➔ *Technische und organisatorische (!) Fails* im *Signatur- und Zertifikatswesen*:
  - Fehlverhalten von CA's
  - Einbrüche in CA's
  - Missbrauch und kriminelle Aktivitäten von Signaturen und Zertifikaten
  - Probleme durch hartkodierte Zertifikate, untergeschobene Zertifikate, abgelaufene und nicht rechtzeitig erneuerte Zertifikate, ...
  - Sicherheitsrelevante Vorfälle bei automatischen Software-Updates usw., aber nur soweit kryptografisch bedingt.

  ➔ Vorfälle mit kryptografischem Hintergrund (nur solche!) bei *Krypto-Währungen.*

- Zu jedem Vorfall sollen

  ➔ … die ***Fakten*** kurz dargestellt werden:
  Wann ist wo/bei wem was passiert, mit welchen Folgen?

  ➔ … die ***technischen Hintergründe*** analysiert werden:
  – Wie ist der Vorfall aus technischer Sicht abgelaufen,
  was ist warum schiefgegangen, wo lag das Problem / die Ursache?
  – Wie lässt sich das in unseren Lehrstoff einordnen?

  ➔ … soweit sinnvoll aus ***technischer Sicht***
  die tatsächlichen und/oder die möglichen ***Folgen*** dargestellt werden:
  – Warum hatte der Vorfall welche Folgen?
  – Welche Folgen hätte der Vorfall haben können,
  was wären die Alternativen gewesen?

Abgabe

- *Schriftlich in elektronischer Form* (per Mail als PDF).
- Als *Textdokument*, nicht als Präsentation.
- Umfang rund *10 Seiten*.

  Grafiken in angemessenem (!!) Umfang dürfen darin enthalten sein.
- Abgabefrist *11. Juli*
- Vorgaben zu Form und Struktur: Keine besonderen.
  Inhaltsverzeichnis, Abbildungsverzeichnis, Deckblatt usw. sind *nicht* erforderlich!
  (und ein Abkürzungsverzeichnis schon gar nicht)
  Auch eine Einleitung und ein Fazit für alle Fälle gemeinsam ist nicht nötig,
  aber ein *Fazit pro einzelnem Vorfall* kann sinnvoll sein.
- Eine *saubere und lückenlose Quellenangabe* ist hingegen zwingend gewünscht
  (am besten gleich direkt bei bzw. unmittelbar nach jedem Vorfall).

FAQ

- **Ist Teamwork erlaubt?**

  Nein, jeder soll allein und selbständig Vorfälle suchen, analysieren
  und zu Papier bringen.

  Aber wenn jemand mehr Vorfälle findet oder weiß, als er braucht,
  darf er die überzähligen Vorfälle an andere weitergeben.
- **Dürfen mehrere Studenten denselben Vorfall wählen?**

  Ja, solange sie ihn unabhängig voneinander bearbeiten.
- **Wie viele Vorfälle sind zu auszuarbeiten?**

  Es ist *nur die Seitenzahl* vorgegeben.

  Wenn sich die 10 Seiten mit zwei umfangreichen, inhaltlich interessanten und komplexen Vorfällen gut und sinnvoll füllen lassen, sind diese zwei Vorfälle genug.
  Wenn die 10 Seiten 15 Vorfälle enthalten, die jeweils nur eine kurze Beschreibung und Analyse hergeben, ist es auch ok.