Midterm Review & Memory Efficient General Attacks to Hashes

Yan Huang

- 1. Economy of mechanism
- 2. Fail-safe defaults
- 3. Complete mediation
- 4. Open design
- 5. Separation of privilege
- 6. Least privilege
- 7. Least common mechanism
- 8. Psychological acceptability

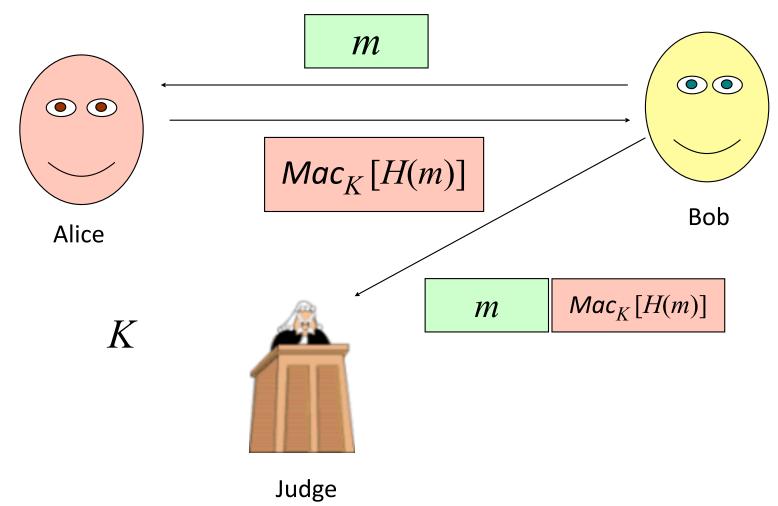
Least Common Mechanism

	Safari File Edit View History Bookmarks Window Help			_							_		0000000000	(iii) Kharged: Mon 10:20 PM Q
	000 Chatfix-Compatition	0.0	0		Induce (3.1	110 message	es, 1428 unread)			0		eoo /	roductivity101 + Edit — WordPress	
	2-0 B M m-m- # 0 0 1 2 8 5 m H .	-			0						- 1	a n G S a grap / www.protection	001.com/wp-admin/post.php?action-edit&post	a-451 Q Couple
	New Open Save New Linds Reds Farmut Tables Catures Drow Naripaton Callery Taulous Jone	Galwa	el .		Delete		phy Reply All Parwar							
	Desument Dements Quick Tables Charts SmartAt Graphics WordArt	MALL		-			Alleber 303-p			1 2 54		Destitioned		-In Meh.2mali Les.Out Mile Broms
	the withheir ratings. The score from half of these saleslated ratings is show publicly. The other half are used by Kerlin to determine if the prior has been wen. This is done to prevent contentants from merely training their algorithm to get a			30	* G	angle Alerts	Geogle Alert	link.htt	fay 8.48 PM			Productivity501		
	high score as the test ratings.		Apple Mail To Do	- 11		Coogle Alerta Coogle Alerta								
	The scoring system used by Norfla is the root nean square error (IMNE). If an algorithm predicts that a user will root a more a 43, but the user adually roots it a 3, then prediction was off by 1.5. "No value is squared to come up with a		antik E-mail			revelar	Welcome to G					Write Manage Design Comments	Contact Form	Settings Rugins Users
- 29	value of 2.25. This is done for all the assumes and their value is averaged (arthmetic mean). The square root of the mean gives the RMM. So for the example above, with only one rating the RMM would be 1.5.		iii kii iii kuum (Ы		Project Wonder Project Wond		bil 4 Tol						
8	Constant per use solar, the set on stample server, was may use strong, on boost water or 1.0. Constants has a MOR of 1.9125. They plan to award the price to the inam that can improve on this by 1.0% and		in the second se	-11		Project World	ler Highbid notice		1/08 2.57 AM			Posts Pages Links Categories Tags	Link Categories Media Library Impo	rt Export Subscriptions
6	achieve as RMEE of 10563. The current top team to at 10628 (510% toppowenest). As eigenthis that put tendenly antiges a value between 1 and 1 will end up with an RMEE of 131 on the text data. Simply using the average rating of all					ederico Albert Federico Albe		n 16				Automatic Upgrade		
· 🖪	other users for a movie results in an IMGE of L1044 with the test data set?			8		Federics Albe		Tel deline Tel				Write Post		
5	description description			811		RU Alumni	Allieber pro-h ORU April Alui	nni e-N	fay 5.26 Pe	1 11				
	Some Existing Approaches Some of the more successful approaches have been methods that rely on singular value decomposition (1970)7. 1970			۳		eve Roesler Sone Roesler	Thanks and H Re: Thanks and	1 10	fay 4.55 Pe			Title		Preview this Post
· 🕹	allows the grouping of movies and users in order to look for relationships. It appears that it will also allow pourts identify groups of users and movies that share particular attributes without assessing to define these attributes. SHD is	*C	Dafa Retu	0		Steve Apeuler			14/08 12:22 PM			Getting the Most from a La	me Monitor	
۲	used to help determine a group of nearest neighbors in order to form the basis for a prediction.			ŏ						20				Publish Status
	Possible Approaches		E Harvard					01-procrast:				Parmalinic http://www.productivity101.com/getting-0	e mo -large montar/105/ Eds.	Unpublished 8
-	The current Northa rating prediction algorithm does not make use of the date or the movie titles. Assuming a similar approach, the date on he risualized on a grid as shown before:			0			Started by Stephe 124 unread					Post Add	media in 1. 5 0 Visual HTML	Change this post private
	Duer 10 Dans 20 Dans 20 Dans 20 Dans 20 Dans 20			0			104 04440	2.28 1012						T Addish immediately Edg
	Novie1 1 3 4 2	1.0	Sere		 Allan Laur. 		500-procrast			Today Today		word was you waw things in variety of prevent		
10	Marvie 2 2 5			D	· Alise	Alleber	500-procrast			Today		most effective way to view your page is in Wel	Layout mode. Up until recently it was	Save Publish Owlets post
0	Novie 6 1 2 Novie 5 3 2 4 4		C mail C Nanani	L	 Kovi. Dout 		500-procrast			Today Today		called something else imaybe draft model, but Layout mode, your text wraps to the width of		Last added by Wark Shead on April 7,
E			C Grai	1	· Carel	. Alleber	500-procrast			Today		complete sentence without needing to scroll a		2008 at 9:04 pm Oral-Samed at 10:22:34 pm.
- 64	The nearest neighbor method, view in find another user who has raind movies in a similar manner and use their rainage to determine the unknown rating. In the example above, assume the send to produc the noting for Marie 4 by User (d.		HAR, ACTIVITY		K Charl		500-procrant			Today Today		level you use or how big of font you are typin		
1	A searest angliber solution would dentify they 30 as the searest neighbor and can they 30's ruting of Morie 4 to help predict liner of a ruting of that morie. With a large data set the searest neighbor would be a group of users. Their				 Patrix Line / 	ck Alleber	500-procest			Today Today		designed to let you focus on writing not layout		Related
	values would need to be averaged.				 Jacely 		500-procrast			Today		Web Lautout mode is great if you have a small very useful if you are writing while referencing		 See Comments on this Real
2	Furtherst Neighbor A possible approach would be to factor in the opposite approach. The "furtherst neighbor" would look for committee				 josh opial 		500-procest			Today		web layout of a document in Word on the rig	N) while keeping email visible, writing	 Manage ALContinents
- QI	would hate each other's selections and use that to influence the predictions. Obviously this would only be useful in	-			· Sergi	 AWeber 	500-procrant:			Today -		this article (on the right) and previewing it (or		 Macasan Al Ponto Macasan Al Campanina
-	certain attuations. Nost people have a good idea about what movies they don't like and won't oven wanth them. The place it could come into play it where two users both like action movies, but like very different drags. In they are likely	10.00	X 0-		· maily		500-procrast			Today 2				 Macaum All Tass
	to view the same movies, but have polarized ratings of the same movie. Unite Data Information	000	Cetting the Most From a Large Monitor ProductivityS01									However, on a large doesn't really take advant	the of the larger scenes if you are last	- Yes Data
2	It appears that must been are following Kertfar's example and disregaring data information. In at least one of	a a d S0 e Thtp://www.productivity101.com/1p=0106preview=true										focusing on your document and not using oth	er programs. If you switch to the print	
÷.	contestant is using the date information to try to normalize the and/oring effect. This is the sites that if a core vestilled three mories over a weekend that they would normally rate a line, they may rate are a line, the lawerise of the three as	_		_					search parts	а.	layout you can see an entire page as it will be	printed. This can be ideal if you are		
	a bit, and four that fourth and f								th Word white referencing web pages					
. V #	Date information ends also be used to identify different types of users. For example fomeone who likes action mories for their special efforts to more likely to worth a more usen after to release while someone who-examp other aspects may	bases 1	tone (Met / detroy the Most from a Larg					eNews & Up	adates.	100	н.	If you are just focusing on writing, you may w		
· U	empty after montex is the same genes. It is possible that this could be used to help predict ranking.							Sign up to measive new posts delivered				pages side by side. In the newest version of C		
14	Deter information mold also be used to determine nearest neighbors. Nearest neighbors mold be identified not just haved as having emdar notings, but as having emdar notings in a emdar order or securing at endar powers in tens.	Gettin	g the Most from a Larg	20 M	onitor			directly to your in		~3.8v		Path p		
P	A potential problem with this type of approach is in the Netflin scoring. The text data asks the algorithm to product using and information. The predictions are then compared to the actual rating. It does not appear that the data information is		108 Print The Article					Enter your error	il address					
à.	previded.	l anno	I read about a study that showed produ		constant when	a nannia usati	a la construction de la construc				н.	Tags		
	Genetic Algorithm One of the more interesting approaches would be to use genetic programming to predict ratings. Some basic level testing	1										Add new tes		
š	with 550° were to indicate that this is unlikely to perform well compared to other approaches. Rowever from a		the past 3 years, five learned a few thir				et real estate.1	Out a senter podcast Out the latest information about data center				departure tage with commun		
- 63	research standpoint it would be very intervening. It appears that creating a reasonable solution using a genetic approach would involve programming the spream to	Birk Liero	ow why productivity doesn't continue to	90-101	with even large	er screene.		Get the latest in technology via	policari	data center				
Ø	dentity amend key attributes and bridge the generic evolution field the best way to contribut these attributes. For example, the generic algorithm sould be previded with the average ruting of the morie in question, the average ruting by	By arrend key attributes and letting the genetic evolution find the best way to contribut those attributes. For To use a larger r					eryears of using	Cardo anno				Categories		
- 5	nearest neighbors, the average rating of furthest neighbors, etc. The genetic evolution would attempt to create		laplay devices. This is a lot harder then et more from your screen as well as so											
Gelo	relationships between these attributes in order to predict a rating. Green a large chatter of computers (Die Amasse's Elastic Computing infrastructure) to let the algorithm evolve, it might	which any		a spe	a long young	er o can jobri	and your second	Poduat Dear	tree inter			1. Add New Colours		
- 65	teres a separation of memory and the Annual is there (imposing intervention) to at the approxime event, it report he possible to come up with an unexpected within.							Beginner or Pro finest sound	, come see What	t we offer for the		All Categories Mature	n	
	Key Reading Links	Don't M	aximize Out of Habit					to der sound				Moli Jusi Chevelagement		
	Netter has a paper that describes the competition and looks at the current progress of the competitors.	Design of	ho are use to a 17 inch monitorrand to	-	in the latence	and along the	the second is the					() Money	-	
T	http://www.aetflaprim.com/aweta/Netflad/int/20.in.approx.pdf		y prevalent in Mindows users, bull've i							Anay Google		Organization Organization	10	
	The current top placed team has written a paper exclusing their approach. It lats many at the different approaches they are using and have the results are blended together.		his may be exactly what you need to do				on, it is hard to	_				(Tooperand)	*	
ы	http://www.search.et.com/codes/ortho.Tragenet/cis/2017/billior/side.com	work who	If you constantly need to scrol back an	10.00	to see everyth	ing.		Recent Poels						
			when you do the same thing on a 30 i					Delays with 8				Advanced Options		
-	Other Reading Links http://windex.topped.com/windex/2007/07/06.testadaes.html							C Enail Related Links				1 course		
	http://www.invelopies.com/whenes.com/http://www.invelopies.com/											• Excerpt		
100	http://withoutang/organization.com/community.com								Changes at Productivity501			1		
<u> </u>		Padrata 10 2 Auto					7.4	D Summer School				Trackbacks		
	L			-	-		40.0	The second second	-	_				
			A STATE OF A STATE OF A STATE					Notest Contracts				- Custom Fields		
	*http://whimsinctoopped.com/whimsinc/2007/07/the instantionalized	Phtp://white/insigns.page.com/white/en/2001/10//de-len/atou/deal Phtp://white.eng/Pht/amou/count/2000/2111/cont						Mark Sheed @Oat - Checkout his article about Intersections and Unions in echorons. If was very				Loading "Mp These production/101 contrapt adminipted phylo-	Non-selfdport-WW, completed 54 of 57 lines.	
	*Nep/JerrorationLone/additio/media/magnine/34.43/mLantila/tacronit/age-all	0					hepfulinione		a contraction of the					
					100			Andrew Core	ting Very nice. 1 e	specially the the	E.			
					100 C				and the second second second	A REAL PROPERTY AND A REAL	121			

Basic Crypto

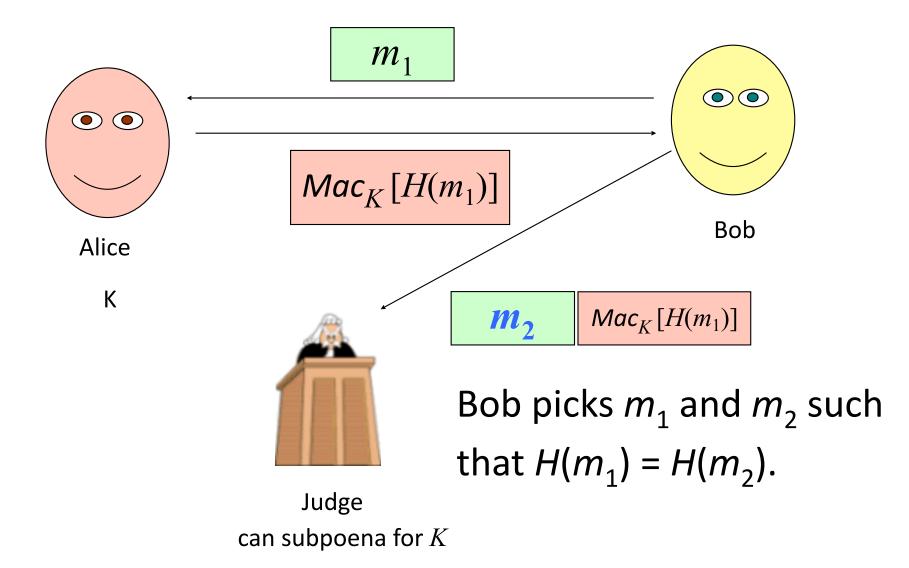
Memory Attacks

IOU Request Protocol



can subpoena for K

Attacking IOU Request Protocol



Finding m_1 and m_2

Bob generates different agreeable m_1 messages:

I, {Alice | Alice Hacker | Alice P. Hacker | Ms. A. Hacker}, {owe | agree to pay} Bob{the sum of | the amount of}{\$2 | \$2.00 | 2 dollars | two dollars}{by | before}{January 1st | 1 Jan | 1/1 | 1-1}{2016 | 2016 AD}.

How many different-text messages are there?

Finding m_1 and m_2

Bob generates 2^{10} different agreeable m_2 messages:

Bob's Quadrillionaire Plan

- For each message $m_{1,i}$ and $m_{2,i}$, Bob computes $H(m_{1,i})$ and $H(m_{2,i})$.
- If $H(m_{1,i}) = H(m_{2,j})$ for some *i* and *j*, Bob sends Alice $m_{1,i}$, gets $Mac_K[H(m_{1,i})]$ back.
- Bob sends the judge $m_{2,j}$ and $Mac_K[H(m_{1,i})]$.

Chances of Success

• Assume the Hash function *H* is good (uniform randomly distributed outcome)

What is the probability that $H(m_{1,i}) = H(m_{2,j})$ for some *i* and *j* ?

Birthday "Paradox"

Assuming real birthdays assigned randomly: N/D = probability there are no duplicates 1 - N/D = probability there is a duplicate

 $= 1 - 365! / ((365 - k)!(365)^k)$

Applying to Birthdays

For n = 365, k = 20:
 P(365, 20) ≈ .4114

• For
$$n = 365$$
, $k = 40$:
P (365, 40) $\approx .8912$

Chances of Success

• Assume the Hash function *H* is good (uniform randomly distributed outcome) but has only 128-bit outputs

What is the probability that $H(m_{1,i}) = H(m_{2,j})$ for some *i* and *j* ?

For
$$n = 2^{128}$$
, $k = 2^{65}$: P (2^{128} , 2^{60}) > 0.86

Only Half of the chance will the

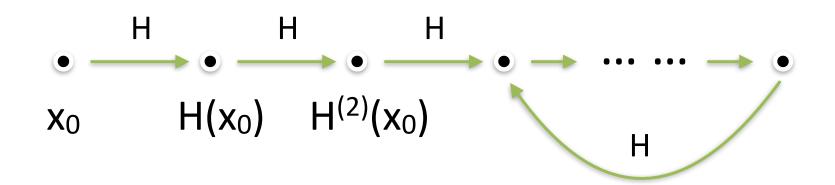
two pre-images of the collision come from two different message groups.

How much memory does birthday attack require?

>16 x 2⁶⁰ bytes!

Realistic?

Constant Memory Hash Attacks (1)



Hash meaningful messages

Set 0 = Bob is {good, hardworking} and {honest, trustworthy} {worker, employee}.

Set 1 = Bob is a {difficult, problematic} and {taxing, irritating} {worker, employee}.

Define function *g*:

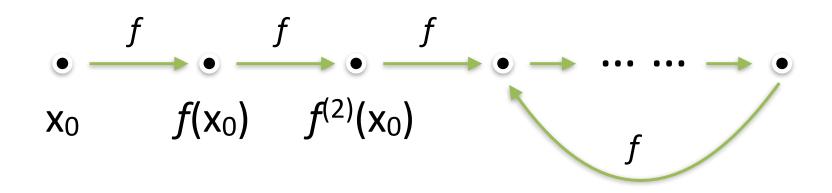
g(0000) = Bob is a good and honest worker.

g(0001) = Bob is a difficult and taxing worker.

g(1010) = Bob is a hardworking and honest worker.

g(1011) = Bob is a problematic and taxing employee.

Constant Memory Hash Attacks (2)



Define f: $\{0,1\}^l \longrightarrow \{0,1\}^l$ f(x) = H(g(x))