Topic

- **Einleitung**
  - Wer bin ich?
    - Studium Mathe/Informatik in Berlin
    - 6 Jahre Sysadmin an der FH-Furtwangen
    - 6 Jahre Softwareentwicklung+Betrieb im schweizerischen Bankenumfeld
    - 10 Jahre Vorlesungen im Bereich Unix+Internet+Security
    - Seit 2005 in Regensburg bei der art of defence GmbH (Web-Application-Firewall)
    - CCC, OWASP, GUUG
  - Wie wird das hier ablaufen?
    - Prüfungsleistung ist eine schriftliche Klausur (90 min).
      Voraussetzung zur Prüfungszulassung ist: die Abgabe der Übungsblätter
    - Übungen
      - Vorlesungsbegleitend
        Sie sollen die in der Vorlesung theoretisch angesprochen Dinge praktisch ausprobieren
      - Übungsblätter in der Vorlesung, Abgabetermin +2-3 Wochen
      - Arbeit in Gruppen von 2 Personen möglich
      - Abgabe der Übungsblätter und Vorführung der Resultate im Rahmen der Übungen bei mir.
      - Erfolgreiche Teilnahme an den Übungen ist Voraussetzung zur Teilnahme an der Klausur
      - TODO: Teilnehmerliste
  - Kontakt
    - Email: mirko.dziadzka(at)gmail.com
    - Web: mirko.dziadzka.de/vorlesung
  - Literatur
    - Siehe Webseite
    - Claudia Eckert: IT-Sicherheit, Oldenbourg Verlag, 6. Auflage,
    - Matt Bishop: Computer Security, Addison Wesley,
  - Worum soll es in der Vorlesung gehen
    - Umfrage und Diskussion
    - Die Vorlesung will ein Bewusstsein dafür schaffen, das Sicherheit im IT Bereich ein sehr komplexes Unterfangen ist
    - Wir werden und auf Verfahren und Protokolle, ihre Probleme und Möglichkeiten konzentrieren
      Dabei werden im wesentlichen Open-Source Produkte und Protokolle betrachtet
    - Best practices, HowTo
      Praktische Anleitungen zum Lösen von Problemen
- **Einführung in den Bereich IT Security**
  - Definition: Information Security
    - Products
      - Hardware, Software, Netzwerke, Protokolle, Tools
    - People
    - Procedures
      - ISO 2700x
  - Ziele der Informationssicherheit
    - Confidentiality, Integrity, Authenticity
    - Availability
    - Non-repudiation
    - Anonymity
  - Bedrohungsanalyse / Status Quo
- **Probleme mit der TCP/IP Protokollfamilie**
  - Wie ist TCP/IP entstanden und warum gibt es Probleme
  - Ethernet
    - Adressierung über (theoretisch) eindeutige MAC Addresse
    - Kann trivial gefälscht werden
    - War früher ein reines Broadcastmedium - jeder Teilnehmer konnte jeden Datenverkehr sehen.
    - Heute in der Regel via Switch eine direkte Kommunikation zwischen zwei Rechnern
      - Kann via MAC-Flooding und MAC-Spoofing umgangen werden
    - Switch

Topic

- Port Security
- VLAN - 802.1Q
  - Ein Mittel um den Datenverkehr zu trennen, allerdings sollte man sich vom Security Standpunkt aus nicht allzusehr darauf verlassen
    - switch ist in der Regel fail-open
  - www.corecom.com—vlansec.htm
- Authentisierung: 802.1X

- WLAN
  - Ethernet over the air - jeder kann senden und mithören
  - Eingebaute Sicherheit:
    - WEP - öffentlich tot seit 2001
    - WPA
      - PSK (pre-shared-key) kann der verbindungsaufbau aufgezeichnet und dann mit brute-force der key ermittelt werden. Normale Passwörter sind hier ungeeignet.
      - Ist akademisch gebrochen (seit 2008)
    - WPA2
      - auch hier das Problem mit PSK - gute Passwörter wählen - d.h. einen kryptographischen Zufallsgenerator nehmen
      - EAP stat PSK
  - Empfehlung
    - Das WLAN ist als unsicheres Netz anzusehen und zu behandeln
    - Es ist unsicherer als Kabelgebundenes Netz, das der physikalische Zugriff einfacher ist.
    - VPN over WLAN ist eine gute Möglichkeit den mobilen Zugriff zu schützen
      - Zugriff aus dem WLAN Netz nur auf den VPN Server, kein Zugang zum internen Netzt oder ins Internet

- IPv4
  - Interessante Header Felder:
    - Fragmentierung (Paket-ID, Fragment Offset)
      - used to avoid detection in Firewalls and for IDS systems
      - firewalls should reassemble today
      - IDS should flag such packages
    - TTL
      - Network Architecture Discovery
      - Block incoming Packages with TTL < N in the Firewall
    - Absender-IP
      - Nicht vertrauenswürdig
    - IP-Optionen (z.B. Source-Routing)
      - heute werden eigentlich alle Pakte mit IP Optionen in der Firewall verworfen
  - ARP - Address Resolution Protocol
    - Umsetzung von IP (Layer 3) auf Ethernet (Layer 2) Adressen
    - Broadcast anfrage, unicast Antwort

      ```
      0:80:c8:f8:4a:51 ff:ff:ff:ff:ff:ff arp who-has 192.168.99.254 tell 192.168.99.35
      0:80:c8:f8:5c:73 0:80:c8:f8:4a:51  arp reply 192.168.99.254 is-at 0:80:c8:f8:5c:73
      ```

    - Jeder Rechner sieht alle Arp Requests und kann ARP Replies senden
    - Ein Rechner cached die arp replies
    - Es kann durchaus legitim sein, Arp Replies für fremde IPs zu beantworten
      - Virtuelle Machinen und Routing
      - Cluster, bei denen die IP umzieht
    - Tools zum Arp-Spoofing

      ettercap.sourceforge.net
    - Entdecken über monitoring (nicht immer möglich)
      - ArpWatch
  - DHCP

    Auch der DHCP Server authentisiert sich nicht gegenüber dem Rechner. Die Anfrage erfolgt über Broadcast und die schnellste Antwort gewinnt. So kann ich dem Rechner einen anderen Rechner im selberb Netzt als Nameserver

Topic

oder Router unterschieben. Als einzig sinnvolle Gegenmaßnahme ist Monitoring im LAN zu empfehlen. Hint: Bringen Sie nicht ihren HOME-Router mit ins Firmennetz, der bietet ungefragt DHCP an. Auch gewisse Windows Server installationen machen das den Gerüchten nach per default.

- IP
- Nameserver
- Router

- IPv6
  - Kurze Geschichte ... warum und wann
    - In 2 Jahren gehen die IPv4 Adressen aus
    - Kommt ... irgendwann
  - IPSec eingebaut
    - authentication, encryption
  - Kein "Schutz" mehr durch NAT und private Adressen
  - Mobile-IP
- Routing
  - statisch
  - dynamisch
    - local
    - BGP
      - Internet Core Routing Protokoll
      - Viel gegenseitiges Vertrauen auf dieser Ebene (da Zugang limitiert)

        Screen shot 2010-03-17 at 23.57.43
      - Google Tech Talk: BGB
- TCP / UDP
  - Sequence number, 3-way handshake
    - initial SN muß zufällig sein - sonst ist IP Spoofing trivial möglich
  - Wenn ich die Pakete sehe, kann ich Daten in den Datenstrom einfügen
  - synfload
  - NAT
    - ist keine Sicherheitsmassnahme
      - helper plugins (z.b. FTP, SIP, ...)
- DNS
  - dezentrale funktionierende Datenbank
  - spielt indirekt eine sehr große Rolle im IT Security Bereich

    Wenn ich DNS kontrolliere, kann ich E-Mail umleiten. Wenn ich Mail umleiten kann, kann ich SSL Zertifikate für Domains bestellen. Damit hängt die Sicherheit von SSL an der von DNS
  - DNS-Spoofing (reverse DNS lookup)
  - Cache Poisioning
    - Altes Problem

      Request/Response werde durch ein 16 Bit Feld aneinander gebunden.
    - Dan Kaminsky / 2008 - neue Methode es auszunutzen

      www.doxpara.com—DMK_BO2K8.ppt
  - Alles wird gut, wenn wir endlich DNSSEC haben
  - DNS SRV
- SMTP - Simple Mail Transfer Protocol
  - Keine Authentisierung
  - ESMTP
    - STARTTLS - opportunistic encryption
    - SMTP-Auth
  - Port 25, Port 587 (Message Submission), Pot 465 SMTP over SSL
  - Spam
    - SPF (Sender Policy Framework)
    - DomainKeys
  - Mail und Helper Programme - Wo kommen die VIren her?
- FTP
- Telnet

Topic

- HTTP
  - Kein State
  - Keine Authentisierung
  - Web Server Security
  - Helper Programme - Wo kommen de ganzen Trojaner her?
- SMB / NFS / WEBDAV
- Multicast / Broadcast
- Zeroconf
  - Apple: Bonjour (früher Rendevous)
  - Unix: avahi(sp?)
  - MDNS
    - pgpkey-hkp.__tcp.local
- Übungen
  - Wireshark
    - mitsniffen der Protokolle und Passwörter
  - DNS
    - Zeichnen sie mit dem Netzwerksniffer ihrer Wahl eine DNS Abfrage nach der IP von scanme.bithalde.de auf. Was bedeuten die einzelnen Felder der Antwort.
    - Was ist das DNS Cache Posioning Problem und welchen neuen Angriff hat Dan Kaminsky 2008 gefunden
    - Warum löst DNSsec das Problem
      - Wann wird DNSsec eingeführt (finden sie den Zeitplan im Netz)
      - Welche Nachteile hat DNSsec gegenüber dem jetzigen DNS
  - senden einer echt aussehenden email mit telnet
    - Absender: mirko.dziadzka@gmail.com
    - Empfänger: mailtest@bithalde.de
    - Subject: Vorlesung IS 2010 : Ihr Name
  - nmap
    - scannen sie scanme.bithalde.de mit nmap
    - Welche Ports sind offen, welche Dienste laufen wirklich auf diesen Ports
    - Was könen sie über das Beriebssystem auf diesem Rechner herausfinden
- **Netzwekbasierte Sicherheit**
  - Firewalls
    - Definition
      - Koppelung von Netzen verschiedener Sicherheitsstufen
      - Realisierung einer Sicherheitsstrategie
    - Komponenten
      - Paket Filter
        - Analyse des Datenstroms auf Paketebene
          - Durchsetzung der Protokolldefinitionen (check von Paketlängen, IP und TCP Optionen, ...)
          - Zugriffsmatrix
        - Pakete können erlaubt oder geblockt werden, eventuell auch modifiziert (NAT)
        - Heute in der Regel mit Stateful Inspection auf Layer 3 + 4, d.h. mit Zustand
        - Router und eventuell Switche haben auch Paketfilter, aber nur auf Layer 3 - IP. Kein richtiger State.
      - Circuit-level gateway
        - proxy auf TCP oder udp ebene
        - rinetd
        - socks (ssh -D 1080)
      - Proxy Server - application level gateway
        - Terminiert UDP und/oder TCP Verbindung
        - Validiert Datenverkehr auf Application-Layer Level
        - Typische Beispiele: DNS Server, Mailserver, Webproxy
        - Content Filter (Viren)

Topic

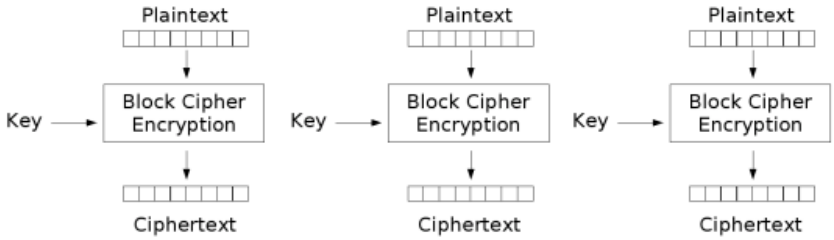
- DMZ
  Datei-DmzSchema
  - `Dual-homed`
  - `Screened Host`
  - `Screened Subnet`
- Beispiele
  - Einfacher Paktfilter mit NAT und DNS Proxy
  - Mail und Webserver in der DMZ
  - Webserver mit Zugriff auf eine Datenbank im internen Netzwerk
- Hinweise
  - Beim Design eines Systems an die Filterregeln denken
    - Kommunikation vom sicheren system zum unsicheren
    - tcp
    - kommunikation dokumentieren
  - Beim nachträglichen einbau einer Firwall
    - erst mal Mitlaufen lassen und kommunikationsbeziehungen protokollieren
    - Kommunikation verstehen
    - Monatsabschluss, Jahresabschluss, Failover
  - Tunneln kann man nicht verhindern
  - UDP am besten über Proxy (braucht man eh nur für DNS :-)
  - Ausgehende Pakete nach Absender-IP filtern
  - TCP Conections mit reject stat mit drop ablehnen
- Administration
  - seperates admin netz
  - sichere verbindungen
  - audit log
  - vier augen prinzip
- Vorteile / Nachteile / Grenzen
  - Bündelung von Sicherheitsdiensten
  - Komplexe Anforderungen / Regelwerk
  - Fehler in der Konfiguration sind schwerwiegend
  - Webservices
  - Risikokompensation
- Schlagwörter
  - Deep Inspection
    - Content Filter / Viren Scanner
  - Personal Firewall
- IDS / IPS
  - Definition
    - Netzwerkbasiert
    - erkennen von Anomalien durch beobachten des Netzwerkverkehrs
    - in der regel pattern basiert
  - IDS Evasion
    - payload obfuscation
    - fragmentation
    - small packages
    - ttl tricks
    - encryption
    - attacks against ids
  - Consider
    - false positives vs. false negatives
    - use in DMZ
  - Data Leakage Prevention

Topic

- Inline IDS
- Übungen
  - iptables unter Linux
  - fwbuilder
  - apache als proxy server
  - snort
- **Hostbasierte Sicherheit**
  - Rechtekonzept unter Unix
    - Discretionary Access control
      - Klassisch
        - user-group-other, rwx
        - SUID/ SGID
        - check-on-open
      - Capability System
        - split root permission
      - ACL
    - Mantatory Access Control - SELinux / AppArmot
      - **Security-Enhanced Linux** (**SELinux**)
        - NSA / OPenSource seit 2000
      - Bell LaPadula
        - 1973 - US Air Force
        - Schützt Vertraulichkeit von Informationen
        - Unterscheidet Zuständigkeitsbereiche und Level
      - Biba Modell
        - Schützt Datenintigrität
      - Tainted data
        - implement a trusted computing modell
        -
      - Windows:
        - Integrity Levels: low, medium, high und system
  - Compartments / Zonen
  - chroot
  - jail
  - system hardening
  - Virtuelle Maschinen
  - IDS
    - tripwire?
  - RootKits
- **Grundlagen der Kryptographie**
  - Ziele
    - Vertraulichkeit
    - Integrität
    - Authentizität
    - Nichtabstreitbarkeit
    - (Anonymität)
  - Historisches
    - Von Cäsar zu One-Time-Pad
      - Transposition / Substitution
        Skytala&EmptyStrip-Shaded
      - Monoalphabetische Chifren
      - Polyalphabetiesche Chiffren
      - One-Time Pad
    - **Kerckhoffs'sche Prinzip**
  - Angriffe
    - Replay

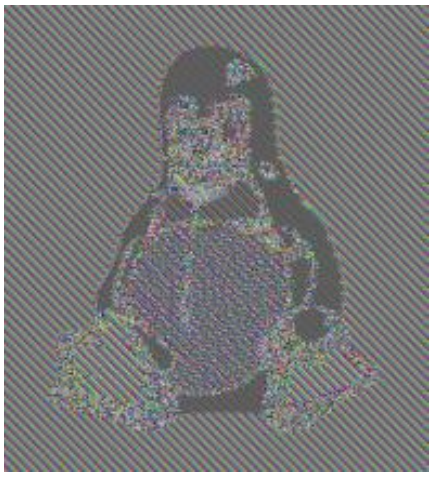
Topic

- known plaintext
- choosen plaintext
- Symetrische Kryptography / Shared Key
  - Blockchiffre
    - Verschlüsselt einen Block (früher 64, heute meistens 128) mit einem geheimen Schlüssel
    - Schlüssellänge heute 128-256 bit (DES: 56 Bit)
    - Sowohl blocksize als auch schlüssellänge sind wichtig
      - Schlüssellänge: Brute-Force gegen den Schlüssel
      - Blocksize: Geburtstagsparadox, verschlüsselung des selben blocks
    - Bekannte Chiffren: DES, 3DES, AES, TwoFish
    - Feistel-Chiffre:
    - blockmodi: en.wikipedia.org—Block_cipher_modes_of_operation
      - ECB Electronic Code Book



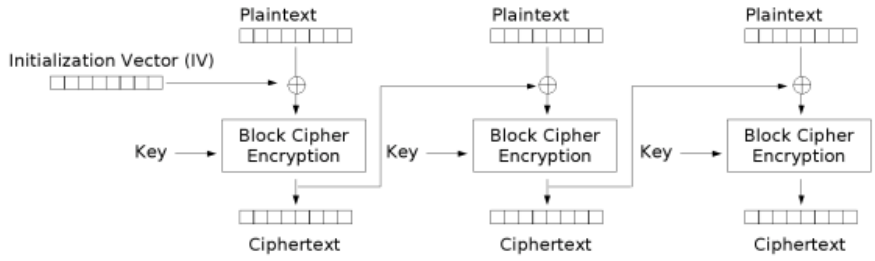
Electronic Codebook (ECB) mode encryption

- Nachteil: Identische Blöcke werden identisch verschlüsselt

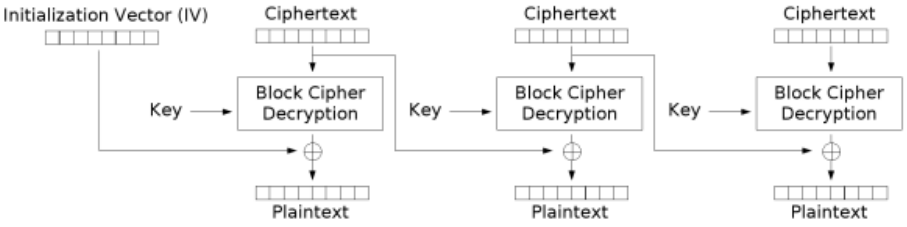


Topic

- CBC - Cypher Block Chaining

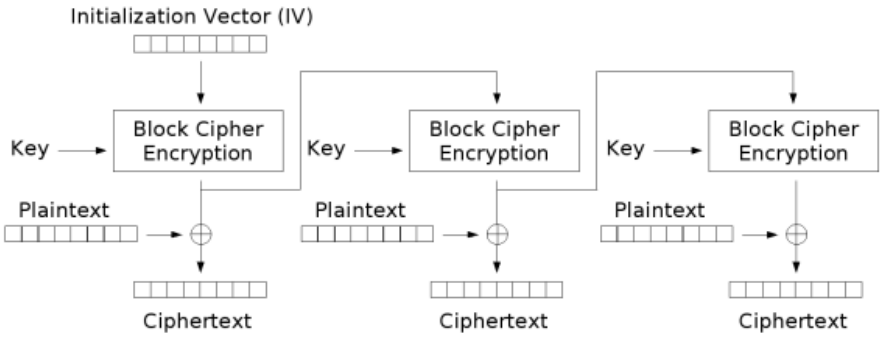


Cipher Block Chaining (CBC) mode encryption

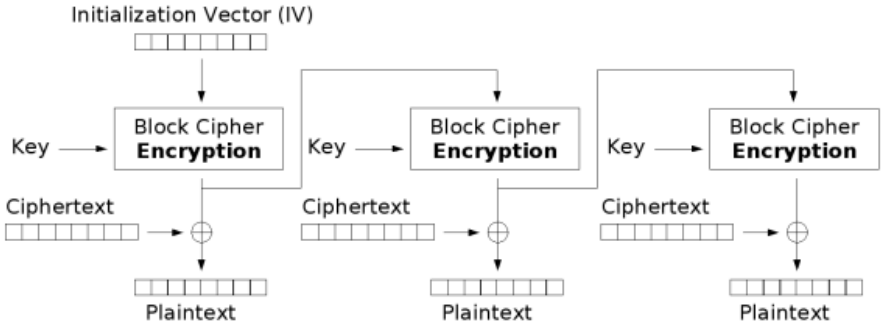


Cipher Block Chaining (CBC) mode decryption

- OFB - Output Feedback Mode



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

- erzeugt eine Stromchiffre
- CTR - Counter mode

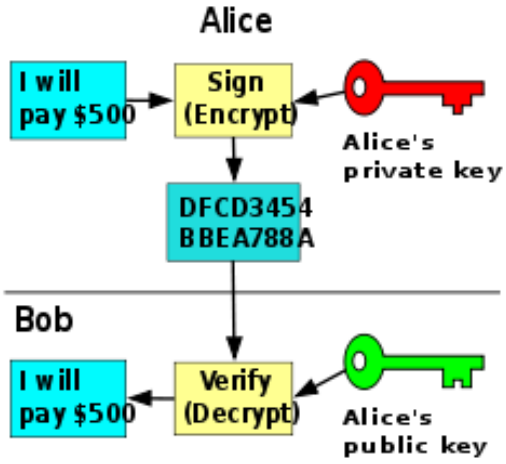
  Ctr_encryptionCtr_decryption
  - Gut für Verschlüsselung von Random Access Files (z.b. Festplatten)
- Padding
- Hint: use AES-256 - forget everything else. Combine it with other algorithms of the last round of the standard process
- Keine Integrity Protection - Flipping one or more bits is possible

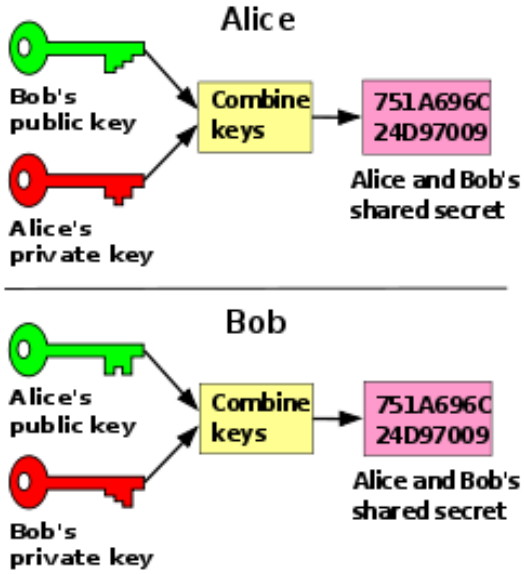
Topic

- Stromchiffre
  - Benutzung einer Blockchiffre als Stromchiffre
  - rc4
  - A5/1

    280px-A5-1_GSM_cipher.svg
- Vergleich von Strom und Blockchiffren
  - Latency ist bei Stromchiffren geringer -> Audio und Video Streaming
    - ein bit kann encoded/decoded werden wenn es ankommnt
  - Flipping a single given bit is possible
    - Bit 20 bei ihrem Kontostand
- Asymetrische Kryptography / Public Key

  wurde erschaffen, als man nachweisen wollte, das es so was nicht geben kann :-) Diffie / Hellman 1976
  - Probleme mit Symetrischer Krypto: Keymanagement
  - Idee



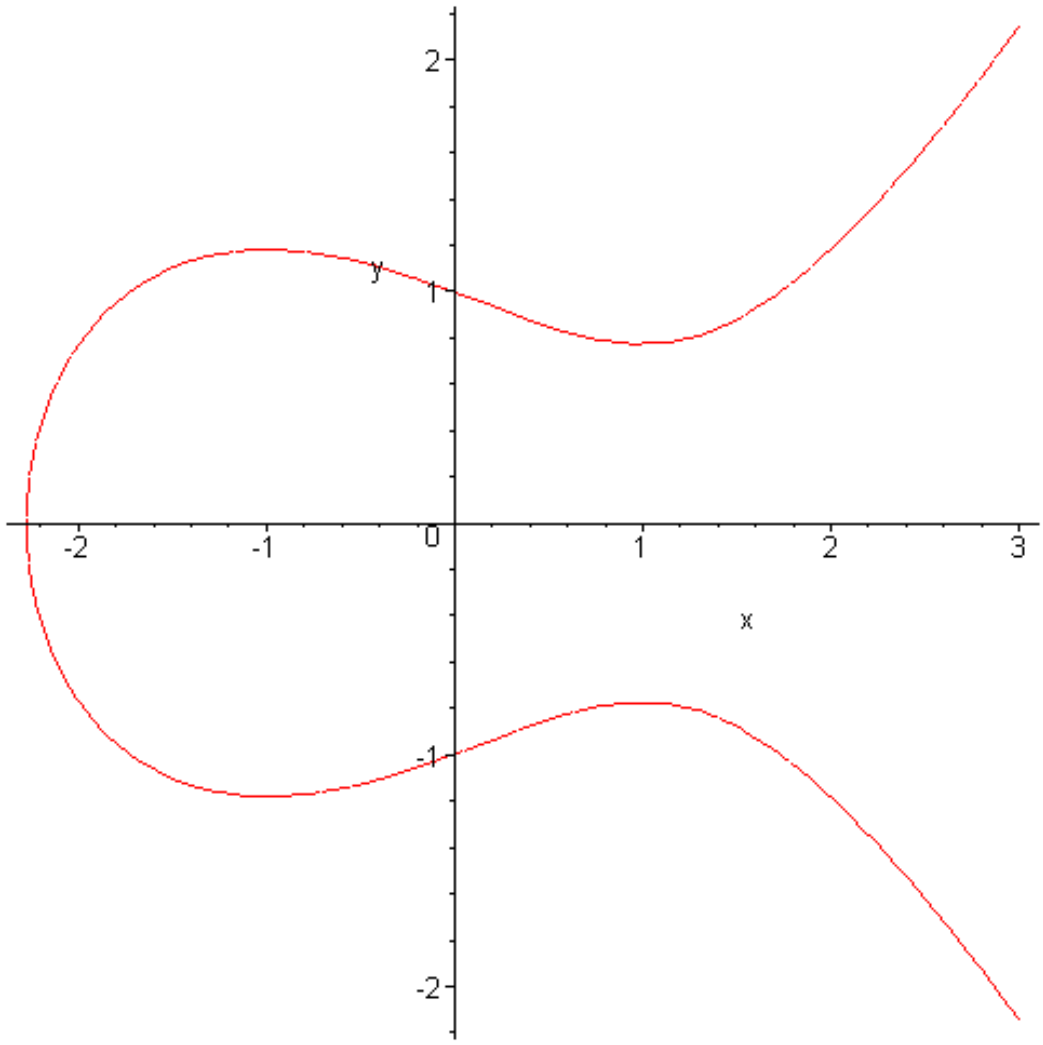


  - Protokolle
    - DH (Diffie-Hellman Key Exchange)
      - discrete logarithm
      - public prime p, base g
      - k, r = exp(g,k) mod p
    - RSA (Rivest-Shamir-Adleman 1978)
      - integer factorization
      - n = pq
      - e relative prime to phi(n) = (p-1)(q-1)

Topic

- de = 1 mod phi(n) (mittels erweiternen euklidischen algorithms)
- c = exp(m,e) mod n
- m = exp(c,d) mod n

- DSA (Digital-Signature-Algorithm)
- ECC (Eliptic-Curve-Cryptography)



b47b19e5899585c30c875b983ddfba04

- use RSA 4096
- Nachteile: langsam

- Hybride Verfahren
- Hash Funktionen
  - Ziele
    - eindeutig, fixe länge (meist 160, 256 oder 512 bit)
    - praktisch nicht umkehrbar
    - no second preimage
    - praktisch keine kollisionen erzeugbar (Geburtstagsparadox!)
  - MD4 - schon lange broken, RootCA Zertifikat?
  - MD5 - 160 bit, Broken in Bezug auch Kollisionen
  - SHA-1 (Secure Hash Algorithm)
  - SHA-2 (SHA-256, SHA-512) <- use this
  - MAC
    - Hash mit Nachricht und Passwort
  - Probleme: Extension Attacken bei allen gängigen Hashfunktionen
    - Struktur benutzen
      - mhash(S) = hash(len(S) ":" S)
      - HMAC
      - hash(hash()))

Topic

- Zufallszahlen
  - wie erzeuge ich die
  - Sammeln von Entropie im Betriebssystem
  - spezielle Hardware
  - use /dev/urandom oder /dev/random
- Nonce
  - Replay atacken
  - IV
  - timestamp (wenn zeit nicht rückwärts geht)
    - das muss man prüfen!
- Primzahlen
  - primzahlentest
- Sicherer Kanal
  - Ziele
    - Integrität
    - Authentizität
    - Vertraulichkeit
  - session key, regelmässig neue keys
  - hash über alle bisherigen daten
  - perfect forward secrecy
- Digitale Signatur
  - kombiniert hash function und signatir
- Secret sharing
- secret splitting
- Big-Fails
- Übungen
  - Was besagt das Kerckhoff'sche Prinzip. Warum ist es wichtig?
  - Microsoft Office bietet eine Verschlüsselungsfunktion für Dokumente. Finden Sie Informationen zu den Details dieser Verschlüsselung und Ihrer Sicherheit in
    - Office 95, XP, 2003, 2007
  - Testen sie die Unterschiede zwischen CBC und ECB Mode und anderen blockmodi
    - openssl

- **Anwendungen der Kryptographie**
  - Sicherer Kanal
    - SSL
      - Erfunden von Netscape für eCommerce im Netzscape Navigator 2?, ca. 95?
      - SSLv2 unsicher, SSLv3 und TLS 1.0
      - Client und Server handeln die Art und Weise der Verschlüsselung aus
        - Null Encryption
      - Authentisierung des Servers ist Pflicht, des Clients optional
      - Protokoll
        - Client
          - ClientHello: Protokoll Version, Nonce, CipherSuites, Optional Session ID
        - Server
          - ServerHello: choose proto, cipher-suite, add nonce
          - Certificate
          - Server HelloDone
        - Client
          - ClientKeyExchange: preMasterSecret (encrypted with master public key)
          - ChangeCipherSpec
        - Server
          - ChangeCipherSpec
    - X.509
      - ITU Standard für PublicKeyInfrastruktur
        - certificate, revocation lists, OCSP Online Certificate Status Protocol

Topic

- Structure = ASN1
  - Version
  - Serial Number
  - Algorithm
  - Issuer
    C=US, O=VeriSign Inc, OU=, ...CN=
  - Validity
    - Not before
    - Not After
  - Subject
    C=DE, O=Fachhocschule Regensburgm OU-=Informatik, CN=www.informatik.fh-regensburg.de
  - Subject Public Key Info
    - Algorithm
    - Key
  - Extensions
  - Signatur algorithm
  - signatur
- Beispiel: banking.postbank.de

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
26:65:19:20:52:6d:3e:d6:5f:e1:da:8a:ba:11:7d:00
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at www.verisign.com—rpa (c)06, CN=VeriSign Class 3 Extended Validation SSL SGC CA
Validity
Not Before: Jul 16 00:00:00 2009 GMT
Not After : Aug 15 23:59:59 2011 GMT
Subject: 1.3.6.1.4.1.311.60.2.1.3=DE/2.5.4.15=V1.0, Clause 5.(b)/serialNumber=HRB6793, C=DE/postalCode=53113, ST=NRW, L=Bonn/streetAddress=Friedrich Ebert Allee 114 126, O=Deutsche Postbank AG, OU=Systems AG, CN=banking.postbank.de

jurisdictionOfIncorporationStateOrProvinceName

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:cb:ae:35:94:6f:e3:37:f8:39:38:9a:91:b0:4e:
.....
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Subject Key Identifier:
9A:E7:84:B2:3B:B7:B3:2B:0B:64:D2:F6:F1:9E:20:A7:8C:F2:EB:D4
X509v3 Key Usage:
Digital Signature, Key Encipherment
X509v3 CRL Distribution Points:
URI:EVIntl-crl.verisign.com—EVIntl2006.crl

X509v3 Certificate Policies:
Policy: 2.16.840.1.113733.1.7.23.6
CPS: www.verisign.com—rpa

X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, Netscape Server Gated Crypto
X509v3 Authority Key Identifier:
keyid:4E:43:C8:1D:76:EF:37:53:7A:4F:F2:58:6F:94:F3:38:E2:D5:BD:DF

Authority Information Access:
OCSP - URI:EVIntl-ocsp.verisign.com
CA Issuers - URI:EVIntl-aia.verisign.com—EVIntl2006.cer

1.3.6.1.5.5.7.1.12:
0`.^.\0Z0X0V..image/gif0!0.0...+.....Kk.(.....R8.).K..!..0&.$logo.verisign.com—vslogo1.gif
Signature Algorithm: sha1WithRSAEncryption

Topic

1e:0d:f2:68:4b:bc:ad:61:d9:d0:6d:50:38:fb:8d:24:23:a6:....

- server.key
- server.csr
- server.crt
- Zertifikate, wer prüft die? HTTP? Mail?
  - HTTPS
    - Webbrowser hat liste der "vertrauenswürdigen Root CA"
    - Prüft Zertifikatskette
    - Muss dabei auf extensions achten: Basic Constraint: CA = False
  - CA, PKI
    - nimmt csr entgegen
    - prüft die darin enthaltenen angaben
    - prüft die Identität des Antragstellers
    - stellt ein Zertifikat aus
    - Stellt CRL zur Verfügung
    -
  - CAcert
    - Offene CA ohne finanzielles Interesse
    - Leider noch nicht in die Browser integriert
  - Inband / outband
    - SMTP STARTTLS
    - HTTPS
      - Probleme mit IP Addressen
  - Angriffe
    - 2009 - plain text injection during re-negotiation
    - 0 Bytes
    - In 2008, Alexander Sotirov and Marc Stevens presented at the Chaos Communication Congress a practical attack that allowed them to create a rogue Certificate Authority, accepted by all common browsers, by exploiting the fact that RapidSSL was still issuing X.509 certificates based on MD5 [2].
- ssh
  - genereller Aufbau - wie funktioniert ein System ohne CA
  - weniger bekannte Features von OpenSSH
    - forced-commands
    - ProxyCommand
- VPN
  - IPSec (standard in IPV6)
  - OpenVPN
  - PPTP
  - ssh
- Sichere Nachrichten (email)
  - PGP und S/Mime
    - Wie ist das Trustmodell
- Sicheres DNS
  - DNSSEC
- Verschlüsselte Dateisysteme
  - Warum will man das haben
    - gestolener, verlorener Laptop
    - verlorene, gestolene, defekte Platte
    - gestolendes, verlorendes Mobile Phone
  - Disk Encryption
    - LUKS

Topic

- TrueCrypt
- PGP Disk
- Windows and MacOS haben eigene encryptete Filesysteme, Folder
- Probleme: Backup
- File Encryption
- encfs
- gpg
- Praktische Fragen:
- Passwörter Ablegen
- Brute Force Passwort knacken
- Übungen
- openssl Kommando
- CA aufbauen (von Hand und mit tiny-CA)
- Key für Webserver erzeugen, CSR erzeugen
- OpenVPN aufbauen
- Shared Secret
- Certificate
- ssh
- IPSec connection aufbauen
- PGP Key erstellen, Keysigning
- entschlüsseln von Passwörtern
- **Applikationsicherheit**
- Saltzer, Schroeder, The Protection of Information in Computer Systems
- Basic Prinziplec of Information Protection
- Economy of mechanism
  KISS
- Fail-safe defaults
  Base access decisions on permissions rather than exclusion
- Always consider that something could fail - go on the safe stat
- whitelist vs. blacklist
- virus scan vs. bekannte md5 summen
- immer ein problem, wenn die menge nicht abschliessen bekannt ist
- hostname vs. hostname:80 vs. ip vs. ip:80
- Beispiele:
- Ampel nur grün, wenn die andere das erlaubt
- Unix su (alter code)
- Smartcard
- Complete mediation
  Every access to every object must be checked for authority
- file access / db access
- session permissions
- Open design
- Speration of privileges
  4-Augen Prinzip
- Least privilege
- Root account? Administrator account?
- Least common mechanism
- gemeinsame ressource vermeiden
- /tmp directory, memory, disk-space, network
- Psychological acceptabliliy
- paswort policy
- Side Channel Attacks
- Was ist das
  Bebachte das verhalten des Systems an nicht-dokumentierten Schnittstellen: Timing, CPU Last, Plattenplatz, Stromverbrauch, Speicherverbrauch und schlisse darauf auf internen eigenschaften
- Beispiele

Topic

- smartcard pin raten
- smartcard cryptokey
- Passwörter ermitteln
- Smartcard aufschleifen und key auslesen

- Aktuelle - non -web - Exploits, wie sie funktionieren, kurze Historie
  - Code injection (Buffer Overflow in stack und heap)
  - integer overflow
  - null pointer reference
  - access of freed memory
- Gegenmassnahmen
  - stack carnary
  - non executable stack
  - randomized address-space
  - Aber: Hilft alles nur begrenzt -> Fehler im Code müssen behoben oder der Angriffsvektor muss anderweitig geschlossen werden.
- Übung: statische Source Code Analyse
  - Welches Tool?

- **Authentisierung, Autorisierung**
  - LAN
    - LDAP
    - Radius
    - Kerberos
    - PAM
    - Username+Password
  - Web
    - Challenge+Response
    - Username+Password
      - HTTP Basic Auth
      - Digest
      - Form Based
    - OAUTH
    - OpenID
    - X509 client Certificate / Smartcard
  - PIN/TAN - Banken
    - iTAN
    - mTAN
    - HBCI
  - Sonstiges
    - OTP
    - SecureID
    -
- **Web Application Security (Client)**
  - Der Browser - das Einfallstor in das Firmennetz
    - Google / Microsoft
  - Plugins
    - Flash
    - Java
    - Video
    - Images
  - Trennung von Browser und Produktive-Netz
    - Visual Firewall via Terminalserver
- **Web Application Security (Server)**
  - OWASP TOP 10
    - Reference for Web-Application-Security
      - PCI-DSS

Topic

- TOP-10 2010
  - Injection
  - Cross-Site-Scripting
  - Broken authentication and Session Management
  - Insecure Direct Object Reference
  - Cross-Site-Request Forgery
- Anatomie von HTTP
  - stateless
    - Request-Response
    - GET, POST, ...
  - Beispiele ....
  - Forms
  - cookies
  - hidden Form fields
  - Session-Cookie
  - JavaScript, Java und Flash machen auch nichts anderes
    Ok, Java und Flash können eigenen TCP connection offen halten und State haben, aber in der Praxis machen die auch viele via HTTP
- Datenhaltung
  - Im Server, in der Session
  - Beim user, aber signiert
- Prinzipielles Problem: Trennung von GUI und Applikation. 'Normale' Applikationsentwickler trauen ihrer GUI.
- Angriffe
  - Injection
    Das Prolblem besteht darin, dass Daten - in diesem Falle Nutzereingaben - als Code interpretiert werden.
    - SQL-Injection
      - Immer wenn per String Operationen ein SQL Statement zusammengebaut wird, ist äußerste Vorsicht angeraten.
      - Quoting - aber welche Zeichen müssen gequotet werden?
      - Entweder strikt whitelisten oder das Quoten der Datenbank überlassen. Prepared Statements, Stored Procedures, ...
      - Benutzen Sie den ORM Layer ihres Frameworks - aber lesen sie vorher nach, ob sie quoten müssen oder nicht. Wenn sie quoten müsse, schmeissen sie den ORM Layer weg.
    - Shell-Code-Injection
    - LDAP Injection
  - Cross-Site-Scripting
  - Session Handling
    - Session-Hijacking
    - Session Fixation
  - Hidden Parameter Tampering
    - nur weil ein form-field hidden ist, heist das nicht, das es der user nicht ändern kann
    - nur weil der Wertebreich einer Variable in der GUI mit JavaScript geprüft wird, heist es nicht das man nicht was anderes zum Server schicken kann
- Beispiele
  - aktueller Facebook Wurm
- Lösungen
  - Schulung der Entwickler - Secure Software Development Process
  - Source Code Analysis
  - Pen Test / Vulnerability Scanner
    - Pen Testing vs.Vulnerbility Assesment
  - Web Application Firewall
    - zweites Sicherheitsnetz
    - Hot Patching
  - Malware Scanner
    - erkennt veränderte Webseiten und eingeschleuste Trojaner
- **Prozesse**

Topic

- Security Engineering
  - Secure Software Development Process
  - Security Development Lifecycle
    - Secure by Design
    - Secure by Default
    - Secure in Deployment
  - Bedrohungs- und Riskoanalyse
  - BSI Grundschutzhandbuch
  - BSI Sicherheitsprozess
  - Sicherheitskonzept
  - KonTraG
  - Basel II
  - SOX
  - Schutzbedarfsermittlung
  - Schutzbedarf
  - Bedrohungsanalyse
  - Bedrohungsmatrix
  - Bedrohunsbaum (engl. Attack Tree)
  - Risikoanalyse
  - PenTest
  -
- en.wikipedia.org—Trusted_Computer_System_Evaluation_Criteria
- en.wikipedia.org—Common_Criteria
- Risk Management
- Business Continuation
- Sicherheitsprozess
- Schutzbedarf / Sicherheitsziele
- Bedrohungs- und Riskioanalyse
- Sicherheitsbewertung
- Common Criteria
- ISO 27001
- Audits
-

- **Unsortiertes**
- **Lessons Learned**