Information Security Management at Certificate Authorities

István Zsolt BERTA
istvan@berta.hu

PKI lectures

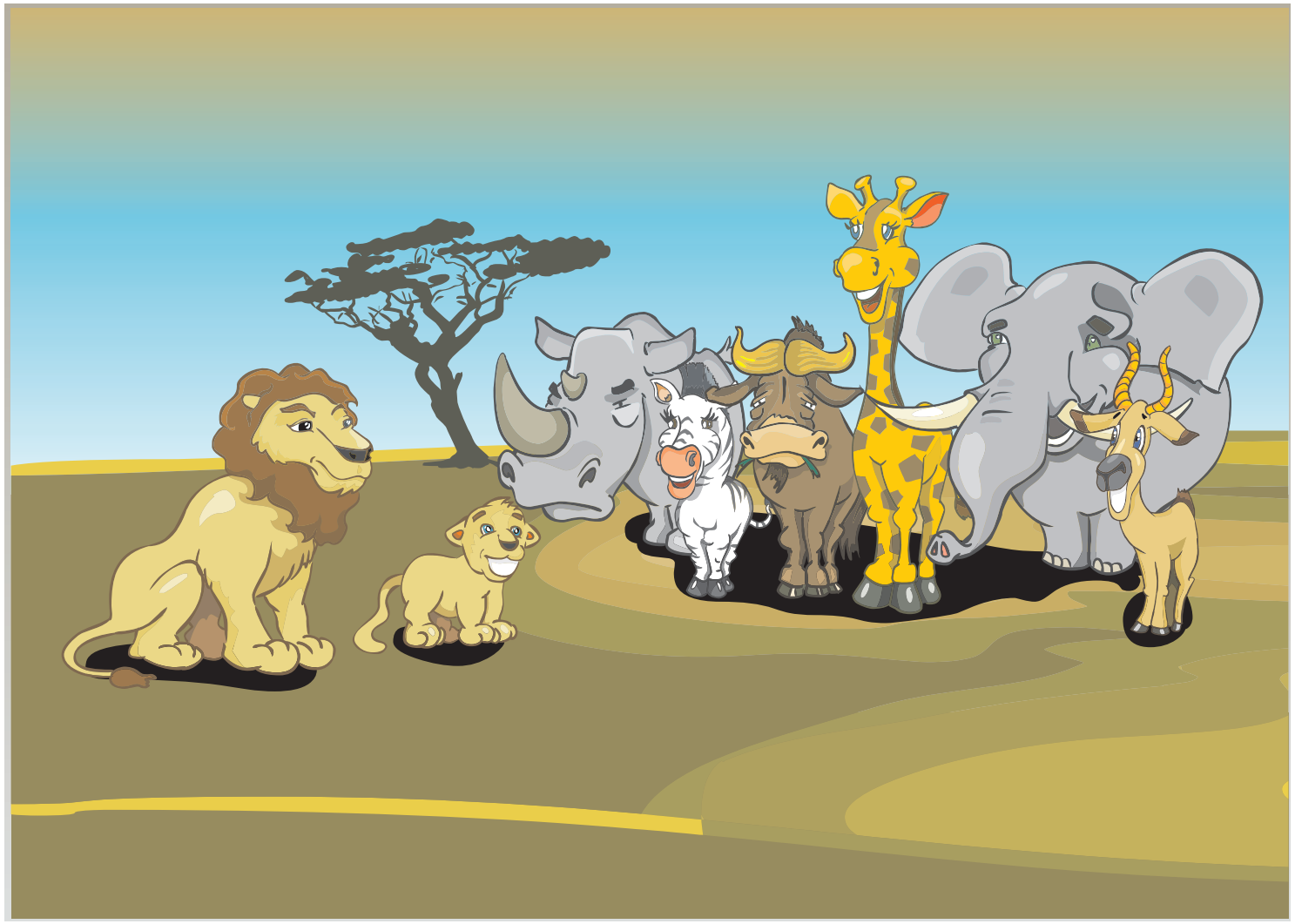
1. Public key cryptography primitives
2. Certificates, Certificate Authorities, Certification Paths
3. Electronic signatures: signature creation & validation
4. **Information security management at CAs**
5. PKI Business

Information Security Management (@CAs)

- Risk Assessment
- Information Security Management
- Information Security Management @ a Certificate Authority

Risk Assessment

How to be secure in the middle of Africa?



source

Step 1: Define Assets

- The first step is to define the assets we would like to protect
- Not only financials and tangible objects, can be assets
- Examples: Information, good reputation, trust, etc.
- In this example, we would just like to stay alive
- We have one asset: Our Life

Step 2: Identify Threats

- List what you are afraid of
- Try to make general categories

- Lions
- Bandits
- Zebras
- Rain
- Mosquitoes
- Earthquakes
- Elephants
- Snakes

Risk

- More things can happen than will happen
- We try to deal with uncertainty by assessing
  1) how like is that an even will occur and
  2) what impact can it have upon us

- **Risk = Likelihood x Impact**

- In (information) security we usually deal with risk that have negative impact

Step 3: Assess likelihood and impact

Threat	Likelihood	Impact
▪ Lions	low/medium	high
▪ Bandits	low/medium	medium/high
▪ Zebras	low	low
▪ Rain	high	low
▪ Mosquitoes	high	high/medium
▪ Earthquakes	low	medium
▪ Elephants	low	medium
▪ Snakes	low	high

Decide which threats to focus on

	Low Impact	Med Impact	High Impact
Low Likelihood	Zebras	Earthquakes Elephant	Snakes Lions
Med Likelihood		Bandits	
High Likelihood	Rain		Mosquitoes

Practical notes

- A generic risk assessment considering all possible threats for all different areas is almost never practical; one rarely sees such a matrix of everything
  - keeping it up-to-date requires a vast amount of resources
  - it will always be very-very subjective; risks from different areas are extremely hard to compare
- Both likelihood and impact can be very hard to determine
  - lack of experience, lack of data
  - subjective
  - black swans
- Still, an organization must make decisions on where to allocate its resources

What can you do with a risk?

1. Mitigate via controls/countermeasures (eliminate if possible)

2. Accept the risk
   - because there is no way to mitigate it
   - because it is not feasible to mitigate it
   - because we have no resources for it
   - because there is no point in mitigating it
   - …

Step 4: Design countermeasures

- Design countermeasures to lower the risk of threats
- Countermeasures may reduce the likelihood and/or the impact of threats
- Countermeasures also have costs
- Note that some countermeasures are specific to certain threats while others can address more

Possible countermeasures:

- Armed guards
- Mosquito net
- Stockade walls
- Doctors, medicine
- Insurance
- Traps
- Campfire
- …

Controls can be

- Preventive
  - with the aim of preventing an incident from happening
- Detective
  - with the aim of detecting an incident, so any action / intervention / correction becomes possible
- Corrective
  - taking an action after an incident has happened to repair any damage

- Compensating control
  - the 'ideal' control is not in place, we use some lesser controls instead

Risk-based approach to security

- You have limited resource to address threats
- The risk-based approach helps us allocate our resources in the most efficient way; i.e. to reduce risks as much as possible
  - reduce risk to an acceptable level
  - reduce risk as much as you can with the available resources

- Modern information security management systems follow a risk-based approach (too)

Approaches to security

1. Baseline: a standard set of controls everywhere
   - easy-to implement, easy to check
   - can become a waste of money
2. Risk-based: allocate controls based on risk
   - hard to assess risk, hard to implement properly, can always be debated
   - financially optimal solution (if done well)
3. Continuous improvement
   - regardless of what you do, focus on doing a better job than before
   - straightforward
4. Bring your own security policy ☺
   - define your requirements, check if they are implemented correctly
   - very flexible
   - very hard to understand & evaluate by outsiders

Note the contradictions between these approaches…

Information Security Management

Information Security

- Information is an asset for businesses/organizations, so information needs to be protected
- The aim of information security is to protect this information with respect to
  - confidentiality: ensuring that unauthorized parties cannot obtain/learn the information
  - integrity: ensuring that unauthorized changes cannot happen to the information
  - availability: ensuring that authorized parties have access to the information they need

- IT Security (protects IT or via IT) vs
  Information Security (protects information regardless of the media/system it resides one)

Information Security Management

- Management: getting things done through others
- Information Security Management describes controls an organization needs to implement to ensure that it sensibly reduces information security risks
- Information security management standards
  - provide frameworks for establishing information security management systems in an organization
  - allow information security to be assessed or compared at different organizations
  - provide means to express that you are secure towards management / customers / etc.

ISO/IEC 27001

- A key standard for information security management
- Defines an Information Security Management System (ISMS)

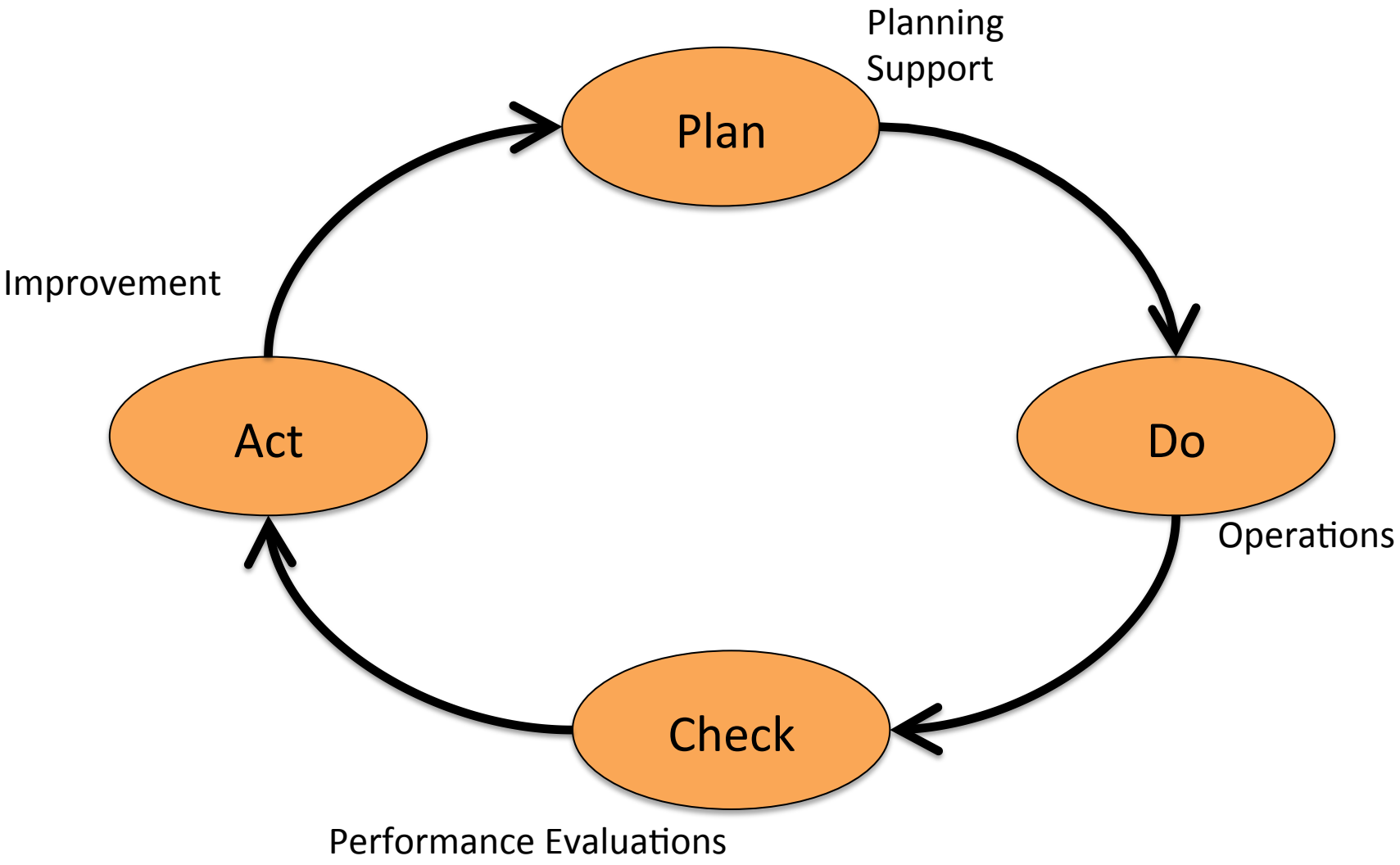
- Follows the philosophy of the quality management standard ISO 9001
  - quality vs security
- Based on previous BS 7799 standards

- COBIT is another widespread IS management / IT governance standard, but this presentation follows ISO 27001

ISO 27001 – contents at a high level

- Context of the organization
  - who are the stakeholders? what are their requirements/expectations?
- Leadership
  - commitment form senior management for infosec
  - information security policy
  - defined infosec roles and responsibilities
- Planning & Support
  - risk based, based on stakeholder expectations
  - documented plans, retaining evidence
- Operation
- Performance Evaluation
  - check if we are doing the right things; internal audit
- Improvement
  - handling incidents, taking corrective actions, continuous improvement
- Annex A: Reference control objectives

ISO 27001: Plan – Do – Check – Act



ISO 27001 – key concepts

- Ensure you understand stakeholder requirements
- Gain support for senior management to information security
- Maintain an inventory of assets, follow a risk-based approach when planning controls
- Check for security gaps, check if you are going the right way
- Learn from your mistakes, improve the system continuously

ISO 27001 Annex A: Reference controls

- Information security policies
- Organization of information security
- Human resource security
- Asset Management
- Access Control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationship
- Information security incident management
- Business continuity management
- Compliance

Statement of Applicability

- The organization states that it applies ISO 27001
- States which controls it applies
- And justifies which controls it does not apply
- Must be output of risk assessment

InfoSec Management requirements at Certificate Authorities

Assets

Key assets of the CA are:

- CA signing keys
  - signing certificates, revocation lists, OCSP responses, etc.
- Registries
  - which certificate was issued to which person
  - what verification has been performed
  - which certificate has been revoked and when

Threats - Attackers

- Cybercriminals
  - they are in for the money
  - want to maximize their profit
  - attack targets where the most money can be gained with the least investment / risk
- Hacktivist groups
  - loosely organized
  - follow ideologies, not for financial gain
- Government-sponsored
  - supports real-world activities of a state
  - not only works in cyberspace, not for financial gain
  - cyber war vs cyber espionage

Anatomy of an cyber attack

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions
8. (Covering tracks)

Source: Hutchins, Cloppert, Amin (2011)

Normative documents

- EU
  - ETS TS 101 456: Policy requirements for certification authorities issuing qualified certificates
  - ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates
  - CEN CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
  - National + EU-wide regulations
- US + international
  - Webtrust
  - CAB Forum Baseline Requirements
  - (CAB Forum EV Guidelines)
  - CAB Forum Network Security Controls

Key points

- CA signing keys must be in an HSM with a security certification (e.g. FIPS 140-X)
- CA must act with ‘due diligence’ when verifying the
  - request / requestor
- CA must accept revocation request continuously and take timely action to revoke the necessary certs
- CA must employ trusted people (e.g. clear criminal record) who are competent (must be trained, must formally accept responsibility)
- CA is liable for the certificates issues
  - financial requirements (e.g. liability insurance)
- CA must maintain continuous operation, revocation information must be available to relying parties
- CA must be audited regularly, with some parts of the audit made public

Summary / conclusions

- "Cryptography is bypassed, not penetrated" – Adi Shamir
- Crypto can only work if there are good key management processes behind it
- CAs also need good, secure processes
- Information security management can ensure that an organization and its processes are secure; key principles:
  - Support from senior management
  - Risk-based approach for distributing resources
  - Learn from mistakes (Plan-Do-Check-Act)
  - Continuous improvement
- ISO 27001 is one of the key infosec management standards