PEARL: Plausibly-Deniable Flash Translation Layer

Chen Chen
Stony Brook University

Anrin Chakraborti
Duke University

Radu Sion
Stony Brook University
Increasingly Intrusive Privacy Laws

“The United Kingdom’s Regulation of Investigatory Powers Act makes it a crime to not surrender encryption keys on demand from a government official authorized by the act.”

Unlawful Detention & Searches

Egypt: An opposition in exile whose loved ones pay the price

Authorities in Egypt have targeted relatives of activists who live abroad in an attempt to further stifle dissent.

Oppressive Regimes

“Kazakhstan police detained an activist in Astana on suspicion of inciting social discord … police confiscated a computer, a laptop, a mobile telephone, an iPod and documents. The authorities have not issued a record detailing the search and confiscation of items from Blyalov’s home, as they are required to do under Kazakh law” … Human Rights Watch (2015)

Need more than conventional encryption
Plausible Deniability

“Security property of a mechanism that allows parties to claim to others (e.g., an officer in an oppressive regime) that some information is not in their possession or that some transaction has not taken place” – StegFS (1998), McDonald *et al.*
Threat Model

- Observe (multiple) snapshots of storage device
- Cannot observe device at runtime (memory, caches etc.)
- No system compromise
- Coerce users for key(s)
- Rational
Deployment

Hand over your phone.

You have encrypted data, hand over your key.

Fine, my data is encrypted.

Fine, I will give up the public key.

Public data

Public key
Hidden key
Plausibly-Deniable Storage Systems

- Steganographic Filesystems:
  - StegFS* [Anderson et al. IH ’98], [McDonald et al. IH’99] [Pang et al. ICDE ‘03]
  - DEFY [Peters et al. NDSS ‘15], INFUSE [Chen et al. PETS ‘20]
  - …

- Hidden volumes:
  - TrueCrypt, HIVE [Blass et al. CCS ‘15], DataLair [Chakraborti et al. PETS ‘17], PD-DM [Chen et al. PETS ‘19]
  - …

- Flash-Based:
  - DEFTL [Jia et al. CCS ‘17]
  - ?
What Makes Flash Devices Different?

- Cells are basic unit of storage
- Group of cells make up a page
- Group of pages make up a block
- Page-level programming
  - $0 \rightarrow 1, 1 \not\rightarrow 0$
- Block-level erase before write
  - Slow
  - Wear from P/E cycles
Flash Translation Layer (FTL)

- Interface between FS and raw flash
- Maps logical address to physical address space
- Wear levelling
- Garbage collection

FTL conflicts with upper layer deniability
PEARL: FTL with Plausible Deniability

- Deniability logic implement in FTL
- DEFTL [Jia CCS ‘17]: Single-snapshot deniability
- Multi-snapshot resistant → All changes due to “public data”

A data encoding scheme where public + hidden data = plausible public data?
Write-Once-Memory (WOM) Code

- Write-once-memory: $0 \rightarrow 1$, $1 \nrightarrow 0$
- More writes before erase
  - reduce wear, P/E cycles

(2,3) WOM Code

<table>
<thead>
<tr>
<th>data</th>
<th>1st write</th>
<th>2nd write</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>000</td>
<td>111</td>
</tr>
<tr>
<td>01</td>
<td>001</td>
<td>110</td>
</tr>
<tr>
<td>10</td>
<td>010</td>
<td>101</td>
</tr>
<tr>
<td>11</td>
<td>100</td>
<td>011</td>
</tr>
</tbody>
</table>

WRITE 01
WRITE 10
ERASE
WOM Codes with Hidden Bits

- Additional capacity for a hidden bit
- 2 public writes = public + hidden write

<table>
<thead>
<tr>
<th>data</th>
<th>1st write</th>
<th>2nd write</th>
<th>HB = 0</th>
<th>HB = 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>000</td>
<td>000</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>001</td>
<td>001</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>010</td>
<td>010</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>100</td>
<td>100</td>
<td>011</td>
<td></td>
</tr>
</tbody>
</table>

(2,3) WOM Code + 1 Bit Hidden

Hidden bit decides Codeword for public
Not all WOM Codes work!

Distribution of public only codewords = distribution of public + hidden codewords
### (3,5) WOM Code with Equal Partition

<table>
<thead>
<tr>
<th>Public Data</th>
<th>First write</th>
<th>Second write</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>00000</td>
<td>11110</td>
</tr>
<tr>
<td>001</td>
<td>00001</td>
<td>11001</td>
</tr>
<tr>
<td>010</td>
<td>00010</td>
<td>11010</td>
</tr>
<tr>
<td>011</td>
<td>00100</td>
<td>11100</td>
</tr>
<tr>
<td>100</td>
<td>01000</td>
<td>11111</td>
</tr>
<tr>
<td>101</td>
<td>10000</td>
<td>11101</td>
</tr>
<tr>
<td>110</td>
<td>11000</td>
<td>11000</td>
</tr>
<tr>
<td>111</td>
<td>10100</td>
<td>11011</td>
</tr>
</tbody>
</table>
More Challenges

• Page allocation & transition
• Garbage collection
• Wear Levelling
• ...

Throughput

IOPS ($x10^3$) for Read, Write.
Higher is better

<table>
<thead>
<tr>
<th></th>
<th>DFTL</th>
<th>PEARL Public</th>
<th>PEARL Hidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>85</td>
<td>51</td>
<td>17</td>
</tr>
<tr>
<td>Write</td>
<td>25</td>
<td>13</td>
<td>2</td>
</tr>
</tbody>
</table>
Conclusion

• FTL with plausible deniability

• WOM codes for multi-snapshot resilience

• Practical
Questions?

Thats all Folks!