

Sichere und effiziente Authentifizierung

Lösungen zur Thematik der 4. Berner Tagung für Informationssicherheit* vom November 2001

Sein und Schein sicherer Authentifizierung

Best Practice und rechtliche Dimensionen

Dr. Urs E. Zurfluh CEO Ad Vantis AG und lic. iur. Beat Lehmann Fürsprech

Anschliessend vier parallele Diskussionsforen:

Forum 1: Interne Authentifizierung von berechtigten Personen in geschlossenen Systemen

Forum 2: Authentifizierung von Mitarbeitern, Kunden und Dritten in offenen Systemen

Forum 3: Authentifizierungsmittel und ihr Einsatz

Forum 4: Selektiver Zutritt zu sensiblen Bereichen und Authentifizierung im Ausnahmefall

Veranstaltung: Fachgruppe Security der Schweizer Informatiker Gesellschaft

Datum: Donnerstag, 21. März 2002, 13:15 – 18:00 Uhr

Ort: HSW Gebäude Bahnhof Luzern

.....
Organisation:



Fachgruppe Security
(FGSec) der Schweizer
Informatiker Gesellschaft

HOCHSCHULE TECHNIK+ARCHITEKTUR LUZERN



Sichere und effiziente Authentifizierung

Leitidee des Praxisforums sichere und effiziente Authentifizierung

Identifizierung und Authentifizierung, d.h. die zweifelsfreie Zuordnung von Erklärungen oder Handlungen zu einem eindeutig bestimmbareren Urheber sind Grundvoraussetzungen für den Aufbau sicherer Systeme. Verschiedene Techniken und Verfahren der Authentifizierung führen zu unterschiedlichen Sicherheitsstufen. Neben allgemein verbreiteten Mitteln wie User ID und Passwort mit ihren bekannten Schwächen stehen heute die Einführung neuartiger Techniken wie «**Single Sign On**» und die «**Public Key Infrastructure**» (PKI) in Kombination mit intelligenten Chipkarten und der Überprüfung unverlierbarer biometrischer Merkmale zur Verfügung.

An der Veranstaltung wird aufgezeigt, welche Techniken und Verfahren der Authentifizierung heute und künftig in der Praxis für welche Zwecke eingesetzt werden können. Ein besonderes Gewicht wird auf die Anwendung der Authentifizierungs-Verfahren gelegt: Welche Kombination von körperlichen Merkmalen, Besitz von Objekten wie Schlüsseln, Chipkarten usw. und von geheimem Wissen kann in Zukunft in welchem Bereich zur Authentifizierung eingesetzt werden? Werden sich die heutigen Zugangskontrollen zu integrierten Systemen der Identifizierung und Authentifizierung der berechtigten Benutzer beim Zugang zu geschützten physischen und logischen Bereichen und zu den Einrichtungen elektronischer Kommunikation entwickeln? Werden diese Systeme und Verfahren primär innerhalb der Organisations-einheiten von Unternehmen und Verwaltung oder immer mehr auch im Verkehr mit externen Stellen Anwendung finden? Welche Haftungsrisiken drohen beim Versagen der Authentifizierung und welche Schranken ergeben sich aus dem Datenschutz?

In den Diskussionsforen werden sich die Teilnehmer zusammen mit Vertretern von vier ausgewählten Anwendungsbereichen mit diesen Fragen auseinandersetzen. Die erarbeiteten Einsichten und Lösungsvorschläge werden am Ende der Tagung allen Teilnehmern vorgestellt. Später ist eine Zusammenfassung der Thesen zur Publikation auf www.fgsec.ch vorgesehen.

Ablauf der Tagung

- 13:15** Eröffnung durch *Prof. Dr. Bernhard M. Hämmerli, HTA Luzern*
- 13:30** Einführungsreferat *Dr. Urs E. Zurfluh CEO Ad Vantis AG und lic. iur. Beat Lehmann Fürsprech*
- 14:20** Parallele Diskussionsforen (Inhalt siehe gegenüberliegende Seite)
- 16:20** Pause
- 16:40** Fachreferat: PKI Challengeprojekt zur Evaluation der Europäischen Referenz PKI, *Frank Jorissen, Projektleiter*
- 17:00** Präsentation und Diskussion der Resultate aus den Praxisforen im Plenum
- 18:00** Abschluss und Apéro

Anmeldungen mit der beiliegenden Anmeldekarte oder per E-Mail.

Referat: Sein und Schein sicherer Authentifizierung: Best Practice und rechtliche Dimensionen

Dr. Urs E. Zurfluh CEO Ad Vantis AG und lic. iur. Beat Lehmann Fürsprech

1 Interne Authentifizierung von berechtigten Personen in geschlossenen Systemen

Leiter: Marcel Frauenknecht, Leiter Bereich Informatiksicherheit, Informatikstrategieorgan Bund

Co-Leiter: Pascal Lamia, Informatikstrategieorgan Bund

Diskussionsteilnehmer: Josef Zehnder, Head Corporate Information Security, Syngenta Int. AG; Rolf Haefelfinger, Swiss Infosec AG

Wie können sich Mitarbeiter authentifizieren? Wie kann generell die Authentifizierung erleichtert werden? Muss zwischen einer Extranet und Intranet Authentifizierung unterschieden werden? Ist eine Authentifizierung der Mitarbeiter im Intranet sinnvoll? Wie lange leben User ID und Passwort noch? Ist ein Einsatz von Biometrics sinnvoll? Welche Alternativen gibt es?

2 Authentifizierung von Mitarbeitern, Kunden und Dritten in offenen Systemen

Leiter: Thomas Kohler, UBS AG

Co-Leiter und Diskussionsteilnehmer: Dr. J. Bruckner, UBS AG; Dr. R. Müller, UBS AG; H.P. Koller, UBS AG

Wie kann der Remote-Zugriff von Mitarbeitern auf interne Systeme sicher gewährleistet werden? Können Kunden und Mitarbeiter von extern auf gleiche Art Zugriff erhalten? Wird eine Person bezüglich Zugriff auf interne Systeme in ihrer Rolle als Kunde oder Mitarbeiter unterschieden? Wie sicher sind Remote-Zugriffsverfahren? Wie identifiziert und authentifiziert man Anrufer am Telefon?

3 Authentifizierungsmittel und ihr Einsatz

Leiter: Dr. Marcus Holthaus, Geschäftsführer IMSEC; Co-Leiter: Anthony Thorn, Geschäftsführer ATSS

Diskussionsteilnehmer: Viktor Calabro, Trivadis eSecurity; Thomas Kessler, InOut; Dr. Robert S. Zergenyi, KPMG Fides PEAT

Wie unterscheiden sich Identifikation, Authentifizierung und Autorisierung? Welche Verfahren bestehen? Haben, Sein oder Wissen als Träger von Authentifizierungsinformationen? Worin bestehen die typischen Stärken und Schwächen der Verfahren? Wie lassen sich PKI und Biometrie effizient einsetzen? Welche Kriterien sind bei der Auswahl relevant? Können Authentifizierung und Autorisierung delegiert und automatisiert werden? Ist Outsourcing sinnvoll?

4 Selektiver Zutritt zu sensitiven Bereichen und Authentifizierung im Ausnahmefall

Leiter: Ulrich Brügger, IT-Security Consultant IBM Schweiz; Co-Leiter: Lukas Burger, Si-Beauftragter Strategic Outsourcing Delivery, IBM Schweiz

Diskussionsteilnehmer: Kuno Rudolf-von-Rohr, Leiter Unternehmenssicherheit VIA MAT Gruppe, Kloten; Siegfried Wagner, Leiter Stabstelle Mktg und Einsatzführung, Generaldirektion Securitas AG, Zollikofen, in Begleitung vom Einsatzleiter der Securitas AG

Anhand welcher Kriterien definiert man Sicherheitszonen? Wieviele Stufen von Sicherheitszonen sind sinnvoll? Wie authentifiziert man Personen für den Zugang in die jeweilige Zone? Welche Sorgfaltsregeln sind dabei anzuwenden? Wer haftet bei Verstössen? Welche Regeln gelten in Ausnahmesituationen, wie zum Beispiel Brand, Wasser und Katastrophen?

Organisation

Veranstalter Fachgruppe Security der Schweizer Informatiker Gesellschaft
E-Mail: martinzimmermann@hta.fhz.ch, Internet: www.fgsec.ch/events/ft2002.03

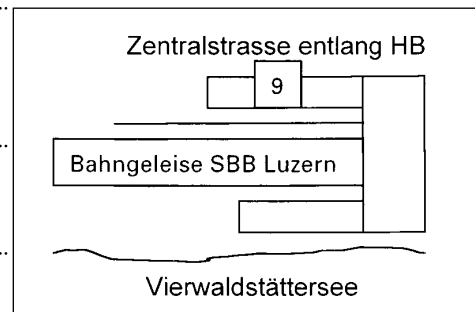
Datum, Ort Donnerstag, 21. März 2002, 13:15 – 18:00 Uhr
Auditorium 124 im 1. OG
HSW Gebäude, Zentralstrasse 9, 6002 Luzern
(Der Konferenzsaal befindet sich im Westtrakt des Hauptbahnhofes und ist ca. in 5 Minuten vom Zug und vom Parkhaus Luzern Bahnhof zu erreichen)

Fahrplan

Basel ab:	11:52	Luzern an:	13:05
Bern ab:	11:43	Luzern an:	13:03
Zürich ab:	12:01	Luzern an:	12:49

Organisation Forschungsbereich Informationssicherheit HTA
Tel: 041 349 33 31, Fax: 041 349 39 60

Kosten Fr. 350.- (inkl. Dokumentation und Apéro)
Fr. 250.- für Mitglieder der Fachgruppe
Security der SI, sowie von CLUSIS und ISACA



Anmeldungen Mit Anmeldekarte oder per Internet, Berücksichtigung nach Eingangsdatum

Sponsoren:

