

Developments in Public Key Certificate Revocation

Norsk Kryptoseminar 2004

08.11.2004

André Årnes, PhD student
andre.arnes@q2s.ntnu.no

Background

- NORDSEC 2000 “ Selecting Revocation Solutions for PKI”
- The thesis ‘Public Key Certificate Revocation Schemes’ was submitted to the Norwegian University of Science and Technology in February 2000.
- Based on work at Queen’s University in co-operation with Entrust Technologies. The work was supervised by Henk Meijer, Steve Lloyd, Mike Just, and Svein J. Knapskog.

Agenda

- Certificate revocation
- Certificate revocation schemes
- Discrete event simulations
- Conclusion
- Further work

Certificate Revocation

- The action of declaring a certificate invalid before its validity period is at end
- Requires a separate mechanism to inform all users about revoked certificates
- The revocation status of all certificates in the certification path must be checked
- Example reasons:
 - Key compromise
 - Change in user or identification data
 - Change of relationship between user and CA
 - Change of key allowed key usage

*“A nuisance or system bug that
defeats the very purpose of PKC”*

Certificate Validation

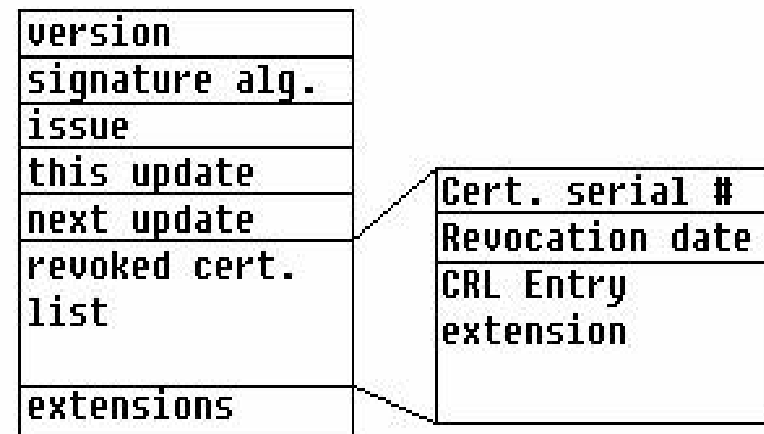
- Process for checking certificate validity;
- Tester:
 - Validity Period;
 - Integrity;
 - Certificate path;
 - Intended key usage;
 - Revocation status

Evaluation Criteria

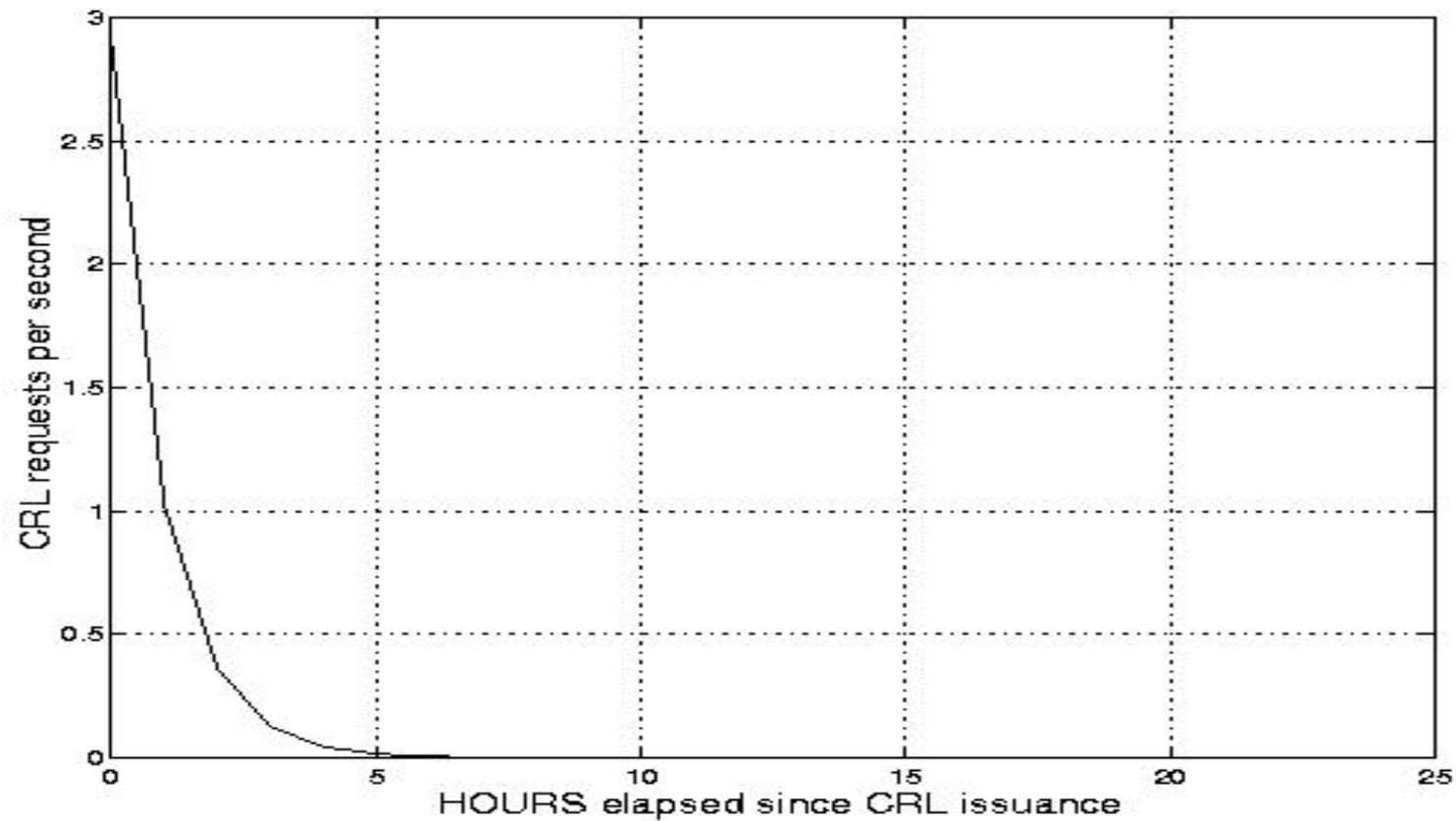
- Performance
- Timeliness
- Scalability
- Security
- Standards compliance
- Expressiveness
- Scheme management
- On-line v. Off-line

CRL - the Traditional Approach

- CRL - certificate revocation list: A periodically distributed list of all recorded revocations
- Similar to a 'blacklist'
- The most common scheme
- Accused of being inefficient and untimely due to the size of the lists



Typical CRL request rates

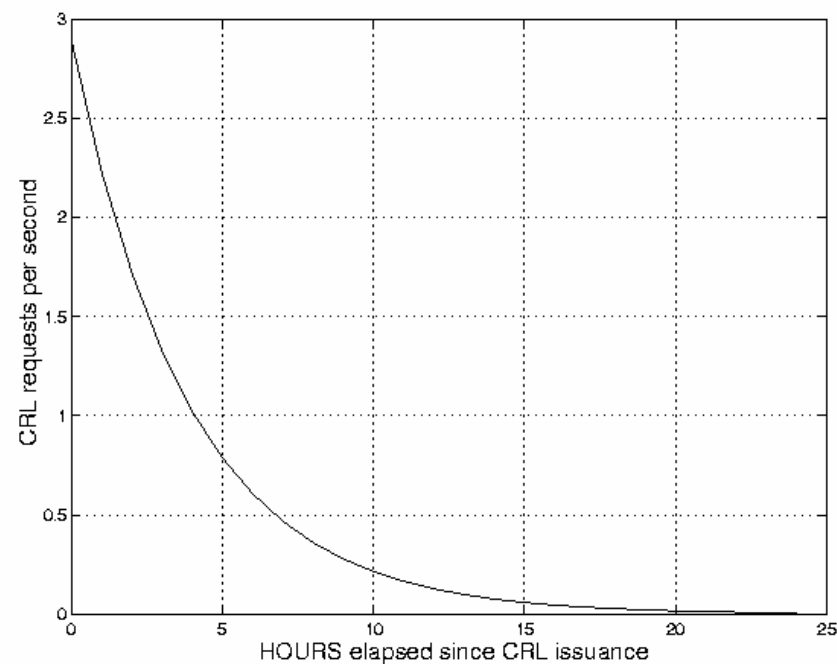
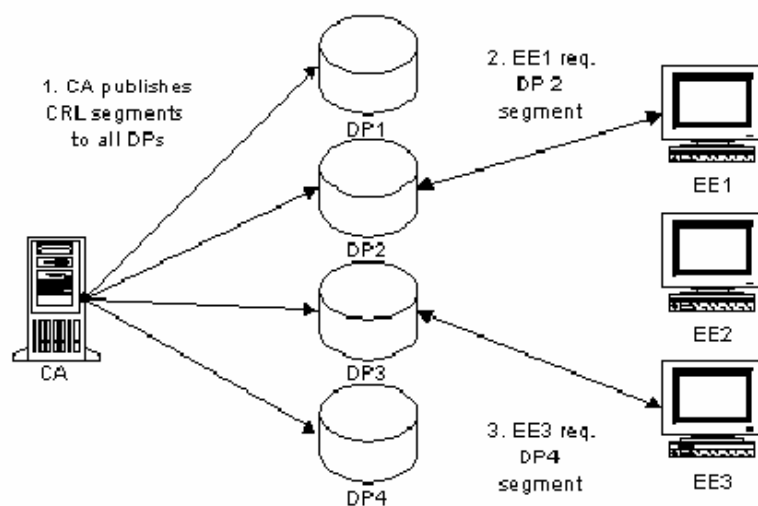


CRL Modifications

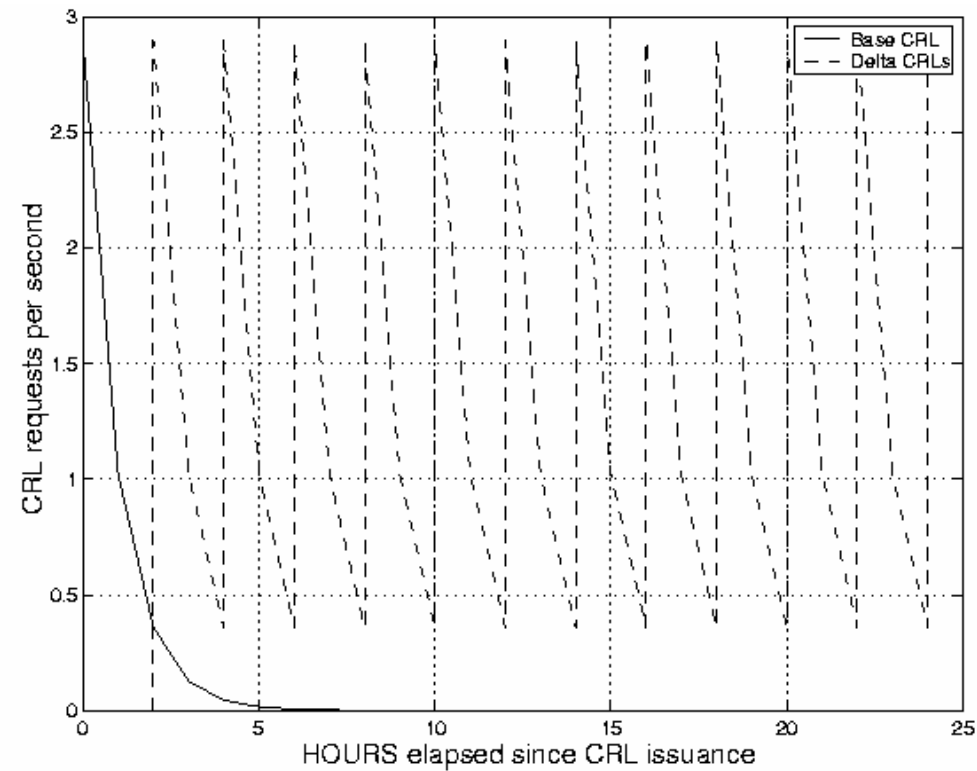
A number of modifications have been suggested in order to improve CRL. These modifications are either parts of or proposed as part of the X.509 framework.

- Distr. Points (DP)
- Delta CRLs
- Over-issuing
- ARL
- Indirect CRL
- Dynamic DP
- Freshest revocation information

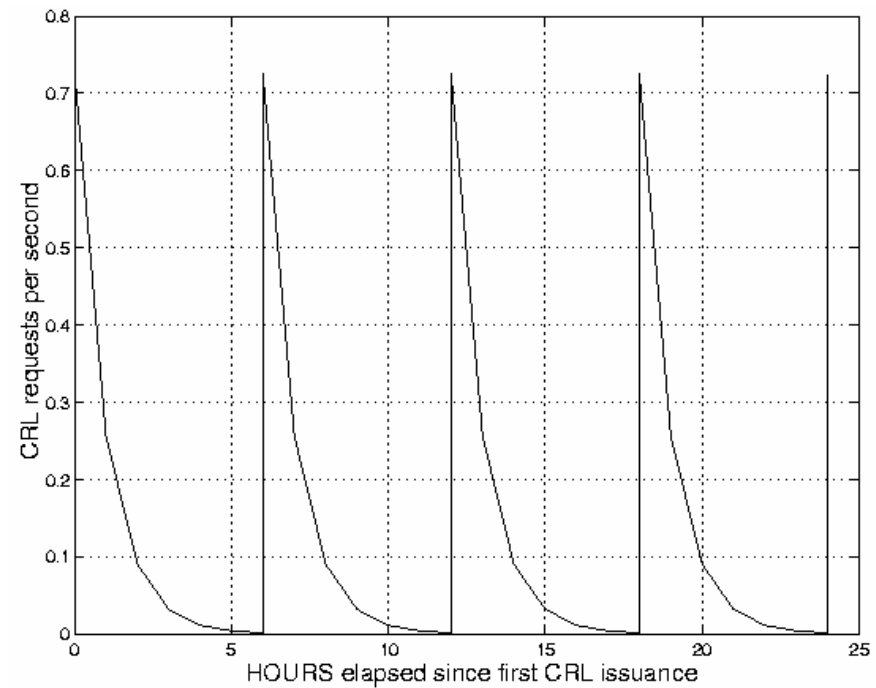
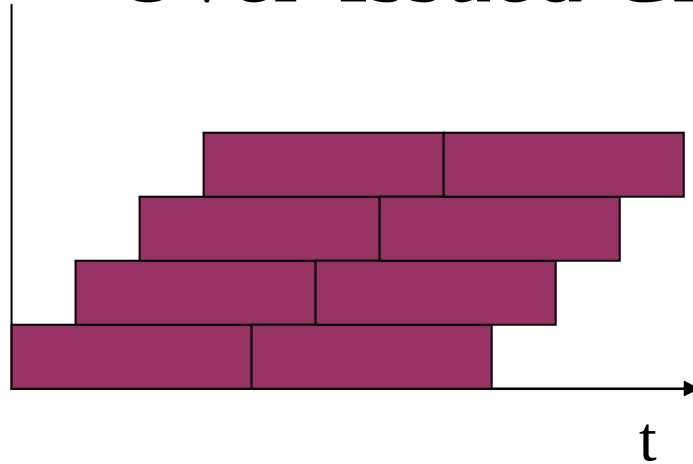
CRL Distribution Points



Delta CRL



Over-Issued CRL



On-line Approaches

- An attempt to create timely or even real-time revocation information
- OCSP - On-line Certificate Status Protocol
- The problem is that each response have to be digitally signed, causing a high processing load on the server
- OCSP-X: OCSP Extensions
- SCVP: Simple Certificate Verification Protocol
- DCS: Data Certification Server

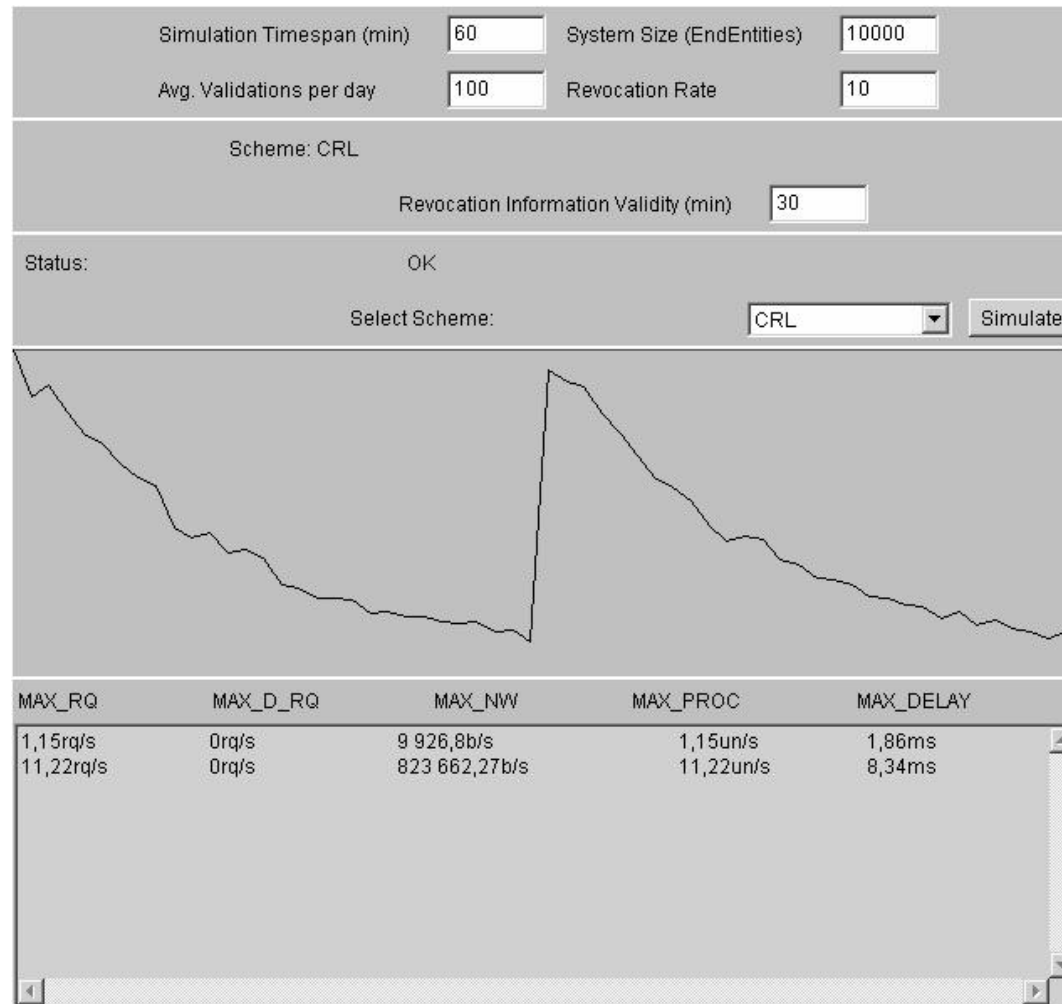
Reducing the load

- Reducing the size of the revocation information as well as reducing the load involved in digitally signing responses
- Certificate Revocation Trees (CRTs): All revocation information is represented by a hash tree. The use of secure hashes ensures the authenticity and integrity of the revocation information in a compact format.
- CRS: Certificate Revocation Status Directory
- HCRS: Hierarchical Certificate Revocation Scheme
- Naor/ Nissim

Object Oriented Discrete Event Simulations

Environment	Size	Validation Rate	Validity Period	Revocation Rate
A	100	5/day	2 weeks	10%/year
B	1000	100/day	60 min	10%/year
C	10000	25/day	30 min	10%/year

Simulation Interface



Simulation Results

- Simulated CRL, CRL DP, Delta CRL, Delta CRL with DP and OCSP
- Combinations of Delta CRL and CRL Distribution Points improved timeliness and provided reduced network load and delay;
- OCSP provides low network load, but high CPU load and delay.

Conclusions

- Different mechanisms for different problems; no optimal solution;
- Possible to improve performance by combining mechanisms;

Comparison of Schemes

	Perform.	Timeliness	Scalability	Security	Standards	Off-line
CRL	High load and req.	Low	Low	2-party	X.509	Suitable
CRL DP	Improves CRL	Improves CRL	Improves CRL	2-party	X.509	Less suitable
Delta CRL	Improves CRL	Improves CRL	Improves CRL	2-party	X.509	Generally suitable
OCSP	High processing	High	Linear growth	3-party	IETF PKIX RFC2560	Unsuitable
CRT	Reduced size and processing	High (unless caching is allowed)	High	3-party	Patented	Suitable if caching is allowed

Combining revocation schemes

- Improved performance, scalability and timeliness at the cost of higher complexity.
- Non-repudiation issue as a result of several valid revocation information sources.
- Examples: Over-issuing with delta-CRL or CRL DP, Freshest revocation scheme, Delta CRL with distribution points

Further Work

- Find good solutions for revocations in specialized environments, e.g. mobile systems, distributed processing;
- Study new mechanisms for revocations;
- Extend simulations to include more mechanisms;
- Perform statistical analysis on simulation data;
- Perform statistical analysis on live systems.

Infrastructure Specific Schemes

- NPKI (Nested PKI): “*Reducing Certificate Revocation Cost using NPKI*”, Albert Levi and Cetin Kaya Koc, IFIP TC11, 2001
- Globe – revocation of authorization certificates in distributed systems: “*A Certificate Revocation Scheme for a Large-Scale Highly Replicated Distribution System*”, Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum, IEEE ISCC03, 2003
- Revocation as a risk control strategy: “*Nonmonotonicity, User Interfarcers, and Risk Assessment in Certificate Revocation*”, Ninghui Li and John Feigenbaum, Proceedings of the 5th International Conference on Financial Cryptography, 2002
- Peer-to-peer CRL exchange in ad-hoc environments: “*Certificate Revocation System Based on Peer-to-Peer CRL Distribution*”, Matei Ciobanu Morogan, Sead Muftic, The 9th International Conference on Distributed Multimedia Systems, 2003

Questions ?

Also, take a look at: <http://www.pvv.ntnu.no/~andearn/certrev>

A. PKI - Public Key Infrastructure

- An infrastructure for implementing public key cryptography (PKC)
- A public key certificate represents a user's public key, identity and other attributes. It is digitally signed by a trusted third party, called a Certification Authority (CA).
- ITU-T X.509 and IETF PKIX

B. References

- Andre Årnes, Mike Just, Svein J. Knapskog, Steve Lloyd, Henk Meijer. "*Selecting Revocation Solutions for PKI*", Proceedings of NORDSEC 2000 Fifth Nordic Workshop on Secure IT Systems, Reykjavik, 2000.
- Andre Årnes. "*Public Key Certificate Revocation Schemes*", Siv.ing. (Master) Thesis, Norwegian University of Science and Technology, February 2000.