



Presented By: Cole Sherer

Vanish: Increasing Data Privacy with Self-Destructing Data

Problem

- Personal Data Privacy
- Third Party Archiving
- Carelessness
- Theft
- Legal Action



Where is this Problem?

- Corporate / Private Emails
- FaceBook Messages
- Google Docs
- Flickr
- Text Messages



Solution

- Delete all Copies after Certain Time
- No User Action to Delete
- Impossible to Decrypt after Expiration



Contributions

- Identify Requirements for Self-Destructing Data
- Implement System using DHTs
- Demonstrate Correctness of System
- Evaluate the Implementation



Possible Approaches

- Manual Deletion / Cron Job
 - What if Machine is Stolen?
- Traditional Encryption
 - Attacker Gets Key
- Deny Existence of / Hide Data
 - Computationally Implausible
- Trusted 3rd Party Escrow
 - Users are Wary to Trust Service



Goals

- Complete Destruction After Timeout
- Remain Accessible Until Timeout
- Leverage Existing Infrastructures
- No Secure Hardware
- No New Privacy Risks
- No Passwords



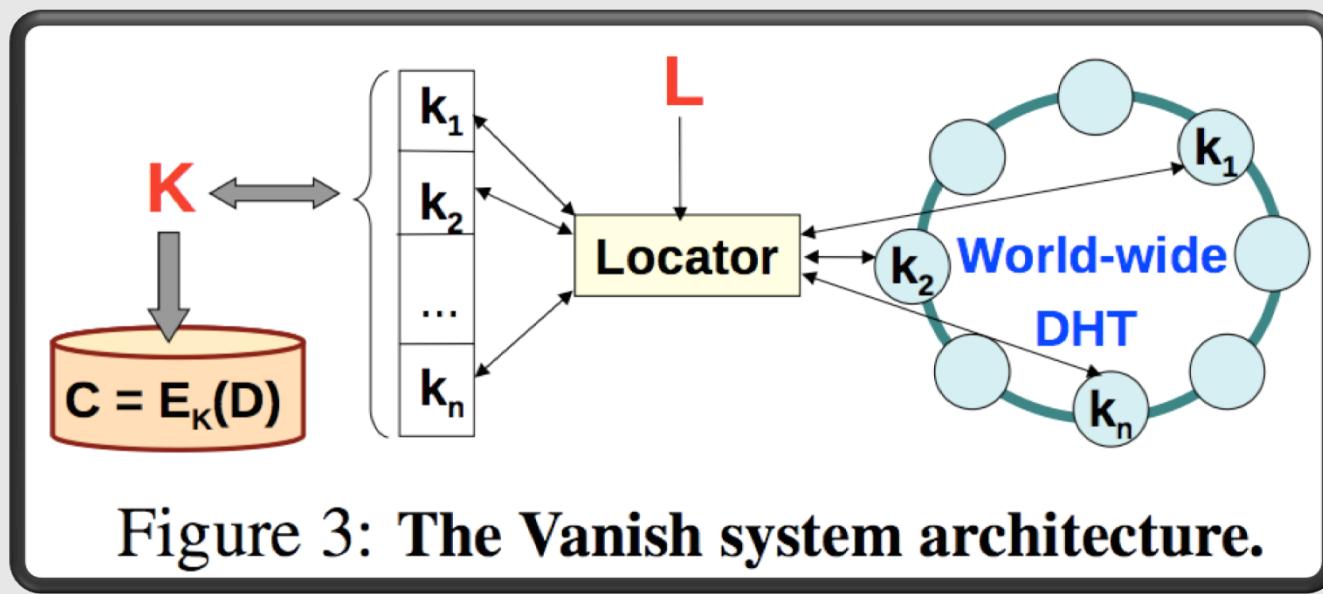
Assumptions

- Time-Limited Value
 - Data Not Important After Timeout
- Known Timeout
- Internet Connectivity
 - Required for Encrypt & Decrypt
- Dispensable Under Attack
 - Expire Early
- Trusted Data Owners
- Attacks are Retroactive

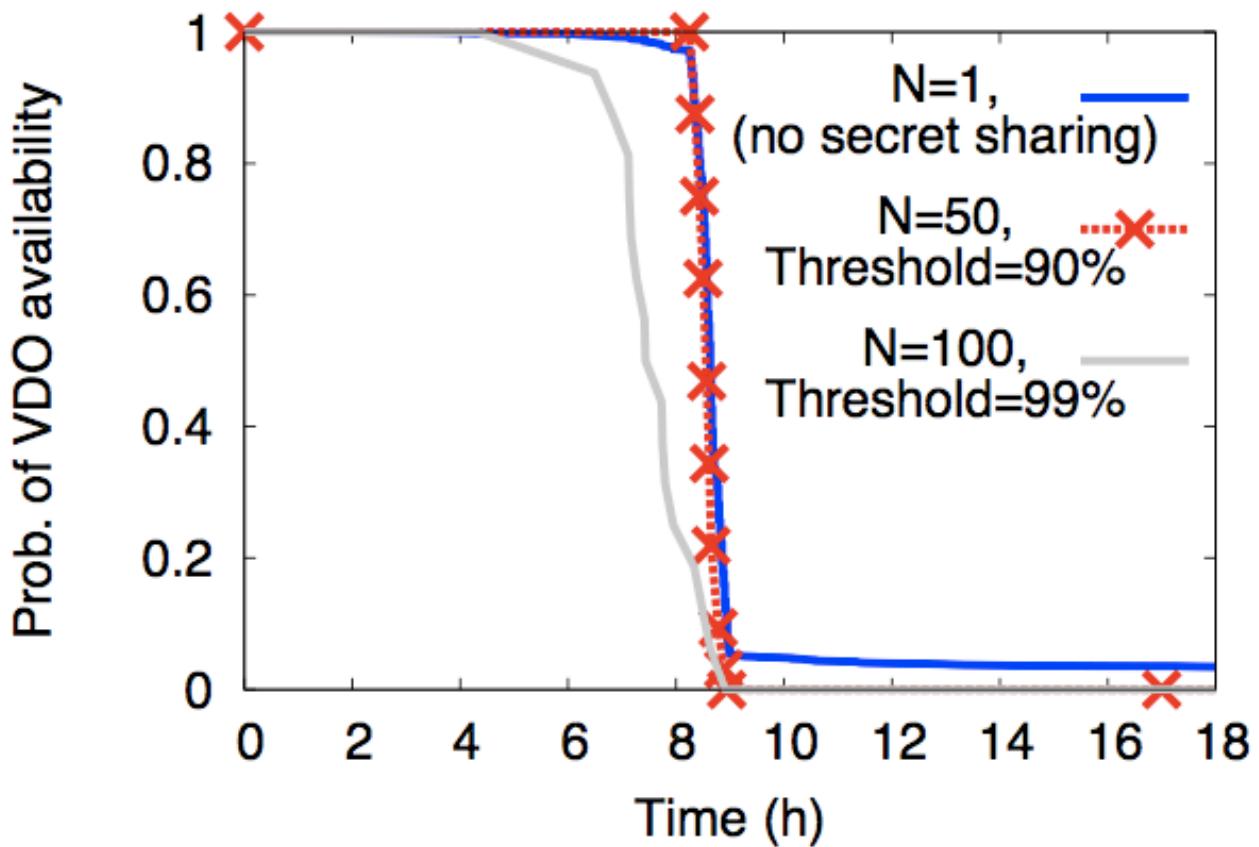


Vanish Architecture

- Uses DHTs
 - Allow Huge Name Space (2^{160})
 - Availability
 - Decentralization
 - Churn



Vuze (Azureus)



FireVanish

facebook Home Profile Friends Inbox

Inbox Sent Messages Notifications Updates

Advice on divorce document
Between You

Today at 3:15pm

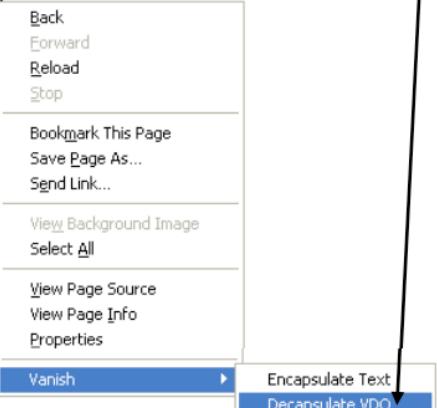
---BEGIN VDO MESSAGE---

<http://vanish.cs.washington.edu/>

AR +LCAAAAAAAACVkj8sBEEUxt
+dnH+hERoFrWJXgYLqcFjuQiI0
is1kd3lz7M6umXc4QjQShU6p0N
BR06hU12pcp6W4Qk5H4R13XHuT
liILnYOGCONZkrP/5WzP2L9yd
PObry2G/2n9mKglbhD1OD5V
5UvNPVzixWbiybB0+rY5XChi
jjytPFGLnv1u7dLV5EykJ83wW/
EST24pgQ0q0iTDMjvWbx8kB
KVe/6xqzeIPYYuUq7h3M9Ce8
Cw3CRCtuc8ur/zUkV33H09g
glsY61wPrX4uGhXLreHzplQs
gbo3NUDypT5WB7pVIXSNoIS
hCQbuIAr92liGPCujS7PubilmC
j7REESL0ZTfZDrMDpvL2Kmp
3yMUU3RQdFJ0jbOrP6fjX6ev
8IWq3h5sP2aq34LSGGK4AgA

---END VDO MESSAGE---

Decapsulate VDO



(a) Vanishing Facebook messages.



- GPG Based
- Gmail
- Web Input

Performance

N	Time (seconds)		
	Encapsulate VDO		Decapsulate VDO
	Without prepush	With prepush	
10	10.5	0.082	0.9
20	16.9	0.082	2.0
50	32.8	0.082	4.7
100	64.5	0.082	9.2
150	94.7	0.082	14.0
200	124.3	0.082	19.0

(b) VDO operation execution times.



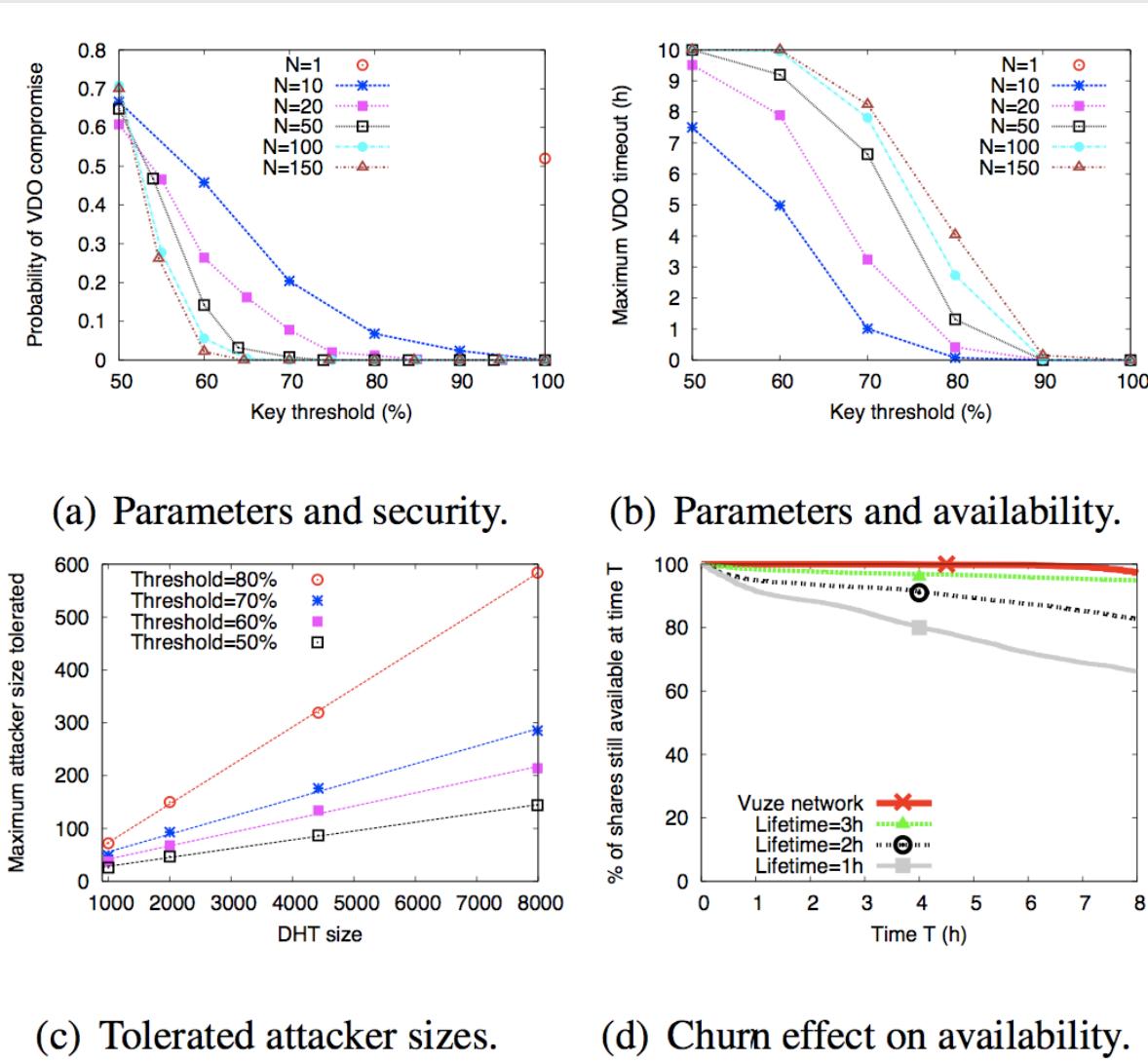
- Most Execution Time from DHT
- Larger Data == More Encryption & Decryption Time

Attack Strategies

- Decapsulate VDO Prior to Expiration
 - Encrypt VDO Using PGP or GPG
- Sniff User's Internet Connection
 - Compose with TOR
- Integrate into the DHT
 - Too Costly (\$860K / year)



Security Analysis



Conclusion

- Implemented Prototype
- Uses DHTs and Key Sharing
- Files Irreversibly Self-Destruct
- Relatively Efficient
- Safe From Attack

