# QUANTUM CRYPTOANALYTICS

Current situation 2013

# WHAT IS A QUANTUM COMPUTER?

- A quantum computer can calculate an algorithm on many input values at the same time, but it can only give one result.

- A quantum computer uses quantum mechanical physical effects to calculate with many values at the same time.

- quantum computers can execute a few algorithms that would not scale on normal computers.

# COMMERCIAL INTEREST

- The first quantum computers have been sold in 2013 on the free market, so we should take a look at the topic now.

# DIFFERENT QUANTUM COMPUTER ARCHITECTURES

- There are currently 2 different architectures of quantum computers known (which can be thought of like the Von-Neumann, Turing and Harvard architectures)
- Adiabatic Quantum Annealing
  - finds the global maximum of a mathematical function
  - are commercially available (~ 20-50 Mio. EUR) from D-Wave-Systems
  - useable for pattern matching, optimisation, image recognition and similar topics, and they are successful.
  - the architecture is not usable for Shor and Grover algorithm
- universal register based quantum computer architecture
  - is usable for the shor algorithm
  - is commercially not that interesting
  - has not been scaled up and is not commercially available yet

# SIMULATION

- with a good supercomputer / cluster, you can simulate small quantum computers
  - a univerity is offering 7 Qubits as a cloud service

# SHOR ALGORITHM

- can factor prime numbers  (and
- has been successfully tested and it works on small universal register quantum computers
- breaks the following algorithms if scaled up:
  - RSA, DSA, ECC(elliptic curves)  (all public-key encryption and signature algorithms in widespread use)
  - DH (Diffie-Hellman) (a key-negotiation algorithm, which is in widespread use)
- therefore affected:
  - X.509 certificates (RSA,ECC), OpenPGP keys, Bitcoin addresses
  - SSL/TLS, HTTPS, OnlineBanking, …
  - SSH
  - Digital Signatures, XMLDSig -> e.g. Austrian citizen card / Bürgerkarte
  - IPSEC -> VPN, S/Mime
  - IEEE802.1X (Ethernet Authentication used for WLAN)

# HISTORY

- 1982: publication of the idea and necessity for a quantum computer by nobel price winner R. Feynmann
- 1994: publication of Shor algorithms
  - Open questions: Does Shor algorithm work at all? Does quantum mechanics work that way in practice?  Is it possible to build a quantum computer so large that it can break pracitcal keys (~ 2000 Qubits are necessary)?
- 2001: realisation of a quantum computer on a universal register quantum computer architecture by IBM Lab in the USA with 7 Qubits, which broke 15 into 5 * 3
  - IBM seems to have hit scaling limitations with their architecture back then, and later tried a different way, but no further successes have been reported.
- 2013: D-Wave has doubled from 2008 – 2013 their quantum annealing computer every year, reaching 512 Qubits in 2013, and estimating 1024 Qubits for 2014

# PROOFS

- 2001 was prooven that the Shor Algorithm works in practice.
- 2013 was prooven that it´s possible to scale up quantum computers
- But both proofs are not directly related, nobody demonstrated a scaled implementation of the Shor algorithm yet.
- In 2014, D-Wave claimed that they could build a universal register quantum computer, but they are currently not interested in doing it, since there is no interesting commercial market for it.

# MEDIA ATTENTION

- Question:
  - If somebody scales up Shor, will he tell us?

- What does he gain from telling us? As soon as the public will know it, the affected algorithms will be exchanged, so the investment costs of the project will likely only be fruitful for a short period of time, if it became public.
  - Due to that risk, only few will be interested in really doing the investment.
  - When someone does the investment (likely >50 Mio. EUR), there is likely a big interest in keeping the investment secret

# MEDIA ATTENTION

- Question:
  - Will he be allowed to tell us?

- Therefore:
  - I estimate 90% probability, that Shor is scalable
    - I see a few spots though, where it might not scale
  - I estimate 50% probability, that we will be told when someone does it
  - I estimate 25% probability, that it happened already
  - I estimate 70% probability , that it will happen within 15 years

- Do we want to read "New quantum computer breaks all internet encryption" in the newspapers, unprepared?

- How can we secure OnlineBanking, VPNs, … again?
  - Due to several network-effects on multiple layers, it is very hard
    - Clients and Servers
    - Clients and Servers and Certificate Authorities

# A THEORETICAL COMPARISON

- This migration project from classical public-key algorithms to Post-Quantum Crypto can be compared to the IPv4->IPv6 migration:

- IPv4 would be: We have a potential problem with the material PVC
  - the ressources for it are exhausted.
    - We cannot build any new water pipes
      - ok, we have to find a new material and produce new pipes

- Quantum computers: We have a potential problem with PVC
  - it might start to leak water within the next 15 years
    - we have to find and replace all existing PVC pipes,
      - preferrably before it happens

# WHAT DO WE WANT TO SECURE?

- 1x E-Commerce, please. What do I have to do to secure my E-Commerce site?
  - implement new crypto algorithms into the crypto libraries
    - add support in all Browsers (approx. 10 important vendors)
  - upgrade the whole certificate hierarchy
    - SureTrust Global CA
      - Company Subordinate
        - Company.com
  - the new algorithms need to be implemented into the load-balancers, SSL-Hardware accelerators, …

# POST-QUANTUM CRYPTOGRAPHY

- We currently do not have any post-quantum secure algorithm alternatives on the market for RSA, ECC, DH
  - but we have a few algorithms in the academic kindergarten, which have not fully matured yet
- Some scientists around D. Bernstein have worked between 2004-2007 on the project "Post-Quantum Cryptography", but there does not seem to be much activity there since then
- At the most important vendors, I did not see any indications that they are seriously working on a solution yet.
  - Microsoft Research has at least shown academic interest
  - Most academics prefer to play around with ECC, but ECC is similarlily affected by quantum computers (and possibly hit even harder)

# UPGRADE

- The vendors will need some time to bring their software update into the field
  - How long will it take Microsoft to update the Windows XP installations they caused?
- Time-to-Market: approximately **5-20 Years**
- **But we expected it to be broken within the next few years, right?**
- therefore:
  - We should start with the rollout now!

# ONE OF THE POSSIBLE SOLUTIONS

- There are several algorithms that might be usable
- most of them are unpractical, e.g.: McElisie keylength ~ 1 MB
- Currently potentially realistically usable is **NTRUencrypt+PASSsign**
  - both are based on mathematical lattices
  - both are being developed by SecurityInnovation in Boston, US
- A replacement for Diffie-Hellmann might be "supersingular elliptic curve isogenies"
- NTRUencrypt
  - has already survived a decade of Cryptoanalysis (with attacks and further improvements)
- PASSsign
  - at first there was NTRU-Signature-Scheme(NSS), then NTRUsign, both were broken, therefore PASSsign was chosen as successor.

# POTENTIAL PROBLEMS

- Licensing
  - NTRU is patented, but the patents will expire within 10 years
  - NTRU is licensed unter the GPLv2
  - Commercial licenses are available for 0.5-2$ per Device
- There are attacks from Ngujen and others
- http://arxiv.org/abs/1301.6176

# SOLUTION PROPOSAL: DECOUPLING DEPENDENCIES

- We need a way to be able to silently start upgrading clients, servers, certificate authorities and certificates independently from each other, so that we can increase the effective security as soon as possible
- we can´t wait 20 years for every system to support new technology before we start rolling out new certificates, and existing systems and solutions should continue unaffected by the migration.
- We should start with the rollout now, even though we are not 100% sure, whether NTRU and PASSsign will withstand further attacks. Therefore we should augment the current RSA certificates with NTRU and PASSsign, so that we have at least the security level RSA provides and at best security against Quantum computers
- We should design the rollout in a way that we can start it now, and that the rollout can scale up easily and securely if RSA becomes publically broken
- The new security level should not get below the existing RSA/ECC level

# MIGRATION SCENARIO

- Migration scenario RSA -> RSA+NTRUencrypt+PASSsign
- 1. Adding optional NTRU+PASSsign keys into Certificate Requests and Certificates
  - Double Encryption RSA+NTRU and double Signature RSA+PASSsign where possible, therefore we decouple the rollout from security issues inside NTRU/PASSsign
  - and we decouple the Clients from the servers, since the extensions are optional, so peers do not need to be able to recognize the extensions in the beginning.
- 2. Using RSA + the now existing NTRU keys and certificates
- 3. If we are sure in the future that NTRU is strong engough, we can then start replacing RSA completely, by issuing certificates with NTRU only. But this will not start before 2025.

- At the moment, nobody else seems to seriously work on a practical migration scenario of Post-Quantum Cryptography for praxis-relevant products.

- but if we start with it now, it will hopefully not be too late when we really need it.

# TODOS

- We need to establish a community for the implementors of Post-Quantum Crypto
- Implementing the crypto-functions in OpenSSL, Firefox
- Analysis of all places where we are using RSA, ECC, DH, and where and how the keys are stored, …
  - doing a small risk-analysis
    - Priority – What do we want first ?
      - Slowest vendors first or biggest cost/effect ratio?
- Developing and documenting Solution proposals, how the new keys are stored, managed, …
- Building reference implementations
  - WolfSSL+BouncyCastle both have some NTRU integration, more work will be needed

# TODOS

- driving Standardisation
- organising Interoperability tests
  - For an IETF Standard we will need 2 interoperable Implementations-> WolfSSL+BouncyCastle
  - For practical implementations, we should do OpenSSL
- developing Security Standards for NTRU/PASSsign
  - What do we have to look for when we develop an application?

# REFERENCES


- Shor:
  - http://de.wikipedia.org/wiki/Shor-Algorithmus
  - http://web.physics.ucsb.edu/~msteffen/papers/nature_shor.pdf
- D-Wave:
  - http://www.dwavesys.com/
- Post-Quantum Cryptography:
  - http://en.wikipedia.org/wiki/Post-quantum_cryptography
  - http://pqcrypto.org/
  - http://pqcrypto2014.uwaterloo.ca/
- NTRU
  - http://de.wikipedia.org/wiki/NTRUEncrypt
  - https://www.securityinnovation.com/security-lab/crypto.html
  - http://yassl.com/

# FINANCING IDEAS

- Bitcoin community
- Credit card operators
- Security Community
- Kickstarter-campaign
- NLnet.nl (next Deadline: 1.11.2013)
- netidee.at (next Deadline: 10.2014)