Mathematical Weaknesses of Cryptographic Systems

Fernando Sánchez Villaamil, Philipp Kuinke, Peter Rossmanith

Lehr- und Forschungsgebiet Theoretische Informatik

Übersicht

Die Thematik

Organisatorisches

Die Themen

Die Thematik

Die Entwicklung von Kryptosystem war immer eng an das Brechen von Kryptosystemen gekoppelt.
Interessant als Seminarthema:

- Jede neue Generation von Kryptosystem erfordert eine neue Art der Kryptoanalyse
- Schwächen sind nicht notwendigerweise theoretischer Natur: schlechte Implementierung oder fehlerhafte Hardware können ebenso gefährlich sein
- Sowohl historische Themen (Enigma) als auch aktuelle Vorgänge (SHA-1, MD5)
- Betrifft inzwischen unseren Alltag

Organisatorisches

Zeitplan (außer für die ersten Themen)

Vier Wochen vor dem Vortrag	Literatur ist gesichtet, Thema eingegrenzt, Gliederung und Inhaltsangabe
Ein Monat nach dem Vortrag	Abgabe der Ausarbeitung
Nach Rückmeldung	Letzte Überarbeitung der Ausarbeitung

- Dauer der Vorträge: 45 Minuten, danach ca. 15 Minuten Diskussion
- Vortragsprache Deutsch oder Englisch (ebenso Ausarbeitung)
- Höhere Erwartungen an Masterstudenten!

1. Angewandte Kryptographie (Einleitungsthema)
2. Die Enigma
3. WEP
4. DES
5. MD5
6. SHA-1
7. Merkle-Hellman
8. Power Analysis
9. Schlechte RSA-Schlüssel
10. Bluetooth-Verschlüsselung
11. Fehlerhafte Hardware
12. Heartbleed

Angewandte Kryptographie

- **Erster Vortrag**
- Übersicht der Thematik: Verschlüsselung, Hashing, Protokolle...
- Anwendung im Alltag
- B. Schneier: Applied Cryptography

Die Enigma

Die Enigma war eine in Deutschland entwickelte Verschlüsselungsmaschine, die im Ersten aber insbesondere im Zweiten Weltkrieg auf Deutscher Seite weitverbreitet Verwendung fand. Das Brechen des Verschlüsselungsverfahrens durch eine geschickte Mischung aus Brute-Force, Protokollschwächen und mathematische Einsichten im “Bletchley-Park” ist ein spannendes Stück moderner Geschichte.

- R. Kippenhahn: Verschluesselte Botschaften
- S. Singh: Geheime Botschaften

WEP

WEP (Wired Equivalent Privacy) war ein weitverbreitetes Protkoll um drahtloses W-LAN Verbindungen zu sichern — obwohl es erwiesenermaßen unsicher war! WEP hat mehrere Defekte, die für praktische Angriffe ausgenutzt werden können. Oft kann eine WEP-Verbindung nur mit Hilfe von passiv erlangten Informationen binnen Minuten gebrochen werden.

- http://saluc.engr.uconn.edu/refs/stream_cipher/fluhrer01weaknessRC4.pdf

DES

Eine von IBM entwickelter und von der NSA empfohlener Chiffrierungsalgorithmus. Die Beteiligung der NSA gibt dem Algorithmus einen interessanten historischen Hintergrund. Die Hauptschwäche dieses Algorithmus ist, dass der Schlüssel zu klein gewählt wurde. Mit genügend Resourcen kann mit einer brute-force Attacke eine DES-Verschlüsselung gebrochen werden.
Zudem hat der Algorithmus andere Schwächen, mit denen theoretisch besserer Attacken entwickelt werden können, die aber in der Praxis nicht besser als eine brute-force Attacke sind.

- http://link.springer.com/article/10.1007/s001459900027#page-1

MD5

MD5 ist einer sehr verbreitete kryptographische Hashfunktion. Mittlerweile ihre Benutzung nicht mehr empfohlen: In den letzten zwei Jahrzehnten wurden mehrere Schwächen in dem Algorithmus festgestellt. Es wurde sogar eine Methode entwickelt, um zwei Dateien mit den gleichen Hashwert zu generieren.

- http://www.infosec.sdu.edu.cn/uploadfile/papers/How%20to%20Break%20MD5%20and%20Other%20Hash%20Functions.pdf
- http://www.schneier.com/blog/archives/2008/12/forging_ssl_cer.html

SHA-1

Eine andere sehr verbreitete und von der NSA abgesegnete Hashfunktion die gebrochen wurde. Auf anfängliche Hinweise, welche die Unsicherheit der Hashfunktion andeuteten, folgte ein Algorithmus, mit dem Kollisionen deutlich schneller als per brute-force gefunden werden können.

- http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html
- http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf

Merkle-Hellman

Eines der ersten Public-Key-Verfahren. Basiert auf der Idee, dass es schwierige und einfache Instanzen von NP-schweren Problemen gibt. Die Idee ist prinzipiell elegant und einfacher als z.B. RSA. Leider wurde jedoch gezeigt, dass man diese Methode in polynomieller Zeit brechen kann.

- http://dx.doi.org/10.1109%2FTIT.1978.1055927
- http://dx.doi.org/10.1109%2FSFCS.1982.5

Power Analysis

Smart-cards finden in vielen verschiedenen Bereichen Anwendung, wie z.B. Verkaufstransaktionen, Pay-TV, Diebstahlsicherung, etc. Diese Karten enthalten meistens einen Mikroprozessor und scheinen deswegen besonders geeignet, um sie für Kryptographische Zwecken zu verwenden. Es gibt aber mehrere mögliche Angriffe auf Smart-card basierte Systeme, unter denen die sogenante Power-Analysis Methode.

- http://www.cl.cam.ac.uk/~osc22/docs/smartcards.pdf

Schlechte RSA-Schlüssel

RSA ist wohl das bekannteste Public-Key-Verfahren. Es gilt weiterhin als sicher, da die grundlegenden numerischen Annahmen bis heute solide erscheinen. Die Methode basiert aber auf zufällig gewählten Primzahlen: Unsicherheiten können auftauchen, weil diese Zahlen nicht “zufällig genug” gewählt werden. Tatsächlich sind diese Probleme in der Praxis relevant.

- http://eprint.iacr.org/2012/064.pdf

Bluetooth-Verschlüsselung

Bluetooth ist ein weitverbreiteter Standard für kleine Meshnetzwerke und Punkt-zu-Punkt-Verbindungen. Da Bluetooth insbesondere für Smartphones eingesetzt wird (Headsets, Datentransfer) ist es essentiell, dass eine sichere Verschlüsselung verwendet wird. Das im Standard festgelegte Verfahren E0 hat jedoch erhebliche Schwächen.

- http://link.springer.com/chapter/10.1007%2F978-3-642-24209-0_2
- http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.84.627

Fehlerhafte Hardware

Selbst fehlerfreie Implentierungen theoretisch sicherer kryptographische Algorithmen können unerwartete Sicherheitslücken bergen, wenn die darunterliegende Hardware nicht perfekt funktioniert. Tatsächlich reichen oft schon wenige Fehlerhafte Bits, um ein kryptographisches Geheimnis offenzulegen!

- http://cs.tau.ac.il/~tromer/courses/infosec11/Boneh%20DeMillo%20Lipton%201997%20---%20On%20the%20importance%20of%20eliminating%20errors%20in%20cryptographic%20protocols.pdf

Heartbleed

Der Heartbleed-Bug ist ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können. Ein großer Teil der Online-Dienste, darunter auch namhafte Websites wie auch VoIP-Telefone, Router und Netzwerkdrucker waren dadurch für Angriffe anfällig.

- http://heartbleed.com/