

Introduction Starlight Applications Conclusion

Security when applications become web sites

Andrea Bittau, Arti Gupta, and David Mazières

April 30, 2010

Web and apps perceived differently

Introduction Starlight Applications Conclusion



	Name: .	Agent32.exe	- t	
	Publisher:	Unknown Publi	iner	
	From: 1	\\serverdc\cor	e	
			Run	Cancel
~	This file doos	not have a valid o	inital simatum Har	t unifica ita



Users know software can do bad things.
Conservative: only install "trusted" software.

- Users believe web sites cannot do "bad" things to system.
- Liberal about visiting dubious web sites.

Introduction Starlight Applications Conclusion



The Web's evolution: rich apps (e.g., Gmail, games)

- Ever increasing functionality and performance demand.
- Security problems will only get worse.

Browser becoming platform for running applications

	Could I	when Street package Namenda	
Be Edit Yeve Higto	ry Goolemarka Taola Hala		
🔶 🛶 - 😂 😆 (🖌 💓 grangin com Miljas //mail.gov	egit combrail?hive=14span 🦙 🙀 Coope	
C LOADO	+		
Small Calandar Dacar	ants web fander max .	Mill working bittanti-granit.com (Sating)	Indo I Signout
Gmail		Searchited Search Ramas, Manager Ladies,	
Company Mail	Cabla barner but your interest	an interest Mercatheren Indeeds E-Set of Sea ch	ber cline +
14.00	Galery Al, Horse, Read, Dresad, Dan	red, Uniternal	
Cucz 🔛	Delete all spart companys can fit	messares that have have in Searc more than 10 days all he externation!	Adved
Test Past	C C Alexander Hote	hand PERFORCE change 177408 for states - http://www.i	21720
Read Class	C Almander Halls	Install PERPORCE shares 177408 for ending "http://doi.org/1	1.32.000
	C Parts	Andrea Oktas, are you using a safer brawser? (ind out no	015 am
123	C i brow treis	use Lowers handbags at amoting prices Look like a peet	9.69 am
- Care	C Ber Contate returns	ARYANA CYRERA AGRE TECHNA EZETEK LOPES: Ch. Tudo h	7.02.00
	C weder declarates	13 Wednesday renderator remarkits) making. The Volume	12/65 (m)
Cattada	wedge-more-bounces	13 Wedge-upon moderator request(a) waiting - the wedge	3246 am
10000	11 Nr. Anthony Pitter	Resideder Andrea Sillian - Have you residented - Profession	Apr 20
 Andrea Bitter 	C webs declarates	13 Wednesday renderator remarking making. The Volume	Act 28
	C wedge ware beenes	13 Medecaters mederater remential soldies. Do ticks	Jan 28
	C C State Manufa Propie	Contact M. Bichard Place , historicary we are alconative infor-	Meg 27
· trute a friend	C Smart University	MEM, SOA and Recordly Engineering Stablings - London, but	Acr 27
	C D British Lettery	werken General D Hann Marrier, This is to inform you that say h.	NY 27
	C hemerics for our cost.	one from andre, Catch 72% discounts inform, source trush	100.27
	weber-brebeauses	13 Wedge-day medicator requestion waiting - the makes di-	Acr 27
	C weder were beenen	13 Wednesdays made day remarked a wattern. The titular	ALC: UT
	17 C Mail College Sectors	Mail delivery failed returning measure to perder. This me	Arr 20
	C Brand darmale Marca co-	Bear bitter: Catch 17b discouts apartic, source tradical	100.00
	C Dentre	Get Direction, Get Plant, - Dender Plad Offer (TE COD), Early to v	ALC IN
Townshind and data from	and mode over		dater
	The groupe to rea		101 + 10

Gmail







Flash game

NaCl: run x86 in browser

Introduction Starlight Applications Conclusion



Google Native Client—run x86 code in browser:

- High performance.
- Easy porting of legacy code.



Quake 91,582 LoC

NaCl: run x86 in browser, securely

Introduction Starlight Applications Conclusion



Problem: how to sandbox x86 code?



Solution:

- Compile code to verifiable form.
- ② Verify code prior to launch.



Our work: add syscalls, securely

Introduction Starlight Applications Conclusion



Problem: how to securely allow syscalls?



Our work: add syscalls, securely

Introduction Starlight Applications Conclusion



Problem: how to securely allow syscalls?



Our work: add syscalls, securely

Introduction Starlight Applications Conclusion



Problem: how to securely allow syscalls?



Challenge: figure out policy and enforce it

Motivating examples

Quake

• Online gaming.

VOIP client

• Live support while shopping online.

Peer-to-peer streaming video player

• No need for server bandwidth.

Photo editor and publisher

• No need for server CPU expense.

ntroduction Starlight Applications Conclusion





In CA. (see April Delevanto Juli	And And Park Street.		-
		2 C 2 C 1 - p	_
Lanuara Age			
NaC	CL SIP ph	one	
	5-265-6277		





Example: Hypothetical Flickr

Introduction Starlight Applications Conclusion





2. Choose file to upload

1 4 1 10 0 V 10 10	Shown fisie carri Contin	C • Gauge	<u> </u>
Andream Internet			
			P 1
Lookin Pasticip	1		
Same Same	[Same	• Paster 14	
C. Inwith	100	000400	
A Recently Used	Astronomic and a source -3.9.0	12/25/99	P
A 1993	C MAN	1323/07	
Constant In Constant	D Bustwethfamote	152501	
AND IT FIT SYSTEM	B 099	02/06/09	
Gater	Condition	00/13/10	
	In Documents	031340	
60	TO FEE OMOU BP1	06/03/09	
	Its Fight Dean L.O.B	0613/00	
	C Fight Dear 1.9-3	073709	
	EL Cháldrag	1323/97	
	Ct 05K San Andreas User Fille	01\52/98	
	D hourging	13/23/07	
	11,90	1218/09	
	Disa Mari	06/23/09	
	Et Madit - Dutky Perkins - A LiP Ught Instrumentals	0013/00	
+500 -500		AI 7944 .	
		Manual Inches	
450 -500	In water comprehension of the operation of the	×1764 •	

3. Edit picture



4. Upload!



Architecture

ntroduction Starlight Applications Conclusion





User actions specify user's intent

Introduction Starlight Applications Conclusion



Security: carry out user intentions and nothing more.

🔁 🔕 🕋 🖬 h	ttp://www.fickr.com/	ू 🔹 🚰 Coo	phe
	OpenTile		×
format +			
	- 1		-
Pocacion: huoocipic	59		
Baces	Name	 Modified 	÷.
R Search	Sa Aam		
Recently Used	AtomicParsley-source-0.9.0	12/29/09	- 11
- root	in BitchX	11/21/07	
in Desktop	BluetoothRemote	11/21/07	- 11
File System	in opp	02/08/09	
C catern	In Desktop	02/17/10	- 81
	Documents	01/17/10	
	FSX ORAOX SP1	06/01/09	- 11
-	Flight Gear-1.0.0	06/13/08	
	FlightOear-1.9.1	01/31/09	- 11
	In GNUstep	11/21/07	- 11
	CTA San Andreas User Files	07/22/08	- 11
	Its incomplete	11/21/07	
	la pa	12/18/08	- 11
	In LineWire	06/21/09	
	Madib - Dudey Perkins - A Lif Light Instrumentals	03/17/08	•
+Add -Ba	move	All Files	-
		Normal Inc	
		e soriel Es	0.51

- User wants to open pic.jpg
- User expects app will read pic.jpg

User action: select pic.jpg via file chooser.



Introduction Starlight Applications Conclusion



Give applications privileges based on user actions [Karp06]



User action	Example of possible capability granted
File chooser	Read file
Textbox	Allow connection to host
Link text	Allow connection to peers specified in
	torrent file obtained from link
Button	Allow microphone access

Policy modules: generic and small (*e.g.*, bittorrent 100 LoC)

Trusted UI gives user action proof

Introduction Starlight Applications Conclusion





add_trusted(TEXTBOX, "SMTP server");

User interface displayed

SMTP server smtp.com

Endorsements (\rightarrow privileges)

textbox://SMTP server/smtp.com \rightarrow tcp://smtp.com:25

Trusted UI gives user action proof

Introduction Starlight Applications Conclusion



Code

add_trusted(TEXTBOX, "SMTP server");

add_trusted(TEXTBOX, "Type warez.com to continue");

User interface displayed

SMTP server smtp.com Type warez.com to continue warez.com

Endorsements (\rightarrow privileges)

textbox://SMTP server/smtp.com \rightarrow tcp://smtp.com:25 textbox://Type warez.com to continue/warez.com

Introduction Starlight Applications Conclusion





Introduction Starlight Applications Conclusion



How to allow sharing data, and avoid exfiltration?



Introduction Starlight Applications Conclusion



How to allow sharing data, and avoid exfiltration?



Introduction Starlight Applications Conclusion



How to allow sharing data, and avoid exfiltration?



Introduction Starlight Applications Conclusion



How to allow sharing data, and avoid exfiltration?



Need Information Flow Control (IFC).

Introduction Starlight Applications Conclusion



- Label data.
- ② Taint processes that hold labeled data.
- 3 Deny tainted processes from talking to network.



Introduction Starlight Applications Conclusion



- Label data.
- ② Taint processes that hold labeled data.
- 3 Deny tainted processes from talking to network.



Introduction Starlight Applications Conclusion



- Label data.
- ② Taint processes that hold labeled data.
- 3 Deny tainted processes from talking to network.



Introduction Starlight Applications Conclusion



- Label data.
- ② Taint processes that hold labeled data.
- 3 Deny tainted processes from talking to network.



Labels control information flow

Introduction Starlight Applications Conclusion



• Red on previous slide represents a category of taint.

Category An arbitrary string, *e.g.*, "secret".

Label A set of integrity and secrecy categories.



Information can flow from x to y if:

- Secrecy categories of $x \subset y$.
- Integrity categories of $y \subset x$.

Category owners control data export

Introduction Starlight Applications Conclusion



Category owners can export data.

• They can remove owned categories from their label.



NaCl applications own the following categories:

Category	Allows sharing between
HTTP origin	Applications in same page
Hash of app binary	Instances of same application
Certificate that signed app	Applications from same vendor

Telephoning from your browser

Introduction Starlight Applications



Make and receive calls from your browser:

- Live phone support while shopping online.
- Sales callbacks.

NaCl benefits:

- Can reuse SIP libraries: 347,501 LoC.
- Need performance for audio codecs.

5	- طدونوف	Performant: Normela						
Ele Edt Yew History	Bookmarks Ipols Help							
🔶 🔶 + 😰 🚳 😧	spore.com https://secure.c	ipgate.com/call		0.4	🌆 🕈 🖓	ogie		9
sipgate - Perform call	+							
🕌 sipgate		D Prove of Pain - +	Pater North	82.82	2452548	41	lined	-
How Call + How East	New Call							
41	Call from		tala	Marrente	of Grypond	Last	ala	
Stervel	Phone of Patter North		2			2	3	
Outgoing				-		5	6	
Archived	14 BURBOT		Tag.				9	
Dealth						0	Ø	
Contacts	C	all						
Citora & NotEculiana								
Labels v								
-	· · · · · · · · · · · · · · · · · · ·							
DODE							AL 81 14	

Client-based video streaming

Introduction Starlight Applications Conclusion



Watch and stream videos using bittorrent.

- No need for server bandwidth.
- High performance for video codecs.

Security requirements:

- Restrict network traffic to bittorrent peers.
- Restrict disk access to bittorrent files.





Introduction Starlight Applications Conclusion



- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.

🖕 🧼 🝷 📚 🏠 💽 file:////root/bit.html		\l] •	Google Google	Q
i file:////root/bit.html				•
Select film:				
<u>http://www.tracker.com/rocky.torrent</u> <u>http://www.tracker.com/caligari.torrent</u> <u>http://www.tracker.com/nosferatu.torrent</u>				
bitplayer.nexe S [], I []	tracker.nexe S [], I []	•		

Introduction Starlight Applications Conclusion



- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.

ሩ 🛶 🝷 📚 🏠 间 file:////root/bit.html		☆▼ 🛐 Google	٩
i file:////root/bit.html			•
Select film:			
<u>http://www.tracker.com/rocky.torrent</u> <u>http://www.tracker.com/caligari.torrent</u> <u>http://www.tracker.com/nosferatu.torrent</u>			
bitplayer.nexe S [], I [[click://rocky]]	tracker.nexe S [], I []		

Introduction Starlight Applications Conclusion



- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.



Introduction Starlight Applications Conclusion



- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.





ntroduction Starlight Applications Conclusion



- Convergence of applications and web sites is inevitable.
 - Web apps need more performance and functionality.
 - Threatens to undermine already tenuous browser security.
- Information flow control transcends complex module interactions.
- Infer user's intent from actions.
 - 1 User action generates endorsement.
 - 2 Policy modules translate endorsements to privileges.