Cloud Security

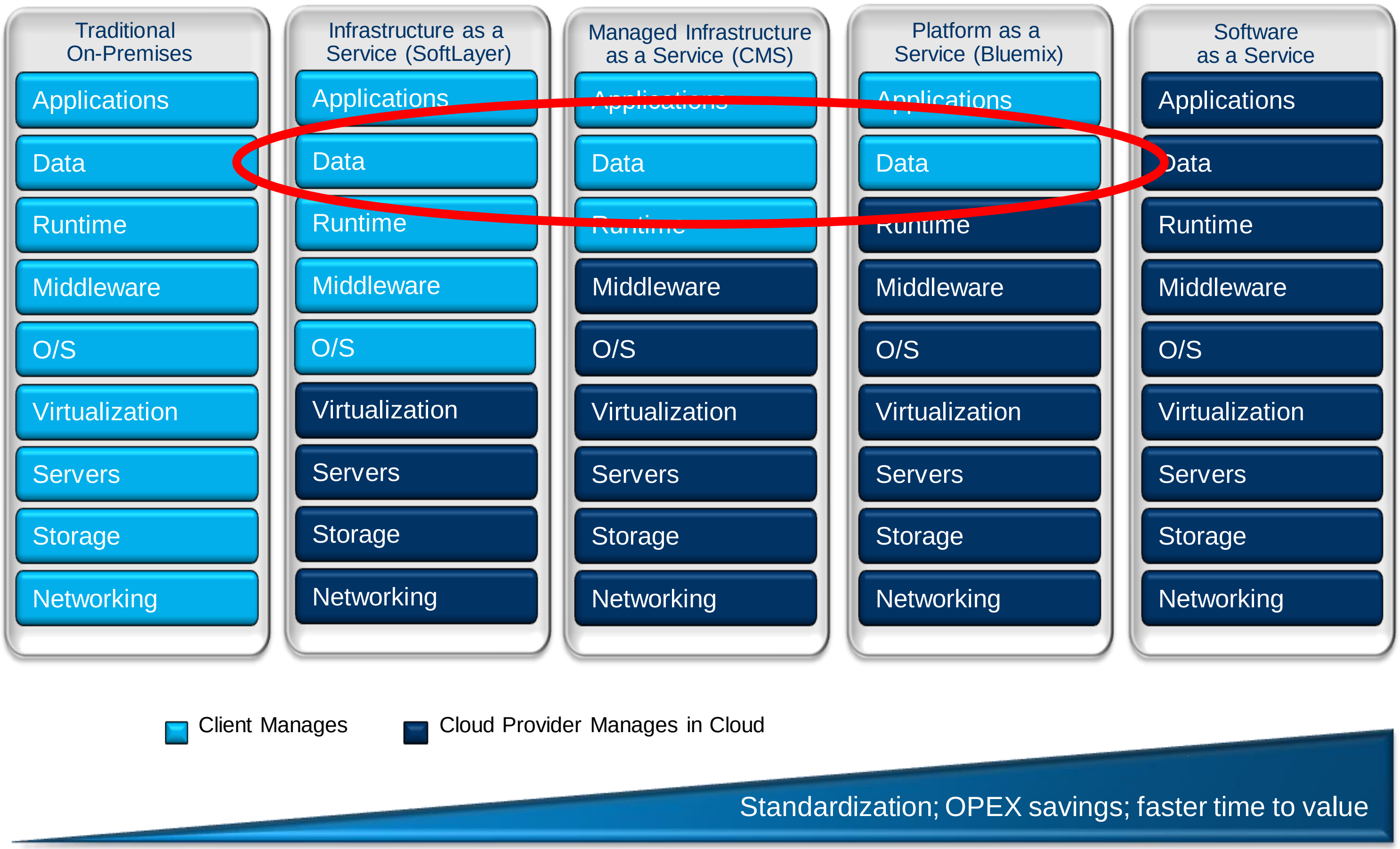
Dr. Andreas Wespi

The Roots of Cloud Computing

Malcolm McLean, one of the founders of Cloud Computing, back in 1956

- Born on Nov. 14, 1913, in Maxton, North Carolina
- Malcolm McLean patented shipping containers in 1956
- He was not an ocean shipper but he was a trucker
- In 1956, loose cargo cost **$5.86 per ton** to load
- Using ISO shipping containers, the cost was reduced to only **$0.16 per ton**

Cloud is Not Equal to Cloud



Cloud Security from the Provider Perspective

- Isolate different clients in the service platform
  - Enforcement
  - Verification

- Protect the infrastructure
  - Trusted computing base (TCB)
  - Integrity of hypervisors, kernels, and applications
  - Strong enforcement with trusted hardware

- Limit insider attacks
  - Least-privilege policy for operators

- Proof to the customer that processes work as designed

Cloud Security from the User Perspective

- What data to move to the cloud?
  - Physical location, legal aspects ("jurisdiction attacks")
- Loss of control and audit mechanisms
  - Physical direct access, log files
- Confidentiality of data?
  - Client "encrypts" all data and computations in the cloud
- Integrity of data?
  - Cloud proves the correctness of responses
- Who manages the keys and how?
  - Cryptography is a powerful technology but merely shifts power to those who control the keys
- How to destroy data in the cloud?
  - Control information proliferation

Cloud – A Platform for Innovation

Compliance by Default
- SAVE – infrastructure as a Service

Mobile
- SAVE Integration

Software as a Service
- Memento as a Service
- Privacy as a service
- SAVE as a service

Future Identity
- Privacy
- Memento

Cloud Storage
- ICStore

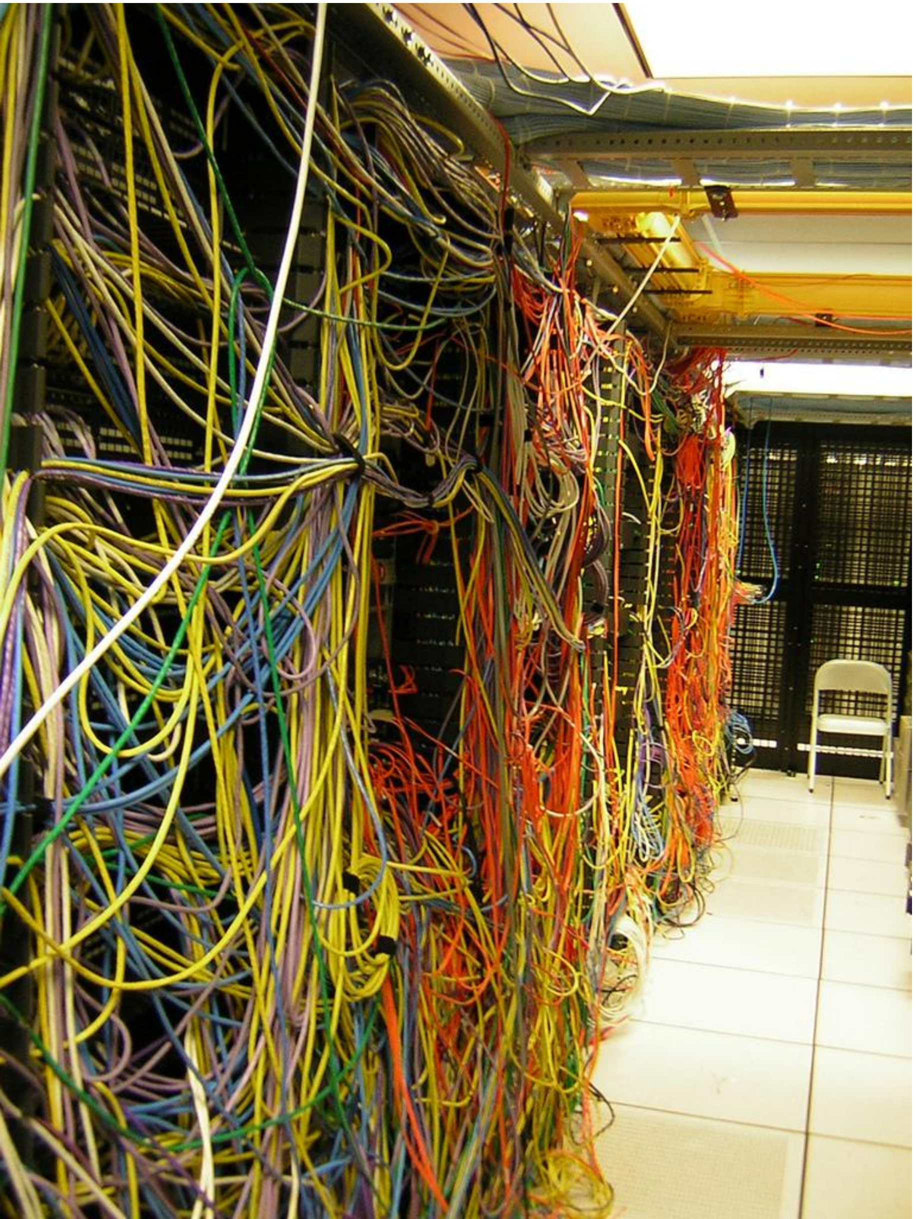
Crypto Research
- Security for Legacy Data – Format Preserving Encryption
- Key management
- Data Integrity
- Secure Deletion

DevOps
- Automated, secure workload migration

Secure by Design
- Innovate, Build, Deploy

Collaborative Innovation
- H2020 projects

Security Audit of Virtualized Environments (SAVE)



What can go wrong in a Cloud (or a Datacenter)?

- Complexity → error-proneness
- Amplified by virtualization
- Multi-tenancy and shared resources

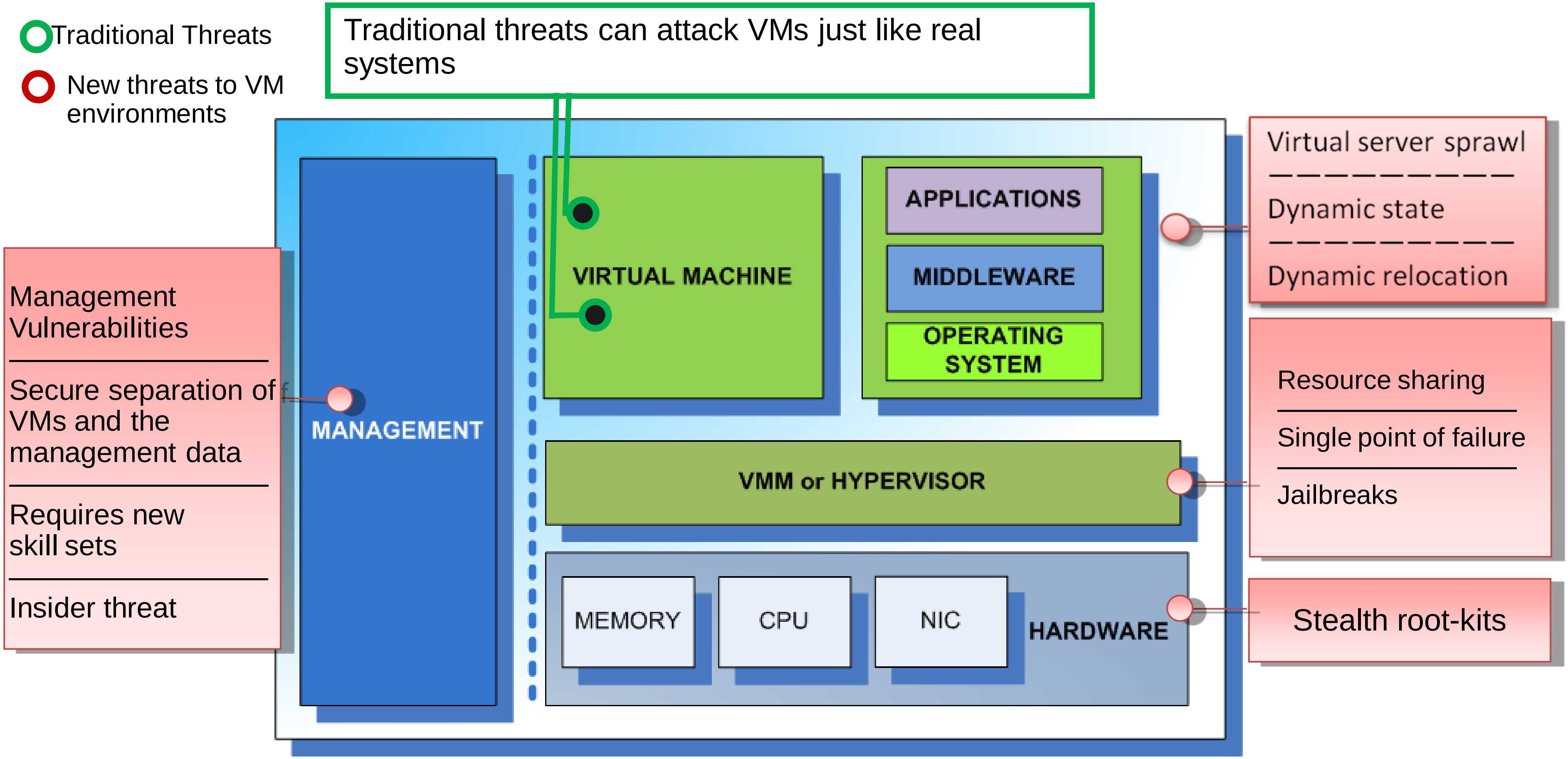
→ Isolation essential

[Photo: http://www.flickr.com/photos/alonzo/113658733]

Virtualization Threats

Traditional Threats

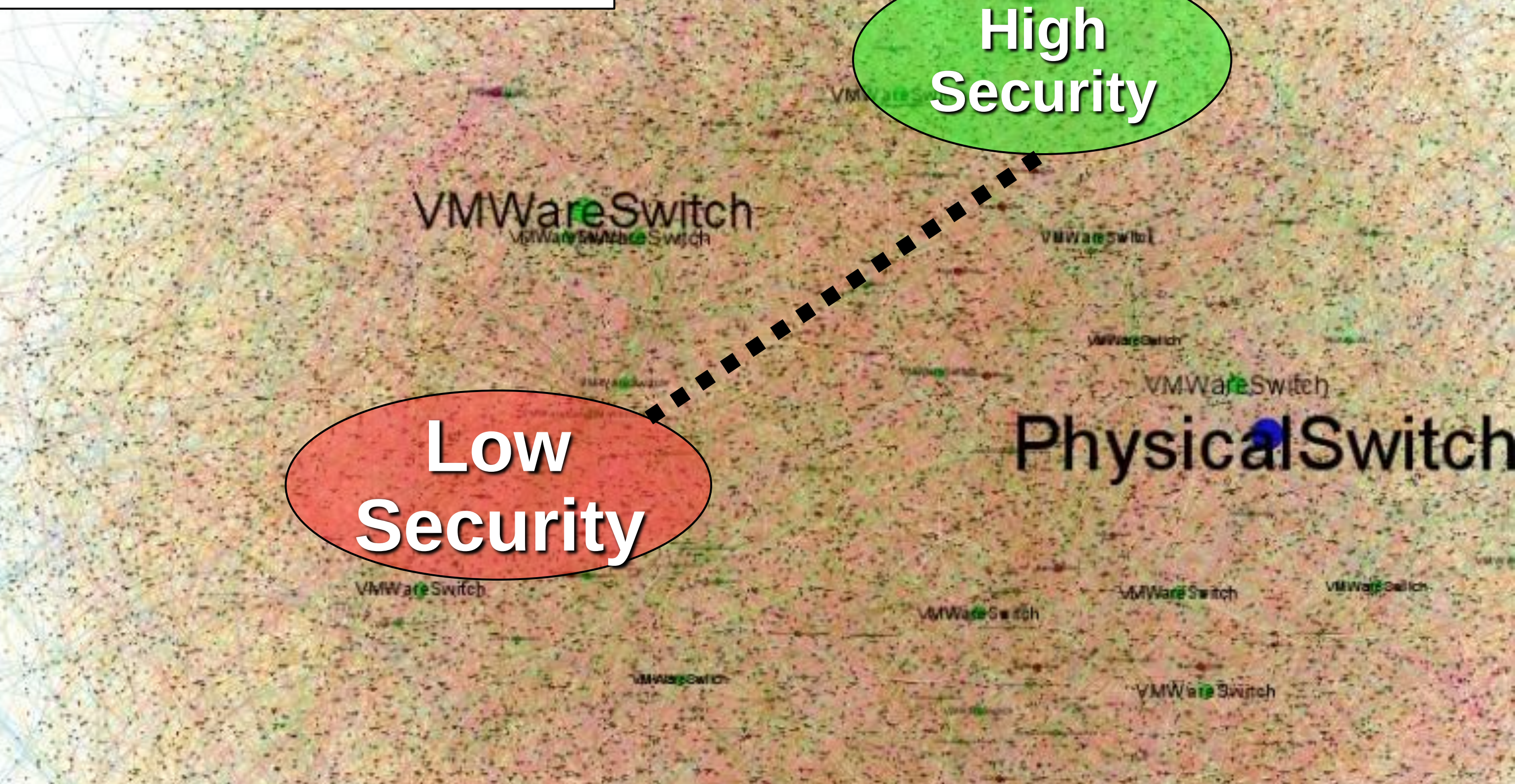
New threats to VM environments



MORE COMPONENTS = MORE EXPOSURE

SAVE – Some Examples

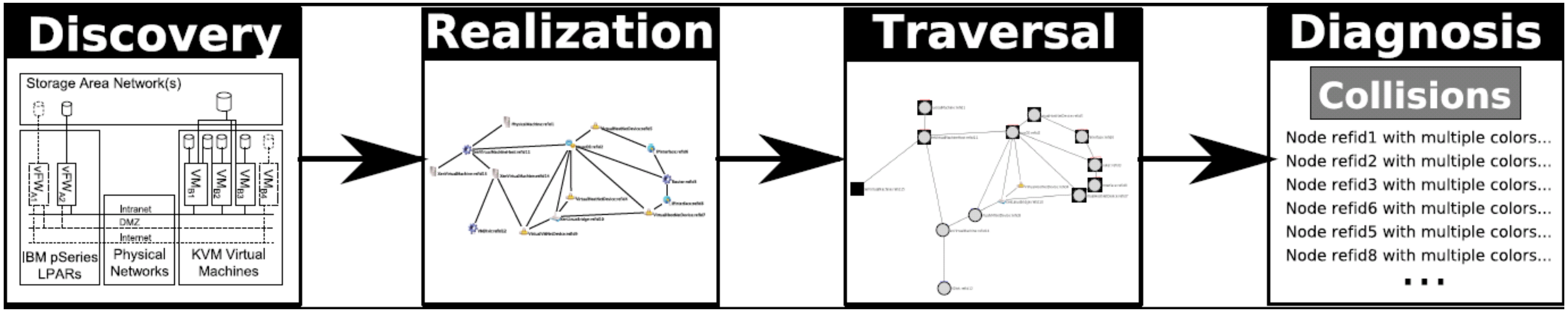
- Are Zones isolated?
- Is my data accessible by other tenants?
- Is my workload running on the right hosts?
- What happens when a host fails?



1,300 VMs
25,000 Nodes
30,000 Edges

[Data from a customer case study with a global financial institution]

SAVE – Virtualization Assurance



Discovery: Inventory of all Systems and all (relevant) Configurations

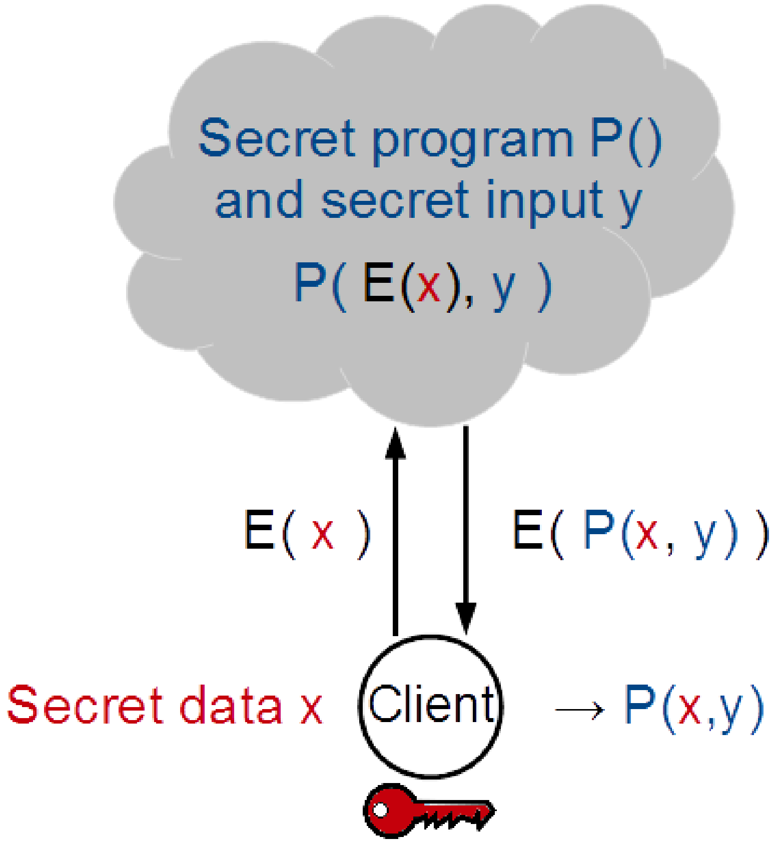
Realization Model: Unification of all data into a common graph-based model

Traversal: Coloring of security zones based on individual trust assumptions

Diagnosis: Analysis to determine unauthorized flows and security failures

Computing on Encrypted Data

- How can one manipulate encrypted data?
  - How can a computer run an encrypted program — without knowledge of what the program does?
- Celebrated research topic in cryptography
  - Formulated in 1978
  - Millionaires problem (Yao 1986)
- Secure two-party computation
  - Garbled circuits
    - Quite practical today for limited functions
  - Fully Homomorphic Encryption
    - Breakthrough result (Gentry 2009) but very far from being practical



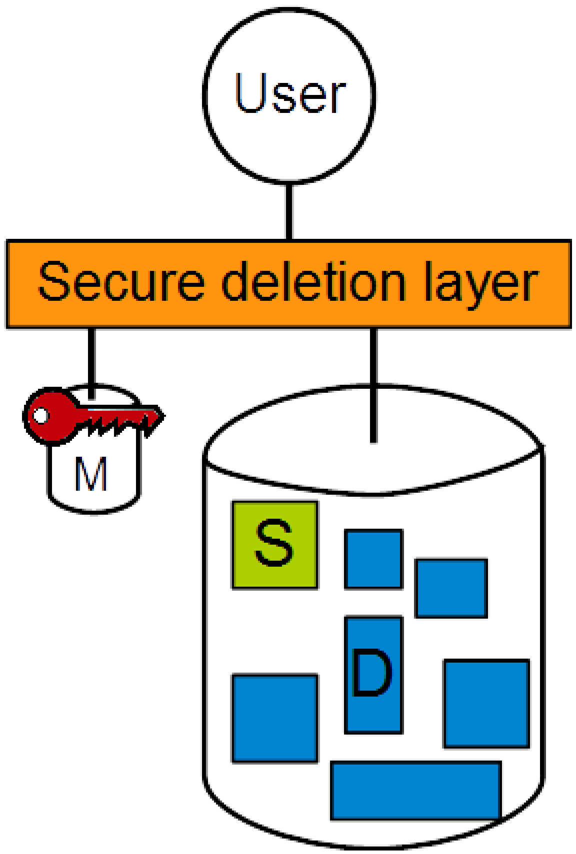
Secure Data Deletion

- Data needs to be erased
  - on client demand
  - by law
  - …

But …

- Modern storage systems cannot easily erase data
- Common storage systems
  - Remove directory pointers
  - Mark space as free
  - Data remains accessible on a lower-level API
- Storage interfaces have no operation for "really erase"
- Virtualized storage systems make deletion impossible
  - Many layers of abstraction
  - Software-defined storage (SDS), cloud storage
- Every storage layer repackages and caches data, this leaves traces

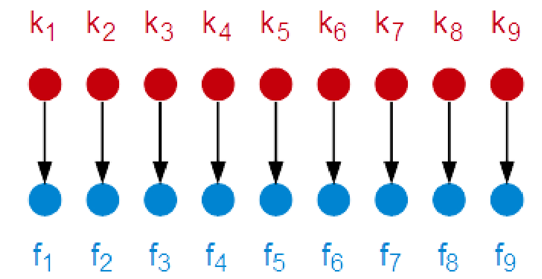
System Model



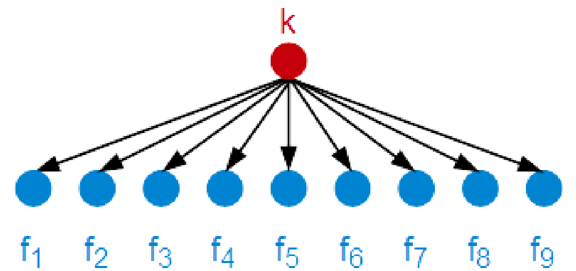
- Basic Approach [BL96, TLLP10]:
  - Encrypt data
  - Keep key(s) in controlled and erasable memory
  - Destroying key(s) makes data inaccessible
- Secure deletion layer
  - Implemented through encryption
- Small, controlled erasable memory M
  - Stores key(s)
- Large, permanent memory
  - Cannot be erased
  - Contains protected data D
  - Auxiliary state S
- Deletion operation
  - Reads/writes/erases keys in M
  - Writes to S
  - Never touches bulk data D

Secure Deletion Schemes with Encryption

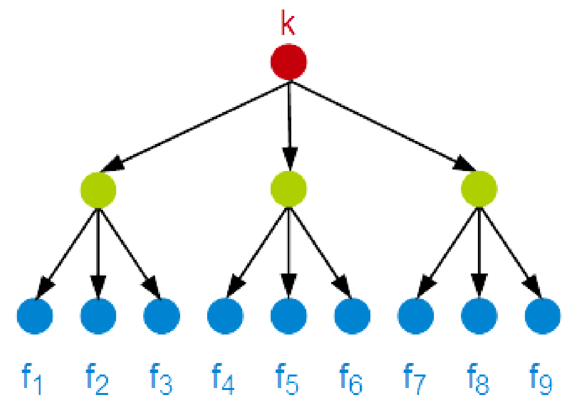
- Use a separate key for every protected item [P07, GKLL09, RCB12]
  - To delete an item, destroy its key
  - Huge master key, difficult to manage
  - Deletion cost is constant



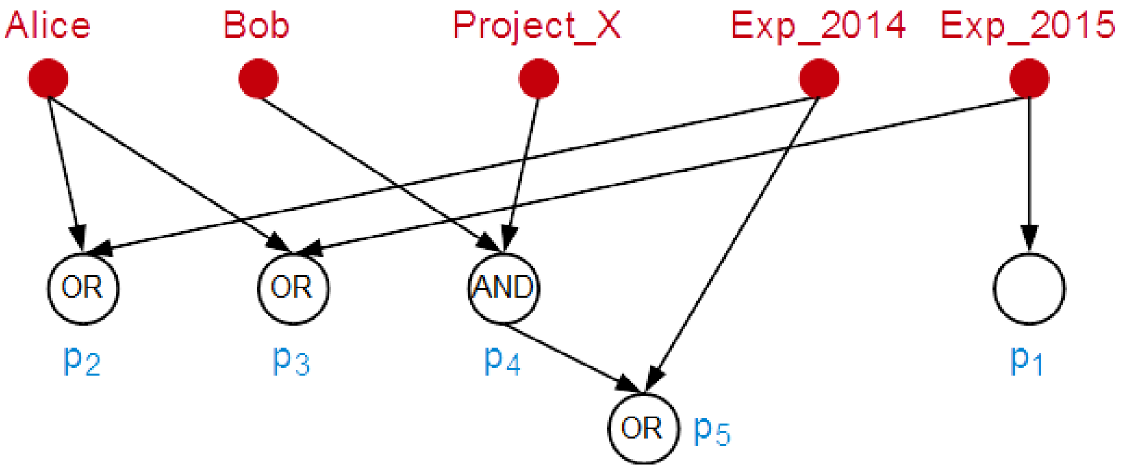
- One key encrypts multiple protected items
  - Secure deletion of one item → rekey operation
  - Choose fresh key
  - Re-encrypt surviving items with new key
  - Destroy old key
  - Small master key
  - Deletion cost is linear



- Tree of keys [DFIJ99]
  - For every tree node, super-key encrypts sub-keys
  - Items protected by keys at leaves
  - Delete one item → rekey along path from root to deleted item
  - Small master key
  - Deletion cost is logarithmic



Our Approach: Policy-Based Secure Deletion



- Scheme supports arbitrary policies that are modeled as a circuit
  - AND, OR, and threshold gates
- Master key contains one key per attribute
- Attributes at input nodes (Alice, Bob, Project_X, …)
  - Initially, all are viewed as FALSE
- Protection classes p_1, p_2, p_3, ... value according to Boolean expression
- Deletion operation specifies attribute(s), for example,
  - Delete(Exp_2014) → p_2, p_5 securely erased
  - Delete(Alice) → p_2, p_3 securely erased
  - Delete(Bob) → no effect; Delete(Project_X) → p_4, p_5 securely erased

IBM Cloud Security Research Collaboration

- **WITDOM** (empoWering prIvacy and securiTy in non-trusteD envirOnMents)
  - www.witdom.eu
- **ESCUDO** (Enforceable Security in the Cloud to Uphold Data Ownership)
  - www.escudocloud.eu
- **SUPERCLOUD** (User-centric Management of Security and Dependability in Clouds of Clouds)
  - www.supercloud-project.eu

- Research projects (2015-18), in the EU Horizon 2020 Framework Programme
- Supported by the Swiss State Secretariat for Education, Research and Innovation (SERI)

European Commission

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

For more Information

- How to reach me
  - Andreas Wespi <anw@zurich.ibm.com>

- IBM Research
  - IBM Research - Zurich
    - http://www.zurich.ibm.com
  - Security research at IBM
    - http://www.research.ibm.com/compsci/security