Cryptographic Applications in Industry (I)

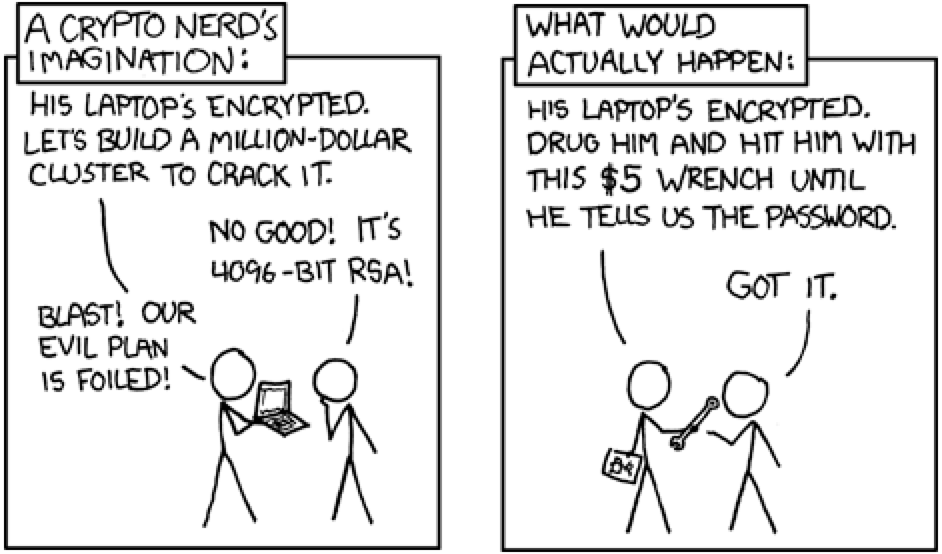
Part 1: Security in Digital Video Broadcast

Turid Herland

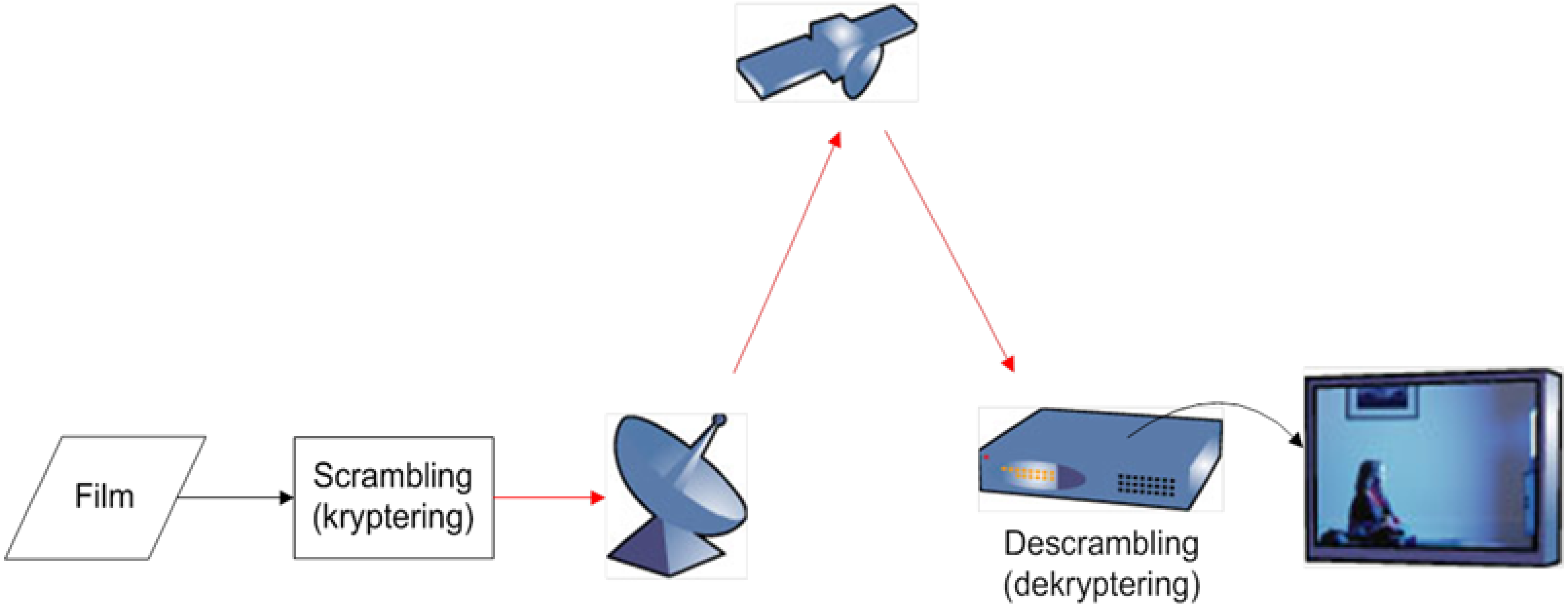
28. April 2016

Finse Winter School

Theory vs the real world…


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Digital Video Broadcast (DVB)



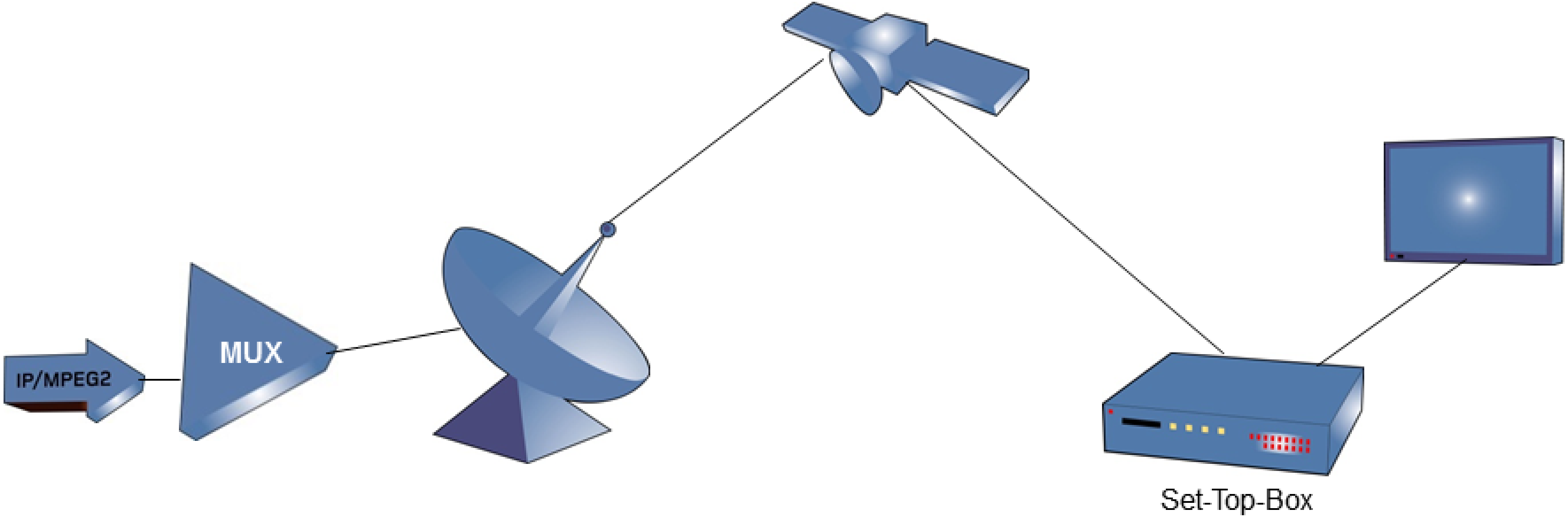
DVB Security

- Video scrambling
  - Scrambling algorithm (encryption)
  - Generation of scrambling keys
  - Distribution of scrambling keys
  - How often to change scrambling key?/How much video content can be encrypted with the same key?
  - Which receivers have payed for access to which TV channels?

DVB Standard

- Specifies transport stream format
  - Video, crypto keys, management messages all broadcast in the transport stream.
- Specifies scrambling algorithm: CSA
  - Common Scrambling Algorithm
- Multiplexer (MUX) assembles the transport stream
  - Multiplexer also generates scrambling keys
  - Multiplexer encrypts video with scrambling key

DVB – more details



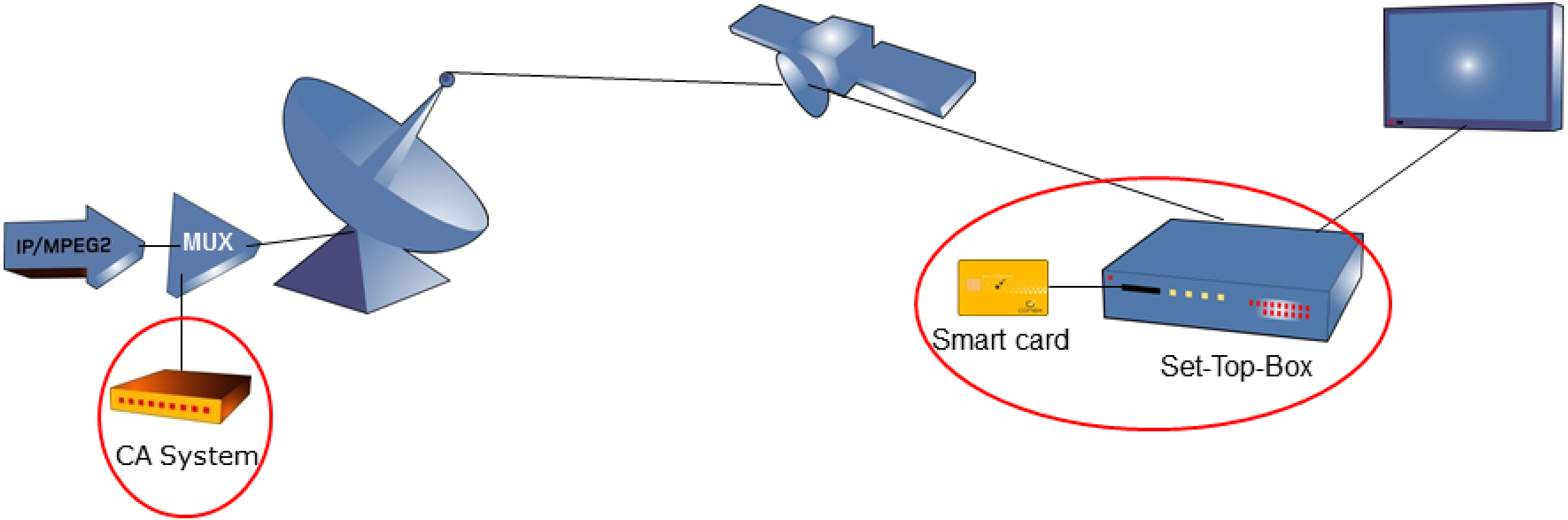
Conditional Access (CA)

- System to control access to TV content.
- Distribution of scrambling keys.
- Management of user access rights.
  - Which TV signal receiver should have access to which channels when.

Key distribution

- Multiplexer has scrambling key.
  - How to deliver scrambling key to TV signal receiver?
- Send key in an encrypted message in transport stream.
  - How to deliver key encryption key to receiver?
- Textbook “solution”: Assume a secure channel…

DVB – even more details



DVB Key Distribution

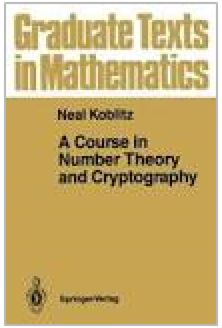
- Keys distributed on smart cards and in STB chipsets.
- Key hierarchies
  - Top level keys embedded in secure hardware – cannot be changed.
  - Lower level keys stored encrypted in regular memory.

Key Management

- Conax has produced millions smart cards.
    - Hundred of millions of keys.
- Requires a good management system to keep track of all keys.
    - Secure storage of keys
    - Key metadata
        - Intended key usage
        - Which customer the key belongs to
- For security reasons, there is cryptographic separation between different TV operators.
    - What if two TV operators want to merge their services into one?

Key Generation

- “A lot has been written concerning efficient and secure ways to generate random numbers, but we shall not concern ourselves with this question here.”



Graduate Texts in Mathematics

Neal Koblitz

A Course in Number Theory and Cryptography

Springer-Verlag

- How do you produce hundreds of millions of keys with good random properties?
  - Dedicated hardware random generators.

DVB Video descrambling

- STB receives scrambled video and message with encrypted key.
- Sends encrypted key message to smart card.
- Smart card decrypts message, and checks if this user is authorized to watch this video.
- If authorized, smart card releases scrambling key to STB.
- STB descrambles video, and sends it to screen.

Involved parties

- DVB standard – specifies scrambling algorithm.
- Multiplexer – generates scrambling key and implements the scrambling algorithm.
- Smart card – decrypts the scrambling key and checks authorization.
- STB – descrambles the content with the scrambling key.

Scrambling algorithm

- Scrambling algorithm CSA2
  - Two ciphers in combination
    - One block cipher
    - One stream cipher
  - 64-bit keys
- Was kept secret until 2002
  - Hard to attack an algorithm you don’t know
- Has some cryptanalytic weaknesses
  - But scrambling key is changed every 10 seconds, so no real impact on security.

Multiplexer

- Good quality random source required.
- Important that next key cannot be predicted from series of previous keys generated.

Smart Card

- Produced by Conditional Access vendor (Conax).
- Includes system to keep track of which channels user shall have access to.
  - Separate encrypted messages in the transport stream manage these access rights.
- Decrypts scrambling key, and releases to STB if access is granted.

Set-Top-Box

- Descrambles video with key received from smart card.
- Descrambling algorithm implemented in HW.

How the internet changed Conditional Access

- Hackers have been able to retrieve the plaintext scrambling keys from some set-top-boxes.
- This was not really a problem, since each key only scrambled 10 seconds of video.
- However, internet turned out to be a great key distribution channel for hackers.

Chipset Pairing

- A solution to internet key sharing.
- When the STB chipset is produced, a secret key is embedded in secure hardware.
- Smart card encrypts scrambling key with chipset key before releasing it to the STB.
- Scrambling key is decrypted in a dedicated HW process that feeds it directly into the video descrambler.

Cryptographic Applications in Industry (I)

conax

Part 2: Why Security by Obscurity Works

Turid Herland
28. April 2016
Finse Winter School

Obscurity

- Obscurity = the state of being known to very few people.
  - Security by obscurity doesn’t work when you don’t have obscurity any more.
  - Keeping things secret is difficult, but not always impossible.

Kerckhoffs's principle

- Originally one of his six design principles for military ciphers:
  - #2. It should not require secrecy, and it should not be a problem if it falls into enemy hands.
- Modern reinterpretation:
  - A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
- Claim: The reverse implication does not hold.

Quality of crypto algorithms

- Quality of modern crypto algorithms secured through peer review.
  - Works really well, especially with competitions like AES, SHA3, eSTREAM.
- Secret crypto algorithms are often assumed to be of lower quality because of lack of this peer review.
  - How many peers does it take? A lot of cryptographers work for the NSA.
  - A lot of cryptographers also work for CA vendors.

Layered security

- Never rely on only one mechanism to keep your data safe.
  - Your data is encrypted, so you don’t need a fire wall?
- Claim: Using both open standards and secret security measures can give you the best of both worlds.

The importance of time

- There is no absolute security.
- High security keeps information secret longer than low security.
- Adding obscurity to overall security approach will often increase the time of a successful attack.
- Sometimes a hacker will give up, and move on to easier targets.

Obscurity Example: CSA3

- CSA3 = Common Scrambling Algorithm 3
  - To replace CSA2 in DVB scrambling
- Based on a combination of 128-bit AES and a confidential block cipher, eXtended emulation Resistant Cipher (XRC).
- Designed by a group of cryptographers from different DVB CA companies
- Designed to be very efficient in HW, and slow in SW.

Obscurity Example: Conax Cardless

- Conax Cardless is a CA system without the smart card.
  - Runs a "virtual smart card" in a secure CPU in the STB.
- Encryption of messages to deliver scrambling keys with a combination approach

Conax Cardless Security

- Attacker must be affluent in both SW and HW security.
- If attacker gains access to proprietary SW algorithm
  - Must spend a lot of time analyzing to figure out how it works.
  - Designed to be hard to understand.

- Crypto algorithms can serve other purposes than adding mathematical complexity.

- Adding confusion is one such purpose.

- Adding “hacking complexity” is another.

Obscurity example: Public key?

- Claim:
  Asymmetric crypto ≠ Public key crypto

- Example: RSA with modulus kept secret.
  - Makes it harder for a hacker.
  - Key distribution solved without making modulus and "public" key public.
  - Asymmetric algorithms may still have desirable properties even without need for a "public" key

Conclusions

- Still not a good idea to rely only on obscurity.
- But obscurity can be a useful layer in a layered security approach.
- Still requires cryptographic competence and skill

Thank you for your attention!

Turid Herland
Senior Security Analyst

Conax AS
Storgata 33 B, P.O. Box 425, Sentrum, N-0103 Oslo, Norway
T: + 47 22 40 52 00, M: + 47 411 62 182, F: + 47 22 40 52 15
Turid . herland at conax . com, www.conax.com