

Verschlüsselungs- und Signaturtechnologien

Von den theoretischen Grundlagen
bis zur praktischen Umsetzung

Dr. Elke Stangl
1.-2.9.2006 | ditact 2006

Herzlich Willkommen!

- Vorstellung
- Erfahrungen und Assoziationen
 - Verschlüsselung?
 - Signatur?
 - Kryptographie?
 - Chipkarte? Bürgerkarte?
 - Wireless LAN?
 - ...
- Erwartungen an diese beiden Tage?
- Was ist ein Nerd | Geek? ;-)

Sicherheit?

- Zwischen Buzz-Word | Trend und Paranoia
- Zwischen Technik und Organisation
 - Technologie
 - Menschen
 - Prozesse
- Definitionen von Sicherheit | Security
 - Confidentiality | Vertraulichkeit
 - Integrity | Integrität (von übertragenen Daten)
 - Authenticity | Authentizität (des Senders)
 - Non-Repudiation | Nicht-Abstreitbarkeit
 - Availability | Verfügbarkeit

Überblick | Agenda | 1.9.2006

- 09:00 - 10:30 (1) Einführung
 - Grundprinzipien: Security | Kryptographie
 - Geschichte: Code-Erfinder gegen Code-Knacker
- 11:00 - 12:30 (2) Protokolle
 - Wie wirft man eine virtuelle Münze?
 - Wer bist Du?
- 13:30 - 15:00 (3) Authentifikation | Umsetzung
 - Beispiel Bürgerkarte
- 15:30 - 16:15 (4) Moderne kryptographische Methoden
- 16:15 - 17:00 (5) Schlüsselmanagement in Organisationen
 - Public Key Infrastructure (PKI)

Überblick | Agenda | 2.9.2006

- 09:00 - 10:30 (6) Benutzer- und Computerauthentifikation in Netzwerken:
 - Beispiel: Kerberos in der Praxis
 - Passwortsicherheit
- 11:00 - 12:30 (7) Absichern von Netzwerkverbindungen
 - Risiken für drahtlose und andere Netzwerke
 - Verschlüsselung
 - Aussperren nicht vertrauenswürdiger Personen / Computer
- 13:30 - 15:00 (8) Datenverschlüsselung
 - Risiken bei Notebook-Diebstahl
- 15:30 - 16:15 (9) Aktuelle Herausforderungen und Ausblick
 - Quantentechnologien
 - RFID



(1) Einführung | Grundprinzipien

Risiken als Maßstab

- Risiken?
 - Was sehen Sie subjektiv heute als größte Bedrohung / Risiko für einen typischen PC-Benutzer?
 - Wonach beurteilen Sie das Risiko
- Maßnahmen?
 - Wie legen Sie Maßnahmen fest?
- Risikoanalyse und –management:
 - Werte
 - Bedrohungen
 - Wahrscheinlichkeit und Auswirkung
 - Bewertung, Reihung
 - Maßnahmen

Historische Methoden

- Verstecken der Botschaft in unauffälliger Verpackung (Steganographie)
 - Chinesische Seide und Wachs
 - Geheimschrift
 - Kopfhaut
 - Unter der Wachsschicht
- Transpositionen
 - "Rail Fence Transposition"
 - Die aufgerollte Botschaft
- Substitutionen
 - Cäsar's Methode
 - Begriff: Schlüssel

Knacken durch Frequenzanalyse

- Abzählen aller Buchstaben im verschlüsselten Text
- Vergleichen der herausragenden Werte mit Standardwerten für verschiedene Sprachen
 - Deutsch: e...20%
 - Englisch: e...10%, 5 sehr seltene Buchstaben
- Suche nach häufigen Doppellauten
- Suche nach häufigen 2-/3-Buchstabenwörtern
- Abstimmung mit der Art und Charakteristik des Textes (Weglassen von Wörtern, Telegrammstil...)
- Suche nach "Cribs"
- Ist "e" auch im verschlüsselten Text der häufigste Buchstabe? → Transposition statt Substitution!

Verbesserung der Substitutionsmethoden

- Austricksen der Frequenzanalyse durch Homophone
- → Knacken durch Fokussieren auf Doppellaute
- Besser: Verwendung mehrerer Substitutionsalphabete
- Vigenère-Verschlüsselung (16. Jahrh.)
 - Auswahl von Alphabeten durch periodisches "Anwenden eines Codewortes"
 - Frequenzanalyse nicht mehr möglich, da der gleiche Buchstabe (und gleiche Doppellaute) immer anders verschlüsselt wird.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Bildquelle:

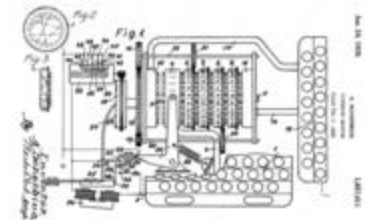
http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

Knacken der Vigenère-Verschlüsselung

- "Nicht knackbar" für 200 Jahre
- Intuition von Charles Babbage
- Suche nach Sequenzen von 3-4 Buchstaben, die sich wiederholen → mögliche Schlüssellänge oder Vielfache
- Verschiedene Sequenzen → verschiedene Varianten → Schlüssellänge als Schnittmenge
- Frequenzanalyse für Teilmengen, Suche nach Mustern (charakteristische "Berge und Täler")
- Bestimmung aller Buchstaben des Codewortes / Schlüssels, ständiger Check durch Entschlüsselung.

Enigma

- Mehrere Substitutionen hintereinander, verstellbare Walzen ("Scrambler")
- Zweimalige Anwendung durch den Reflektor, damit kann Entschlüsselung auf die gleiche Methode durchgeführt werden
- Zusätzlich: Steckboard zum Vertauschen von Buchstaben
- Schwächen:
 - Einschränkung der möglichen Stellungen, um Masche "sicherer" zu machen → Irrtum.
 - Buchstabe kann nicht auf sich selbst abgebildet werden.



Bildquelle:

http://de.wikipedia.org/wiki/Enigma_%28Maschine%29

Knacken der Enigma

- Kauf der Baupläne (Spionage)
- "Cribs"
 - Fixe Komponenten typischer militärischer Nachrichten ("WETTER")
 - Verwendung eines "Message Key" am Anfang der Nachricht, der mit dem Hauptschlüssel verschlüsselt wurde.
- Testen von Möglichkeiten durch Entschlüsselungsmaschinen ("Bombes")
- Erkennen von Ketten als "Fingerprints"
 - Auswerten der Verschlüsselung des "Message Key": Kette von Buchstaben, bis wieder der Ausgangsbuchstabe erreicht wird = Fingerprint der Walzenstellung
 - Interne Schleifen durch Cribs ("known plaintext"):
 $w \rightarrow E, e \rightarrow T, \dots, t \rightarrow W$ für unterschiedliche – jeweils um 1 "weitergedrehte" Walzenstellungen → Testen mit parallel laufenden Maschinen
- Entkoppeln von Walzen und Steckboard: Verbinden der 3 Test-Enigmas in der Kette (Stromfluss) → Vertauschungen durch Steckboards heben sich in der Kette auf!

Worauf beruht Sicherheit?

- Sicherheit ist NICHT: Etwas zu verstecken
 - in einem versteckten Safe
 - Mit unkanntem Sperrmechanismus
 - an einem unbekanntem Ort
 - zu hoffen, dass niemand den Ort zufällig findet
 - Zu hoffen, dass niemand zu lange Zeit hat, den Safe zu untersuchen
- SONDERN: Sicherheit ist, etwas zu verstecken...
 - In einem Safe mit publiziertem Sperrmechanismus
 - Öffentlich bekannt zu machen, wo der Safe steht
 - Dem Angreifer Monate Zeit zu geben, den Safe zu untersuchen
- Nicht der Algorithmus muss geheim sein, sondern der Schlüssel.

Schlüssel | Begriffe

- Plaintext
 - Anwendung des Schlüssels
 - Ciphertext
- Begriffe
 - Verschlüsseln / entschlüsseln
 - Encipher / decipher
 - Encrypt / decrypt
- Schlüssel: Zahl, String, "Wort" im weitesten Sinn
- "→" ... Algorithmus
- Alice und Bob (und Trent, Carol, Mallory,...)
- One-Way-Functions, Hash-Funktionen
- Random Numbers

Symmetrische Kryptographie

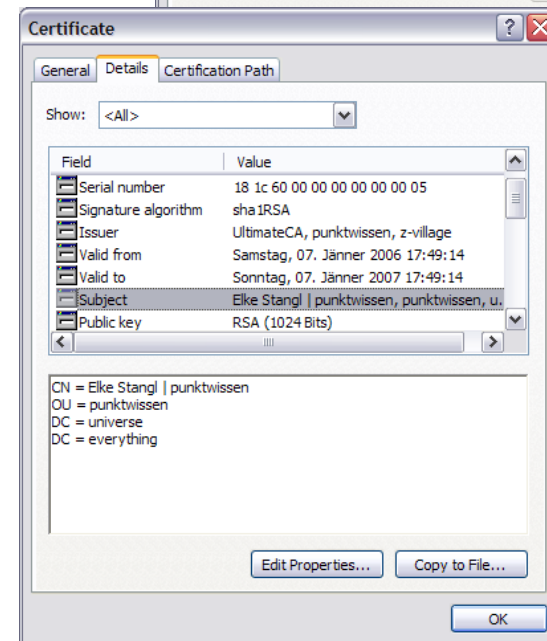
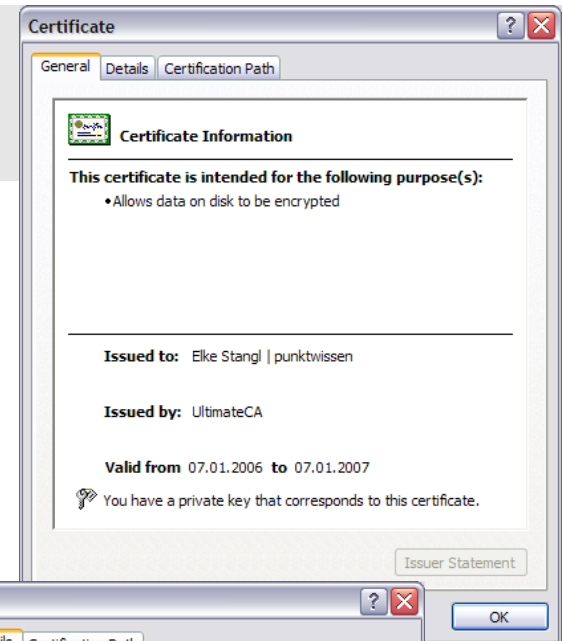
- Historische Methoden waren alle symmetrisch
- Alice und Bob haben den gleichen Schlüssel
- Herausforderung:
 - Wie wird der Schlüssel verteilt?
- Oft kombiniert mit asymmetrischer Kryptographie
- Vorteil: Geschwindigkeit der Verschlüsselung
- 1. standardisierter Algorithmus: DES – Data Encryption Standard

Asymmetrische Kryptographie

- Alice und Bob haben je ein Schlüsselpaar
- Öffentlicher und privater Schlüssel
 - Werden gemeinsam aus Zufallszahlen erzeugt
 - Öffentlicher Schlüssel kann nur unter extrem hohem Aufwand aus dem privaten Schlüssel errechnet werden (100e Jahre)
- Verteilung über öffentlich zugängliche Verzeichnisse
- Beispiel: Bürgerkarte
 - A-Trust-Verzeichnis
 - Öffentlicher Schlüssel des Bürger kann gesucht werden
- Zertifikat
 - Digitaler Ausweis, der Schlüssel und Identität gegenüberstellt

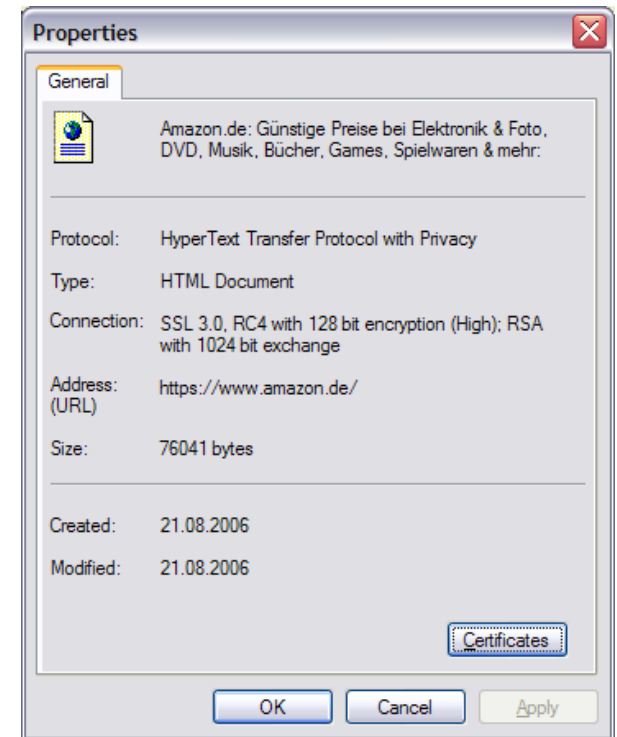
Demo: Zertifikat

- Typische Zertifikate:
 - Webserver
 - Datenverschlüsselung
 - E-mail-Sicherheit
- Inhalt und Felder von Zertifikaten
- X.509v3-Standard
 - Pflichtfelder
 - Erweiterungen



Anwendungsbeispiel: Webshop

- Demo und Details: Was steckt hinter einer https-Verbindung?
- Benutzer überprüft Server-Zertifikat
 - Demo Server-Zertifikat
 - Warum ist das sicher? Was sind mögliche Risiken?
- Benutzer und Server einigen sich auf Verschlüsselungsstärke
 - Geschichte: Export-Beschränkungen, alte Browser
 - Erzeugen eines "Session-Key"
- Verschlüsselte Session



Kryptographie und Kryptoanalyse

- Wie würden Sie versuchen, verschlüsselten Text zu "knacken"?
- Schwächen von sprachbasierter Kryptographie
- Strategie abhängig von vorhandenen Informationen
 - Nur verschlüsselter Texte
 - Verschlüsselter plus unverschlüsselter Text (oder Teile)
- Ziel?
 - Knacken des Schlüssels oder nur einer Botschaft?
 - Mithören oder verändern
 - Denial of Service
- Angriffe "um die IT-Security herum": Think simple!
 - Social Engineering
 - Daten vor der Verschlüsselung anders abfangen

Absolute Sicherheit...

- ... ist technisch möglich
 - Lösung: One-Time-Pad
 - Schlüssel wird nur einmal verwendet
- Praktisches Problem:
 - Schlüsselverteilung
 - Datenmenge
- Absolute Sicherheit versus "Computational Security"
 - Wie lange muss ein Schlüssel sicher sein?
- Praktische Kryptographie braucht nicht nur sichere Algorithmen, sondern auch:
 - Umsetzbare Protokolle



Protokolle

Was ist ein Protokoll?

- Wie teilt man eine Pizza gerecht?
 - Alice schneidet
 - Bob wählt
 - "Cut and choose protocol"
- Wie vergewissert man sich, dass der andere der der ist, der er vorgibt zu sein – ohne ihn zu sehen?
- Wie wirft man eine virtuelle Münze?
- Welche Fehler und Lücken kann ein Protokoll haben?
- Kann man einen Schlüssel austauschen, ohne ihn auszutauschen ;-)?

Wozu braucht man Protokolle?

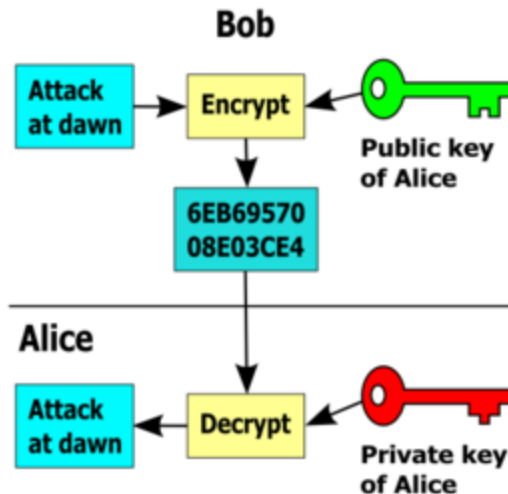
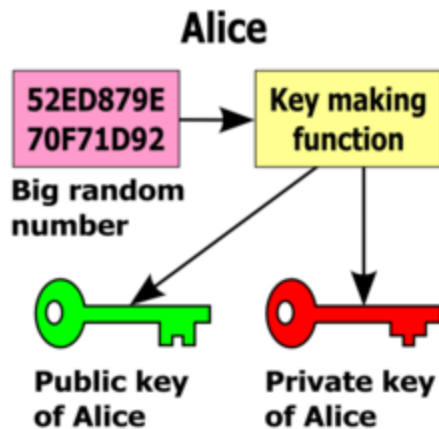
- Kein direkter Kontakt zwischen Alice und Bob
- Gerechtigkeit
- Keine Chance zum Schwindeln für Alice und Bob
- Keine Chance zum Mithören für Eve
- Keine Chance zum Eingriff für Mallory
- Alice und Bob kommen an eine Grenze
 - Vertrauenswürdiger Dritter nötig: Trent
 - Trent kann ebenfalls korrupt sein, abgehört oder angegriffen werde.

Das "Koffer-Schloss-Protokoll"

- Alice bringt ihr Schloss auf ihrem Koffer an und sendet den Koffer an Bob
- Bob bringt zusätzlich sein Schloss an und sendet den Koffer zurück an Alice
- Alice nimmt ihr Schloss ab und sendet den Koffer wieder an Bob
- Bob nimmt sein Schloss ab und öffnet den Koffer
- Mathematik: Operationen müssen kommutativ sein.

Ver- und Entschlüsselung | Variante 1

1. Alice sucht den **öffentlichen** Schlüssel von Bob in einem öffentlichen Verzeichnis
2. Alice verschlüsselt die Daten mit dem öffentlichen Schlüssel von Bob (asymmetrisch)
3. Alice sendet die verschlüsselten Daten an Bob
4. Bob entschlüsselt die Daten mit seinem **privaten** Schlüssel
5. Bob kann die Daten lesen



Bildquelle:
http://en.wikipedia.org/wiki/Public-key_cryptography

Ver- und Entschlüsselung | verbessert

1. Alice verschlüsselt Daten mit Ihrem symmetrischen Schlüssel
2. Alice sucht den öffentlichen Schlüssel von Bob in einem öffentlichen Verzeichnis
3. Alice verschlüsselt den Datenverschlüsselungsschlüssel mit dem öffentlichen Schlüssel von Bob (asymmetrisch)
4. Alice sendet die verschlüsselten Daten an Bob
5. Bob entschlüsselt den symmetrischen Dateiverschlüsselungsschlüssel mit seinem privaten Schlüssel
6. Bob kann die Daten lesen.

Signatur | Variante 1

1. Alice verschlüsselt Daten mit Ihrem **privaten** Schlüssel
2. Alice sendet die verschlüsselten Daten an Bob
3. Bob sucht in einem öffentlichen Verzeichnis nach dem **öffentlichen** Schlüssel von Alice
4. Bob entschlüsselt die Daten mit dem öffentlichen Schlüssel von Alice
5. Lassen sich die Daten entschlüsseln = ergibt der Text einen Sinn, weiß Bob
 - o dass die beiden Schlüssel von Alice zusammenpassen
 - o dass die Daten von Alice stammen müssen
 - o dass die Daten während des Transportes nicht verändert worden sind.

Signatur | verbessert

1. Alice erstellt einen **Fingerprint / Hashwert** der Daten
2. Alice verschlüsselt den Hashwert mit Ihrem **privaten** Schlüssel
3. Alice sendet an Bob:
 - o die Daten im Klartext
 - o den verschlüsselten Hashwert (inkl. Angabe der genauen Hash-Methode)
 - o ihr Zertifikat mit ihrem öffentlichen Schlüssel
4. Bob entschlüsselt den Hashwert mit dem öffentlichen Schlüssel von Alice
5. Bob erstellt mit der gleichen Hashmethode einen Hashwert der Daten.
6. Bob vergleicht die beiden Hashwerte. Sind sie gleich, weiß er, dass die Daten von Alice stammen und dass sie unterwegs nicht verändert worden sind.

Schlüsselaustausch

- Alice und Bob senden einander ihre öffentlichen Schlüssel
- Will Alice oder Bob die Kommunikation starten
 - erstellen sie jeweils einen zufälligen Session-Schlüssel
 - Verschlüsseln ihn mit dem öffentlichen Schlüssel des anderen
 - und verschicken den verschlüsselten Schlüssel
- Nur der Empfänger kann den Session-Schlüssel entschlüsseln.
- Risiken? Schwächen?

Man-in-the-Middle

- Alice will Ihren öffentlichen Schlüssel an Bob schicken
- Mallory fängt die Botschaft ab und ersetzt Alice's Schlüssel durch seinen
- Vice versa für Bob's Versuche, Alice seinen Schlüssel zu schicken.
- Ab jetzt täuscht Mallory vor:
 - Gegenüber Alice: Bob zu sein
 - Gegenüber Bob: Alice zu sein
- Alice → Bob:
 - Alice verschlüsselt in Wirklichkeit mit Mallory's Schlüssel
 - Mallory fängt die Botschaft ab, entschlüsselt sie mit seinem privaten Schlüssel
 - Er verschlüsselt sie neu mit Bob's öffentlichem Schlüssel und schickt sie weiter an Bob
 - Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel.
- Gegenmaßnahmen?

Interlock-Protokoll

- Alice und Bob senden einander ihre öffentlichen Schlüssel (Mallory kann diese ersetzen)
- Alice verschlüsselt eine Botschaft mit Bob's öffentlichem Schlüssel und schickt die Hälfte der verschlüsselten Botschaft an Bob, Bob vice versa
- Jeder schickt die zweite Hälfte, die kompletten Botschaften können zusammengesetzt werden
- Warum wird Mallory ausgetrickst?
 - Die Botschaft kann erst entschlüsselt werden, wenn beide Hälften angekommen sind (Block-Verschlüsselung, jeder Bock geteilt)
 - Mallory kann die halben Botschaften noch nicht entschlüsseln sondern müsste sie komplett durch andere Botschaften ersetzen
 - Mallory müsste die Art der Kommunikation zwischen Alice und Bob sehr genau kennen.

Rolle von Trent

- Begriffe
 - Zertifizierungsstelle | Certification Authority, CA
 - Key Distribution Center | KDC
 - Key Escrow
- Trent = KDC, CA
- Zertifikate sind signierte Dateien,
 - Die den öffentlichen Schlüssel enthalten
 - Verbindlich darüber Auskunft geben, wem der öffentliche Schlüssel gehört
- Keine Chance für Mallory

Schlüsselaustausch | Beispiel Webshop

- Alice (Benutzer) möchte mit Bob (Webserver) Daten austauschen und fordert dessen öffentlichen Schlüssel an
- Bob sendet Alice seinen öffentlichen Schlüssel
- Alice überprüft den Schlüssel durch Anfrage bei Trent
- Alice erstellt einen Session-Schlüssel und sendet ihn an Bob, verschlüsselt mit seinem öffentlichem Schlüssel
- Bob entschlüsselt den Session-Schlüssel mit seinem privaten Schlüssel
- Für eine gewisse Zeit ("Session") wird dieser Schlüssel für symmetrische Verschlüsselung verwendet

Werfen einer virtuellen Münze I

- Protokolle als Lösung für "verteilt ablaufende Prozesse"
- Alice wirft eine Münze
- Bob soll raten (auf Kopf oder Zahl setzen)
- Wie kann Bob sicher sein, dass Alice nicht schummelt und ihm das Ergebnis korrekt mitteilt?

Werfen einer virtuellen Münze II

Realisierung:

- Alice wählt eine Zufallszahl x und berechnet Hashwert $f(x)$
- Alice schickt $f(x)$ an Bob
- (Bob kann x praktisch nicht daraus berechnen)
- Bob rät: x ist gerade oder ungerade | sendet seine Schätzung an Alice
- Alice nennt x und sendet x an Bob
- Bob berechnet $f(x)$, um sicherzugehen, dass Alice nicht geschummelt hat.

Bit Commitment

- "Wähle eine Zahl und halte sie geheim"
- "Ziehe eine Karte und merke sie Dir"
- Realisierung
 - Alice wählt "ihr Bit" b
 - Bob erzeugt eine Zufallszahl R und sendet sie an Alice
 - Alice erzeugt aus der Zufallszahl und ihrem Bit eine Botschaft und verschlüsselt sie mit einem zufälligen Schlüssel - $E_K(R,b)$
 - Alice sendet $E_K(R,b)$ an Bob
 - "Auspacken": Alice sendet den Schlüssel K an Bob
 - Bob entschlüsselt $E_K(R,b)$
 - Bob überprüft, dass die Botschaft R enthält

Zero-Knowledge Protocol

- Wie kann man jemand anderem beweisen...
 - ...im Besitz geheimer, wichtiger Informationen zu sein
 - ...ohne die Information selbst preiszugeben?
 - ...und sicherzustellen, diese Information nur an eine bestimmte Person weiterzugeben? (Beobachter des Protokoll-Vorganges dürfen sich nicht sicher sein)
- Modell: Geheimes Tor in einer Höhle mit zwei Zugängen
 - Peggy ist im Besitz des geheimen Kennwortes
 - Victor steht am Eingang
 - Peggy nähert sich dem Tor von rechts oder links (Zufall | 50%)
 - Victor ruft "Rechts!" oder "Links" = wo Peggy die Höhle verlassen soll (Zufall | 50%)

Höhlenbeispiel

- Victor hört nicht, wenn Peggy das Kennwort sagt
- Der Test wird mehrmals wiederholt. Kennt Peggy das Kennwort nicht, ist die Wahrscheinlichkeit sehr klein, dass Victor immer die Seite aufruft, auf der Peggy gerade steht.
- Carol (die "third party") kann durch ein Video des Vorganges nicht überzeugt werden.

Mathematisches Gegenstück

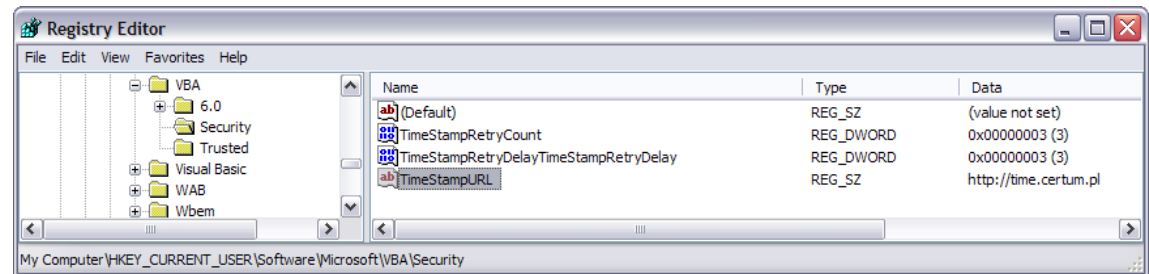
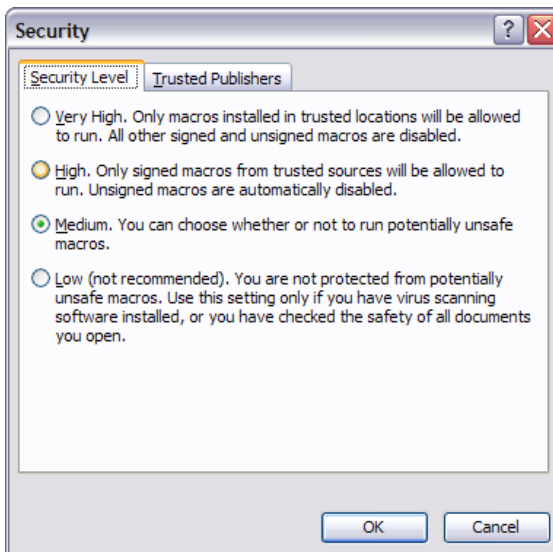
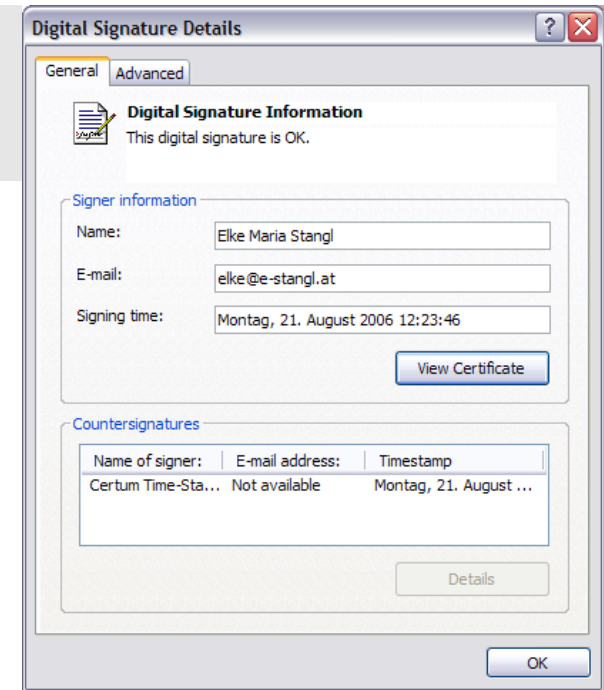
- Peggy kennt die Lösungsmethode für ein "hard problem"
- Nebenbermerkung: Isomorphe Probleme
- Peggy verwendet ihre geheime Information und eine Zufallszahl, um die Problemstellung in eine isomorphe Problemstellung zu transformieren. Sie löst das isomorphe Problem.
- Peggy behält die Lösung für sich, unter Nutzung von "Bit Commitment"
- Peggy nennt Victor die isomorphe Problemstellung, der sie nicht "rücktransformieren" kann.
- Victor bittet Peggy (50%!)
 - Entweder: die Isomorphie zu beweisen
 - Die "committede" Lösung aufzudecken und zu zeigen, dass das eine Lösung des isomorphen Problems ist
- Der Vorgang wird n mal wiederholt.

Zeitstempel

- Bedeutung
 - Zeitstempel wichtig für rechtliche Bedeutung einer Signatur
 - Zeitstempel wichtig für rückwirkende Bestimmung der Gültigkeit (Beispiel: Makrosignatur in MS Office)
 - "Replay Attacks": Wiederverwendung einer Botschaft
- "Notarielle Beglaubigung"
 - Notar (Trent) soll keine Kopie des Dokumentes erhalten
- Realisierung
 - Alice erzeugt einen Hashwert der Datei
 - Alice sendet den Hashwert an Trent
 - Trent fügt Datums- und Zeitwert aus einer "offiziellen" Zeitgebers (Atomuhr...) an und signiert alles gemeinsam
 - Alice erhält den signierten Hash + Zeitangabe retour

Demo: Makrosignatur

- Begriffe | Komponenten
 - VBA-Makro in Microsoft Outlook als Beispiel
 - Für Makrosignatur geeignetes Zertifikat
 - Trusted Publisher
 - Makrosicherheitseinstellungen
 - Zeitstempeldienst, Konfiguration





Authentifikation | Umsetzung

Problemstellung

- "System" verlangt die eindeutige Identifikation
- Frage 1: Wer bist Du?
 - Benutzername, Maschinenname
- Frage 2: Kannst Du das beweisen?
 - Eingabe eines Kennwortes oder
 - Verwendung eines geheimen Schlüssels
- Authentifikation führt zur Identifikation, wenn die Ausgabeprozesse für Passwörter und Karten ausreichend sicher sind.
- Authentifikation ist die Basis für Authorisation

Herausforderungen

- Eindeutige Kennzeichnung einer Person (oder einer Maschine) in unterschiedlichen Kontexten:
 - Als Bürger eines Staates: "Bürgerkarte" ähnlich Personalausweis)
 - In ihrer Rolle in einer Organisation: "elektronische Prokura")
 - als Berechtigte(r) für eine bestimmte "privilegierte Tätigkeit":
Führerschein
- Keine (einfache) Rückverfolgbarkeit im Sinne von Rasterfahndung (Datenschutz)
- Gültigkeitsbereich:
 - Internationale Gültigkeit, zumindest Europa-weit. Beispiel:
Rechnungslegung
 - Gültigkeit von "privaten" Zertifikaten einer Organisation außerhalb von dieser.
- Verwaltungsaufwand für immer mehr Karten, Zertifikate etc.

Beispiel Bürgerkarte

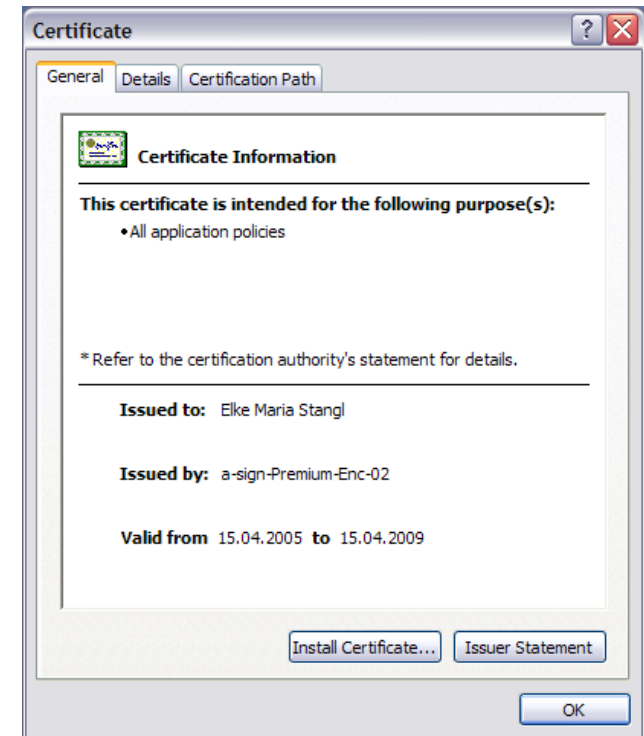
- Juristisch-organisatorischer Hintergrund:
 - Signaturgesetz und Signaturverordnung
 - Certificate Policy und Practice Statement
 - Jedes Zertifikat ist nur so vertrauenswürdig wie die Ausgabeprozesse sicher sind!
- A-Trust, RTR, Registrierungsstellen
- Validierbarkeit für 33 Jahre
- Gewährleistung der Dienste, auch wenn A-Trust den Signaturdienst einstellen würde

Sichere Signatur

- ... ist mehr als nur "die Karte selbst"
- (Erinnerung: Protokolle!)
- Sichere Anwendungen: Secure Viewer
 - WYSIWYS: What You Sign is What You See
- Sicherer Transfer der Signatur-Daten im PC
 - Kartenleser mit eigenem PIN-Pad

Demo: Bürgerkarte

- Zertifikatsinhalte
- Qualifiziertes versus fortgeschrittenes Zertifikat
- Verwendung in unterschiedlichen Applikationen
- Softwarekomponenten:
 - Zertifikatsfähige Applikation
 - Bürgerkartenumgebung
 - Management-Software
 - Cryptographic Service Provider



Ausgabe | Zertifikatserstellung

- Schlüsselpaar wird lokal auf der Karte erstellt
 - Alternative zur Karte: Software-Zertifikate: Erstellung in einem wieder verschlüsselten Container auf der Festplatte)
- Erstellung erfolgt..
 - durch den Benutzer selbst
 - oder einen vertrauenswürdigen "Registration Officer" im Beisein / nach einer persönlichen Überprüfung des Benutzers
- Der private Schlüssel verbleibt i.A. immer auf der Karte und verlässt diese nie
 - Ausnahme: Key Escrow, Key Recovery → nicht erlaubt für reine Signaturzertifikate
- Der öffentliche Schlüssel wird gemeinsam mit Identitätsdaten des Benutzers an eine Zertifizierungsstelle geschickt
- Die Zertifizierungsstelle stellt das Zertifikat aus und schickt die Zertifikatsdatei an die beantragende Stelle
- Das Zertifikat wird auf der Karte oder im Benutzerprofil "installiert"

Verwendung der Karte (Demo)

- FinanzOnline
- Sozialversicherungsportal
- E-mail-Signatur und –Verschlüsselung
- Banküberweisungen
- PDF-Signatur (z.B. für elektronische Rechnungen)
- (Wenn Zeit bleibt)
 - Wechselseitige Authentifikation von Benutzer und Webserver (https, SSL)
 - Beispiel: Verwendung der Bürgerkarte, um Benutzer am firmeneigenen Webportal anzumelden.

Widerruf und Lebensende

- Zertifikate sind öffentliche Dateien und können nicht "zurückgeholt" werden.
- Geht eine Karte verloren, wird das Zertifikat "widerrufen", um Missbrauch zu verhindern
- Widerruf: Seriennummer der Karte kommt auf eine "Schwarze Liste"
- Applikation muss die Einträge der Widerrufsliste bei der Validierung des Zertifikates prüfen.
- Jedes Zertifikat hat eine begrenzte Lebensdauer, Erneuerung bedeutet de facto: Ausgabe eines neues Zertifikates (+ Signatur des Antrags mit dem vorhandenen Schlüssel)

Demo Widerrufsliste

- Herunterladen einer Widerrufsliste von ldap.a-trust.at



Moderne Algorithmen und Methoden



RSA, Diffie-Hellman

Sichere Algorithmen...

- ...sind:
 - Veröffentlicht
 - Theoretisch auf Schwachstellen geprüft
 - Praktisch getestet.
- Die schlechtere Option: "Security by Obscurity"

Diffie-Hellman

- Schlüsselaustausch ohne Schlüsselaustausch
- Mathematisches Analogon zum "Koffer-Schloss-Protokoll"
- Herausforderung: Umkehrbarkeit
- Whitfield Diffie und Martin Hellman: 1976
- Ideen:
 - One-way-Funktionen
 - Modulare Arithmetik

Modulare Arithmetik

- Uhrenarithmetik
- Umkehrbarkeit?
- Beispiel:
 - $3^x \bmod 7 = 1 \quad x = ?$
 - $3^5 \bmod 7 = 243 \bmod 7 = 5$
 - Durch Probieren: $x = 6$
- Große Zahlen $4711^x \pmod{420815} = 666$
 - Probieren wird schwierig
 - → Computational security
 - Problem der Berechnung diskreter Logarithmen

DH-Verfahren

1. Alice und Bob wählen je eine geheime Zahl (A, B)
 2. Alice und Bob einigen sich öffentlich auf zwei Zahlen Y und P (mit $Y > P$)
 3. Alice berechnet $Y^A \bmod P = a$ | Bob berechnet $Y^B \bmod P = b$
 4. Sie tauschen die Ergebnisse öffentlich aus
 5. Alice berechnet $b^A \bmod P$ | Bob berechnet $a^B \bmod P$
 6. Beide erhalten das gleiche Ergebnis (Verwendung von (*)):
$$b^A = [Y^B \bmod P]^A = [Y^{BA} \bmod P] = [Y^A \bmod P]^B = a^B$$
 7. ... das somit als gemeinsamer Schlüssel verwendet werden kann!
 8. Voraussetzung: Kommutative Operation
 9. Eve müsste aus a und b auf A und B rückschließen...
 10. ... was aufgrund der praktischen Unumkehrbarkeit sehr aufwändig ist.
- (*) *Kommutativgesetz: $a \bmod n * a \bmod n = a * a \bmod n \bmod n = a^2 \bmod n$*

RSA: Rivest-Adleman-Shamir

- Ron Rivest, Adi Shamir, Len Adleman 1977
- Bereits 1973 durch Clifford Cocks beschrieben: "classified", Government Communications Headquarters
- Patentierter Algorithmus (bis 2000)
 - vermarktet von RSA Security Inc.
 - Patent ursprünglich verletzt durch erste Versionen von PGP (Pretty Good Privacy) von Phil Zimmermann

Zahlentheorie

- Euler'sche Phi-Funktion: $\Phi(n)$ = Anzahl der zu n teilerfremden Zahlen kleiner als n
- Ist n eine Primzahl, ist $\Phi(n) = n - 1$
- Ist n das Produkt zweier verschiedener Primzahlen p und q ist $\Phi(n) = (p - 1)(q - 1)$
(n kann nur die Teiler p und q gemeinsam haben \rightarrow mögliche Teiler sind alle Vielfachen von p : p mal 1 bis p mal $(q - 1)$...)
- Inverse modulo n = diskrete Logarithmen
 - $1 = (ax) \bmod n \Leftrightarrow a^{-1} \equiv x \pmod{n} \Leftrightarrow a^{-1} \bmod n = x \bmod n$
- Satz von Euler-Fermat: $a^{\Phi(n)} \bmod n = 1$
- \rightarrow Berechnung $x = a^{\Phi(n)-1} \bmod n$

RSA-Verfahren

1. Erzeugung großer (zufälliger) Primzahlen $p \neq q$
2. Berechnung von $n = p * q$
3. Euler-Funktion $\Phi(n) = (p - 1)(q - 1)$
4. Auswahl von e mit $1 < e < \Phi(n)$, teilerfremd zu $\Phi(n)$
 $e, n \dots$ öffentlicher Schlüssel
5. Berechnung von d mit: $d * e \equiv 1 \pmod{\Phi(n)}$
 $d \dots$ privater Schlüssel
6. Verschlüsselung einer Botschaft M
 $C = M^e \pmod{n}$
7. Entschlüsselung
 $C^d \pmod{n} = (M^e)^d \pmod{n} = M^{ed} \pmod{n}$
 $C^d \pmod{n} = M^{k(p-1)(q-1)+1} \pmod{n} = M * M^{k(p-1)(q-1)} \pmod{n}$
 $C^d \pmod{n} = M * M^{k*\Phi(n)} \pmod{n} = M * 1$ [Euler-Fermat]

Sicherheit von RSA

- e kann standardisiert werden:
 - Für e werden aus Performance-Gründe oft bestimmte Werte gewählt, z.B. $65537 = 2^{16} + 1$ (nur zwei "1er", einfachere Potenz-Operationen)
 - Zusätzlich werden Zufallszahlen an die Message-Blöcke angehängt (auch zur Vermeidung "schwacher M")
- Ermittlung von p, q aus n und e ist extrem langsam:
 - RSA Factoring Challenge
 - Stand: n mit 200 dezimalen Stellen faktorisiert während Äquivalent von 55 Jahren, 2GHz Prozessor
 - Ca. 450 bit
- Derzeit gilt
 - 1024 bit für sicher bis ca. 2010
 - 2028 bit als sicher bis ca. 2030
 - Siehe z.B. www.keylength.com

Zwei Schlüsselpaare

- Empfehlung: verschiedene Schlüsselpaare für Verschlüsselung und Signatur
- Verschiedene Behandlung von Schlüsseln
 - Key Escrow nur für Verschlüsselungsschlüssel
 - Signaturschlüssel darf nur einmal existieren: Vergleichbar mit Fingerabdruck.
- Bei Verlust eines reinen Signaturschlüssels gehen keine Daten verloren
- Implementierung z.B.
 - Signaturschlüssel wird lokal erstellt und bleibt beim Benutzer
 - Verschlüsselungsschlüssel wird zentral erstellt und dem Benutzer zugesendet, verschlüsselt mit dessen öffentlichen Schlüssel.
- Außerdem: Mögliche Angriffsflächen je nach Protokoll

Angriff durch Bestätigung

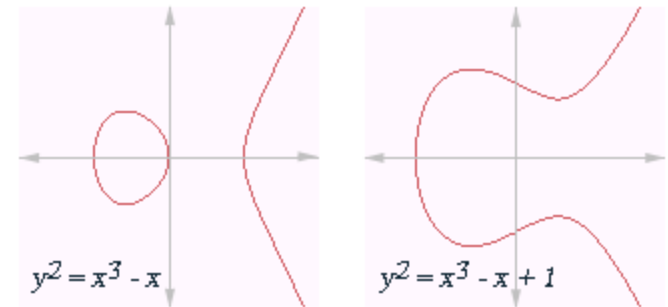
- o Angriff auf doppelt verwendetes Paar, wenn eine Bestätigung verwendet wird (S_x ist jeweils = D_x , V_x ist jeweils = E_x)
 1. Alice signiert und verschlüsselt für Bob: $E_B(S_A(M))$
 2. Bob entschlüsselt und verifiziert: $V_A(D_B(E_B(S_A(M))))$
 3. Bob signiert und verschlüsselt für Alice als Bestätigung: $E_A(S_B(M))$
 4. Alice entschlüsselt, verifiziert und vergleicht
 5. Mallory jubelt Bob Alice's Botschaft unter, die Entschlüsselung ergibt für Bob keinen Sinn:
 $V_M(D_B(E_B(S_A(M)))) = E_M(D_B(E_B(D_A(M)))) = E_M(D_A(M))$
 6. Bestätigung von Bob an Mallory:
 $E_M(S_B(E_M(D_A(M)))) = E_M(D_B(E_M(D_A(M))))$
 7. Mallory erhält M durch $D_M \rightarrow E_B \rightarrow D_M \rightarrow E_A$

Signatur nach Verschlüsselung

- Üblich: Verschlüsselung nach Signatur. (Achtung – Virens Scanner!)
- Attacke auf RSA, wenn umgekehrt:
- Alice verschlüsselt für Bob und signiert dann:
 - $(M^{e_B} \bmod n_B)^{d_A} \bmod n_A$
- Bob behauptet, eine andere Nachricht M' erhalten zu haben
 - Da er die Primfaktorzerlegung von n kennt, kann er relativ ein x finden (diskreten Log. berechnen) mit $M'^x = M \bmod n_B$
 - Er behauptet, sein "neues e " ist $= x * e_B$, das Alice angeblich verwendet hat.

Elliptische Kurven

- Punkte auf einer Kurve vom Typ $y^2 = ax^3 + bx + c$
- ... bilden Abel'sche Gruppe:
 - Operation: Geometrische Addition: Punkte verbinden, spiegeln
 - Kommutativ
 - Geschlossen
 - Nullelement, inverses Element
- Potenzbildung vergleichbar schwierig mit mod-Multiplikation
 - Verdopplung: Tangente durch Punkt + Spiegelung
 - $3P = 2P + P$, $4P = 3P + P$ usw.
- Praktisch verwendete Felder:
 1. Zahlen $x, y < \text{Primzahl } p$, Kurvengleichung gilt mod p
 2. x, y sind Bitstrings mit Länge m
- Derzeit gilt ein Bitstring mit $m = 160$ als sicher



Bildquelle

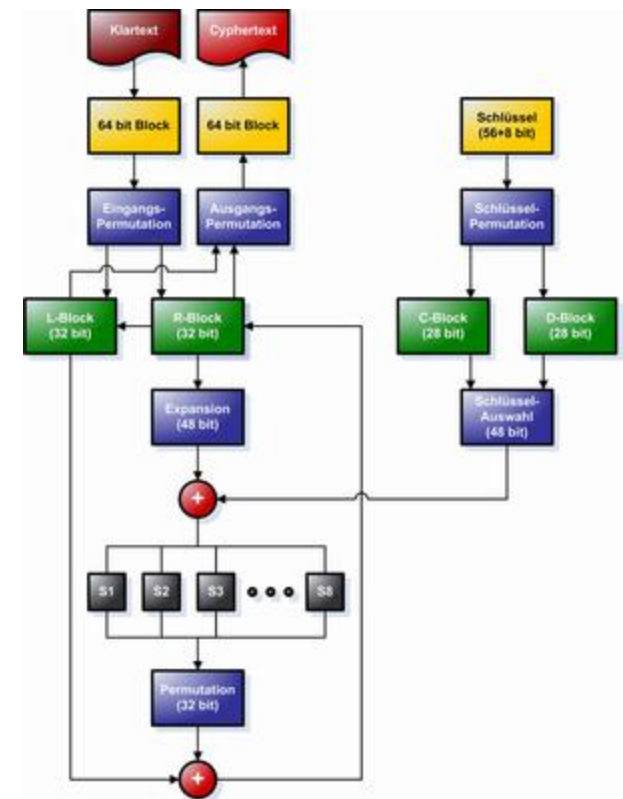
http://en.wikipedia.org/wiki/Elliptic_curve

Data Encryption Standard

- Erster standardisierter symmetrischer Algorithmus
- Von IBM für die NSA entwickelt
- Spekulationen:
 - Verkürzte Schlüssellänge auf Wunsch der NSA (56bit statt 112bit)
 - Hintertür aufgrund Designänderungen durch die NSA?
- 1998 durch Brute-Force-Attacke in 56 Stunden geknackt
- Verbesserung: 3DES
- Nachfolger-Algorithmus seit 2001: AES, Advanced Encryption Standard

DES-Verfahren | Überblick

- Teilung in 64bit-Blöcke
- 64bit-Schlüssel wird auf 56bit reduziert, Rest für Parity-Check
- 16 Runden:
 - Daten werden jeweils mit einer Variante des Schlüssel kombiniert
 - Vom Schlüssel werden pro Runde 48bit in einer anderen Reihenfolge verwendet (Compression)
 - Datenblock-Bits werden jeweils mehrfach verwendet (Expansion)
 - S-Boxen ("kleine Matrix")
- Jeweils die rechte Hälfte wird bearbeitet
- Mit der linken Hälfte kombiniert → Resultat wird die neue rechte Hälfte
- Die linke Hälfte wird die neue rechte Hälfte



Bildquelle

http://de.wikipedia.org/wiki/Data_Encryption_Standard

DES | Details I

- Ziel: Jedes Bit des Ciphertext soll von jedem Bit vom Plaintext abhängen innerhalb weniger Runden
- XOR Exclusive OR,
 - $1 \text{ XOR } 1 = 0$, $0 \text{ XOR } 0 = 0$
 - $1 \text{ XOR } 0 = 1$, $0 \text{ XOR } 1 = 1$
 - Oft verwendet, da $a \text{ XOR } b = c \Leftrightarrow b \text{ XOR } c = a$
- Schlüssel-Transformation (Compression):
 - Geteilt in zwei 28bit-Hälften
 - Jeweils um 1-2 bit weitergeschoben, je nach Runde
 - Permutation innerhalb des Key (Tabelle mit "Bauanleitung")
 - Weglassen einiger Bits
- Daten-Transformation (Expansion)
 - Wieder Tabelle als Bauanleitung, manche Bits kommen häufiger vor

DES | Details II | S-Boxen

- Substitution
- 6bit Input → 4bit Output
- Pro 6bit eine andere S-Box
- Definition einer S-Box
 - Tabelle mit 4 Zeilen und 16 Spalten
 - 6bit Input: Koordinate der gesuchten Zelle
 - In der Zelle der 4-bit-Output, auf den hin transformiert wird
- Nichtlinear
- Die wichtigste Komponente hinsichtlich Security in DES

DES-Entschlüsselung und 3DES

- Entschlüsselung: mit dem gleichen Verfahren (!) wie die Verschlüsselung.
- DES definiert keine geschlossene Gruppe, sonst wäre Mehrfachverschlüsselung sinnlos:
 $EK_2(EK_1(P)) = EK_3(P)$
- Triple-DES: Encrypt-Decrypt-Encrypt
 - Kompatibilität
 - 3x gleicher Schlüssel → entspricht Einfachverschlüsselung

DES-Nachfolger AES

- 2000 in "Wettbewerb" ermittelt
- Von der NSA für Top-Secret-Dokumente zugelassen
- Mehrere Transformationen von 4x4-Datenblöcken:
 1. Kombination mit einem Key-Block
 2. Nicht-lineare S-Box
 3. Verschieben
 4. Polynom-artige Multiplikation
- Angriffe nur möglich durch Side Channel Attacks (*)
 - Timing-Attacke: Messung der Dauer von Operationen
 - (*) Generell: Physikalische Auswirkungen der Verschlüsselungen werden überprüft

Hash-Algorithmen MD5 und SHA-1

○ MD5

- Ergänzen durch "padding" auf 512 minus 64 bit: ein 1er und Nullen. Die 64bit enthalten die genaue Länge als Zahl
- Anwendung auf 512bit-Blöcke
- 4 Start-Variablen
- 4 nicht-lineare Funktionen (AND, OR, XOR, NOT) für 4 Durchgänge
- In jedem Durchgang 16 Varianten einer Funktion → 64 Schritte
- Funktionen wirken auf: jeweils auf 3 von Eingangsvariablen, einer Konstanten (anders pro 1 von 16 Schritten), einem Teil des Plaintext-Blocks
- Hinzugefügt zur vierten Variable und einem Textblock
- Pro Schritt: Ersetzen einer Eingangsvariable, Verschieben um einige Bit

○ SHA-1

- 5 Eingangsvariablen
- Kompliziertere Funktionen
- Mehr Schritte

A decorative graphic consisting of a vertical grey line on the left side of the slide. In the center, there are two rows of circles. The top row has three circles: the first is a white circle with a grey outline, and the second and third are solid grey circles. The bottom row has three circles: the first and second are solid grey circles, and the third is a white circle with a grey outline. The text 'Schlüsselmanagement' and 'Public Key Infrastructure' is centered over the top row of circles.

Schlüsselmanagement Public Key Infrastructure

Wozu Zertifikate?

- Signieren von Rechnungen (fortgeschrittene Signatur)
- Verschlüsseln von Daten auf Notebooks
- Signatur von ausführbaren Programmen, z.B. Office Makros
- Aussperren von "verseuchten fremden Computern" aus dem Netzwerk
- Anmelden am PC mit Chipkarte
- Anmelden über das Internet am Firmennetzwerk mit Chipkarte (Telearbeiter)
- Sichere drahtlose Netzwerke
-

Public Key Infrastructure (PKI)

- Beinhaltet "Trent": Vertrauenswürdige Zertifizierungsstelle(n)
- Verzeichnisse für
 - Öffentliche Schlüssel / Zertifikate von Benutzern
 - Öffentliche Schlüssel / Zertifikate von Zertifizierungsstellen
 - Öffentliche Schlüssel / Zertifikate von vertrauenswürdigen Herausgebern
 - Widerrufslisten
- Werkzeuge und Prozesse für
 - Zertifikatsausstellung, -erneuerung, -sperre, -widerruf
 - Laufende Überwachung, Überprüfung
- Clients und Applikationen
 - Private Schlüsselspeicher (unterschiedliche Algorithmen und Protokolle)

Gefahren

- Zu hoher Anspruch, "eierlegende Wollmilchsau" PKI: System bleibt "akademisch" und kann nicht verwendet werden
- Zu schnelle Umsetzung ("next – next – finish"), Unterschätzung der organisatorischen (!) Komplexität wegen vermeintlich einfach zu bedienenden technischen Kernkomponenten
- Zu kurzfristige Planung, mangelnde Dokumentation für künftige Betreuer

Bausteine

- Langfristige Planung!
- Richtlinien! Richtlinien! Richtlinien!
- Prozesse! Prozesse! Prozesse!
- Vertrauenswürdige Personen
- Hierarchie von Zertifizierungsstellen
 - Externe oder interne Zertifizierungsstellen
 - Unterordnung oder Quer-Zertifizierung
- Interne Zertifizierungsstelle
 - Besonders geschützter Computer (Server)
 - Verfügt über ein Zertifikat und ein Schlüsselpaar
 - Signiert Benutzer-Zertifikate mit ihrem privaten Schlüssel
- Anwendungen, die mit Zertifikaten umgehen können
- Clienttests! Clienttests! Clienttests!
- Verzeichnisdienst(e)
- Widerrufsdienst(e)
- Notfallplanung: Hardwareausfall oder Schlüsselkompromittierung

Hierarchie

- Zertifikat einer CA wird signiert mit dem privaten Schlüssel der übergeordneten CA
- Warum eine Hierarchie?
 - Sicherheit durch physische Abschottung
 - Delegation der Verantwortung an verschiedene Abteilungen
 - Bessere zukünftige Erweiterungsmöglichkeiten
 - Trennung nach Standorten
 - Trennung nach "Wert" von Zertifikaten
- Typische Hierarchie
 - Selbst-signierte offline Root CA
 - Offline Intermediate / Policy CA
 - Online Issuing CA: Gibt Zertifikate an Benutzer oder Maschinen aus

Szenarien

- Welche Arten von Zertifikaten könnten in Ihrer Organisation / in ihrem Umfeld benötigt werden?
- Auswahl von 2-3 Szenarien, Beispiele:
 - E-mail-Signatur und –Verschlüsselung
 - Sicheres WLAN
 - Datenverschlüsselung
 - Makroverschlüsselung
- Entwicklung des Designs der Infrastruktur für diese Szenarien (Flipchart)
 - Benötigte Komponenten
 - Routine-Prozesse: wie kommt ein Benutzer am PC zu einem Zertifikat?

Designbeispiel

- o Siehe Flipchart

Externe versus interne CA

- Intern betrieben heißt nicht automatisch: von außen nicht erreichbar
- Komponenten, die von extern erreichbar sein müssten:
 - Publikationspunkte für Widerrufslisten
 - Publikationspunkte für CA-Zertifikate
 - Verzeichnisse für Benutzerzertifikate (wenn benötigt)
- Varianten des Betriebes:
 - Zukauf einzelner Zertifikate (z.B. auch A-Trust)
 - Betrieb einer oder mehrere CAs in der Hierarchie durch Externe
 - Quer-Zertifizierung einer intern betriebenen CA durch Externe

Demo : PKI-Komponenten

- Demonstration verschiedener PKI-Komponenten

PKI-Praxis: Zertifizierungsstelle

- Eckdaten eines CA-Service
 - Schlüssellänge und Algorithmen
 - CA-Datenbank
 - Namen
- Verteilungspunkte für CA-Zertifikate und Widerrufslisten
- Physische Sicherheit
- Routine-Prozesse im Laufe des Lebenszyklus
 - Ersterstellung des Schlüssels
 - Publikation einer Widerrufsliste
 - Erneuerung des Zertifikates
 - Routine-Wartung

PKI-Praxis: HSMs

- Hardware-Schlüsselspeicher | Hardware Security Module
- Strenges Vieraugenprinzip
- Sichere Hardware
 - Privater Schlüssel verlässt die Hardware nie
 - Vergleichbar mit Smartcard für Benutzer + zusätzliche Sicherheit
 - Selbstzerstörung des Schlüssels bei versuchtem physischem Zugriff

PKI-Praxis: Verzeichnisdienst

- Standard LDAP: Lightweight Directory Access Protocol (Teil des sehr umfangreichen X.500-Standards)
- Beispiele Microsoft Active Directory, Novell NDS, iPlanet
- Begriffe:
 - Objekte, Attribute, Schema
 - Directory Partitions, Replikation
- Zertifikate und Widerrufslisten werden binär als Attribute gespeichert

PKI-Praxis: Client-Applikation

- Client-seitiger Zertifikatsspeicher
 - Eigene Zertifikate mit Schlüssel
 - Geschützter Speicher für Softwarezertifikate
 - Vertrauenswürdige Zertifikate von Zertifizierungsstellen
- Nutzung von Zertifikaten in Applikationen
 - Verweis auf Zertifikatspeicher
- Konfiguration der Zertifikatsvalidierung – Beispiele
 - Internet Explorer
 - Outlook
 - Acrobat Reader

PKI-Praxis: Client-Routine-Prozesse

- Festlegung, wer ein Zertifikat erhalten soll
 - Berechtigungen für Benutzer oder "Registration Officers"
 - Vergabe von "Officer-Zertifikaten" für privilegierte Administratoren
- Client-Prozesse
 - Ausstellung eines neuen Zertifikates: automatisch, durch den Benutzer oder durch einen Registration Officer
 - Widerruf eines Zertifikates
 - Änderung der Autorisierung auf der Basis der Daten in einem (nicht widerrufenen) Zertifikat
- Abhängige Prozesse in anderen Systemen
 - Neuer Benutzer im HR-System
 - Neue Maschine im Asset-Management

A decorative graphic consisting of five circles and a vertical line. The top row has three circles: a white circle with a grey outline on the left, a solid grey circle in the middle, and a solid grey circle on the right. The bottom row has three circles: a solid grey circle on the left, a solid grey circle in the middle, and a white circle with a grey outline on the right. A vertical grey line is positioned on the far left side of the slide.

Benutzer und Computer in Netzwerken

Kerberos und Passwortsicherheit

Zentrale Benutzer-Verwaltung

- Verwendung einer Identität, um Zugriffe auf verteilte Systeme zu ermöglichen
- Zentrale Benutzerdatenbank
 - Kerberos Realm
 - Windows Domäne
- "Netzwerk-Betriebssystem"
- Anforderung an Authentifizierung
 - Keine Speicherung von Kennwörtern im Klartext oder von exportierbaren privaten Schlüsseln
 - Nutzung auf unterschiedlichen Systemen
 - Sichere Authentifikation über (ungesicherte) Netzwerke

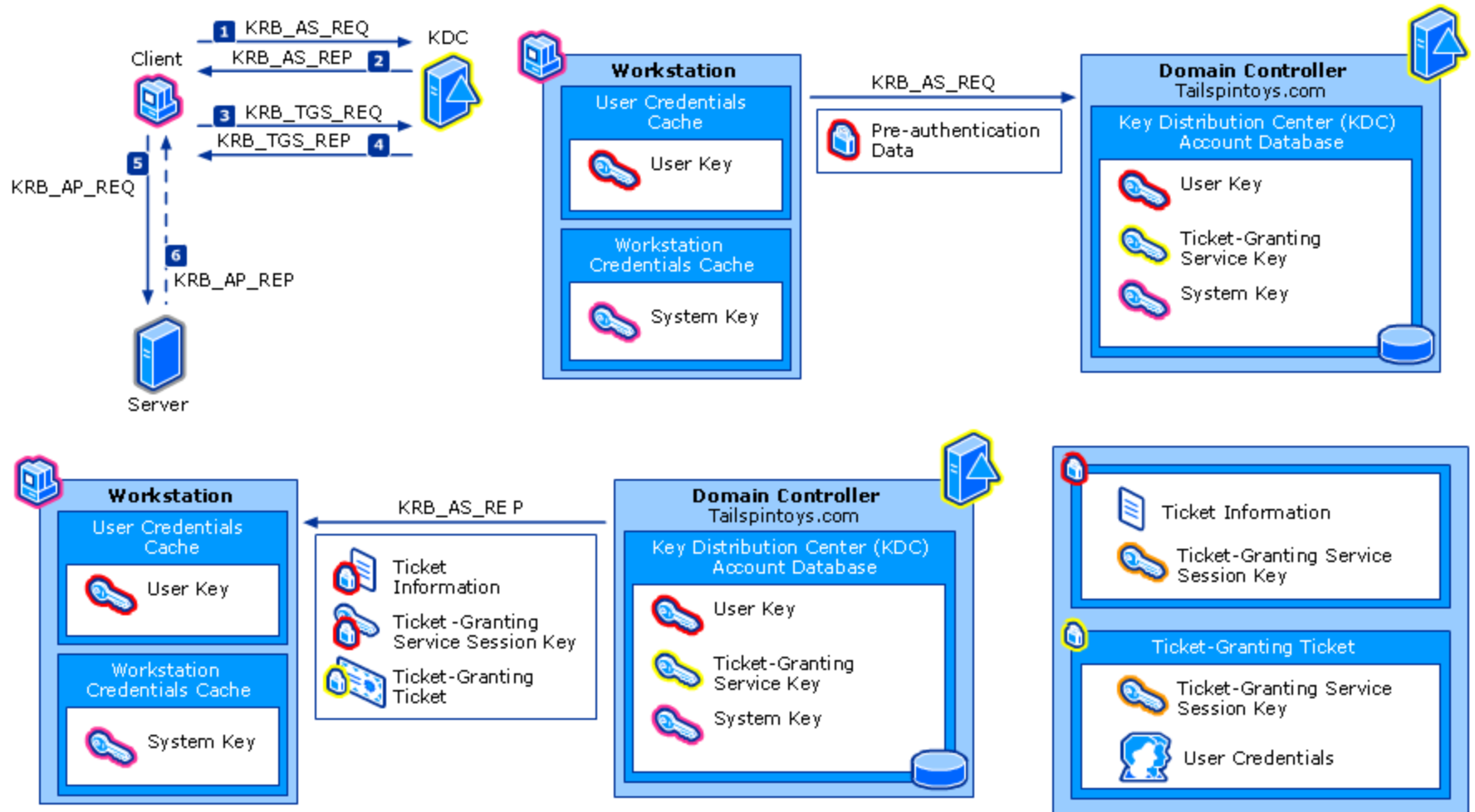
Kerberos-Protokoll

- Kerberos Distribution Center als "Trent"
 - Alice und Bob haben jeweils einen symmetrischen Schlüssel gemeinsam mit Trent
- Ablauf des Protokolles im Überblick
 1. Alice → Trent: Ihre Identität und die von Bob: A, B
 2. Trent erzeugt: Zeitstempel, Gültigkeitsdauer, zufälliger Session Key und sendet → Alice:
 $E_A(T, L, K, B)$ und $E_B(T, L, K, A)$
 3. Alice kann nur den ersten Teil entschlüsseln. Alice → Bob:
 $E_K(A, T)$ und $E_B(T, L, K, A)$
 4. Bob entschlüsselt sein (2.) Paket und mit K das erste und → Alice: $E_K(T + 1)$

Kerberos praktisch

- Benutzer und Server (Alice und Bob) haben einen langlebigen symmetrischen Schlüssel mit dem KDC gemeinsam:
 - wird durch kryptogr. Funktion erzeugt aus dem Passwort: Hashwert, verschiedene Algorithmen möglich (z.B. DES + MD5)
 - Oder: Verwendung eines asymmetrischen Schlüssel, z.B. auf einer Smartcard
- User erhalten "Tickets":
 - Ticket Granting Ticket (TGTs) zum Zugriff auf den Ticket Granting Service (TGS – Bob 1)
 - Service Tickets vom TGS zum Zugriff auf Services (Bob 2)
- $E_K(A,T)$... Authenticator, $E_B(T,L,K,A)$... Ticket

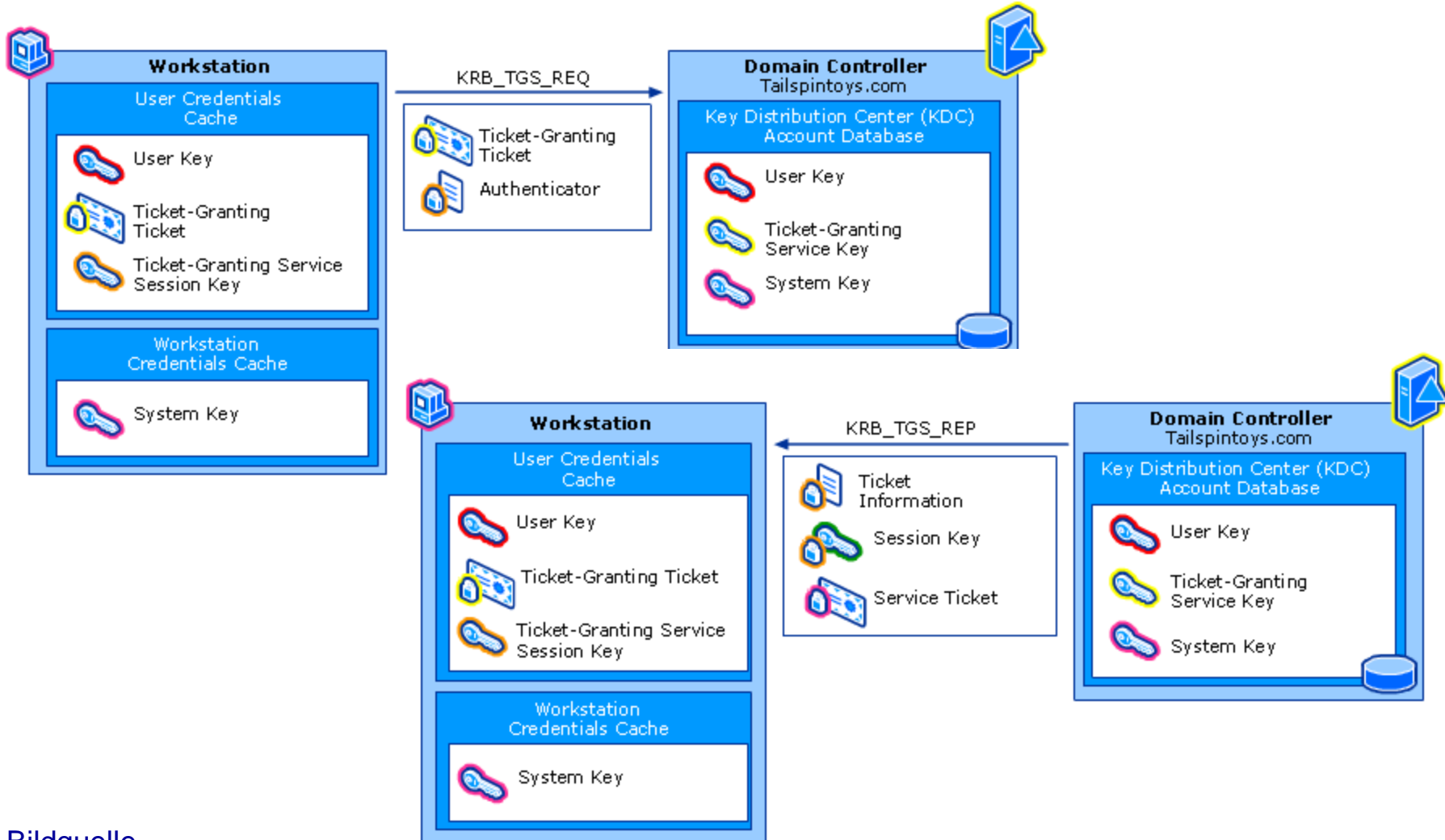
Lokale Anmeldung I



Bildquelle

<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.aspx?pf=true>

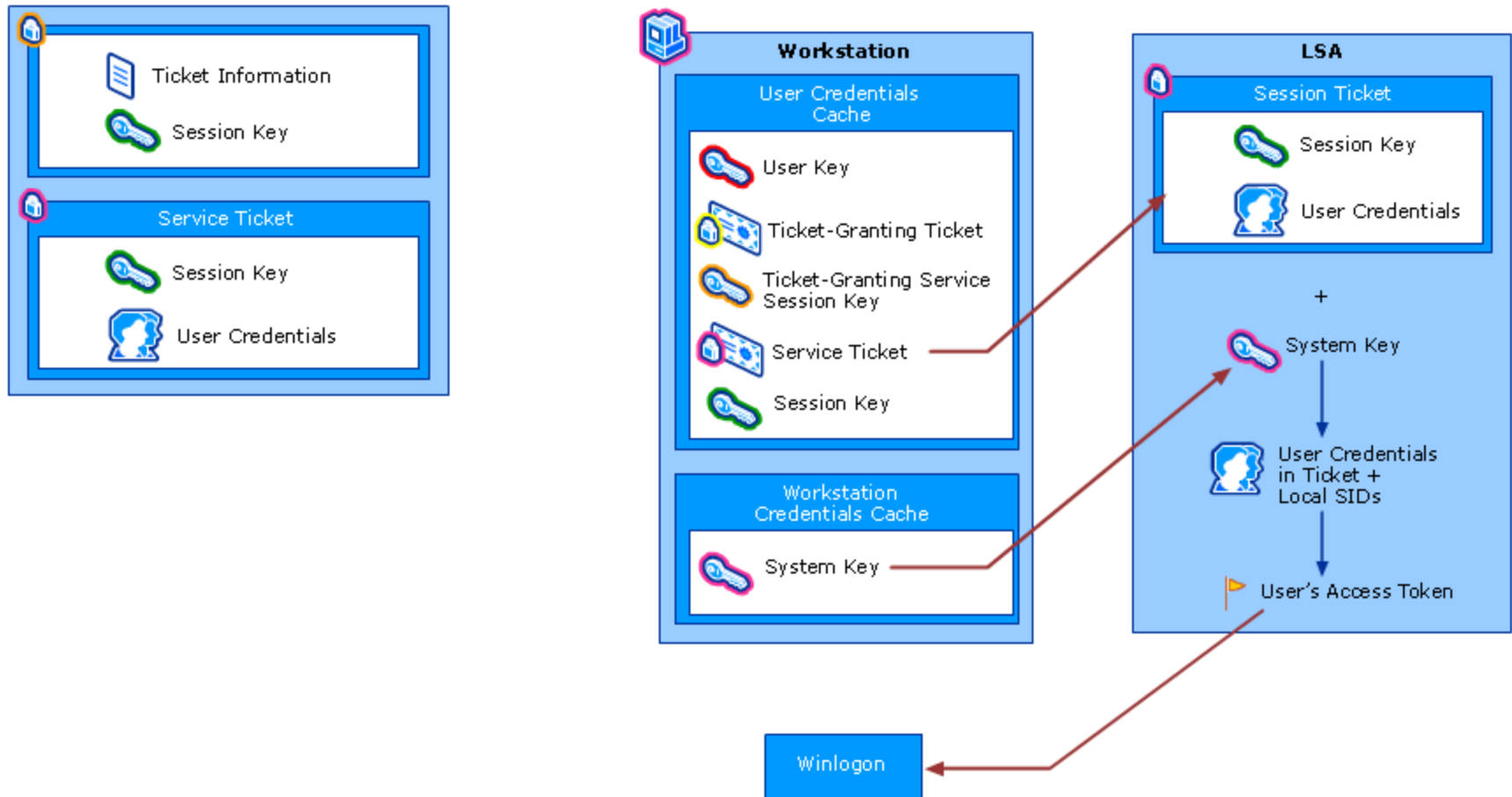
Lokale Anmeldung II



Bildquelle

<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.msp?pf=true>

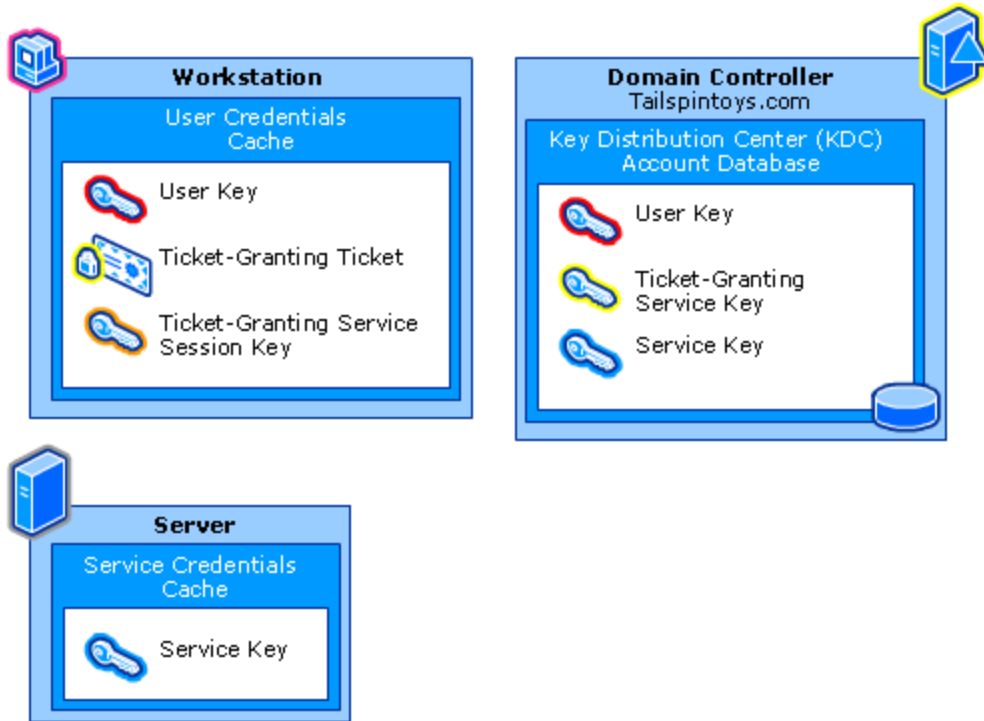
Lokale Anmeldung III



Bildquelle

<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.aspx?pf=true>

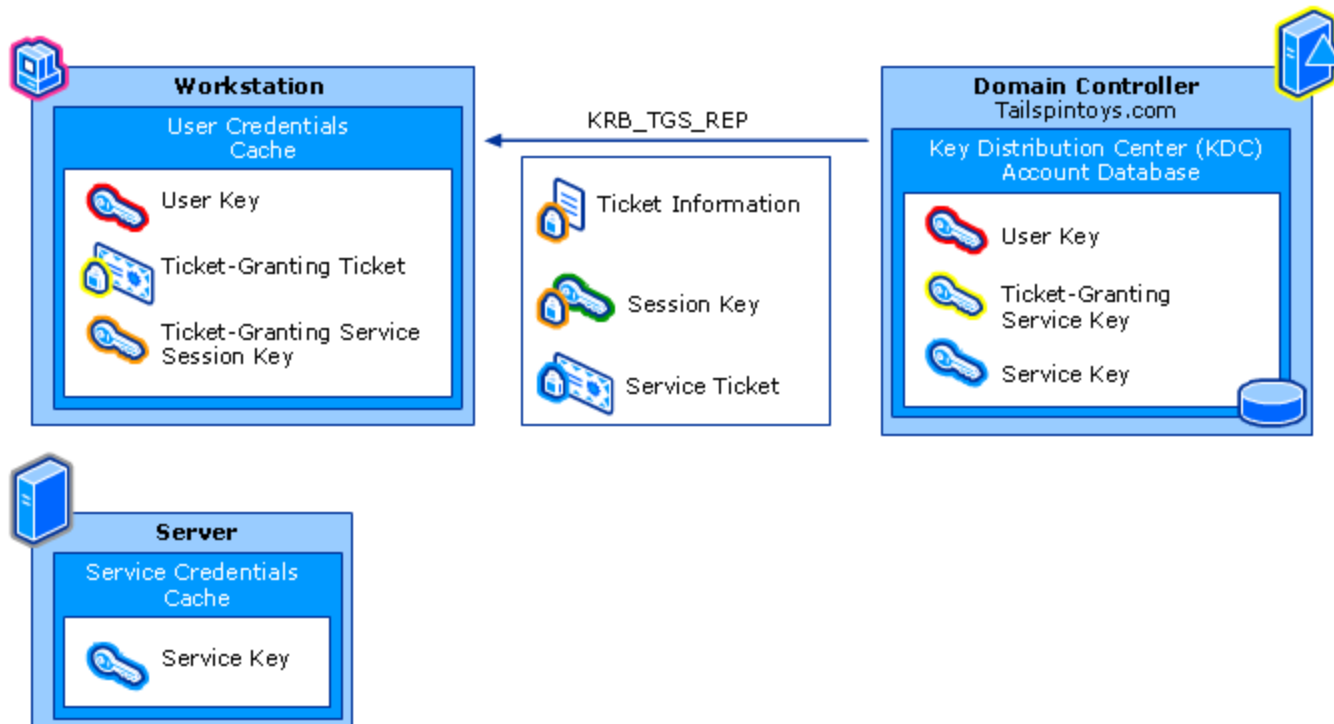
Zugriff auf anderen Server I



Bildquelle

<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.aspx?pf=true>

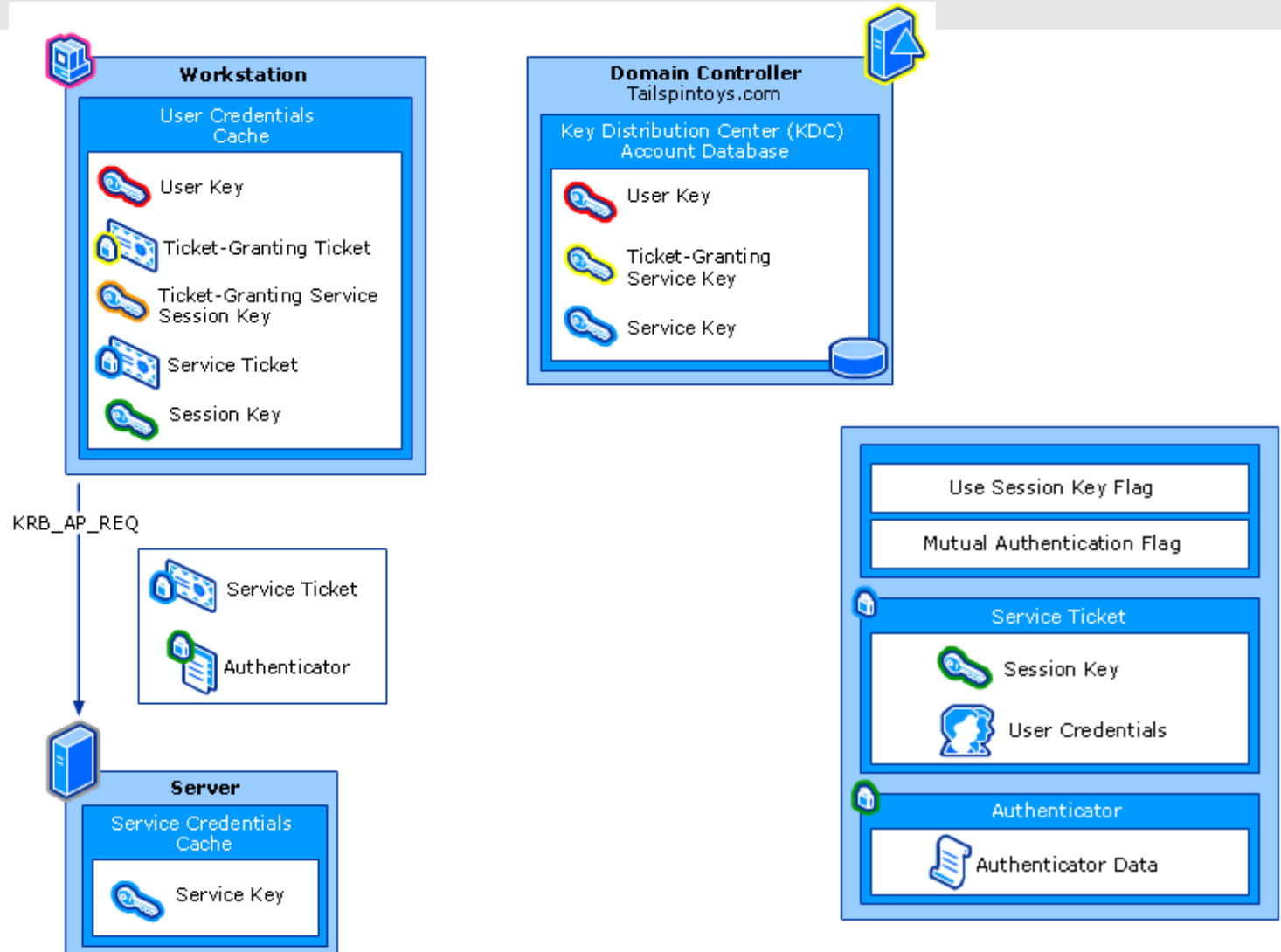
Zugriff auf anderen Server II



Bildquelle

<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.aspx?pf=true>

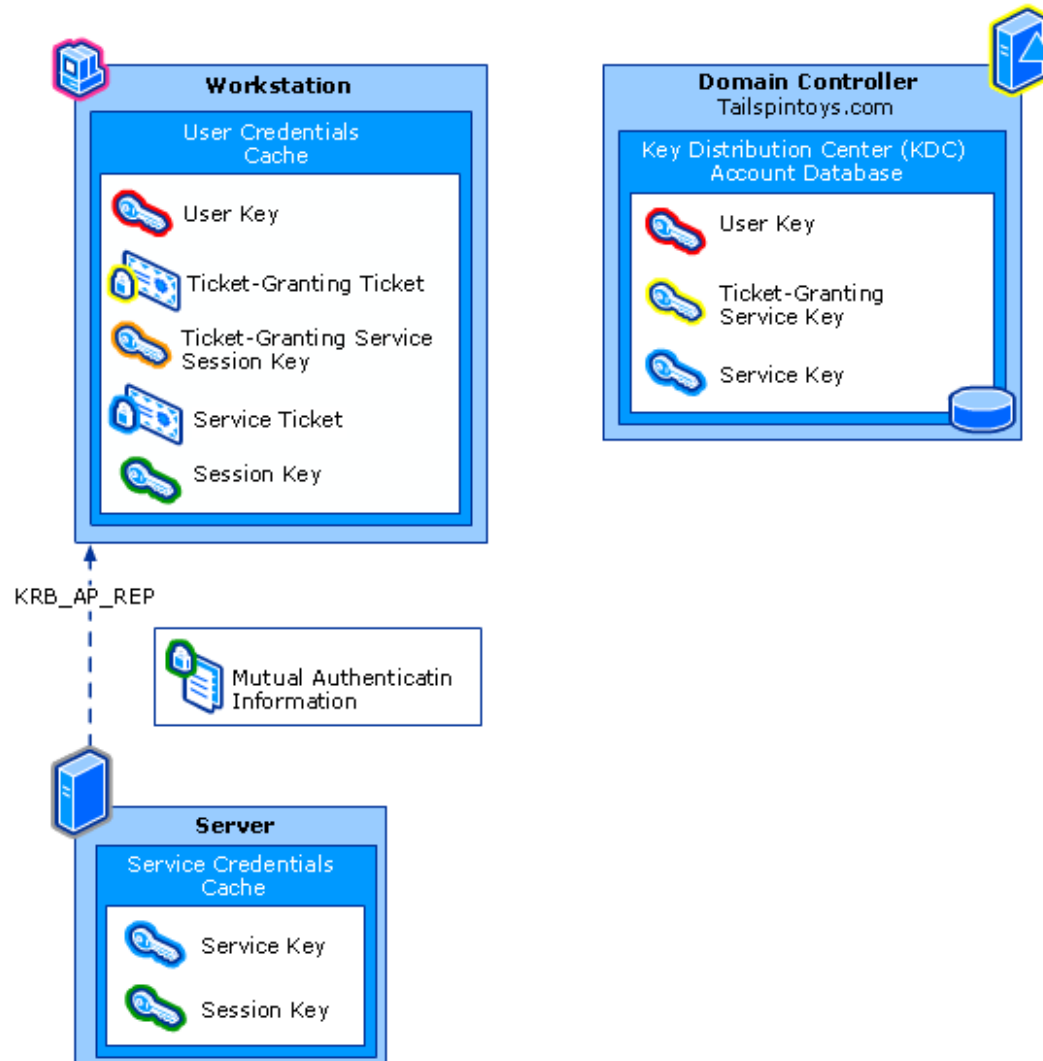
Zugriff auf anderen Server III



Bildquelle

<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.msp?pf=true>

Zugriff auf anderen Server IV



Bildquelle


<http://technet2.microsoft.com/WindowsServer/en/library/4a1daa3e-b45c-44ea-a0b6-fe8910f92f281033.msp?pf=true>

Angriffe auf Passwörter

- Brute-Force-Attacke
- Dictionary Attacke
- Rainbow Tables
- Angriffe auf den Hashwert statt auf das Passwort
 - LM-Hash aus Kompatibilitätsgründen
- Sichere Passwörter:
 - "Passphrases" statt Passwörter
 - Lang und komplex (> 7 Zeichen, wenn LM Hash verwendet)
 - Ausschalten von LM Hash
 - Häufiger Wechsel
 - Smartcards statt Passwörter

Demos: Passwörter und Logon

- Logon mit Smartcard (PKI, Kerberos)
- Passwort-Cracken mit unterschiedlichen Attacken



Sichern von Netzwerkverbindungen

IPsec, SSL, WLAN

Risiken

- "Erschnüffeln" vertraulicher Daten
- Einschleusen von Viren durch nicht "gemanagete" Geräte
- Mitnutzung von Netzwerkverbindungen (Huckepack auf fremdem WLAN)
- Vortäuschen, ein andere (vertrauenswürdiger) Gesprächspartner zu sein

Unterschiedliche Ebenen

- SSL (Secure Sockets Layer)
 - "ganz oben" auf der Ebene der Anwendung (Browser)
 - Vom Benutzer bemerkbar und überprüfbar
 - Authentifikation vom Server gegenüber einem Benutzer und wahlweise auch umgekehrt
 - Verschlüsselte Verbindung
- Wireless LAN Sicherheit
 - Authentifikation: Passwort ("Key", "Pre-Shared Secret") oder 802.1x
 - Verschlüsselung
- IPsec
 - "ganz unten"
 - Unbemerkt von Anwendungen und dem Benutzer
 - Authentifikation von Maschinen
 - Verschlüsselung und / oder Integrität

Wireless LAN | 802.11?

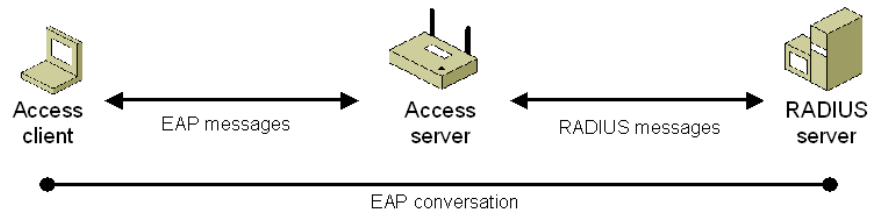
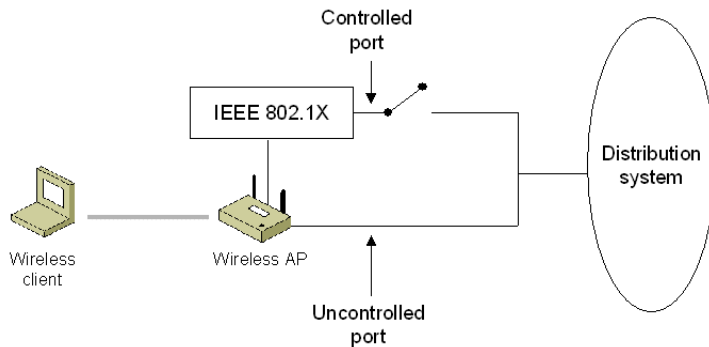
- 802.11a,b,g
 - Beschreibt Netzwerkverbindung zwischen Computer und Access Point
 - "Ethernet über drahtlose Verbindung"
 - Ermöglicht Verschlüsselung mit WEP, WPA oder WPA2
- 802.1x
 - Rahmenprotokoll für Authentifikation
 - Zusätzlich zu 802.11
 - Kann Schwächen der 802.11-Verschlüsselung ausgleichen

WLAN-Verschlüsselung

- WEP – Wired Equivalent Privacy
 - Kann mit gängigen Tools je nach Datenvolumen innerhalb kurzer Zeit geknackt werden
 - Zu kurzer Initialization Vector (IV) für RC4
 - Master-Schlüssel wird immer direkt verwendet und nie geändert
 - Schwache Identitätsprüfung
 - Datenpakete können abgefangen und wiederverwendet werden (Replay)
- WPA(2) – WiFi Protected Access (2)
 - Längerer IV
 - Neue Protokolle für Verschlüsselung (TKIP/Michael, AES) und Integrität (AES)
 - Temporäre Schlüssel werden aus Master-Schlüsseln erzeugt
 - Paket-Nummern gegen Replay-Attacken

WLAN-802.1x-Authentifikation

- WEP oder WPA(2)-Schlüssel wird für jeden Computer separat erstellt
- Maschinen und/oder Benutzer werden gegenüber einem zentralen Authentifizierungssystem wie Kerberos authentifiziert.
- WEP/WPA-Schlüssel werden nur ausgegeben und die Netzwerkverbindung hergestellt, wenn die Authentifikation erfolgreich ist.



Quelle: IEEE 802.11 Wireless LAN Security with Microsoft Windows, Microsoft

Demo: WLAN-LAN-Konfiguration

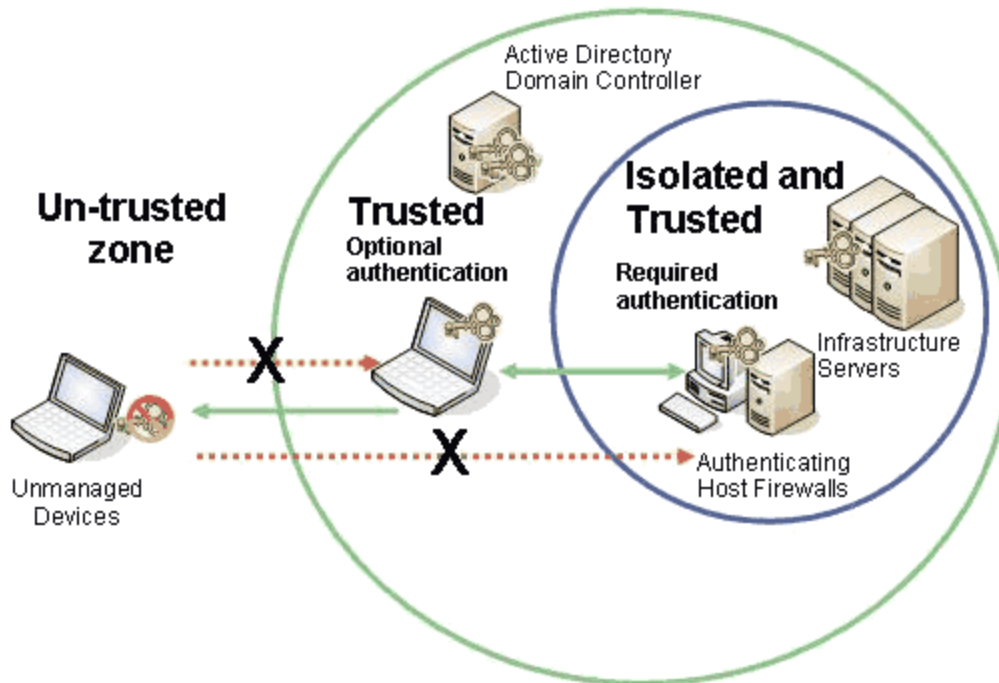
- Client-Computer-Einstellungen:
 - WEP / WPA
 - 802.1x – mit Zertifikat (EAP-TLS) oder Passwort (PEAP)
 - Überprüfung eines Server-Zertifikates
- Access-Point-Einstellungen (Screenshots)
 - WEP / WPA
 - RADIUS-Server
 - SSID, Broadcast
 - Geschwindigkeit
- RADIUS-Server
- Authentifikation, Kerberos

IPsec

- Nicht nur Verschlüsselung!
- Nicht nur VPN (Virtual Private Network)
- Abschottung bestimmter Maschinen von anderen, z.B.
 - Hochsicherheitsserver, die nur mit bestimmten anderen Maschinen kommunizieren dürfen
 - Maschinen, die nach außen kommunizieren dürfen, aber nicht von außen "angesprochen" werden
 - Ähnlichkeiten zu Desktop-Firewalls
- Eine weitere Variante der logischen Segmentierung von Netzwerken, "Network Access Protection"

IPsec "Isolation"

- Isolationszone, Randzone und nicht vertrauenswürdige



Bilduelle: <http://www.microsoft.com/technet/itsolutions/network/sdiso/default.msp>

Demo: IPSec-Policies

- IPsec-Regeln
- IPsec-Filter
- IPsec-Filterlisten
- Authentifikation
- Kryptographische Methoden

Herausforderungen in Projekten

- Design der technischen Lösung
 - Zusätzliche "Topologie"
 - Viele Ausnahmen und Sonderfälle
 - Bei Problemen ist kein Fernwartungszugriff auf Computer mehr möglich
- Prozesse:
 - Neuer Computer oder Ausscheiden von Computern
 - Computer hat kein Zertifikat mehr, aber auch keinen Zugang mehr zum Netz
 - Anfragen beim Helpdesk



Sichern von Daten

Risiken

- Gestohlenes Notebook
 - Zugriff auf die Daten
 - Nutzung des Notebooks, um sich Zugang zu anderen Ressourcen zu verschaffen
- Nicht vertrauenswürdige Administratoren
- Versehentliche Zugriffe und Änderungen von Daten
- Verletzung regulatorischer Vorgaben

Teil eines Gesamtkonzeptes

- Defense-in-Depth
- Lokale Datenverschlüsselung ist der letzte Schutzwall!
- Physische Sicherheit
- BIOS-Passwörter
- Berechtigungen im Dateisystem
- Zugriffsberechtigungen auf Computer
- Sichern der Netzwerkverbindungen (802.1x, IPsec)

Festplattenverschlüsselung

- Verschlüsselung der gesamten Platte
 - Booten ohne Passwort oder Karte nicht möglich
 - Zugriff im Betrieb über das Netz meist möglich
- Verschlüsselung von "Containern"
 - Große Dateien als "Behälter" für verschlüsselte Dateien
 - Werden wie Laufwerke angesprochen
- Datei- und Ordnerverschlüsselung
 - Einzelne Dateien verschlüsselt
 - Datei- und Ordnernamen sind lesbar

Demo: Container-Datei

- Software: truecrypt
- Erstellung eines Standard-Volumens
- Mögliche Algorithmen
- Erstellung eines Hidden Volumens
- Routine-Arbeitsschritte
- Traveller-Disk

Demo: Datei-/Ordnerverschlüsselung

- Windows Encrypting File System
- Erstellung eines Zertifikates
 - Mit Zertifizierungsstelle
 - Ohne Zertifizierungsstelle
- Arbeiten mit Zertifikaten und Schlüsseln
- Verschlüsseln von Dateien
- Verschieben, Kopieren und Sichern von verschlüsselten Dateien

Algorithmen | Protokolle

- Symmetrische Verschlüsselung der eigentlichen Daten
 - AES
 - 3DES
 - DES
 - Blowfish (Bruce Schneier)
- Asymmetrische Verschlüsselung des Dateiverschlüsselungsschlüssels oder
- Erzeugen des Schlüssels aus einem Passwort (z.B. standardisierter Algorithmus PKCS#5)
- Wiederherstellung des Zugriffs durch
 - Entschlüsselung des Dateiverschlüsselungsschlüssels
 - Oder Wiederherstellung des asymmetrischen Benutzerschlüssels

Gesamtlösung | Bausteine

- Zentrale Richtlinien (technisch umgesetzt)
 - Berechtigte Recovery Agents
 - Erlauben und Verboten von Verschlüsselung
 - Mehraugenprinzip für Wiederherstellung von Dateien oder Schlüsseln.
- Infrastruktur und Verwaltungswerkzeuge für
 - Zertifikate
 - Private Schlüssel
 - Passwörter

Prozesse!!

- Key Escrow, Archival, Recovery!
- Datenschutz: Unternehmensinteressen versus Privatsphäre des Einzelnen
- Lifecycle-Management
 - Mitarbeiter verlässt Unternehmen
 - Mitarbeiter verliert Schlüssel
 - Recovery-Agent verlässt Unternehmen
- Mitarbeiterschulung
 - Andere Handhabung von Dateien
 - Kein Dateiaustausch mit Privatcomputer möglich



Ausblick

Science Fiction, Realität oder Paranoia?

RFID

- Radio Frequency Identification
- Relativ "alte" Technologie (~ 1945)
- Identifikation von Konsumgütern, Büchern etc. vergleichbar zu einem Barcode
- Interessant z.B. für Konsumgüterindustrie und Produktion
 - Rückverfolgbarkeit von Komponenten eines Produktes
 - Auch im Sinne regulatorischer Vorgaben.
- → Sicherheit kommt ins Spiel durch im Vergleich zum Barcode einfachere Rückverfolgbarkeit, auch wenn der Tag seine Funktion erfüllt hat

Technologien

- Komponenten:
 - Antenne zum Senden und/oder Empfangen von Signalen ("Stromschleife", elektromagnetische Induktion)
 - Transponder-Chip mit Identitätsdaten
- Aktive Tags
 - Eigene Stromversorgung
 - Unempfindlicher bei Störstrahlung
 - Antenne kann auf Senden optimiert werden
- Passive Tags
 - Energie aus dem Signal des Senders ("Reader") weckt den Chip auf, Antenne muss auf Energieaufnahme optimiert werden

RFID-Tags



Bilduelle: <http://en.wikipedia.org/wiki/RFID>

RFID-Sicherheit

- Pässe mit RFID-Chips
 - In Planung / Produktion für USA und Deutschland
 - Reichweite aller wireless Protokolle etwas größer als spezifiziert
 - Einfach lesbar durch verschiedene Reader, Schutz durch Metallnetz bei geschlossenem Pass
 - Keine Verschlüsselung, Kopieren bei physischem Zugriff auf einen Originalpass möglich
 - Integrität durch Hashwert gewährleistet, Daten können nicht verändert werden
- Zugangskarten für Hotels, Corporate Cards etc.
 - Ebenfalls oft ohne Verschlüsselung
 - Standard-Passwörter verwendet
- Caveat: RFID ist nicht als Sicherheitstechnologie gedacht!

Quantentechnologien

- Quantencomputer
 - Angriff auf heutige Verschlüsselungsmethoden durch wesentlich schnelleres Lösen der "hard problems" (wie: Faktorisieren großer Zahlen)
 - "Paralleles Rechnen" durch Ausnutzung der Überlagerung von Quantenzuständen
- Quantenkryptographie
 - "Gegenmaßnahme gegen Quantencomputer"
 - Quantenphysik: Beobachtung = Messung = Veränderung
 - Abhören wird entdeckt!
 - Einschränkung: Einbettung in reale Protokolle

Quantencomputer | Basics

- Überlagerungen von Zuständen
 - Interferenz einzelner Wellen
 - Analogie: Lichtbeugung am Doppelspalt
- Exakter: Eine Funktion für "mehrere Teilchen"
 - "Verschränkung", keine Information über die "Einzelteilchen"
 - "Weniger Information gleichzeitig" als im klassischen Bild
 - Eine Funktion, die nur Aussagen darüber macht, wie die Eigenschaften der "Einzelteilchen" zueinander in Relation stehen
 - "Die Natur weiß es selbst nicht"
- Messung = Beobachtung
 - "Kollaps der Wellenfunktion"
 - Z.B.: Ein Teilchen wird in Zustand 1 "geklappt", dann nimmt auch Teilchen zwei den gleichen Zustand an.
 - "Spukhafte Fernwirkung", "Beamen"

Höhere Rechengeschwindigkeit

- Beispiel: Finde die Zahl, deren 2. und 3. Potenz miteinander alle Ziffern von 0 bis 9 enthalten
 - Lösung: 69 ($69^2 = 4761$, $69^3 = 328509$)
 - Ein konventioneller Computer könnte eine Zahl nach der anderen testen
- Konstruktion eines passenden Überlagerungszustandes
 - Maximal 9 Infos verfügbar
 - Entweder: Teilchen 1 = 0/1, Teilchen 2 = 0/1 ... (9 Infos)
 - Oder (z.B.): Alle verschieden, 8 von 9 gleich, 7 von 0 gleich etc.
- Quantencomputer:
 - Zustand muss so konstruiert werden, dass durch "Umklappen" eines oder mehrerer Teilchen der Zustand "Alle verschieden" ausgewählt wird.
 - Kann gezielt "gefragt" werden, ob die Ziffern gleich sind
- Siehe auch <http://homepage.univie.ac.at/Franz.Embacher/Quantencomputer/>

Quantenkryptografie | Basics

- Gekippter Poliarisationsfilter
 - Polarisiertes Licht – klassisch: Anteil $\cos^2\Phi$ geht durch
 - Quantenmechanisch: Ein Photon geht durch oder nicht – mit Wahrscheinlichkeit $\cos^2\Phi$
- Hintereinandergeschaltete Poliarisationsfilter
 - Gleiche Richtung: geht durch beide
 - 90° verdreht: geht sicher nicht durch
 - 45° verdreht: geht mit 50% Wahrscheinlichkeit durch
- Komponenten
 - Zwei Arten von Filtern: + oder x
 - Für jeden Filter sind "0" und "1" 90° verdreht
 - Alice schickt polarisierte Photonen an Bob
 - Beide messen mit zufälligen ausgewählten Filtern
 - Es gibt einen zusätzlichen "klassischen Informationskanal"

Quantenkrypto-Protokoll

- Alice bereitet Photonen vor:
X + + X X + X + + X X + + + X + X X
1 0 1 1 1 0 1 0 0 1 0 1 0 1 1 0 1 0
- Bob misst
+ + X X X + + + X X + + + X X X X +
- Alice sendet Bob Ihre Filter-Sequenz (klassischer Kanal)
- Bob scheidet die Bits mit unterschiedlichen Stellungen aus und sagt Alice, welche Bits verwendet werden (klassischer Kanal)
+ + X X X + + + X X + + + X X X X +
- Schlüssel:
0 1 1 0 0 1 1 0 1 1

Probleme für Eve

- Eve ändert die Bits
 - Alice und Bob könnten entweder nur einen Teil der Bits zur Erstellung des Schlüssels verwenden und den anderen im Klartext austauschen, um die Gleichheit zu überprüfen
 - Oder: Verwendung eines Protokoll ähnlich Kerberos, um sich gegenseitig vom gleichen Schlüssel zu überzeugen
- Eve misst einen Teil der Bits falsch (gekippte Filter)
- Eve miss einen Teil der Bits richtig, aber diese werden von Alice und Bob eventuell gerade verworfen.

Danke !

o Kontakt:

- www.punktwissen.com
- elke@punktwissen.com

Literatur | Bücher

- Überblick, allgemein verständlich:
 - Simon Singh: Geheime Botschaften
http://www.amazon.de/Geheime-Botschaften-Verschl%fcsselung-Zeiten-Internet/dp/3423330716/sr=8-1/qid=1158037009/ref=pd_ka_1/028-4498158-2675761?ie=UTF8&s=gateway
 - Website des Autors: www.simonsingh.com
- Details
 - Bruce Schneier: Angewandte Kryptographie
http://www.amazon.de/Angewandte-Kryptographie-Klassiker-Algorithmen-Sourcecode/dp/3827372283/sr=8-4/qid=1158037131/ref=sr_1_4/028-4498158-2675761?ie=UTF8&s=gateway
 - Website des Autors (mit allgemeinen Betrachtungen zu Sicherheit
www.schneier.com

Links | Algorithmen in Wikipedia

- [Vigenere-Verschlüsselung](#)
- [ENIGMA](#)
- [RSA](#)
- [DES](#)
- [AES](#)
- [SSL](#)
- [Kerberos](#)
- [RFID](#)

Links | Sichere Webserver

- Übersicht: Phishing
- Erkennen sicherer Verbindungen:
 - http://www.asit.at/de/dokumente_publicationen/flyer/webserver.php
 - (plus weiter führende Links auf dieser Seite)

Links | Bürgerkarte

- Einführung: www.buergerkarte.at
- Anbieter A-Trust: www.a-trust.at
 - [Suchen im Verzeichnis](#) (nach Zertifikaten anderer Personen)
- Anwendungen:
 - BAWAG/PSK-eBanking: <http://ebanking.bawag.com>
 - FinanzOnline: <http://finanzonline.bmf.gv.at>
 - Sozialversicherung: www.sozialversicherung.at
(rechts unten: die eCard als Bürgerkarte)

Links | E-mail-Sicherheit

- Einführung zu e-mail-Verschlüsselung:
http://download.microsoft.com/download/0/c/6/0c68401c-f74d-4b23-ad5c-de22c29e8dbd/Sonstige/Sicherheit_06_03.pdf
- Verwenden von Zertifikaten in Outlook oder Outlook Express:
<http://www.microsoft.com/technet/prodtechnol/exchange/de/guides/E2k3MsgSecGuide/e6a7d821-3c40-4f8c-b46e-94a37e0186c9.msp?mfr=true>

Links | Public Key Infrastructure

○ Übersicht:

- PKI allgemein: <http://de.wikipedia.org/wiki/Public-Key-Infrastruktur>
- PKI allgemein in Windows:
<http://download.microsoft.com/download/0/c/6/0c68401c-f74d-4b23-ad5c-de22c29e8dbd/Sonstige/Sicherheit-04-03.pdf>
- [Übersicht über Zertifikate](#)

Links | Wireless LAN

- Einführung:
<http://download.microsoft.com/download/0/c/6/0c68401c-f74d-4b23-ad5c-de22c29e8dbd/Sonstige/Sicherheit-10-02.pdf>
- WLAN-Konfiguration in kleinen Netzwerken:
 - [10 Schritte zum Absichern von WLAN](#)
 - <https://www.microsoft.com/germany/technet/sicherheit/newsletter/wlansec.mspx>
- WLAN-Konfiguration in großen Netzwerken:
 - [Securing Wireless LANs with Certificate Services](#)

Links | Passwörter

- [Frequently asked questions about passwords](#)
- Tool Cain von oxid.it: www.oxid.it
- Kerberos-Authentifizierung in Windows:
[How Kerberos Works](#)

Links | Datenverschlüsselung

- Container-Dateien: www.truecrypt.org
- Datei- / Ordnerverschlüsselung: [Verschlüsselndes Dateisystem](#)

Links | Quantentechnologien

- Anschauliche Demonstrationen zu Quantencomputer und – kryptographie:
<http://homepage.univie.ac.at/franz.embacher/Quantentheorie/>
- Einstein's Schleier von Anton Zeilinger:
http://www.amazon.de/Einsteins-Schleier-neue-Welt-Quantenphysik/dp/3442153026/sr=8-1/qid=1158037745/ref=pd_ka_1/028-4498158-2675761?ie=UTF8&s=gateway
- Aktivitäten in Österreich (oder unter Österr. Koordination):
 - www.quantenkryptographie.at
 - www.secoqc.net