# Forschungsgruppe Systemsicherheit

Patrick Horster · Peter Schartner

Forschungsgruppe syssec · Universität Klagenfurt
{patrick.horster | peter.schartner}@syssec.at

## Zusammenfassung

Neben Kernkompetenzen in den Bereichen Sicherheitsinfrastrukturen und Angewandte Kryptologie verfügt die Forschungsgruppe Systemsicherheit (syssec) über Erfahrungen beim Aufbau komplexer sicherheitsrelevanter Systeme in unterschiedlichen Anwendungsfeldern, etwa im Kontext elektronischer Passsysteme, tokenbasierter Sportereignisse und bei Sicherheitssystemen für Automobile. Von besonderer Relevanz sind dabei der Einsatz von Chipkarten und weiterer Security-Token sowie ein bedarfsgerechtes Schlüsselmanagement. Zudem steht syssec als unabhängiger wissenschaftlicher Projektbegleiter und Berater für sicherheitsrelevante Projekte, auch im Konfliktfall (z.B. bei Patentverletzungen oder der Auslegung von Pflichtenheften), zur Verfügung. Durch unser grenzüberschreitendes Netzwerk zu zahlreichen universitären und industriellen Forschungseinrichtungen und zur relevanten Industrie können wir komplexe Probleme – auch interdisziplinär – behandeln.

# 1 Die Forschungsgruppe syssec

Im Bereich der Institute für Informatik wurde der Lehrstuhl für Systemsicherheit im April 1997 eingerichtet und mit o. Univ.-Prof. Dr. rer. nat. Patrick Horster besetzt. Das Kernteam umfasst derzeit drei wissenschaftliche Mitarbeiter (PD Assoc.Prof. Dr. Peter Schartner, DP Ass.-Prof. Dr. Stefan Rass und Dipl.-Ing. Raphael Wigoutschnigg), zwei Techniker zur Be-treuung der Hard- und Software und zur Unterstützung bei Software-Projekten sowie zwei Sekretärinnen zur administrativen und organisatorischen Unterstützung.

Ein zusätzlicher Projektassistent (Matthias V.) ist im Projekt „Risikomanagement für simultane Bedrohungen“ beschäftigt. Im Bereich der Lehre wird die Forschungsgruppe zudem von zwei Studienassistenten unterstützt. Wenn es die Rahmenbedingungen zulassen, werden zudem Studienassistenten und Studierende bei der Bearbeitung von Projekten eingebunden, wobei gegebenenfalls auch eine (interdisziplinäre) Zusammenarbeit mit anderen Forschungsgruppen (intern wie extern) erfolgt.

Durch Grundlagenforschung und anwendungsorientierte Forschung ist die Forschungsgruppe Systemsicherheit ein kompetenter Ansprechpartner im Bereich der Sicherheit komplexer IT-Systeme, wobei die aktuellen Schwerpunkte in den Gebieten bedarfsgerechter Sicherheits-infrastrukturen, des relevanten individualisierten Keymanagements und hierfür geeigneter Security-Token zu sehen sind.

Insbesondere werden Aspekte sicherer Informations- und Kommunikationssysteme und die zugrunde liegenden kryptographischen Mechanismen behandelt. Hierbei wird dem Einsatz innovativer Chipkartensysteme besonders Rechnung getragen, wobei die Sicherheitsanforde-rungen (mobiler) vernetzter Kommunikationssysteme, des eCommerce und der Multime-diasysteme besonders berücksichtigt werden.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 330-333.

# 2 Schwerpunkte der Forschung

In der Forschungsgruppe Systemsicherheit werden folgende Arbeitsschwerpunkte behandelt:

- Sicherheit in komplexen IT-Systemen – Sicherheitskonzepte und deren Grundlagen
- Mathematische Aspekte der Kryptologie – Entwurf und Analyse relevanter Verfahren
- (Gruppenorientiertes) Key Management
- Technischer Datenschutz und Informationssicherheit
- Sicherheitsrelevanter Einsatz von Chipkarten und Smartphones
- Implementierung von Prototypversionen der entwickelten bzw. untersuchten Verfahren
- Informationstheoretische Sicherheit
- Risikoanalyse
- Quantenkryptographie und Anwendungen
- Anonyme Kommunikation und Privacy

Eine Vertiefung der Forschungsaktivitäten erfolgt derzeit vor allem in folgenden Bereichen:

- Neben den Standardaufgaben eines modernen Keymanagements (etwa Erzeugung, Verteilung, Archivierung, Aktualisierung, Rückruf und Vernichtung von Schlüsselkomponenten) werden insbesondere die Gebiete „Effiziente Schlüsselvereinbarung", „Dublettenfreie Schlüsselgenerierung" und „Gruppenorientiertes Keymanagement" behandelt.
- Smartphones werden unter Nutzung von Chipkarten zu so genannten Trusted Personal Devices (TPDs) ausgebaut und in sicherheitsrelevanten Anwendungsfeldern eingesetzt.
- IT-Risiko-Management dient der Absicherung einer Kommunikationsinfrastruktur gegen technische, wirtschaftliche aber auch datenschutzrechtliche Schäden aller Art (insbesondere verursacht durch menschliches Fehlverhalten). Das Vorgehen hierbei ist häufig geprägt von Best-Practices, i.d.R. Maßnahmenkataloge auf Basis von Erfahrungen. Eine allgemeingültige und fundierte Theorie hierzu fehlt weitgehend und ist zentraler Gegenstand der Forschung.
- In Zeiten allgegenwärtiger Internet-Konzerne wie Google und Facebook spielt das Thema Privatsphäre eine immer wichtigere Rolle. Durch die massive Vernetzung von Webseiten und der dadurch einhergehenden Verfolgung der Benutzer-Aktionen ist es notwendig, Techniken zu etablieren, um der Überwachung der Benutzer entgegenzuwirken. Hierzu zählen speziell Protokolle zur Anonymisierung der Benutzer-Aktionen.

Interessierte Studierende werden in Forschungsaktivitäten eingebunden, zudem fließen die aktuellen Forschungsergebnisse unmittelbar in Lehrveranstaltungen ein. Qualifizierte und motivierte Diplomanden vermitteln wir gerne zur Ableistung eines obligatorischen Praxissemesters an Forschungseinrichtungen und unsere industriellen Partner. Zahlreichen Absolventen wird dadurch nicht nur ein Einblick in ihr späteres Berufsleben ermöglicht, es ergeben sich auch Kontakte zwischen potentiellen Arbeitgebern und möglichen zukünftigen Mitarbeitern.

# 3 Ausgewählte Projekte

In den letzten Jahren wurden von der Forschungsgruppe Systemsicherheit zahlreiche Projekte erfolgreich bearbeitet und abgeschlossen. Im Folgenden werden exemplarisch externe und interne Projekte kurz aufgeführt.

**Externe Projekte** (mit externen Partnern)

- SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography: Subprojekt „Certification according to Common Criteria“.
- SECON: Entwicklung eines Konzepts für Section-Control unter besonderer Berücksichtigung des Schutzes von personenbezogenen und Fahrzeugdaten.
- SERIMA: Das SERIMA System realisiert (transparent für den Nutzer) einen vertraulichen Kommunikationskanal zwischen zwei Rechnern, wobei die maximale Abhörwahrscheinlichkeit beliebig klein gemacht werden kann.
- SECOM: Studie "Sichere IT-Services auf mobilen Endgeräten".
- Studie für ein Key-Management-System im Kontext von Smart Metering.
- Analyse und Penetration-Test einer Web-Applikation für medizinische Daten.
- Analyse von Authentifikationsmechanismen für elektronische Wegfahrsperren.
- Design und Analyse von Basismechanismen für Low-Cost-Hardware.
- Technische Gutachten bei Patentverletzung.
- Überprüfung der Einhaltung von Pflichtenheften – Beratungen im Konfliktfall.
- Beweissicherung bei deterministischem Fehlverhalten von Systemen.
- Konzeption und Integration beweisbar sicherer Keymanagement-Systeme.

**Interne Projekte** (aus Forschungsarbeiten entstanden)

- Dublettenfreie Schlüsselgenerierung: Implementierung von Mechanismen zur kommunikationslosen lokalen Erzeugung, global eindeutiger Schlüssel.
- Anonyme Authentifizierung: Entwicklung und prototypische Implementierung einer Pseudonym-Infrastruktur zur Wahrung der Interessen aller Beteiligter.
- Schutz der Privatsphäre im Bereich Videoüberwachung: Entwurf und Implementierung einer hierarchischen Zugriffsstruktur auf verschlüsseltes Bildmaterial.
- Sichere Internet-Telefonie: Entwurf und Implementierung eines Prototyps.
- Design und Implementierung sicherheitsrelevanter Smartphone Anwendungen (z.B. Signature Device, Trusted Camera und Chipkarten-Library).
- Labor Systemsicherheit: Mit Industriepartnern wurde ein Labor aufgebaut, in dem Studierende praxisorientierte Projekte aus den Bereichen Chipkarten, RFID und Netzwerksicherheit entwickeln und kryptographische Hard- und Software kennen lernen.

Daneben werden Gutachten erstellt und hoch motivierte Studierende zur Durchführung eines (obligatorischen) Praxissemesters an Forschungseinrichtungen und Entwicklungsabteilungen namhafter Firmen vermittelt. Durch Kooperation mit externen Institutionen entstanden qualitativ hochwertige theoretische, aber auch praxisorientierte Diplomarbeiten.

# 4 Dienstleistungen

Motiviert durch die erfolgreiche Arbeit der letzten Jahre und durch unsere weitgehende Unabhängigkeit als universitäre Einrichtung bieten wir fundiertes Wissen und weitreichende Erfahrungen an, um unseren Beitrag zur IT-Sicherheit zu leisten.

- **Analyse und Bewertung von Kryptomechanismen** und kryptographischer Hard- und Software. Unsere Erfahrung zeigt, dass zahlreiche der am Markt verfügbaren Sicher-

heitsprodukte (Soft- und Hardware) mehr versprechen als sie halten können. Bevor Sie sich für ein Produkt entscheiden, sollten Sie sich Sicherheit verschaffen.

- **Entwurf bedarfsgerechter kryptographischer Mechanismen und Protokolle**, speziell in den Bereichen Keymanagement und Authentifikation. Insbesondere bei Massenanwendungen (etwa im Bereich Automotive) können wir zur Sicherheit entscheidend beitragen.
- **Wissenschaftliche Projektbegleitung** sollte bei jedem (kostenintensiven) Projekt von Beginn an genutzt werden, da hierdurch schon frühzeitig Systemfehler und Fehlinvestitionen verhindert werden können.
- **Beratung im Konfliktfall** ist spätestens dann angezeigt, wenn sich erhoffte Erwartungen nicht erfüllen. Rechtliche Auseinandersetzungen können dabei kostenträchtig und möglicherweise existenzbedrohend sein. Bei konkreten Sachverhalten kann zudem die Schuldfrage oft nicht eindeutig geklärt werden. Das Ziel ist dann eine Schadensminimierung, die durch unabhängige Sachkompetenz erbracht werden kann.
- In vielen Produkten der IT-Sicherheit werden Patente verletzt, den dann beauftragten Patenanwälten fehlt im konkreten Fall oft das technische Fachwissen. Durch unsere Erfahrung können wir gegebenenfalls **Patentansprüche** in Bezug zu konkreten Verletzungsformen bringen. Eine Prüfung im Vorfeld kann zudem Kosten sparen.
- **Organisation und Durchführung** von Informations- und Schulungsveranstaltungen.

# 5 Ziele und Perspektiven

Das Vorhaben, wissenschaftliche Veranstaltungen, Workshops und Arbeitskonferenzen als Bindeglied zwischen Forschung, Lehre und Wirtschaft zu etablieren, wird von den Zielgruppen gut angenommen und trägt zum Fortschritt der IT-Sicherheit bei. Bei den inzwischen etwa 50 Veranstaltungen wurden nicht nur Geschäftsbeziehungen neu geknüpft, neue Produktideen kreiert und Zukunftsperspektiven diskutiert, es wurden auch Schwächen von Sicherheitsprodukten aufgezeigt und Sicherheitsspezialisten auf „Herz und Nieren“ überprüft.

Die Tagungsbände der Arbeitskonferenzen und weitere ausgewählte Titel werden durch die syssec-Buchreihe „IT Security & IT Management“ einer breiteren Öffentlichkeit zugänglich gemacht. Die Buchreihe soll zudem externen Autoren und Veranstaltern zur Veröffentlichung ihrer Werke zur Verfügung stehen, wobei die Qualität der Beiträge grundsätzlich zuvor durch unabhängige Gutachter überprüft wird.

Wenn Sie an einer Partnerschaft interessiert sind, innovative Ideen wissenschaftlich fundiert etablieren wollen, Interesse an einer kooperativen Zusammenarbeit haben oder einen fachlichen Rat suchen, dann wenden Sie sich bitte an uns. PGP-Schlüssel für vertrauliche Anfragen sind über die Homepage des jeweiligen Empfängers (siehe www.syssec.at/staff) abrufbar.

## Kontakt

PD Assoc.Prof. Dr. Peter Schartner
Alpen-Adria Universität Klagenfurt
Forschungsgruppe Systemsicherheit
Universitätsstr. 65-67
9020 Klagenfurt
Österreich

Tel.: +43 (463) 2700-3718 (DW)
+43 (463) 2700-3702 (Sekretariat)
+43 (650) 850 42 08 (Mobil)
skype: peter_schartner
eMail: peter.schartner@aau.at
URL: www.syssec.at/peter_schartner