Preventing Side-Channel Leaks in Web Traffic: A Formal Approach

Goran Doychev

IMDEA Software Institute

joint work with

Michael Backes and Boris Köpf

20th Network & Distributed System Security Symposium San Diego, CA February 25, 2013

S O Puppy - Wi	kipedia, the free encyclopedia - G	sogle Ch	ome			e
<> C A http	s//en.wikipedia.org/wiki/Puppy					☆ =
M Google Mail 🔤 N	ews 🚘 Sport 🚘 Reference 🚘 V	/ork 🐗	носч 🔝 та	C Vista Scree	s 🚘 radio	Cther Bookmarks
1.000						treate account 🛔 Log in
a "	Article Talk	Read	View source	View history	Search	٩
Waynerra	Puppy					
The Fine Encyclopedia Mails page Contents Peatured costeri Canterd events Bandeth st Willipedia Danale fol Willipedia Danale fol Willipedia Danale fol Willipedia Domensity parkti Recent changes Content Willipedia F Tostbox P Foldbox	The analog is advoct the denored A page is a junction day, Some op 1.4 kg, which larger rooms can very? heating papers grow cacks which which are the page grow cacks, which are in the page grow cacks, which are used to the page grow cacks, which are used to the page of the bus cach to the part of the page of the bus cach to the part of the page of the bus cach to the part of the page of the bus cach to the part of the page of the bus cach to the part of the page of the page of the 1.0 million part of the bus cach to the 2.8 million cach are 3.8 million cach are 4.8 million cach are 4.8 million cach are 4.8 million cach are 4.8 million cach are and the page of the page of the 3.8 million cach are an a	log. For or pics may v p to 15–22 th. A puppy rath, puppy rath, puppy in r mammals	er uses, see A eeign 1-3 to (t) to (s.B-20 kg) 5 coat color of 5 coat color of 5 coat color of 6 color of 6 coat color of 6 co	Appy (disorda) A5- A1 my change as the ly to dogs , graffies.		2
Languages Ceaky Detsch Decach	Development Born after an average of 63 days of g amnion that is bitten off and eaten by name almost immediately. If the little	estation, pa the mother exceeds 5	ppies energe dog ^[2] Puppi is publics, pe	in an Is begin to Eccularly if	Three month old C	alden Retiever puppy

B C C Puppy - Wi	kipedia, the free encyclopedia - Ga	ogle Ch	iome			e
< > C @ http	c//en.wikipedia.org/wiki/Puppy					승 표
M Google Mail 🔤 N	ews 🖀 Sport 🛸 Reference 🚘 W	ork 🐗	носч 🖪 та	C Vista Scree	s 📔 radio	Cther Bookmarks
1.000					6	treate account 🛔 Log in 🗧
a "	Article Talk	Read	View source	View history	Search	٩
Wayangord	Puppy					
The Fixe Encyclopedia Main page Contents Peaturel content Cartent events Random article Danak is Walajedia Danak is Walajedia Danak is Walajedia Danak is Walajedia Danak is Majedia Danak is Angela Danak is Angela Danak is Angela	This analog is a device a support of a suppo	og For ot vies may v s to 15–23 h. A puppy anly seen h. puppy n manimals	er uses, see A wigh 1-3 Ib (0 Ib (6.9-30 kg) 'S coal ceter m in breeds such free specifical such as seals	Appy (disambig A5- A1 aiy changa a si the ly to dogs , grattes.	Ī	2
Contact Wildpedia + Tealbox	2 See also 3 References				2	
+ Prindesport	TEACTR PRS				100	a de la
* Languages	Development				These second and C	A des Dessen and C
Deltsch Deltsch	Born after an average of 63 days of ge ammion that is bitten off and eaten by nurse almost immediately. If the litter	estation, pa the mother exceeds s	ppies emerge dog ^[4] Pappie	in an Is begin to Ricelarly if		-

() C D m	wikinedia oo	on which the	knietry is the						
1 Goode Mail 🗃	News Sc	nort PR	efecence wo	ek dincen	БЛ ТА	C Vista Scree		v 😑 011	er Bookm
								0.000	
1.00									
10 0	Article T	Talk		Read	Edit	View history	Search		0
1 1									
Winner A	Ban	kruptc	y in the Ur	nited Stat	es				
The Free Encyclosedia	Fion We	Nipecia, the fi	ee encyclopedia						
	Bankna	alloy in the S	anited States is on	vened under the	United	States Coost	a cice (Artis	ie 1. Section 8.	Chanse (1)
						and of French and	talan danan		Caston 1
sour page	which as	uthorizes Co	noress to enact "un	forn Laws on th				nost the United	
Contents	Which as Congress	athorizes Co is has exerci	egress to eract "ur ised this authority s	iforn Laws on th evenil times sinc	e 1800	1, most recently	y by adopte	ng the Sankrupt	cy Reform
Contents Featured content	Act of 1	uthorizes Co is has exerci 1978, as aree	ngress to enact "ur ised this authority s inded, codified in Ti	iforn Laws on th evenil times sinc tie 11 of the Units	e 1800 M S18	1, most recently tes Code and o	y by adopte commonly re	ng the Sankrupt elemed to as the	cy Melorn
Contents Featured content Current events	Act of S TBankra	uthorizes Co is has exerci 1978, as aree proy Code" (rights to enact "un ised this authority s inded, codified in Tr ("Code"). The Code	iform Laws on th overal times sinc tie 11 of the Units has been amend	e 1800 of State	1, most recently tes Code and o reral times since	y by adoptic commonly re ce, with the	ng the Sankrupt elened to as the resist significant	cy Rotorn
Stain page Contents Featured content Current events Random article	Which au Congress Act of 19 "Bankrap changes	uthorizes Co is has exerci 1978, as ame proy Code" (s enacted in	ngress to enact "ur ised this authority s inded, codified in Ti ("Code"). The Code 2005 through the 8	iform Laws on th evenal times sinc tie 11 of the Units has been amend animuptcy Abuse	e 1800 sd Stat ed sev Prove	1. most recently tes Code and o veral times sinc rition and Cons	y by adopte commonly re ce, with the curner Prote	nost the United ing the Sankrupt elemed to as the most significant ction Act of 200	cy Rotorn Nocent
stain page Contents Featured content Current events Random article Donate to Wikipedia	Which au Congres Act of 19 "Bankraj changes (BAPCP	uthotzes Co is has exerci 978, as ame ptcy Code" (s enacted in PA). Some la	ngress to enact 'un ised this authority s inded, codified in Tr ("Code"). The Code 2005 through the 8 av relevant to banks	iform Laws on th evenal times sinc tie 11 of the Units has been amend annuptcy Abuse uptcy is found in	e 1803 ed Stat ed sev Prove other p	L most recent tes Code and o reral times sinc ation and Cons parts of the Uni	y by adoption to the some only in the some only in the some of the some of the some of the source of	nost the Cristed ing the Berknupt element to as the most significant ction Act of 200 Code. For exam	oy Notorn I nount 6 pia,
soun page Contents Featured content Current events Randon article Docate to Welpedia + Interaction	Which au Congres Act of 19 TBankrap (BAPCP bankrap)	athotzes Co lo has event 978, as ame ptcy Code" (s enacted in PA). Some la fcy crimes a	regress to enact 'ur ised this authority s inded, codified in Tr ("Code"). The Code 2005 through the B ar relevant to banks are found in Title 18 host Street Code (Code	iform Laws on th evenal times sinc tie 11 of the Units has been amend animuptcy Abuse uptcy is found in of the United Sta termit Devenue.	e 1800 ed Stat Prove other p bes Co	 most recently tes Code and o veral times sinc rition and Cons parts of the Uni ole (Drimes). T part to centre. 	y by adopti commonly re ce, with the camer Prote- ited States fair implication	ng the Bankrupt eferred to as the most significant ction Act of 200 Code. For exam- tors of bankrupt fortice of bankrupt	cy Rolom nocent 6 pie, cy ant four
Sear page Contents Featured content Carrent events Random article Donate to Wildpecks • Interaction Help	which as Congres Act of 19 TBankrup (BAPCP) bankrup In Title 2 ans form	uthorizes Co is has event 1978, as ame ptcy Code" (s enacted in PA). Some la fcy crimes a 26 of the Uni 26 of the Uni	regress to enact 'ur ised this authority s inded, codified in Tr ("Code"). The Code 2005 through the B ar relevant to banks are found in Title 18 ted States Code (in of the United States	iform Laws on th evenal times sinc te 11 of the Units has been amend ankruptcy Abuse uptcy is found in of the United Sta temal Revenue C	e 1803 ed Stat ed sev Prove other p bis Co lock).	 most recently tes Code and o veral times sinc ntion and Costs parts of the Unit ofe (Drimes). T and the creatio barbinia recently 	y by adoptio commonly in or, with the armer Prote- ited States fait implication in and jurisco real.	rig the Serieupl rig the Serieupl eferred to as the most significant ction Act of 200 Code. For exam- tons of bankspl diction of bankspl	cy Rolom excent 6 pla, cy are tours ptcy courts
saar page Contents Featured content Current events Random article Donate to Wildpedia • Interaction Help About Wildpedia Content wild control	Which as Congres Act of 19 TBankrap (BAPCP) bankrap in Title 2 are foun	utholizes Co is has exerci (978, as arrie ptcy Code" (s enacted in PA). Some la ficy crimis a 26 of the Uni rd in Title 28	Ingress to enact, 'ur ised the authomy of inded, codified in Ti ('Code'). The Code 2005 through the B ar relevant to banks are found in Title 18 led States Code (the of the United State	iform Laws on th evenal times sinc tie 11 of the Units has been amend ankruptcy Abuse uptcy is found in of the United Sta temal Revenue C is Code (Judiciae)	e 1800 ed Stat ed sev Prove other (bes Co tode), - and J	 most recently tes Code and o veral times sinc nton and Cons parts of the Uni de (Drimes). T and the creatio hudicial procedu. 	y by adoption commonly in or, with the sumer Protective fixed States (an Implication and jurisc are).	Ing the Derived rig the Derived right Derived to as the most significant ction Act of 200 Code. For exam- tons of bankspt diction of bankspt	cy Rolam recent 6 pie, cy are tours ptcy courts
sear page Contents Featured content Current events Bandon article Donate to Walapedia Donate to Walapedia Help Adeut Wilopedia Community postal Becert charapea	which as Congress Act of 19 "Bankray changes (BAPCP) bankraph in Title 2 are foun while bar and foun	uthotzes Co is has exerci 1978, as ane ptcy Code ¹ (s enacted in 24). Some la fcy crimis a ccy crimis a 26 of the Uni d in Title 20 anknuptcy ca enal law reve	Ingress to enact, 'ar issed this authomy is inded, codified in Ti ("Code"). The Code 2005 through the B ar relevant to banks are found in Title 18 led States Code (tr of the United State area area filed in United area area filed in United	iform Laws on th evenal times sinc de 11 of the Units has been amend ankruptcy Abuse uptcy is found in of the United Sta femal Revenue C is Code (Judiciay ed States Backs) deates	e 1800 ed Stat ed sev Prove other p bes Co bode), - and J aptcy C state b	 most recently tes Cade and o veral times sinc ntion and Cons parts of the Uni del (Chrevis). T and the creatio fudicial procedu Court (units⁽¹⁾ o ans are riften a 	y by adoption commonly in co., with the surrer Prote- ized States ion implication and juriso are).	ng the Sankruph elened to as the meat significant clien Act of 200 Code. For exam- tors of bankruph fiction of bankruph distance District in determining in	cy Rolam ecent 6 pla, cy an tour ptcy costs Courts), reserve
sear page Contents Featured content Carrent events Randon article Donate to Wildpedia • Metgaction Help About Wildpedia Community partial Recent changes Context Wildpedia	which as Congress Act of 19 "Bankrap (hanges (BAPCP) bankrap in Title 3 are fourn While bas and hold rights. F	uthotzes Co is has exerci (978, as ane ptcy Code ¹ () s enacted in 24). Some la fcy crimes a gicy crimes a gicy crimes a gicy crimes a gicy crimes a gicy crimes a gick and the Unit of in Title 20 anishaptcy ca end lar gove For example,	regress to enact 'w isid the authority is winded, codified in Ti ('Code'). The Code 2005 through the 8 ar relevant to banks are found in Tife 18 led States Code (in of the United State area are filed in Unit mis procedure in to any openming the i	aftern Laws on th kevenal times sinc tie 11 of the Units has been amend ankruppoy Abuse uptoy is found in of the United Sta- ternal Revenue C is Code (Judiciae) sed States Banton nikupptoy cases.	e 1800 ed State ed Sev Prove other p bes Co code), - and J aptcy C state h state h	 most recently reso Code and o versition and Cons parts of the Unit ofer (Crimes). T and the creatio hadicial proceeds Count (units¹¹⁾ o and save often a protecting cett 	y by adoptiti commonly in se, with the unner Proto- lized States an Implication and jurisc are). of the United applied whe ain property	Incur the United ing the Sentrupt element signaticant ection Act of 200 Code. For exam- tors of banksupt faction of banksup disclose of banksup disclose District in determining pr	cy Rolom incent 6 ppie, cy are foun ptcy courts Courts), operty known as
sear page Contents Featured content Carsent events Bandon article Donate to Wildpedia Help Adout Wildpedia Community pattal Recent changes Community pattal Recent changes	which as Congress Act of 19 "Bankrap (Nanges (RAPCP) bankrap in Title 2 are tourn While ban and Took rights. F ecomption	uthotzes Co is has exerci 1978, as ane ptry Code" (s enacted in 24). Some la ficy crimes a 28 of the Uni rd in Title 28 ankniptcy ca orial law gove for example, form), may de	regress to enact 'us issed this authority of winded, codified in Ti ("Code"). The Code 2005 through the 8 are relevant to banks are found in Title 18 led States Code (t) of the United State area are filed in Unit ms procedure in to law governing the - enver from state law	aftern Laws on the evenal limits sinc the 11 of the Units has been anvent ankruptoy Abute uptoy is found in of the United State ternal Revenue C is Code (Jodiciany and States Banky refluctions and refluctions and or federal law. B	e 1800 ed Stat ed Stat ed sev Prove other p bes Co book() and J spocy C state t state t state t	 most recently tes Code and a veral times sinc mon and Cose parts of the Unit of [Chimsis]. T and the creatio hadicial procedu Court (units^[1] o area are often a protecting ceta a state law play 	y by adoptit commonly in se, with the unner Proce- ized States an Implicat in and jurisc are), of the United applied whe ain property yit a major t	Input the United ing the Derivingly deleted to as the most significant close Act of 200 Code. For exam- tions of banksup diction of banksup diction of banksup diction of banksup distance District in deletermining pr from creditors i from creditors i	cy Rolom incent 6 pla, cy are foun ptcy courts Courts), toperty known as kruptcy
sear page Contents Featured content Carrent events Handon antide Donate to Welgedia • Interaction Help Adout Welgedia Contenues y postal Becent changes Context Welgedia • Teotox What lists here	which as Congress Act of 19 TBankrap Changes (RAPCPP bankrap in Title 3 are foun While ba and fold rights, F estemptic Cases, I	uthofizes Co is hits exerci (978, as ane pftry Code" (s enacted in 24). Some la ficy crimes a 28 of the Uni al in Title 28 anknuptcy ca enal har gove for example, forei, may de it is often uni	regress to enact 'w is load this authority is wride, confided in Ti ("Code"). The Code 2005 Through the B 2005 Through the B 2005 Through the 10 test States Code (tr) of the United State and an anti- trian procedure in bit law governing the environ total state wride to generalize is wride to generalize is and the t	attorn Laws on the evenal times sinc test 11 of the Units has been amend animptoy Abuse optoy is found in of the United Sta ternal Revenue C is Code (Justician) is Code (Justician) is Code (Justician) is of States Banko mitruptoy classs, validity of less or one bankniptoy	e 1800 ed Stat ed Sev Drove other p bes Co ode), - and J spacy C state 1 state 1 state 1 state 1	 most recently tes Code and a veral times sinc non and Core parts of the Unit del (Crimes). T and the creatio hadicial procedu Court (units¹¹⁾ o area are often a protecting cetts a state law play a across state? 	y by adopt commonly in on, with the anner Prote- ited States an Implication and jurisc are), of the United applied who ain property ain property ines.	poor the childe ing the beninged relevant to as the result significant close Act of 200 Code. For exam forms of banknup diction of banknup diction of banknup diction of banknup et from creditors i role in many banknup banknup	cy Rolom secent 6 ple, cy are foun ptcy courts Courts), operty known as forsptcy
stain page Contents Featured content Cartent overtis Bandon antide Danate to Wilipedia Mandon antide Danate to Wilipedia Contact tilliopedia Contact tilliopedia Contact tilliopedia Contact tilliopedia	which as Congress Act of 19 TBankrap (hanges (bankrap) in Title 2 are foun While ba and fold rights, F essential Calord, F	athofizes Co is has event ptcy Code" (s enacted in PA). Some Is fcy crimes a fcy crimes a fcy crimes a for the Uni rd in Title 28 anktuptcy ca erat lare gove for example, form), may de it is often uni	regress to ereach 'we inside this authority of inside, coaffied in Ti (Coder). The Code 2005 through the 8 as relevant to banks are found in Table 120 of the United States Code (in of the United States code (in of the United States are proceedure in bile law governing the i envice to ground the law wrise to ground the law	attorn Laws on the overall times sinc times since the Links has been among animptoy is found in of the United Sta ternal Revenue C is Code (Justiciay) is Code (Justiciay) is Code States Basics inforptry calors, validity of lens or or federal law. B come bankingtry	e 1800 ed Stat ed Sev Prove other p bes Co ode), and J aptcy C state 1 state 1 states issues	 most recently tes Cade and o veral times aloc notion and Const titon and Const and the United (Drimes). T and the creatio class are often a protecting cets a state law play across state 1 	y by adopti commonly not constructive to the States an implication of the United States of the United sphere who ain property is a magin times.	poor the Category og the Sentence deterred to as the meant algorithcart code. For exam- tors of banksup faction of banksup faction of banksup d States District in determining pr from creditors role in many ban	content open pla, cy are foun pla, cy are foun ptcy courts Courts), coperty known as foruptcy
saan page Contents Featured content Content of weat Bandom article Donate in Willpedia Content thingtedia Content changes Content thingtedia Content thingtedia Proteitos What links here Related changes Uppool the	which as Comparison of the Tamkraj Changes (BARCS) Bankraj In Title 3 are foun While ban and fold rights, F exemption Cases, R	athetizes Co is has event 978, as ame pitry Code" (s enacted in AA). Same la toy orimos a So of the Uab So of the Uab So of the Uab So of the Uab anktuptcy ca enal lair gove For example, form, and to form uni-	regress to ereach 'we seed this authority of mided, codified in Ti (Codel). The Code 2005 Precedy the 8- ar relevant to banks are relevant to banks are relevant to banks are fast in Title 2.0 of the United States Code of Law governing the 1- enve from state law while to generalize of Codewhile	atom Law on the event times sinc te 11 of the Units has been amend uptoy is found in of the United State email Revenue C is Code (Judicias) and States Basion rikuptoy Calos, caldidy of Lens of cofe basionstay (mis)	e 1800 ed Stat ed Sev Prove other p bes Co code), - and J spacy C state 1 state 1 state 1 state s	 most recently tes Cade and o veral times aloc non and Cose parts of the Unit de (Drimes). T and the creatio ludicial procedu Coset (units)⁽¹⁾ o auss are often a protecting cets a stabe law play across state 1 	y by actopy commonly in commonly in commonly in the second second in the second and purise are), of the United applied whe are property ps a major times.	proce the carried right because proceedings result algorithment codes. Four exam- tors of bankrupt doction of bankrupt doction of bankrupt doction of bankrupt ad States District in determining pr from creditors i role in many ban	cy Rolom cy Rolom cocert 6 pie, cy are foun picy courts Courts), coperty known as knuptcy
saan page Contents Featured content Content seven Randon antide Danate to Wilipedia Danate to Wilipedia Danate to Wilipedia Danate to Wilipedia Documentification Recent changes Octoactimispedia Contactimispedia Postala changes Wilhat links here Related changes Upload the Special pages	which as Congress Act of 19 "Bankrap (NAPCP) bankrap in Title 3 are foun While ba and fold rights, F exemption Cases, I 1, Heato	athotices Co is has event pitcy Code" (s enatode in 24A). Some la ticty critesia a 26 of the Uni of in This 28 anktuptcy ca and lang gove for example, form), may di it is often uni att	regress to enact 'we seed this authority o instead, coatfield in Ti (Coder). The Code 2005 Brough the 5 are relevant to banks are found in Title 12 of the United State area are field in Uni- tary generative in the law governing the instead to generalize of Contential Instances Totals	atom Law on the event times sinc to 11 of the Units has been amend annuptoy Adobé optoy is found in of the United State Email Revenue C is Code (Judiciasy and States Banton and Code (Judiciasy and States Banton one feature) and so it one federal and so it one bankruptoy (hos)	e 1800 ed Stat ed sev Prove other p bes Co 2009, - and J space of state 1 nJes p course state 1	 most recently tes Cade and o veral times also parts of the Unit offer (Chrimss). T and the creatio hubbal procedu closet (units⁽¹⁾ o ans are offere a protecting cert a state law play a across state 1 	y by actopy commonly in commonly in ca, with the unner Prote- ined States in Implication and jurisc are), of the United applied whe ain property ys a major i mes.	procement cannot in the Sentence element to as the mean significant colors Act of Sentence Code. For examinary diction of banksup diction of banksup diction of banksup diction of banksup diction of banksup dictions in banksup those coeditions i one in meany banksup banksup banksup banksup banksup distance di	control recent 6 pin, cy are foun proy courts Counts), openty known as foruptcy

C 🔒 http	s://en.wikipedia.org/wiki/Puppy			
M Google Mail 🔤 N	lews 📜 Sport 📜 Reference 📒	Work 📲 HCCH [TAC Vista Scree	s 🔤 radio 🔰	Other Bookma
1.000			Creat	a account 🛔 Log in
a w	Article Talk	Read View source View history		Q
" 1	Puppy			
WIKIPEDIA The Free Encyclopedia	From Wikipedia, the hee encycloped	ia		
Pestared content Current events Random atticle Danate to Willpedia	1.4 kg), while larger ones can weig healthy pupping grow quickly after as the puppy grows older, as is co Yorkahim Tenrier. In vernacular En while pup may often be used for o guines pigs, or even rate.	In up to 15–22 ib (E.N–30 kg). All birth: A puppy's coal color may change minarly seen in breeds such as the glish, puppy refers specifically to dogs ther mammals such as seeds, graffies.	Te	•
Help	Contents (Hote)		1 June	1000
About Wikipedia				
About Wildpedia Community partial Recent changes Contect Wildpedia	1 Development 1.1 Docking and declawing 2 See also		E.C.	154
About Wikipedia Community partel Recent changes Contact Wikipedia	1 Development 1.1 Decking and declawing 2 See also 3 References 1.1 Decking and declawing		F	3
About Wilcpedia Community partial Recent changes Contect Wilcpedia F Teolbox P Disdeoport	1 Development 1.1 Docking and declawing 2 Set also 3 References 4 External Intes			-

< > C [] en	ikipedia.o	vg/wiki/Bani						
M Google Mail 🔤 I	lews 📄 S	Sport 🛸 Re	ference 🚞 W	ork 🐗 HCCH	🖾 ТА	C Vista Scree		+ 📄 Other Bookma
1.00								Create account 🛔 Log in
10.	Article	Talk		Read	Edit	View history		Q,
WINIPEDIA	Ban	nkruptcy	in the U	nited Stat	es			
The Free Encyclopedia	From W	Alipedia, the be	e encyclopedia.					
staan page								
Contents Featured content Content events Random article Donate to Wildpedia	Which a Congree Act of 1 "Elanks: change (RAPCI	authorizes. Con riss hills exercis 1978, as amen uptcy Code" (1 ris enacted in 2 PA). Some tau	press to enact "u ed this authority ded, codified in 1 Dole"). The Codi 105 through the 8 relevant to bank	iniform Laws on th sevenal times sinc fitle 11 of the Units is han been amend Sankruptcy Abuse maptcy is found in	e subj e 180 ed Sta ed sev Prove other	ect of Banknupt 1. most recent) tes Code and o veral times sinc rition and Cores parts of the Uni	cies through y by adopting ommonly ref a, with the m uner Protoc ted States C	out the United States." g the Sankruptcy Rolom lened to as the roat significant recent tion Act of 2005 Iode. For example,
Contents Featured content Current events Random article Donate to Wildpecks - Interaction Help About Wildpecks	which a Congre Act of 1 "Banks change (BAPCI bankrup in Title are four	authorizes Con riss has exercis 1978, as amen uptry Code" (* PA). Some law ptry crimis an 26 of the Unite nd in Title 28 o	press to enact "a ed this authority ded, codified in T Code"). The Codi 005 through the b relevant to bank of found in Title 11 el States Code () if the United State	niform Laws on th sevenal times sinc fitte 11 of the Units in has been amond Barkingtoy Abuse cruptcy is found bot the United Sta Internal Revence C im Code (Judiclary	e subj e 180 ed Sta ed Sta ed Sta ed Sta prove other o	ect of Banknupl 2. most recently tes Code and o veral times sinc rition and Cons parts of the Uni ole (Crimes). T and the creatio hudicial procedu	cless through y by adopting ommonity ref a, with the m unner Protec- ted States C ast Implicatio n and jurisoli re).	out the United States." g the Bankruptcy Notorn lened to as the sent algoriticant secent tion Act of 2005 Iode. For example, rei of bankruptcy are found clien of bankruptcy costs
Contentis Featured content Carsent aventa Handom article Donates to Welpecia Patent Status Help About Willopedia Contact Welpedia Contact Welpedia	which a Congree Act of 1 Tilankos (RAPCI bankos in Title are four While b and fed rights. I	authorizen. Con sis hais exercis 1978, as amen- uptry Code" (n propry Code" (n propry Code" (n propry Code" (n propry Code" (n propry Code") (n pro	press to enact 's ed this authority ded, codified in 1 Codin). The Codi D05 through the 0 codin). The Codi D05 through the 1 in relevant to bank of the United States code () if the United State is procedure in to so governing the	nitorn Laws on th sevent limits sinc Fide 11 of the Units I has been amend Sankruptcy Abuse support is found in Softhe United Sta Internal Revenue C an Code (Judiciary Stord States Bastion anhruptcy Calors anhruptcy Calors	e subj e 180 ed Sta ed Sta other other bes Cr kode), and 2 state 1 state 1 state 1 state 1	ect of Banknaph 2, most recently tes Code and or veral times sinc inton and Cons parts of the Unit ofe (Crimes). T and the creation hadroid proceeds Count (units ⁽¹⁾ or and are offen a protecting cett	cless through y by actopting ommonity ref e, with the m unner Protoc ted States C an Implicatio mail, in and jurisola ma). If the United piptied when an property 1	out the United States." () the Bunkuppicy Molann bened to as the next stagnificant recent tion Act of 2005 Gala. For example, ms of bankuppicy are found clion of bankuppicy are found clion of bankuppicy are States Example.
Contents Featured content Carsent avents Randon article Donate to Willpedia + Interaction Help Adout Willopedia Content changes Content mispedia * Trobox What Inkis here	which a Congre Act of 1 "Banks change (BAPCI banks ba	authorizers Con- riss hais exercise 1978; as amen- 1978; as amen- pitry Code' (h is created in 2 PA). Scare Law ptcy crimes are ptcy crimes are ptcy crimes and ptcy crimes are ptcy crimes and ptcy crimes are ptcy crimes and ptcy crimes are ptcy crimes are ptcy crimes are analyzed and ptcy crimes are analyzed and analyzed and analyzed and analyzed and analyzed and analyzed and analyzed and analyzed and analyzed and analyzed analyzed and analyzed and analyzed and analyzed analyzed and analyzed analyzed analyzed and analyzed analyzed ana	press to enact "u and this authenty dot, codified in 1 Dodn"). The Code 005 through the 5 colours to basis in found in Title 10 d States Code () if the United State on are filed in Un- to procedure in the ave governing the size to generalize	iniform Laws on th sevenal times since the 13 of the Units beam amend beam of the United Statistical Statistical Statistics and Code (Juddiage and Code (Juddiage and Code (Juddiage statistics) of less as and code States Bankin and hupping cales, validay of less as some benkingstry	e subj e 180 ed 533 ed 549 Prove other bis Ch kote), and 2 state 1 state 1 state 1 state 1 state 1	ect of Bankhapi 2, most recently tes Cade and o recontly a series and recont and Cons parts of the Unit de (Drimes), T and the creatio kalicial procedu Court (units ⁽¹⁾ o area often o protecting cetts o state law play a across state o	cless through y by adopting ommonly ref a, with the m unser Protoco ted States C as Implicatio n and jurisoli mi). If the United pipfied when in property to in a major to ines.	out the United States* If the Deskinupper Median lened to as the book significant recent tion Act of 2026 Solar. For example, Solar For example, Solar Edition (County), deforming properly deforming properly thor celeblars (hown as Se in many basicrophy
Contents Featured content Content avents Handon article Dontals to Welgedia Dontals to Welgedia Adout Winopedia Community pathal Recent champes Contact Whopedia * Tobbox What Inkis here Related charges United Tick There Related charges	which a Congre Act of 1 Tillarity: change (BAPC) barlong in Tibe are four While b and fud rights. I ecempt Cidors,	authorizers. Con- cisis hais exercisis 1978; as amen- uptray Coder' (1) is enacted in 2 PA). Same Iaw play: criteria an 28 of the Unite and in Tatle 28 o annihrupto; caw derail law govier For example, I tions), may der it is often unite it is often unite	prest to eract. 's ad this authority and this authority and this authority constraints and the constraints and the constraints authority of States Code (r) and States	Iniform Laws on th sevenal times sinc field 11 of the Units bankruppy About 5 of the United Statement 5 of the United State Internal Revenue (and Cate) (Judicing) 6 del States Bankru arthoptry cases, validity of liens or or frederal law. B some bankruptry bis (Judicing)	e subj e 180 ed Saa ed Saa ed Saa other stater state 1 state 1 state 1 state 1 state 1	ect of Banknups 1, most recently tes Code and o endormalites aline retion and Cons retion and Cons parts of the Uait balcoal proceeds balcoal proceeds Court (units ⁽¹⁾ o ans are often a protecting cett o state law play across state 1	cies through y by adopting commonly net a, with the m unner Prodec- ted States C an implication n and jurisdi mi). If the United philot while in property fi or a major to ines.	out the United States* I the Destruction (Mutan lened to as the most significant recent loads. For example, mod hark of 2005 States District County, determing property more creditors (moven as lie in many basicropicy

Puppy - Wikipedia, the free encyclo	opedia - Google Chrome		
Wikipedia.org/wi	Puppy Ence 🔐 Work 🐗 HCCH 🔯 TACN	/lsta Scree 🍃 rad	요구 프 이 📴 Other Bookmarks
1.25			Create account 🛔 Log in
Aricle Tak	Read View source V	Search Search	٩

$\dots\uparrow 778, \downarrow 720, \uparrow 621, \downarrow 735, \uparrow 615, \downarrow 746, \uparrow 607, \downarrow 726\dots$





$\dots\uparrow 633,\downarrow 720,\downarrow 738,\uparrow 66, \downarrow 1320,\uparrow 66,\downarrow 1291,\downarrow 619\dots$



-Wikipedia, the fre x				£
C 🔒 https://en.wiki	pedia.org/wiki/Puppy			☆ ≡
M Google Mail 🚞 News 🚞 Sj	port 👕 Reference 🚞 Work 🍕	HCCH [TAC Vista S	cree 🗎 radio 🔰	Other Bookmarks
1.1.1.10			Creat	account 🛔 Log in 🐣

 $\dots\uparrow 778, \downarrow 720, \uparrow 621, \downarrow 735, \uparrow 615, \downarrow 746, \uparrow 607, \downarrow 726\dots$





$\dots\uparrow$ 633, \downarrow 720, \downarrow 738, \uparrow 66, \downarrow 1320, \uparrow 66, \downarrow 1291, \downarrow 619...



an attack: compare distributions of packet sizes (Liberatore et al.'06)

Puppy - Wik Wikipedia, the	ripedia, the free encyclopedia - Google Chrome	<u>e</u>	Bankruptcy in the United States - Wikipedia	the free encyclopedia - Geogle Chrome
C 🗎 https	z//en.wikipedia.org/wiki/Puppy	☆ =	 C in enwikipedia.org/wiki/Bankruptcy_in_th 	
🜱 Google Mail 🛛 🔤 Ne	ews 🔚 Sport 📓 Reference 📓 Work 🐗 HCCH 📓 TAC Vista Scree	e 🚘 radio 🛛 🚘 Other Bookmarks	M Google Mail 🔛 News 🔛 Sport 🔛 Reference 🔛 V	Aork 📲 HCCH 📓 TAC Vista Scree 🔹 📄 Other Bookma
	Article Talk Read View Source View History	Create accourt @ Log in		Pred Edt Verhittery Erech 0
IIIO, UZ	Appropriate structure and a st		the second	the state of
	2 See also 3 References		v Toolbox v Toolbox	sg certain property from creditors (known as av plays a major role in many basicruptcy
		atter atte	what links here cases, it is often unwise to generalize	e some bankruptzy issues across state lines.
Languages Cesky Detech	Development Born after an average of 63 days of gestation, pupples energy in an service that is fallers off and aster to the mether day 12 purples back to	Three month old Golden Reliever aways/iP	Related changes Conte Uptoint Tile Special pages Permanent Ink. 2. Changes of the Bar Anystey Code 2. Changes of the Bar Anystey Code 2. Changes - Lucadation	15 (100)

- ▶ an attack: compare distributions of packet sizes (Liberatore et al.'06)
- ▶ a countermeasure: Traffic morphing (Wright et al.'09)

Puppy - Will Wikipeda, the	klpedia, the free encyclopedia - Google Chrome	2	😑 💿 💿 Bankruptcy in the United States - Wikipedia, the 🙀 Bankruptcy in the United 🛪 👘	free excyclopedia - Google Chrome
C 🖻 Nitpi	s://en.wikipedia.org/wiki/Puppy	☆ =	🔇) 😋 🗋 en.wikipedia.org/wiki/Bankruptcy_in_the_Uni	ed_states 🔂 🗄
M Google Mail 🚞 N	iews 📓 Sport 📓 Reference 📓 Work 🖪 HCCH 📓 TAC Vista Scr	ee 冲 radio 🛛 🚔 Other Bookmarks	M Google Mail. 🕋 News 🚔 Sport 🚔 Reference 🚔 Work	🖪 HCCH 📲 TAC Vista Scree 🔹 📄 Other Bookman
	Article Talk Read View source View histo	Create account & Log in A	Anson Tax	Create account @ Log in Read Edit View Mistory Smith Q
Main page Contents Produced condents Content events Bandom entitide Donate to Walipedia ** Interaction Held	20, T621, U/35, T615, U/4 in a wave a wave or wave or up re are use, see range power A pappy in a period is done toppen my word 1 = 0.6-6- 1.4 kg, and target one can warp to 1 = 5-21 g (d - 2 kg, A) target poppen group can be able to the set of the set of the set of the paper group can be able to the set of the set of the set warp paper are the set of the set of the set of the set of the set of the set warp paper are the set of th	16, †607, ‡726	 I DOSC, U Z U, U Z U, U Z O, O DOSC, O L Konzysz Konzysz Konzysz Konzysz Konzek konzek Konzek konzek Konzek konzek Konzek konzek Konzek konzek Konzek konzek Konzek konzek Konzek konzek Kon	el under the Variad States Construction (Uniter 1: Section 4: Course 4) clause into exister of interactions intergrand the Variant Orace 4 al treas unter ECC. For levering for advances of the Course of the el course of the Variant Orace 4 and the Variant Orace 5 el course of the Variant Orace 4 and the Variant Orace el course of the Variant Orace 4 and the Variant Orace el course of the Variant Orace 4 and the Variant Orace web, Ter replectation of the March Que to Interd orace 5 and the Variant Orace 4 and the Variant Orace 5 web, Ter replectation of the March Que to Interd orace 5 and the Variant Orace 5 and the Variant Orace 5 web, Ter replectation of the March Que to Interd orace 5 and the Variant Orace 5 and the Variant Orace 5 and the Variant Orace 5 and the Variant Orace 5 and the Variant
About Wikipedia Community partal Recent changes Contect Wikipedia	Cottents 1. Occidents 1. Occidents 1. Discling in 2. See discussed 3. References		Advertiming-endia and stand in This Community-provide the interaction Encount changes and foldored here (Condiciting-edia) engines, For exami- ent Tostilions escentiports (in a	sociedure), stol ¹¹ of the United States District Courts), offern applied when determining property sg cettain property from cerebias (universa so projes) a major stellar transp basicopticy
+ Printesport	Contraction of the	alle alle	What links here Cases, it is often unwise to generalize some	townraptcy tooleto ecitoro teato meto.
* Languages Čenky Detsch	Development Born after an average of 60 days of gestation, pupples emerge in an ammion that is bitten off and eaten by the mother dog. ⁽²⁾ Pupples begin to	Three month did Golden Delever propy	Version Loss gen Uppool the Special pages 2. Chapter 5 Lighting Permanent link. 2.1. Chapter 7. Lighting	

- ▶ an attack: compare distributions of packet sizes (Liberatore et al.'06)
- ▶ a countermeasure: Traffic morphing (Wright et al.'09)



- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)



- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)



- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)

How to show that a countermeasure is "good"?



- an attack: compare distributions of packet sizes (Liberatore et al.'06)
- a countermeasure: Traffic morphing (Wright et al.'09)
- other attacks still possible (Lu et al.'10, Dyer et al.'12)

How to show that a countermeasure is "good"?

> previous work: empirically show that a particular attack does not work



1. models of web applications, web traffic, users and adversaries

- 1. models of web applications, web traffic, users and adversaries
- 2. derive security guarantees based on model

- 1. models of web applications, web traffic, users and adversaries
- 2. derive security guarantees based on model
- \hookrightarrow models provide explicit assumptions

- 1. models of web applications, web traffic, users and adversaries
- 2. derive security guarantees based on model
- $\,\hookrightarrow\,$ models provide explicit assumptions

Main contributions:

- 1. models of web applications, web traffic, users and adversaries
- 2. derive security guarantees based on model
- $\,\hookrightarrow\,$ models provide explicit assumptions

Main contributions:

simple, yet realistic models

- 1. models of web applications, web traffic, users and adversaries
- 2. derive security guarantees based on model
- $\,\hookrightarrow\,$ models provide explicit assumptions

Main contributions:

- simple, yet realistic models
- efficient algorithms for measuring and reducing information leakage

- 1. models of web applications, web traffic, users and adversaries
- 2. derive security guarantees based on model
- $\,\hookrightarrow\,$ models provide explicit assumptions

Main contributions:

- simple, yet realistic models
- efficient algorithms for measuring and reducing information leakage
- demonstrate approach in case studies

Modeling web applications

Static website



Auto-suggest input field



Modeling web applications

Static website



Auto-suggest input field





Modeling web applications

Static website





4 / 16































▶ security measure: difficulty of guessing X when Y is known



- ► security measure: difficulty of guessing X when Y is known
- expected # guesses: captured by entropy H (Massey'94)
Measuring security in the system



► security measure: difficulty of guessing X when Y is known

expected # guesses: captured by entropy H (Massey'94)



• initial uncertainty H(X)

Measuring security in the system



security measure: difficulty of guessing X when Y is known
 expected # guesses: captured by entropy H (Massey'94)



- initial uncertainty H(X)
- remaining uncertainty H(X|Y)







Basic traffic modifiers:





Basic traffic modifiers:



Example (Packet segmentation)



Composed traffic modifier $f_2 \circ f_1$:



Composed traffic modifier $f_2 \circ f_1$:



Theorem

 $H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$

Composed traffic modifier $f_2 \circ f_1$:



Theorem

 $H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$

proof relies on data processing inequality

Composed traffic modifier $f_2 \circ f_1$:



Theorem

 $H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$

proof relies on data processing inequality

Consequence: relative security guarantees for free

Composed traffic modifier $f_2 \circ f_1$:



Theorem

 $H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$

proof relies on data processing inequality

Consequence: relative security guarantees for free

• countermeasure $f_2 \circ f_1$ at least as strong as f_1

Composed traffic modifier $f_2 \circ f_1$:



Theorem

 $H(X|Y_2 \circ Y_1) \geq H(X|Y_1)$

proof relies on data processing inequality

Consequence: relative security guarantees for free

- countermeasure $f_2 \circ f_1$ at least as strong as f_1
- security guarantees preserved when message passes protocol stack



Computing the remaining uncertainty:

►
$$H(X|Y) \ge H(X) - H(Y)$$

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths



Computing the remaining uncertainty:

- $\blacktriangleright H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths



Our approach:

Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths

Our approach:

• assume $X = X_1, \ldots, X_\ell$ is a Markov chain



Computing the remaining uncertainty:

- $\blacktriangleright H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths

Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution



Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths

Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution

$$\Rightarrow H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$$



Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths

Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution

$$\Rightarrow H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$$

Obtaining the stationary distribution: use PageRank algorithm



Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths

Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution

$$\Rightarrow H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$$

Obtaining the stationary distribution: use PageRank algorithm

► PageRank algorithm computes the stationary distribution of X



Computing the remaining uncertainty:

- $H(X|Y) \geq H(X) H(Y)$
- direct computation of H(X) not feasible:
 have to enumerate of all paths

Our approach:

- assume $X = X_1, \ldots, X_\ell$ is a Markov chain
- assume $P[X_1] =$ stationary distribution

$$\Rightarrow H(X) = H(X_1) + (\ell - 1)H(X_2|X_1)$$

Obtaining the stationary distribution: use PageRank algorithm

- PageRank algorithm computes the stationary distribution of X
- random surfer: follow random link or jump to random page













Countermeasures make vertices indistinguishable







Countermeasures make vertices indistinguishable

▶ e.g. c_order: order objects by size, pad, add dummy objects







Countermeasures make vertices indistinguishable

- ▶ e.g. c_order: order objects by size, pad, add dummy objects
- countermeasure induces partition of vertices







Countermeasures make vertices indistinguishable

- ▶ e.g. c_order: order objects by size, pad, add dummy objects
- countermeasure induces partition of vertices

Paths may not be indistinguishable



Countermeasures make vertices indistinguishable

- ▶ e.g. c_order: order objects by size, pad, add dummy objects
- countermeasure induces partition of vertices

Paths may not be indistinguishable

 $\Rightarrow\,$ ensure partition of vertices is a probabilistic bisimulation



there are many possible bisimulations



there are many possible bisimulations



- there are many possible bisimulations
- our approach: consider random bisimulations



- there are many possible bisimulations
- our approach: consider random bisimulations
 - 1. start from random bi-partition



- there are many possible bisimulations
- our approach: consider random bisimulations
 - 1. start from random bi-partition
 - 2. refine it to coarsest bisimulation /* Derisavi et al.'03 */



- there are many possible bisimulations
- our approach: consider random bisimulations
 - 1. start from random bi-partition
 - 2. refine it to coarsest bisimulation /* Derisavi et al.'03 */
 - 3. repeat

Case study

Trading security for overhead : 500 random bisimiulations




Analyzed website:

• bar.wikipedia.org (\approx 3,500 pages)

Analyzed website:

• bar.wikipedia.org (pprox 3,500 pages)

Initial uncertainty:

ℓ	1	3	5	9	15	25	40
H(X)	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	2 ^{36.5}	2 ^{59.8}	2^{106}	2^{176}	2 ²⁹⁵	2 ⁴⁷²

Analyzed website:

• bar.wikipedia.org (pprox 3,500 pages)

Initial uncertainty:

l	1	3	5	9	15	25	40
H(X)	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	2 ^{36.5}	2 ^{59.8}	2^{106}	2^{176}	2 ²⁹⁵	2 ⁴⁷²

No countermeasure:

•
$$H(X|Y) = 0$$

Analyzed website:

• bar.wikipedia.org (pprox 3,500 pages)

Initial uncertainty:

l	1	3	5	9	15	25	40
H(X)	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	2 ^{36.5}	2 ^{59.8}	2^{106}	2^{176}	2 ²⁹⁵	2 ⁴⁷²

No countermeasure:

$$\bullet \ H(X|Y) = 0$$

Applying path-aware countermeasures (path length $\ell = 5$):

Analyzed website:

• bar.wikipedia.org (pprox 3,500 pages)

Initial uncertainty:

l	1	3	5	9	15	25	40
H(X)	10.1	21	31.8	53.4	85.9	139.9	221
# paths	3496	2 ^{36.5}	2 ^{59.8}	2^{106}	2^{176}	2 ²⁹⁵	2 ⁴⁷²

No countermeasure:

$$\bullet \ H(X|Y) = 0$$

Applying path-aware countermeasures (path length $\ell = 5$):

make all webpages have the same fingerprint: expected overhead 73.5 × original size

Trading security for overhead: 500 random bisimiulations



Bonus material in the paper

- limits on overhead of path-aware countermeasure
- case study: auto-complete field
- using other entropy measures
- timing leaks: combining security guarantees with predictive timing mitigation (Askarov et al.'10)





► formal framework for reasoning about security of web applications



- ► formal framework for reasoning about security of web applications
- models of web traffic, user and adversary

- ► formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank
- path-aware countermeasures based on probabilistic bisimulations

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank
- path-aware countermeasures based on probabilistic bisimulations
- demonstrate approach in case studies

Summary

- formal framework for reasoning about security of web applications
- models of web traffic, user and adversary
- algorithm for practical evaluation of websites using PageRank
- path-aware countermeasures based on probabilistic bisimulations
- demonstrate approach in case studies