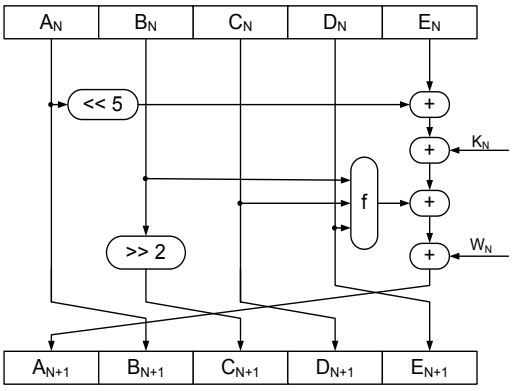
Dipl.-Ing. Christian Rechberger
Institut für Angewandte Informationsverarbeitung
und Kommunikationstechnologie
E-Mail: Christian.Rechberger@iaik.tugraz.at
Tel.: 0316 873 5534

Kryptographie als Fundament für Sicherheit in der IT

Cryptography: the Basis of IT-Security

Schon vor dem Studium habe ich mich mit verschiedenen Aspekten der Informationssicherheit beschäftigt. Bis zwei Jahre vor Ende meines Telematik-Studiums war dieses Engagement jedoch abseits jeder Lehrveranstaltung. Letztendlich konnte ich jedoch diese privaten Interessen mit meinem Studium verbinden, und habe das Telematik-Studium mit einem Schwerpunkt in diesem Bereich am Institut für Angewandte Informations- und Kommunikationstechnologie (IAIK) abgeschlossen.
Seit fast 3 Jahren beschäftige ich mich nun im Rahmen meiner Dissertation in der Forschungsgruppe von Prof. Vincent Rijmen am IAIK [1] mit der Analyse von kryptographischen Grundbausteinen. Die Kryptographie hat sich seit den 1970er Jahren von einer meist im Verborgenen betriebenen Wissenschaft zu einer sehr aktiven akademischen Disziplin und zu einem wichtigen Baustein und Motor der modernen Informationsgesellschaft entwickelt. Ob Bankomat, Internet, Mobiltelefonie oder E-Government - kryptographische Mechanismen sorgen im Hintergrund für die nötige Sicherheit.
Eine kleine Anzahl von kryptographischen Kernbausteinen bildet das Fundament für all diese Anwendungen. Diese müssen zugleich effizient und sehr sicher sein. Einer der wichtigsten Bausteine sind kryptographische Hashfunktionen. Design und Analyse solcher Hashfunktionen sind seit Mitte der 1980er Jahre ein aktives Forschungsfeld. Die Hashfunktion SHA-1(Secure Hash Algorithm 1) wurde 1995 vorgeschlagen und hat seither in vielen nationalen wie internationalen Standards Eingang gefunden und ist weltweit allgegenwärtig. Jeder Webbrowser, viele Passwortschutzmechanismen und Chipkarten verwenden diese Hashfunktion als einen Grundbaustein.
SHA-1 galt lange Zeit als sicher und vertrauenswürdig. Anfang 2005 wurden jedoch nach Vorarbeiten unserer Gruppe von einem chinesischen Team erstmals theoretische Schwächen entdeckt, ohne diese jedoch wegen der großen technisch-mathematischen Schwierigkeit geeignet beschreiben zu können.
Daraus ergeben sich zwei Fragenkomplexe, sowohl für die akademische Forschung als auch für Industrie, Standardisierungsgremien und Behörden. Erstens stellt sich die Frage nach einer realistischen Einschätzung der Sicherheit und damit verbunden die Frage, ob und wann SHA-1 ersetzt werden soll. Zweitens stellt sich die Frage nach einer Alternative. Wie sollen Alternativen aussehen, welche Eigenschaften sollen sie haben, um die in SHA-1 gefundenen Schwächen zu vermeiden?
Zur realistischen Einschätzung der Sicherheit von SHA-1 ist es einem belgischen Gastforscher und mir im Rahmen eines FWF-Projektes gelungen, erstmals einige wichtige Fragen zu klären. Konkret stellen wir in unserer Arbeit einen neuen Ansatz vor, wie die Sicherheit von Hashfunktionen im Allgemeinen und von SHA-1 im Speziellen evaluiert werden kann. Basis dafür ist ein effizientes Verfahren, das verschiedenste Verhaltensweisen bei sich ändernden Eingangsdaten in einer Hashfunktion wie SHA-1 auf systematische Weise findet. Damit wird nun erstmals eine realistische Einschätzung der Sicherheit dieses wichtigen Grundbausteins möglich. Unsere neuen Ansätze stoßen auf großes Interesse. Sie wurden in der kurzen Zeit seit ihrer Präsentation weltweit bereits von mehreren anderen Forschungsgruppen aufgegriffen, um sowohl SHA-1 als auch andere Hashfunktionen damit zu analysieren. Dies bringt mich bereits auf den zweiten oben angesprochenen Punkt: Alternativen zum allseits verwendeten, aber nun angeschlagenen SHA-1.
Unsere aktuellen Ergebnisse lassen darauf schließen, dass die Sicherheit von SHA-1 zwar um einiges geringer ist als ursprünglich angenommen, für Entwickler aber noch genügend Zeit bleibt, um auf Alternativen zu wechseln. Bei der Suche und Auswahl von möglichen Alternativen hat die Amerikanische Standardisierungsbehörde NIST (National Institute for Standards and Technology), aus deren Feder auch SHA-1 stammt, die Initiative ergriffen[2]. Es ist ein mehrjährig angelegter internationaler Wettbewerb in Planung, dessen Gewinner einen neuen Standard hervorbringen. Damit dieser neue Standard einen ähnlich hohen Verbreitungsgrad wie SHA-1 erreicht, ist neben tiefem Vertrauen in dessen Sicherheit auch Effizienz gefordert. Das Entwickeln eines Kandidaten der diesen Kriterien genügt, stellt eine fächerübergreifende Herausforderung dar, der ich mich mit meinen Kollegen stellen werde.
Ein Blick in meine Mailbox zeigt: das Forschungsgebiet ist trotz seiner konkurrenzbetonten Natur international vernetzt und trotz seiner Grundlagenorientierung praxisrelevant. Zum einen äußert sich dies durch regelmäßige Einladungen für Vorträge oder Forschungsaufenthalte, zum anderen durch Anfragen von Firmen oder Behörden zu unseren Resultaten.

Links
[1] www.iaik.tugraz.at/research/krypto
[2] www.nist.gov/hash-function



SHA-1 intern: Reicht eine 80-fache Wiederholung dieser einfachen Funktion, um langfristig sicher zu sein?

Cryptography: the Basis of IT-Security

From a secret science to a vibrant academic community with considerable impact: in a nutshell, that's how the field Cryptography developed since the 1970s. It's almost 3 years since I started my Phd in this area. More specifically, I'm interested in the design and analysis of its basic building blocks. These basic building blocks are used at the very core of many IT systems, for example ATMs, web-browsers, mobile phones, password protection schemes or E-Government applications. One of the most popular building blocks used in these applications is the hash function SHA-1; hence trust in this building block is vital. Our recent results attracted a great deal of attention internationally, and suggest that the security offered by SHA-1 is less than expected – still, there is enough time for developers to switch to alternatives. Design and analysis of alternatives are big unsolved problems and our results shed light on undesirable properties.
A glance into my mailbox is enough to see that the basic research we do at the Krypto group [1] interests other research groups and companies alike. Questions by companies or authorities on our results, and invitations for research visits by internationally renowned groups make a nice contrast to my daily work in Graz.