CAcert Threat-Model - DRAFT

Inhaltsverzeichnis

Abstract

This is the Threat analysis document, which will be the basis for the Security Manual of CAcert.

It is the first step into the direction of Risk-Management.

Further steps that will follow:

- Explaining the unobvious Threats
- Assessment and Estimation of the Risks and the Impact
- Listing of potential, theoretical prevention mechanisms and countermeasures
- Deciding on specific prevention and countermeasures
- Creating a security manual, based on the decided mechanisms

Security Objectives (Wertedefinition)

CAcert is processing secret and confidential information from its users, and issuing certificates which are used in a wide variety of applications. Therefore a high security and secrecy level is necessary to provide the necessary confidentiality, integrity and correctness.

Trust model can be independently audited

Due to the market demands for independent audits of CAs, CAcert´s security procedures have to be documented and audited both by internal and independent auditors.

Integrity of CAcert's infrastructure and data

Non-repudiation (!?!?!) of CAcert's certificates and assertions

CAcert issues digital certificates, and thereby makes statements and assertions about its users, their identity. Due to fundamental lacks of revocation infrastructure of PKI systems, an even higher demand for correctly issued certificates exists.

User privacy

CAcert is dedicated to secure the privacy of its users, and to indirectly provide encryption as a method to improve privacy available to them.

Assets

- Servers

  - Main Webserver
  - Certificate Server
  - Secondary Server
- Datacenter Rack
- Building
- Cabling
  - Network cables
  - Serial cable
- Database
- Archiving
  - External Harddisks
- Personnel
  - Sysadmins
  - Developers
  - Translators
  - Assurers
- Users
- Reputation
- Services
  - Web
  - Mail
  - Certificate issuing
  - Assurance
  - TTP
  - DNS
  - Revocation
- Money
- Domains (cacert.org, ...)
- Administrators personal computers
- Users personal computers
- Data
  - Root keys
  - Root certificates
  - CRLs
  - sensitive User-Data
  - Assurance Forms

  - issued certificates
  - certificate requests
  - assurance data
  - user-passwords
  - codesigning ID scans

Objectives

- high security
- confidentiality
- integrity
- correctness
- authenticity
- non-repudiation

Potential enemies

- Other commercial CA´s
  - Hostile Takeover
  - Bad PR
  - Social Engineering
  - Distraction (e.g. Extended Validation)
  - Attacks on CAcert´s TVerify mechanism
  - Sending Troublemakers
- Intelligence Community
  - Backdoors
  - Espionage
  - Social Engineering
- Governments
  - Key Escrow style laws
  - Policy
  - Subpoenas
- Phishers
- Black-hat Hackers

  - Issueing *.com wildcard certificate
- Frustrated users/members/staff

Potential Targets of Attacks

- Root key
- User database
- Website
- CAcert´s Web-of-Trust
- Reputation
- Hardware
- CAcert personnel
- CAcert Incorporated
- Communication

First Level Threats

First Level Threats are threats that are inherent in the business and can´t be avoided.
Second Level Threats are threats that are emerging due to security mechanisms that can be put in place to mitigate First Level Threats.

Generic Threats

- Unavailability of the service
- Integrity issues of the service
- Secrecy/Privacy Threats
- Espionage
- Sabotage
- Theft

Hardware Threats

- Hostile Vendor (Backdoors in Servers, Switches, Firewalls,...)
  - Pre-installed
  - Exchanged during support procedure
- Hostile Hardware Replacement/Tampering
- Unauthorized physical access
- Hardware Interface attacks (PCMCIA,Firewire,USB-Stack,...)
- Availability due to hardware failures

- The client PCs of CAcert personnel
- Leak of old, used hardware

Hosting Threats

- Flood/High water/Tsunami
- Water-leak
- Earthquake
- Hurricane/Tornado/Storm
- Fire
  - Burning cables
  - Aggressive gases
- Bombing
- Temperatore/Humidity
- Dust and Dirt
- Power outage
- Lightning
- Light
- Magnetic Fields
- Airplane crash
- Burglar
- Not trust checked enough employees
- Other customers having physical access too
- War/Riots
- Virtualisation
- Raiding the servers
- Tempest
  - Through graphic card patterns

Environmental threats

- Unknown environment of administrators and users´ computers
- Ergonomic problems causing bad quality

Software Threats

- Backdoors
- Data leaks

- Spam
- Phising attack against www.CAcert.org
- MITB attack against www.cacert.org
- Virtualisation/Rootkits
- Buffer Overflows
- Security Issues in Protocols
- PHP Security issues
- An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.
- Parser Exploits (Fuzzing) -> Avoid Parsers
- Systemic Threats that spread an attack on all servers at once
  - SSH Exploits
  - SNMP Exploits
  - Linux Kernel Exploits
  - IPTables Exploits
  - Apache exploits
  - PHP exploits
  - SMTP exploits
  - ASN.1 exploits
- Violation of Copyright or specific Software Licenses

Database Threats

- SQL-Injection
  - Database dump
  - Deletion of data
  - Tampering with data
  - privilege escalation
  - Database overloading
-

System Threats

- Failure of one or more system components results in the loss of system critical functionality.

PKI Threats

- Private Key Leak of the root keys

- Private Key Leak of the user´s keys
- Private Key sharing
  - Due to too-low-entropy randomness
- Private Key distribution
  - Software vendors that ship the same private key to all their users together with the software
- Cryptographic weaknesses
  - Attacks against Hash-algorithms
- Design-issues in crypto protocols
- Usability problems that lead to security problems
- Quantum cryptoanalysis
- Threats inherited from the user´s applications
- You can´t know/verify what your computer does
- Proof-of-Possession missing
- Proof-of-Non-Possession missing
- Revocation problems
  - Expiry vs. Revocation
  - Expired certificates
- Digital Signatures
  - Multiple inline-signing of documents changes the document and therefore breaks/invalidates earlier signatures
- Non-Repudiation
- Bad quality of the users´ private key since CAcert can´t verify the quality, and the user doesn´t have much mechanisms to do it either.
- A system or applications developer delivers code that does not perform according to specifications or contains security flaws.
- Browsers or other software that is used by the relying party does not recognize the root certificate
- Unknown history of a root key
- Key-Leaks in Block-encryption
- Forgotten quality control in cryptographic implementations
  - http://labs.musecurity.com/2007/09/18/widespread-dh-implementation-weakness/
  - http://cryptome.org/bug-attack.htm

Identity Threats

- Errorneous ID documents
- People not having any ID documents at all

  - Too costly ID documents
- Middle names
- Single names (lacking a lastname)
- Different official Transliterations of the name
- Bad quality of ID documents

Data Threats

- Publication of user-database / user data
- Loss of user-database
- Leak of personal data
- Unicode Homograph attacks
- Trusting Relevant data in unknown Languages
- TVerify and other mechanisms assigning points to unverified fields
- Different formats (e.g. date formats)
- Naming problems
- Bad data quality due to humans carelessly verifying data instead of humans entering data and computers automatically verifying the data
- Proper deletion/wiping of data
- Stolen Assurance forms
- Domain owner-change not noticed by CAcert.org
- Email owner-change not noticed by Cacert.org
- Software testing with production data

Backup Threats

- No backups
- Lost backups
- Stolen backups
- Missing backups
- Backups that are missing because they were never created
- Deleted data that is restored through backups -> Privacy
- Backups made with software that isn´t available anymore
- Backups made with software that doesn´t run anymore
- Backups made with hardware that isn´t available anymore
- Backups in dataformats that aren´t readable anymore

- Tampered backups
- The usual PKI Threats with encrypted backups

Procedural Threats

- Personal Assurance
  - Poorly done assurance
  - Erroneous assurance
  - Fraudulent assurance
- Organization Assurance
- Super Assurer
- Teenage assurers
- Missing or wrong validation of fields due to insecure workflow

Product Threats

- Code Signing
- Sub-CAs
- Quality control mechanism on assurances missing
- People having control over Cas that are recognized by Tverify are able to inject false identities into Tverify
- Email Ping for Email Addresses or Domains
  - Interception
  - Redirection of DNS/Whois
  - Manipulation of Whois Servers

Privacy Threats

- If the user uses his client certificate for authentication purposes for many sites, it is possible to build a dossier (profile) of him by a collaboration of visited web sites.
- A collaboration of the certificate issuer and the verifier may create a threat to the users privacy right.
- Possibility of creating blacklists based on Certificates on Internet routers
- CAcert collects DOB(day-of-birth) which is not necessary for identification purposes.
- Users might provide sensitive information for the lost pass phrase questions.
- Assurers and TTPs may misuse the information given by the users
- Assurance forms might not be protected enough against unauthorized accesses
- The procedure to send filled applications to CAcert might not be secure enough.

- The victim does not have much chances to get to know when someone mishandles the filled application form.
- The user might not be informed about:
  - The purpose of the information that has been collected by CAcert and the Assurers
  - To whom the collected information will be disclosed
  - The possibility to get the personal information deleted
- CA Personnel might be untrained in privacy issues and correct handling of procedures

Governance Threats

- Missing Dual Control

Communication Threats

- CAcert.org being disconnected from the Internet
  - because of wrongly classified Spam
  - because of Subpoenas
  - because of wrongly configured routers from the ISP
- DDoS attacks are unlikely
- A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.
- Bad information communication on the website
- Sending CAcert-internal confidential communication in plaintext
- Tapping of data by other computers connected to the same networks
- Tempest
- Attacks on CAcert email communication:
  - Tapping
  - Interception
  - Delaying (Greylisting)
  - Manipulation

Audit Threats

- Auditor closing down operation
- Auditor leaking confidential information
- Conflicts of Interest with other customers of the Auditor
- Auditor overlooking problems

- Auditor gaining bad reputation

Vendor Threats

- Conflicts of Interest with other customers
- Hardware+Software vendors:
  - Backdoors
- New, incompatible interfaces from e.g. Microsoft
- Unavailability leading to not closing bugs

Personell Threats

- Affected:
  - Administrators of the Servers and Services
  - Core-Developers (who are developing themselves or approving changes from Non-Core-Developers)
  - Support-Personnel (who can access personal data, and have support-privileges on the database)
  - Internal auditors
- Missing Knowledge
- Trustworthiness
- Social-Engineering
- Extortion
- Loss of daytime job
- Loss of life
- Personal financial problems
- Conflicts of Interest
- Administrators, Operators, Officers or Auditors fail to perform some function essential to security.
- User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.
- User accidentally deletes user data rendering user data inaccessible.
- Loss of knowledge
- Espionage
- Unprofessional Risk-analysis can harm the reputation of involved CAcert personnel

Policy Threats

- Bad policy
- Outdated policy

- inaccurate policy
- unspecific policy
- unknown policy
- wrongly understood policy
- writing policies that sound good, but are impossible in practice
- unwritten policies

TrustCheck Threats

- Background checks on Cacert personell could be too privacy invasive
- Conflicts of interest might go unnoticed

Service Threats

- Revocation unavailable
  - OCSP unavailable
  - CRL´s unavailable
  - DNS unavailable
- Revocation systems give wrong results
  - Internal errors
  - Manipulated data
  - Bugs
- Website unavailable
  - DNS unavailable
  - Server unavailable
    - Webserver
      - Hacked website
    - Physical server
  - Firewall problems
- Certificate issuing unavailable
  - Website
  - Certificate Server
  - CommModule
- Support-contact unavailable
  - Mailserver
  - Website
- Wiki
  - Modifications on unprotected sites

    - Spam
    - During a Slashdot attack
- Slashdot Attacks

Education Threats

- Tests that are too hard can drive people away
- Tests that are too easy can drive people away
- Tests that are stupid can drive people away
- Assurers not knowing what they have to do
- CAcert personnel not knowing what they have to do
- Users not knowing what they have to do

User Threats

- Browsers without included root certificate
- getting phished
- Identity Theft
- inappropriate reliance on the certificates
- Accidental revocation of certificates
- Theft of users private key
- ID + sensitive information revealed
- Arbitration results
- Liability Threats
- Loss of users´ private key
    - Due to not knowing that it exists, and that it is needed
    - Broken Harddisk, Reinstalled computer
- MITM
- MITB, circumventing PKI

Legal Threats

- Subpoena against CAcert
- Confiscation of servers due to bogus claims
- Dataprotection backed data deletion request
- Dataprotection related problems because of TrustCheck
- CAcert´s assurance practices could be prohibited in some countries
- Dataprotection laws in all the countries CAcert operates servers

- Implied gain by the use of certificates might come to us as a lawsuit because we don´t have something that states otherwise clearly pointed out
- Violation of specific Software Licenses

Financial Threats

- Financial Threats from Qualified certificates
- Lawsuits (Class-action?)
- Internal Fraud
- Legal costs
- Liability

Cultural Threats

- Different concepts of roles like public notaries, bank managers, ... in different cultures

Public Relation Threats

- Catastrophe scenarios
  - Leaked root Key
  - Wrongly issued class3 certificate
  - Wrongly issued class1 certificate
  - Wrong assurance
  - Crypto issues
  - Failed Audit
  - Changed Audit Requirements
  - Server-Hack
- Bad PR due to unhappy users
- Assurers without enough knowledge might give interviews or write articles for the press
- Advertising on the website
- Unrelated Advertising on the website (“Spam”)
- Bad information communication on the website
- Security requirements (specifically of the website) hindering effective communication

Board Threats

- Being liable for not acting
- Unavailability for important decisions
- Unavailability of CAcert Inc. assets
- Uncoordinated Handover from a previous board to the next board

Social Engineering Threats

- Users talking assurers into being assured wrongly
- Users talking TTP´s into being assured wrongly
- Users talking support-team into getting
  - password reset

  - a certificate revoked
  - assurances revoked
  - codesigning attribute
  - their name changed
  - their DOB changed
- Users talking Organisation Assurers into doing organisation assurance for someone else´s organisation
- Journalists talking assurers/users into writing articles

External Threats

- A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

Others

- Wrong Risk Analysis
- Threats from Unassured/Anonymous certificates
- Time synchronisation
- Wrong timestamps
- Logfiles
- Too much bureaucracy -> usually leading to availability problems
- we have too many people doing things without official approval and releasing as official

Second Level Threats

Security Mechanism Threats

Full-Disk-Encryption

- Unavailability of key in case of crash
- Unavailability of authorized personnell to boot the machine
- Unavailability of the key in case of harddisk-recovery due to lost key-block, (but available password)

- Key-Logger between Computer and Keyboard (independently whether the keyboard is directly attached or remote. This problem is slightly mitigated by ILOs that are contained inside the computer
- Leakage of password or key or confidential data on unencrypted partitions (swap-partition!)
- Leakage of password or key or confidential data between the installation of the operating system and the installation of the FDE-Software
- Attacks on the processor, the PCI bus, or any other logical access that could be seen as a bypass of the FDE
- Cryptographic or implementation weaknesses of the FDE
- Cryptographic Collision problem with larger harddisks
- Tampering of the Bootloader or the FDE software through a physical access attack

Password Security for Accounts

- Too short passwords
- Unavailability of authorized personnell that knows the necessary passwords
- Stolen passwords
- Leakage of passwords

ITTC

- Leakage of too many shares
- Stability problems
- Worse scalability than normal RSA with larger keylenghts
-

Destination Encryption

Destination Encryption is a mechanism to transfer confidential and secret data to a different machine.

Web-Application-Firewall

- A backdoor in Airlock, providing application-level access
- A leak of the SSL server certificate

Layer3 Firewall

- Unavailability
- Leaking of the SSL server certificate in case of SSL termination
- Disclosure of the internal network structure

Tor

- Tor-Phising (should be irrelevant to our planned scenario)
- Parser Exploits

RPC

- Could make SQL injection possible
- Parser Exploits

3-Tier architecture

- Added complexity
- Session issues

Email-TAN

Encrypted Backups

- Unavailability of authorized personnell or keys or passwords

Encrypted Logfiles

- Unavailability of decryption keys
- Data-Leaks on the Log-Inspection-Computer

Smartcard

- WYNSIWYG – You don´t see what you get

HSM

- Temperature problem (too hot / too cold)
- End-of-Battery (being disconnected from power for too long)
-

Version Control Threats

- Injection of malicious code

Dual-Screen

Offline Root CA

-

References

- http://www.iang.org/ssl/pki_considered_harmful.html
- http://www.iang.org/ssl/browser_threat_model.html
- http://www.iang.org/ssl/rescorla_1.html
- http://wiki.cacert.org/wiki/RisksLiabilitiesObligations
- http://www.bsi.de/gshb/