# Tools and Methodologies for Layered, Diverse, and Renewable Security in Tethered Systems

Clifford Liem
Cloakware, an Irdeto Company

Classification: Unrestricted



## Outline

- Who is Cloakware?
- Applications & Security Risk
  - Example Application: Digital Rights Management
  - Security Risk
  - What are the Threats?
- Cloakware Build Tools
  - Traditional Build Flow
  - Cloakware Security Suite
    - Source and Binary Level Tools
- Threat Analysis
- Diversity
  - What is Diversity?
  - How Does Diversity Address the Security Lifecycle
    - Renewability, Revocation
- Conclusions & Future Work

cloakware
irdeto

## Who is Cloakware ?

(Caution: a few marketing slides ahead)




cloakware
irdeto

## Advancing Software Protection for Digital Assets

- 1997 Company founded
- 2003 Intel licenses Tamper Resistance Software to Cloakware
- 2007 Acquired by Irdeto Access
- 450+ person-years of development in core software protection technology
- Ottawa, Beijing, Washington, California, UK, Switzerland

### Technology Partners

intel, Microsoft, dlna, CORAL CONSORTIUM, marlin, symbian

### Sample Customers

- 4 of the top 5 semiconductor manufacturers
- 3 of the top 5 mobile handset manufacturers
- 3 of the leading smart phone manufacturers
- 4 leading mobile telecom service providers
- 3 of the world's largest software companies
- 2 of the top 3 video card manufacturers
- 3 leading conditional access vendors

Texas Instruments, NXP, SONY, ATI, LAMPREY NETWORKS, CREDANT TECHNOLOGIES, vodafone, irdeto, ANALOG DEVICES, COREMEDIA, Pioneer, VERANCE, mbco, STATE STREET

## Cloakware Lines of Business

cloakware
irdeto

**Consumer Product Solutions**

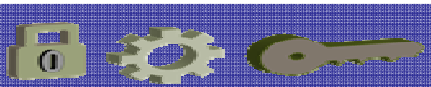
Software security toolkit

DRM client solutions

**Enterprise**

Privileged & application password protection

Identity & access management



**Software Protection Technology**

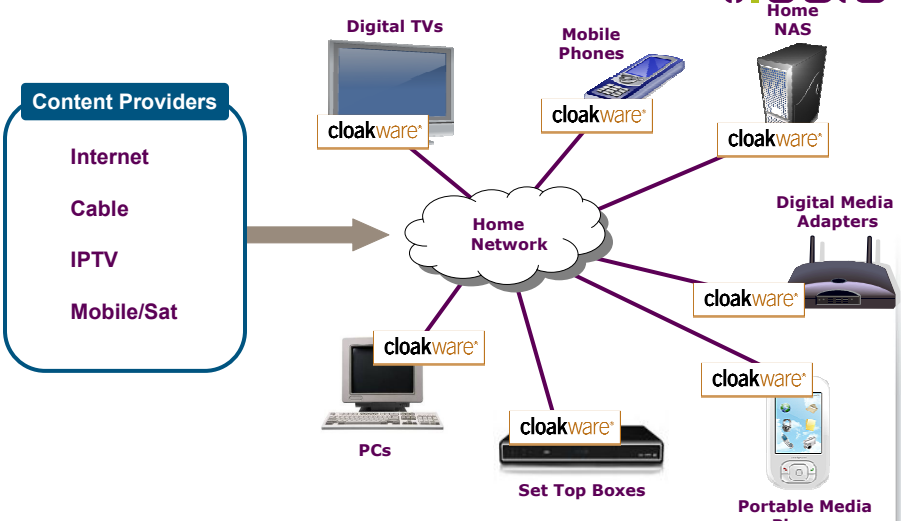


## Cloakware in the Digital Home

cloakware
irdeto

**Content Providers**

- Internet
- Cable
- IPTV
- Mobile/Sat




- *One billion*+ protected applications deployed worldwide.

cloakware
irdeto

## Example Application

Digital Rights for High Value Content

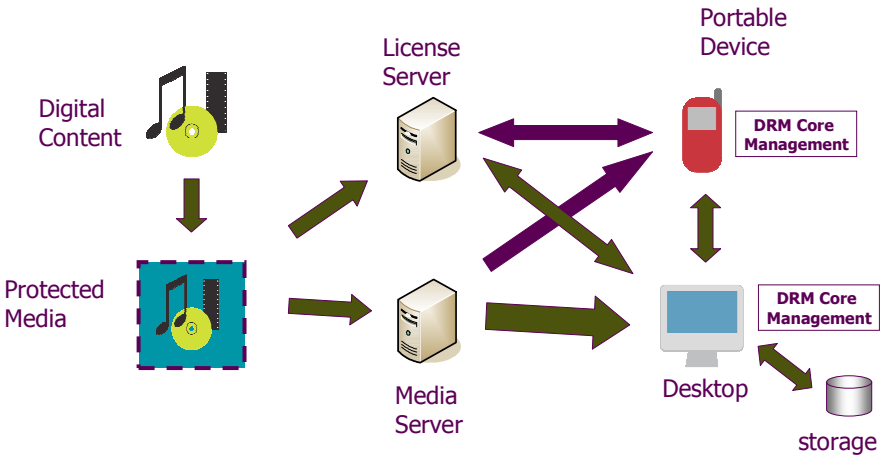




cloakware
irdeto

## Example Application: Digital Rights Management (DRM)

- Content and License distribution model



## What is Security Risk?

cloakware
irdeto

- Multi-Factored Relationship

Threats

Vulnerabilities

Assets

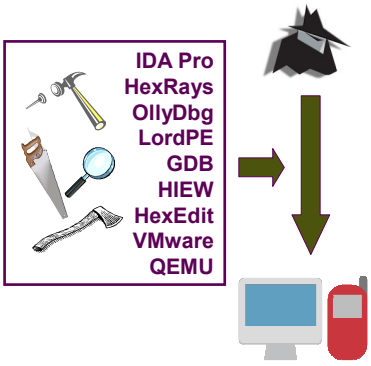
***How do your protection techniques address these?***



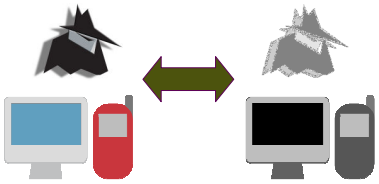
## What are the Threats?

cloakware
irdeto

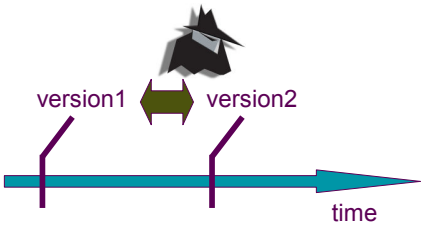
### Direct WhiteBox Attack



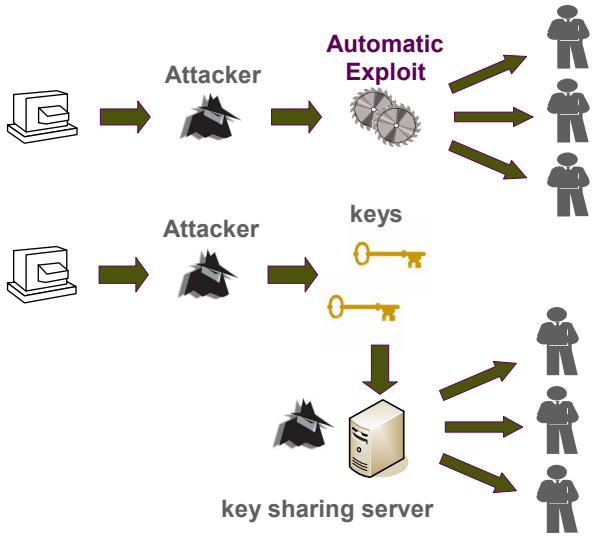

### Colluding Attack



### Differential Attack



## Exploit can Lead to Widespread Damage





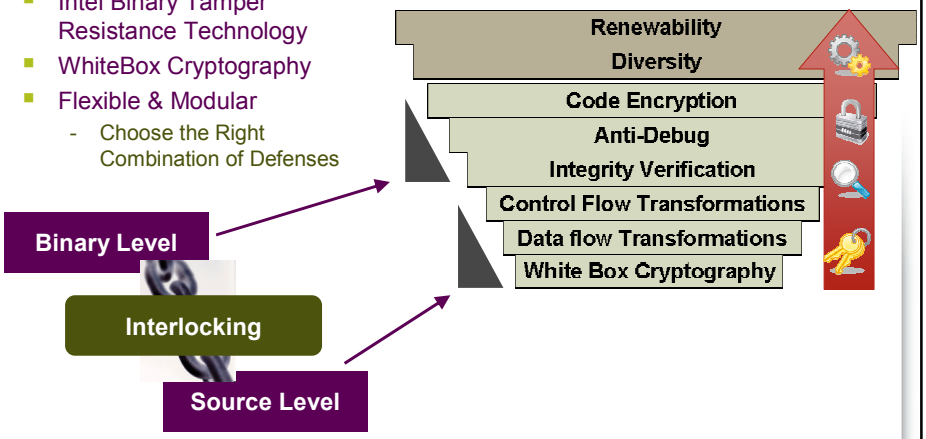

## Cloakware Build Tools

Source & Binary Level

## Cloakware is Multi-Layered Protection

cloakware
irdeto

- Compiler Transformation Technology
- Intel Binary Tamper Resistance Technology
- WhiteBox Cryptography
- Flexible & Modular
  - Choose the Right Combination of Defenses

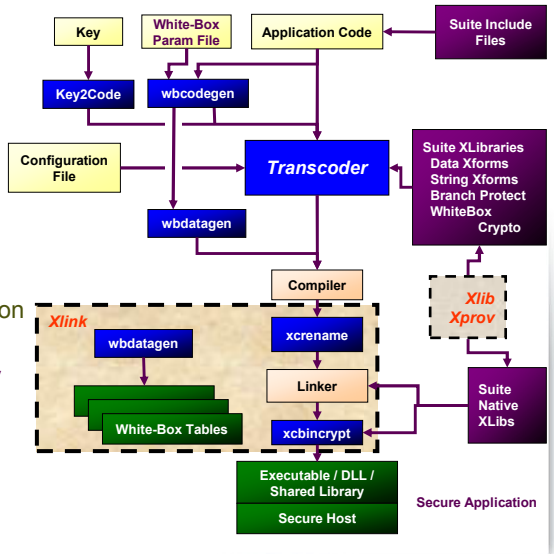



13

## Cloakware Security Suite

cloakware
irdeto

- Traditional Build Tools
  +
- Source-Level Tools
  - The *Transcoder*
  - Key Hiding
- Binary-Level Tools
  - Integrity Verification
  - Anti-Debug
  - Dynamic Code Decryption
  - Symbol Renaming
- White-Box Cryptography
- Libraries
- Utilities
  - Librarian
  - Linker

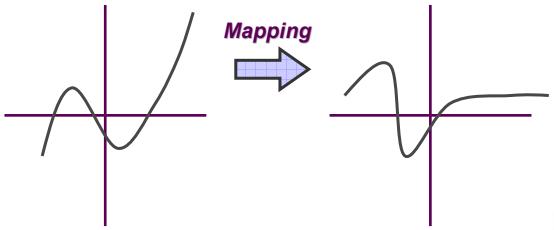


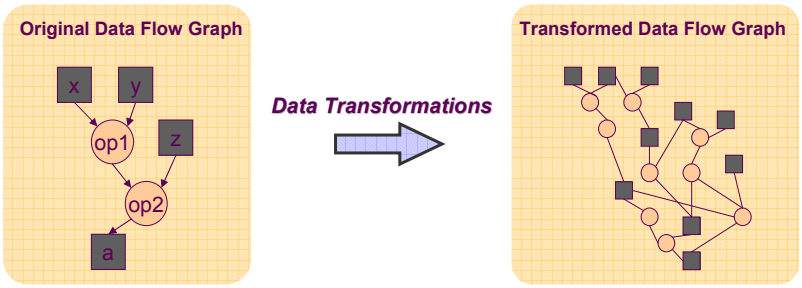

14

## Data-Flow Encoding Principle

cloakware irdeto

- Mathematical Mapping of Data Values
- Data Locations → Mapped
- Data Operations → Mapped
- Many Function Families
- Randomly Chosen Constants



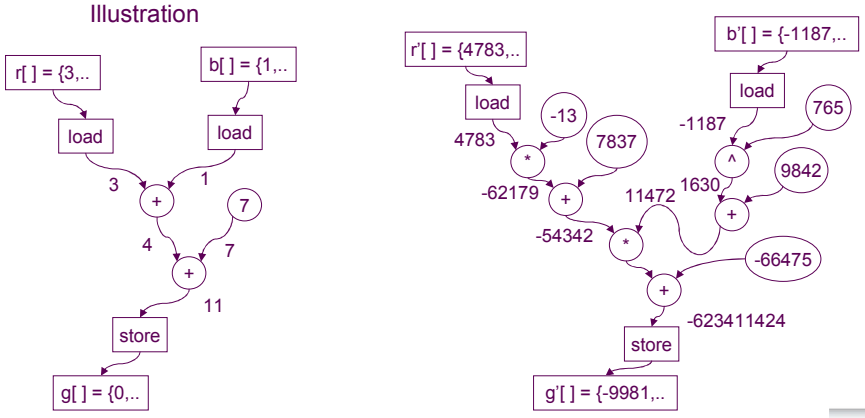



## Data Transforms: Dynamic Concealment

cloakware irdeto

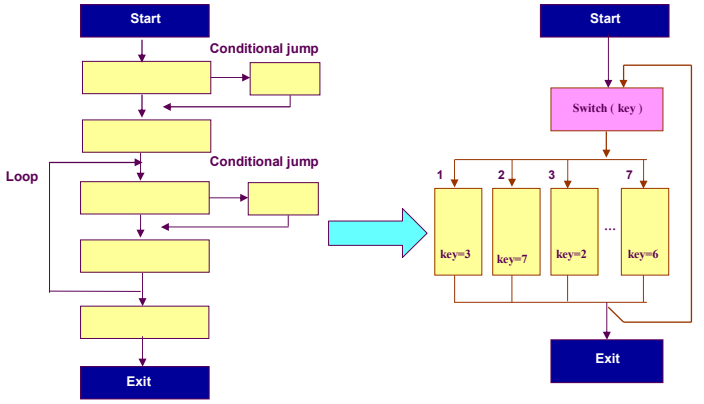
- Data Values are Transformed in Memory
- Operations are Transformed
- Net Effect: Modified values at all intermediate stages

Illustration



## Control Flow Flattening – Basic

cloakware irdeto




Original Program Flow

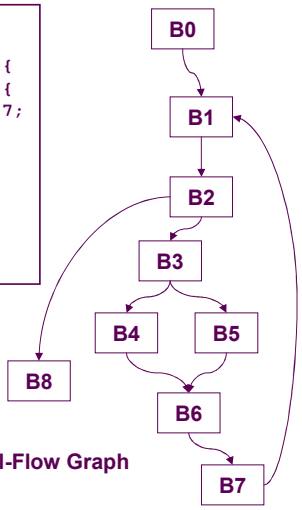
Control Flow Flattened Program



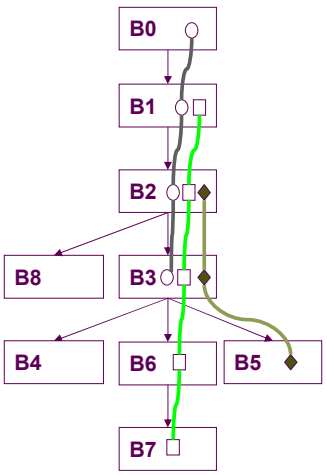
## Use Dominance Property to build History Chains

cloakware irdeto

```
int function() {
  int i;
  for(i=0;i<10;i++) {
    if(a[i] < b[i]) {
      a[i] = b[i] + 7;
    }
    else {
      a[i] = 0;
    }
  }
  a[0] = 6;
}
```

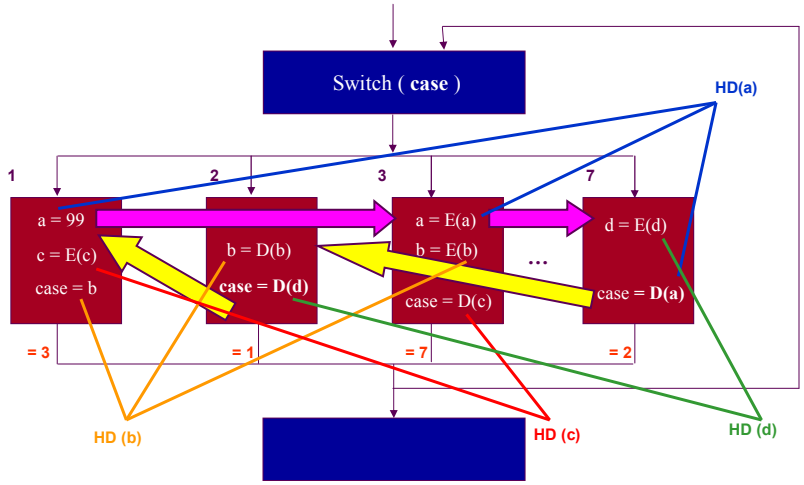



Control-Flow Graph




Dominator Tree
With Sample History Chains

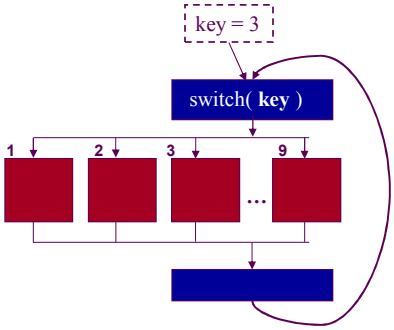
## Control-Flow Flattening: History-Dependencies






## Control-Flow Flattening Advanced Features

- **Dummy Branches**
  - Insertion of non-obvious False Conditions that jump to wrong areas of the code
- **Constant Hiding**
  - Constants are hidden in Opaque Predicates




*X is a user value from the program like a global or a parameter.*

key=(23 | X) - ((23 | X) & -4)

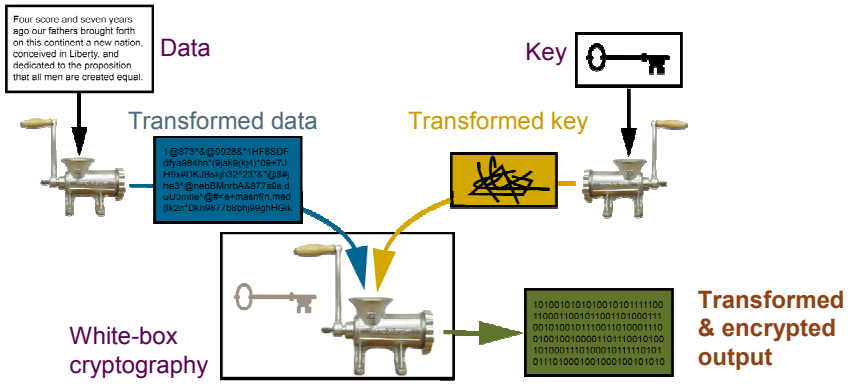
key evaluates to 3

switch( key )

## WhiteBox Cryptography
### Ensures that keys are hidden

cloakware
irdeto

- White-box cryptography ensures the input data, keys and resulting output data are protected at all times
- WB-AES, WB-RSA, WB-ECC, WB-3DES

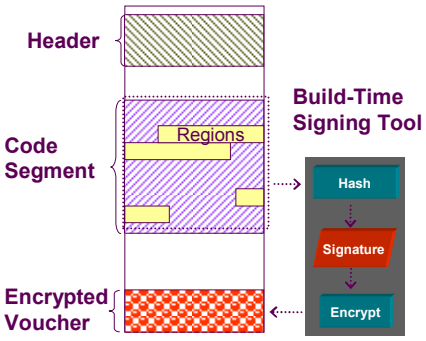





## Binary Technology
### Example: Integrity Verification

cloakware
irdeto

- Run-Time Verification of Build-Time Integrity
- Performance Trade-offs
  - Code Segment is partitioned for integrity checks
- Uses White Box Crypto
- Failure Modes
  - Hard Failures
  - Soft Failures

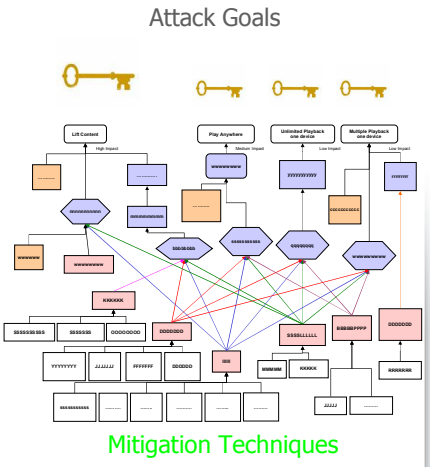



**Other Binary Technologies**

- Anti-Debug: Exception-Based, Signal-Based, Timing-Based
- Dynamic Code Decryption
- Secure Loader (Packer)

## Threat Analysis: Attack Tree

1. Identify and Prioritize Assets
2. Identify Possible Paths to Each Asset
3. Establish a Strategy for Layered Mitigation Techiques
4. Insert Protection Tools into a Flexible Build Environment
5. Explore Trade-offs (Security Tuning Cycle)





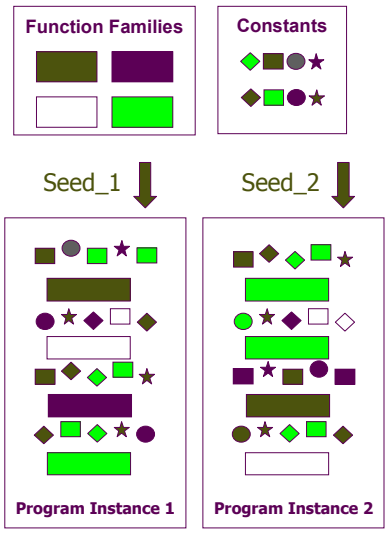

## Diversity

Built into Cloakware Tools

## Diversity: Differing Construction

cloakware
irdeto

- Randomly Chosen:
  - Order & Layout
  - Function Families
  - Constants
- Seeded Build
  - Reproducibility
- Diverse Instances
  - Functionally Equivalent
  - Similar Performance
  - Structurally Differing
- Needle-in-a-Haystack Property





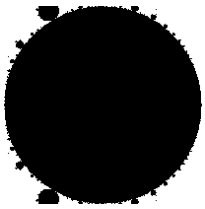

## Diversity Properties

cloakware
irdeto

- Uniformity
  - Showing a single form
  - Always the same
  - At regular intervals
- Diffusion
  - Statistical dissipation of information.
- Confusion
  - Complex dependencies.
- Self-Similarity
  - An object that is exactly or approximately similar to a part of itself
  - The whole has the same shape as one or more of the parts
  - *e.g. shorelines, fractals*

Koch Curve

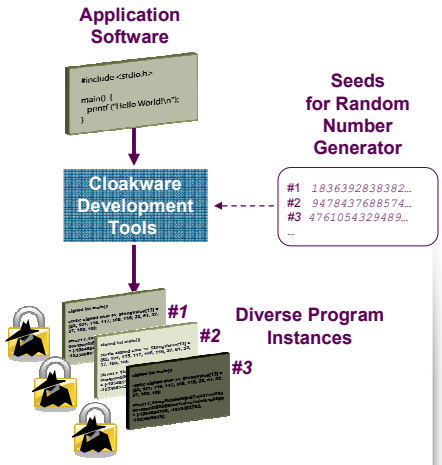
Mandelbrot Set



## Software Diversity

cloakware
irdeto

- Diversity Generation – built into Cloakware Tools
- Each instance - must be attacked separately
- Dramatically increases the work to create an automated attack tool

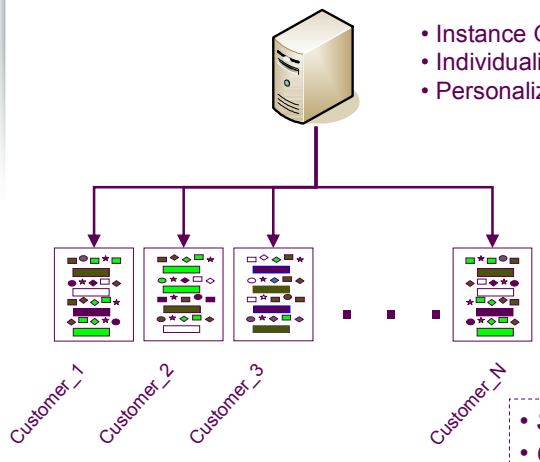



**Break the hacker business model**



## Diversity used across Client Base

cloakware
irdeto




- Instance Generation
- Individualization
- Personalization

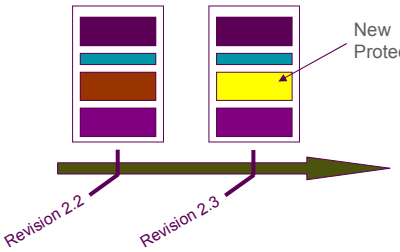
- Customer-Specific Instances

- ***Spatial Diversity***
- ***Customer-Specific Instances***
- ***Anti-Collusion***

## Diversity used across Software Versions

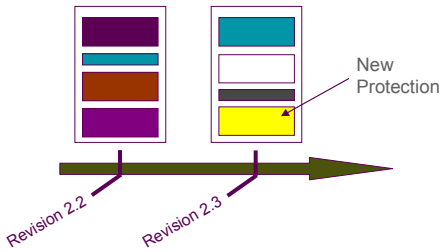
cloakware
irdeto

- Common Scenario




Obvious Differential Attack

- Using Diversity




? Attack Point ?

- ***Temporal Diversity***
- ***Renewability***

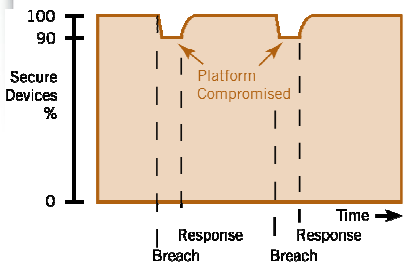


## Attack Mitigation and Recovery

cloakware
irdeto

Deploying Software

- **Strong attack response**
- reduces duration of attack




Hacker Business Model

**Tamper resistance** — Raises cost of attack

**Diverse production** — Reduces scope of attack


**Software Diversity Benefits**

Minimize scope of attack -- Prevent automated attacks

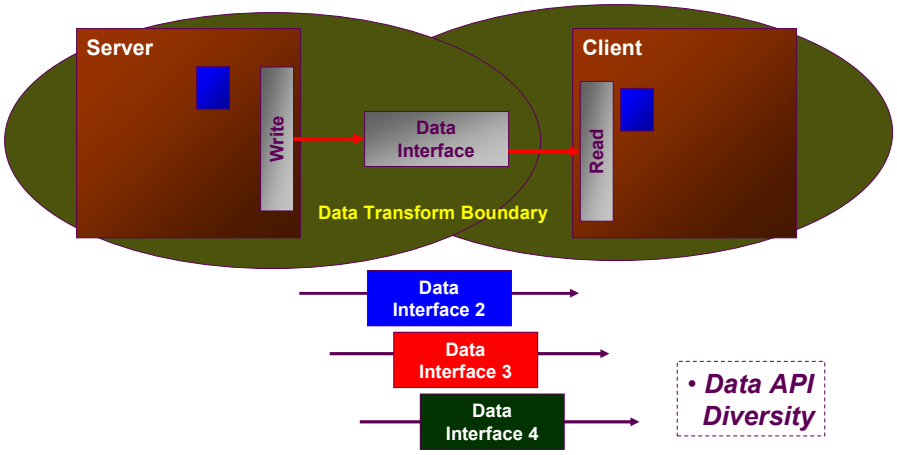
Provide rapid recovery in the event of an attack

Make the business unattractive to the hacker

## Data Interface Diversity

cloakware irdeto

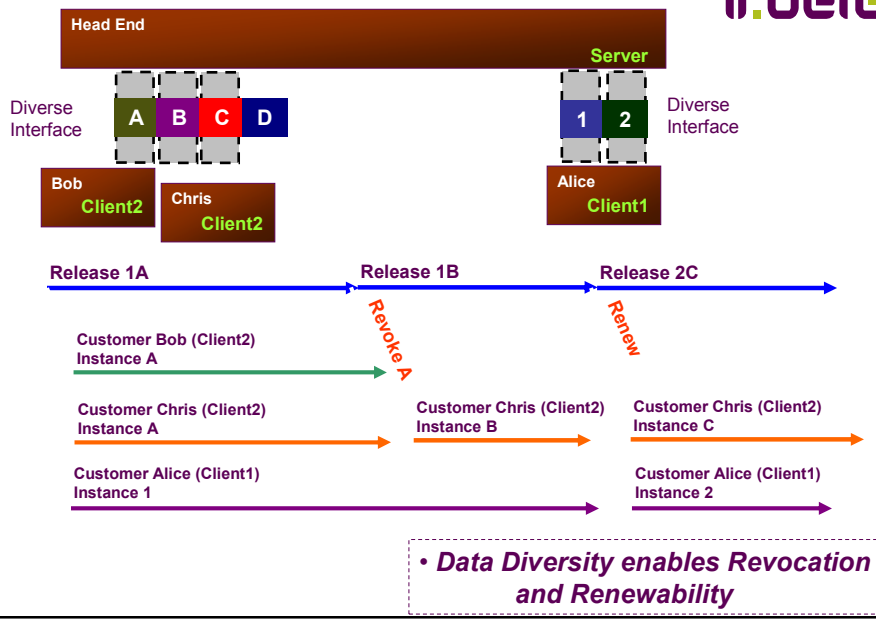
- Extending Data Transformations to Interfaces




31

## Revocation

cloakware irdeto



## Conclusions

cloakware
irdeto

- Threats on Distributed Systems
  - Direct Attacks, Collusion, Differential Attacks
- Cloakware Build Tools
  - Source and Binary Level Tools
  - Data & Control-Flow Transformations
  - White-Box Crypto
  - Integrity Verification, Anti-Debug, Dynamic Code Decryption
- Diversity
  - Properties: Uniformity, Diffusion, Confusion, Self-Similarity
  - Across Client-Base (Spatial)
  - From Version to Version (Temporal)
  - Renewability
  - Revocation



## Future Areas of Study

cloakware
irdeto

- Diversity Metrics and Measurement
- Active Monitoring and Breach Detection
  - Built-In Updatable Security
- Emulation Attacks
  - Examples: VMware, Virtual PC, QEMU, Bochs
- Code Lifting Attacks
- Hardware Anchoring
  - Node-Locking
  - Machine Fingerprinting
- Security Patterns

# Tools and Methodologies for Layered, Diverse, and Renewable Security in Tethered Systems

Clifford Liem
Cloakware, an Irdeto company
Clifford.Liem@cloakware.com