Key Management
in Historical Context

Whitfield Diffie
Internet Corporation for
Assigned Names and Numbers

10 September 2012

Copyleft

- If you are seeing or hearing this presentation, you are entitled to copy it.
- If you have a copy, you are entitled to redistribute it under the same terms.

Managerial View of Cryptography

- Cryptography is an amplifier.

- The security or insecurity of the key is amplified to become the security or insecurity of the message.

Key management systems both reflect and shape the organizations that employ them.

Function of Key Management

- Bind keys to the ``real world''

--- Identities, jobs, clearances ...

Components of Key Management

- Key production --- dominated by testing
- Shipping and storage
- Use (to encrypt or decrypt something)
- Accounting
- Destruction

Key Production

- There is no more critical cryptographic function.

--- If you can produce good key you have

the possibility of good cryptography.

--- If you can't you can't.

Generating Unpredictability (Randomness)

- Card shuffling
- Rotors
- Slot machines
- Thermal noise
- Astable multivibrators
- Atmospheric turbulance in Winchester disks

Generating Unpredictability (Cont'd)

- Human variability
- Half-silvered mirror (ETH)

Desiderata

- Never seen by human eyes
- Failing that, keep it secret, particularly prior to use
- Easy to use
- Hard to copy
- Easy to destroy

Quality Control

- Cycle random source and test
- Testing for the failure of the generator, not for the quality of the method.

- (Don't hash before testing.)

Key Production Costs

- Physical

--- manufacturing rotors

--- issuing whole cellphones as keying material.

Key Production Costs (Cont'd)

- Logical

--- permutations for rotor wirings and permuter board

--- Primitive polynomials for shift registers in the ``long-cycle'' days

--- Primes for RSA today

Distribution

- Physical shipment or electronic transmission
- Storage or buffering

Use

- Code books
- Rotor machine setup
- Plug boards
- Slide switches
- Paper tape --- canisters --- KOI-18
- KYK-13
- KSD64a (STU-III) (similar on KIV-7)

Crypto Museum
cryptomuseum.com
ON
OFF
CHECK
ALL
8
5
4
3
2
1
1
2
3
4
5
6
J1

Accounting (Comsec Material Control System)

- Central facility
- CORs and comsec accounts
- Comsec custodians and user agents
- Hand receipts
- Inventories

Destruction

- Lead jackets to sink code books
- Cutting wires out of rotors
- Burning or shredding cards and tapes
- Zeroising or destroying computer memory

Rolling Keys

- Why change keys?

--- cryptoperiod (intrinsic to cryptosystem)

--- management issues (extrinsic to cryptosystem.

- Rekeying

Rolling Keys (Cont'd)

- Key updating

--- backtrack protection

- Daisy chaining (danger of cascading compromise)

Key Management Failures

- Venona
- Boyce and Lee
- Walkers

Trend: Decentralization

- Producing all keys at central facility gives way to more local production.

Electronic Key Distribution

- Key distribution center (e.g., STU-II)
- Key translation center (ANSI X9)
- EKMS --- Electronic Key Management System
- KMI --- Key Management Infrastructure

Early Examples of Electronic Key Distribution

- PLI and BCR
- Blacker
- ESVN and STU-II (conventional certificate)

Key Escrow

- Clipper chip
- Law Enforcement (Exploitation or Access) Field
- Escrow centers --- handing out key to intercept devices.

Public Key or Non-secret Encryption

- Negotiated keys
- Ephemeral keys
- Signatures

STU-III

- Benign fill
- Firefly
- Annual rekeying by call to KM

Key Management and Organizational Structue

- Hierarchical

- Web of Trust

--- recover heirarchy by having formal (signed) security policies

Quantum Key Distribution

- Channel dependent --- not really cryptography
- Usually runs over optical fiber --- already rather secure
- Intrusion detection and anti-escrow

Overall --- Overhyped

Future Key Management Issues

- Local platform security problems
- Who should pay for certificates?
- All key generated locally with same quality as by using specialized key processors
- Distributed KMF: Multiple KMF's negotiating key among themselves

Future Key Management Issues (Cont'd)

- Quantum Computing

--- will ruin current public-key systems,

elliptic curve worse than DH and RSA

--- Several possibibilities for replacement

Coding theory (Mcleice) systems

Knapsack systems

Lattice-reduction-based systems

END