technische universität
dortmund

Fakultät für Informatik
Lehrstuhl 14 für Programmiersysteme
Arbeitsgruppe Testen und Verifikation

Entwicklung **a**utomatischer **T**ools zur Lösung von **CTFs**

Simon Dierl, Malte Mues und Prof. Dr. Falk Howar | 19. Dezember 2018

Motivation: Return Of Bleichenbacher's Oracle Threat

Der Bleichenbacher-Angriff

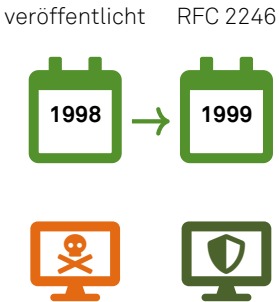
- Schwachstelle in RSA-Implementierungen
- Anfragemuster erlaubt Rückrechnen des privaten Serverschlüssels
- Server kann danach glaubwürdig imitiert werden!

veröffentlicht

Motivation: Return Of Bleichenbacher's Oracle Threat

Der Bleichenbacher-Angriff

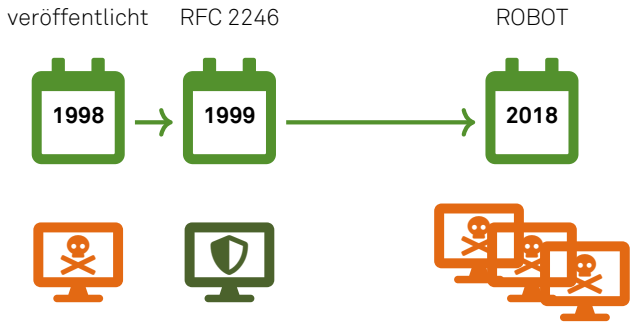
- Schwachstelle in RSA-Implementierungen
- Anfragemuster erlaubt Rückrechnen des privaten Serverschlüssels
- Server kann danach glaubwürdig imitiert werden!

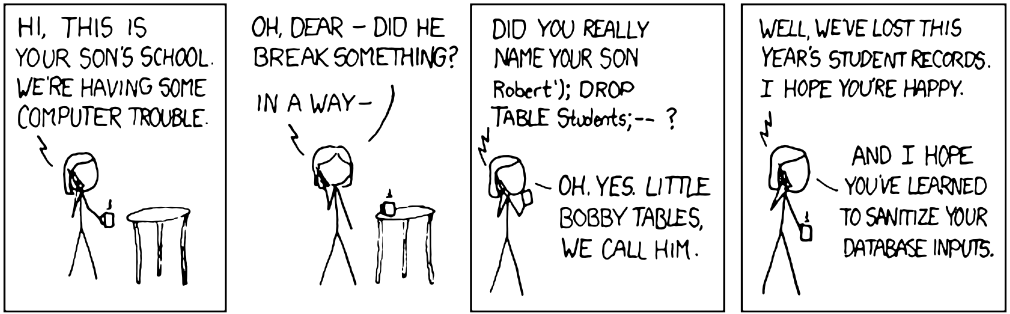


Motivation: Return Of Bleichenbacher's Oracle Threat

Der Bleichenbacher-Angriff

- Schwachstelle in RSA-Implementierungen
- Anfragemuster erlaubt Rückrechnen des privaten Serverschlüssels
- Server kann danach glaubwürdig imitiert werden!

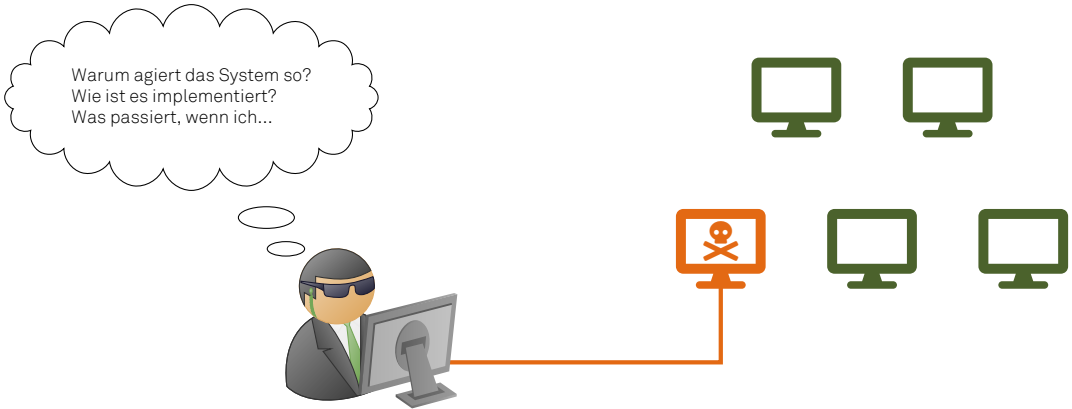




XKCD: Exploits of a Mom. CC-BY-SA 2.5.

Unsere Idee: dem Computer Hacken beibringen

Unsere Idee: dem Computer Hacken beibringen



Unsere Idee: dem Computer Hacken beibringen

Geplante Inhalte & Ziele

Einarbeitung: Sicherheitslücken verstehen

- Studium von Vulnerability-Datenbanken (OWASP, CVE, CWE)
- Manuelles Lösen von CTF-Challenges

Geplante Inhalte & Ziele

Einarbeitung: Sicherheitslücken verstehen

- Studium von Vulnerability-Datenbanken (OWASP, CVE, CWE)
- Manuelles Lösen von CTF-Challenges

Suche: Lücken automatisiert finden

- Klassische „Hackertools“ testen
- Formale Ansätze evaluieren
- Kombinierte Verfahren untersuchen
- Manuellen Aufwand reduzieren

Geplante Inhalte & Ziele

Einarbeitung: Sicherheitslücken verstehen

- Studium von Vulnerability-Datenbanken (OWASP, CVE, CWE)
- Manuelles Lösen von CTF-Challenges

Automatisierung: Einsatz der Werkzeuge

- Benchmark-Suites analysieren
- CTFs möglichst automatisiert lösen

Suche: Lücken automatisiert finden

- Klassische „Hackertools“ testen
- Formale Ansätze evaluieren
- Kombinierte Verfahren untersuchen
- Manuellen Aufwand reduzieren

Geplante Inhalte & Ziele

Einarbeitung: Sicherheitslücken verstehen

- Studium von Vulnerability-Datenbanken (OWASP, CVE, CWE)
- Manuelles Lösen von CTF-Challenges

Suche: Lücken automatisiert finden

- Klassische „Hackertools“ testen
- Formale Ansätze evaluieren
- Kombinierte Verfahren untersuchen
- Manuellen Aufwand reduzieren

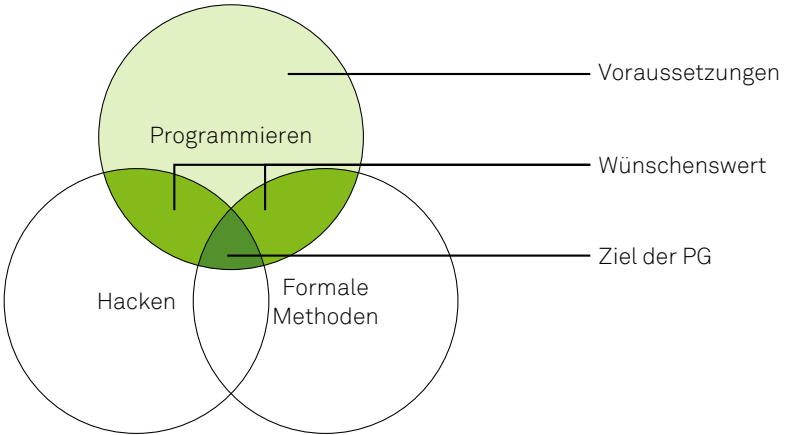
Automatisierung: Einsatz der Werkzeuge

- Benchmark-Suites analysieren
- CTFs möglichst automatisiert lösen

Ziel: Gefordertes Ergebnis

- Studie über geeignete Klassen von Lücken
- 2 VMs, die automatisiert „geknackt“ werden...
- ...und das entsprechende Werkzeug

Erwartungen an die Teilnehmer



Fragen zu Thema und Voraussetzungen:
Gerne sofort stellen!

Fragen zu Inhalt und Details:
Einzelvorstellung am
Montag, 07.01.2019, 10:00 Uhr, OH12 / 2.013