In a change from our advertised program...

Why Passwords Don't Work

Jon Warbrick

What are we trying to achieve?

What are we trying to achieve?

Protection from

- •a bored University student
- a tabloid journalist
- an organized criminal
- the NSA

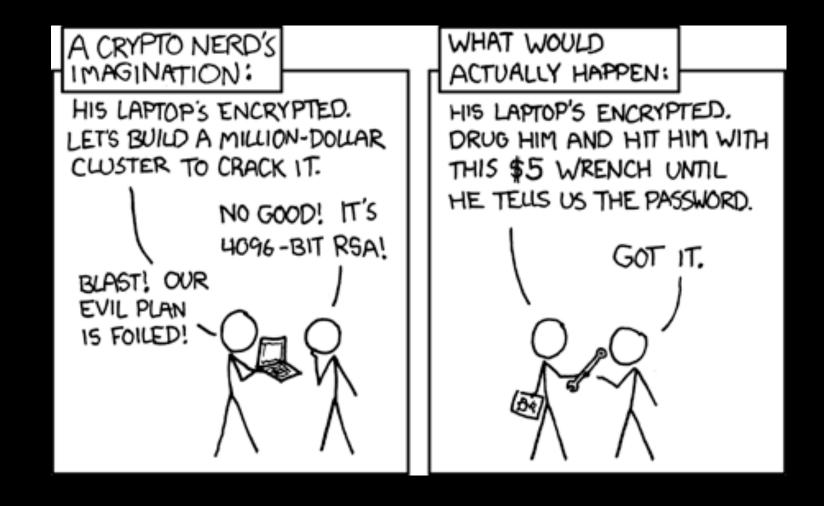
What are we trying to achieve?

Protection from

- •a bored University student
- a tabloid journalist
- an organized criminal
- the NSA

Protection of

- a student's photo archive
- the heir to the throne's email
- the University financial system



Option one: Forget passwords

User-id: jw35
\square override login options for this session?
Submit Cancel [help]

Option two: A single, fixed password

Option three: Distribute a list

Option four: Central verification

Option five: Kerberos (or similar)

UNIVERSITY OF CAMBRIDGE

Raven Authentication Service

University of Cambridge > Computing Service > Raven



The web resource you requested requires you to identify yourself [help - why am I seeing this?]. This resource is provided by the website wiki.csx.cam.ac.uk. You should only proceed if you are happy to be identified to this site.

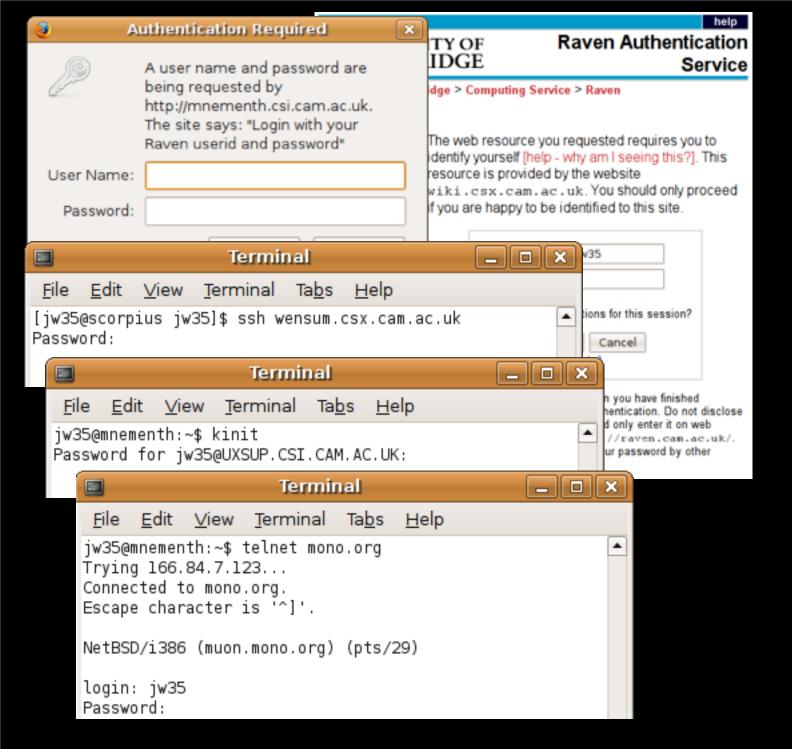
User-id: jw	35
Password:	
🗆 override login opti	ons for this session?
Submit	Cancel
flag	[p]

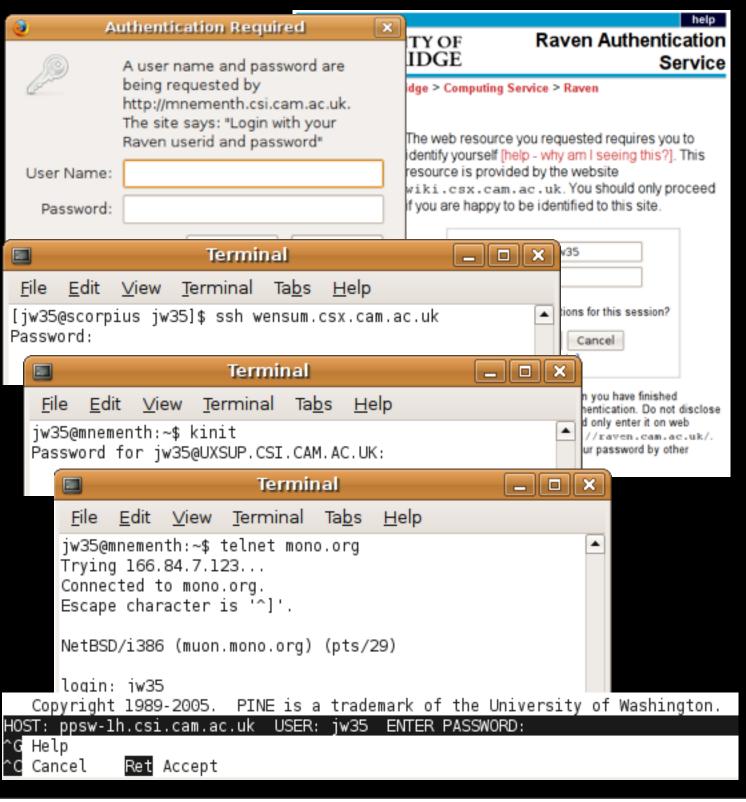
Always quit your web browser when you have finished accessing services that require authentication. Do not disclose your Raven password to anyone and only enter it on web pages with URLs that start https://raven.cam.ac.uk/. Please report attempts to obtain your password by other means.

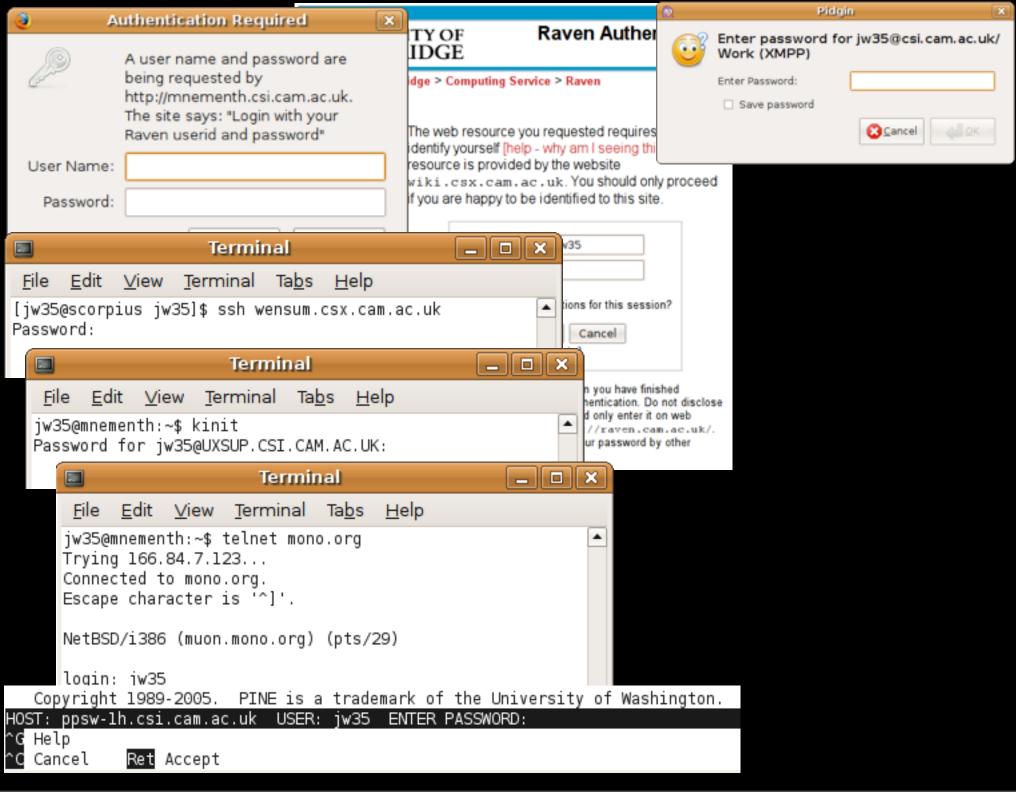
a Al	uthentication Required	×		help
ø	A user name and password are		IDGE	
(John Starten	being requested by http://mnementh.csi.cam.ac.uk. The site says: "Login with your Raven userid and password"		The web	resource you requested requires you to ourself [help - why am I seeing this?]. This
User Name:			resource wiki.c	is provided by the website sx.cam.ac.uk. You should only proceed
Password:			if you are	happy to be identified to this site.
	Cancel 🛁 OK		J	User-id: jw35 Password:
				override login options for this session? Submit Cancel [help]
			accessing your Raver pages with	it your web browser when you have finished services that require authentication. Do not disclose a password to anyone and only enter it on web URLs that start https://raven.cam.ac.uk/. ort attempts to obtain your password by other

a A	uthentication Required	×		help
	A user name and passwor		TY OF IDGE	Raven Authentication Service
Contraction of the second s	being requested by http://mnementh.csi.cam. The site says: "Login with y Raven userid and passwor	/our	The web resour	service > Raven ce you requested requires you to [help - why am I seeing this?]. This
User Name:			wiki.csx.ca	ided by the website m.ac.uk. You should only proceed
Password:			if you are happy	to be identified to this site.
	Terminal			□ × ^{v35}
<u>F</u> ile <u>E</u> dit	<u>∨</u> iew <u>T</u> erminal Ta <u>b</u> s	<u>H</u> elp		
[jw35@scorp: Password:	ius jw35]\$ ssh wensum	.csx.cam.a	c.uk	Cancel
			accessing services your Raven passwo pages with URLs th	web browser when you have finished that require authentication. Do not disclose ord to anyone and only enter it on web hat start https://raven.cam.ac.uk/. hpts to obtain your password by other

Authentication Required	×		help
A user name and password are		TY OF IDGE	Raven Authentication Service
being requested by http://mnementh.csi.cam.ac.uk The site says: "Login with your		dge > Computing Ser	vice > Raven
Raven userid and password*	io	dentify yourself [help	ou requested requires you to - why am I seeing this?]. This
User Name:		esource is provideo viki.csx.cam.a	d by the website ac.uk. You should only proceed
Password:			e identified to this site.
Terminal			× v35
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> e	elp		
[jw35@scorpius jw35]\$ ssh wensum.csx Password:	.cam.ac	.uk	tions for this session?
(
Terminal		العا	
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>T</u> erminal Ta <u>b</u> s	<u>H</u> elp		h you have finished hentication. Do not disclose
jw35@mnementh:~\$ kinit Password for jw35@UXSUP.CSI.CAM.AC	.UK:		d only enter it on web //raven.cam.ac.uk/. ur password by other







3	Authentication Required			2	Pidgir	i	×
	Authentication Required × A user name and password are	TY OF Rave IDGE	n Authe		nter password for Vork (XMPP)	jw35@csi.cam.ac.uk/	1
and	being requested by	dge > Computing Service > Rav	ven	E	nter Password:		
	http://mnementh.csi.cam.ac.uk. The site says: "Login with your				Save password		
	Raven userid and password"	The web resource you re		Authent	icate to Kerberos	All ok	
User Nam	201	identify yourself [help - wf resource is provided by t	An				
Oser Nam		wiki.csx.cam.ac.u 🌏	P	lease type y	our Kerberos passwo	ord	
Passwo	rd:	if you are happy to be ide	\sim				
			Name: j	w35			
	Terminal			JXSUP.CSI.CA	MACIIK		
<u>F</u> ile <u>E</u> di	t <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp		Password:	0A30F.C3I.CA	m.nc.01		
[jw35@sco	rpius jw35]\$ ssh wensum.csx.cam.a		rassword.				
Password:			\$÷		Cancel) (ОК)	
	Terminal		1				
			n you have fin	ished			
	<u>E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp			o not disclose			
	nementh:~\$ kinit		//raven.co ur password b	am.ac.uk/.			
Passwor	rd for jw35@UXSUP.CSI.CAM.AC.UK:			oy onto			
	Terminal		×				
<u>F</u> ile	e <u>E</u> dit <u>∨</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> e	elp					
jw35	5@mnementh:~\$ telnet mono.org						
	ing 166.84.7.123						
	nected to mono.org.						
ESCO	ape character is '^]'.						
Net	3SD/i386 (muon.mono.org) (pts/29)						
	in: jw35	de eff the University.	of Mod				
	µht 1989-2005. PINE is a trademar ∕-lh.csi.cam.ac.uk USER: jw35 EN		or was	nington.			
^G Help							
^C Cancel	Ret Accept						

8	Authentication Required		R	Pidgin	
	A user name and password are	TY OF Raven Authe		Enter password for jw35@csi.cam.ac.u Work (XMPP)	uk/
(Jose)	being requested by	idge > Computing Service > Raven	E	Enter Password:	
	http://mnementh.csi.cam.ac.uk.			Save password	
	The site says: "Login with your Raven userid and password"	The web resource you re	Authen	ticate to Kerberos	
User Name	· · · · · · · · · · · · · · · · · · ·	identify yourself [help - wf resource is provided by t			
Password		wiki.csx.cam.ac.u If you are happy to be ide	lease type y	our Kerberos password	
	Terminal	Name:	w35		
			UXSUP.CSI.C/	AM.AC.UK	
<u>F</u> ile <u>E</u> dit		Password:			
	pius jw35]\$ ssh wensum.csx.cam.a				
Password:		\$×	Cor		X
	Terminal				
File E	dit <u>∨</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp	n you have fin hentication. D		1 <i>1</i>	
	 ementh:~\$ kinit	d only enter it	t on web	he server mnementh.csi.cam.ac.uk at Login with your Rave	en
	for jw35@UXSUP.CSI.CAM.AC.UK:	ur password		serid and password requires a username and password.	
	Terminal		p	/arning: This server is requesting that your username and assword be sent in an insecure manner (basic authenticatio ithout a secure connection).	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> e	elp	U	ser name:	-
jw35(@mnementh:~\$ telnet mono.org		P	assword:	=
Tryir	ng 166.84.7.123		_	Remember my password	
	ected to mono.org.			. Demonster of bassiliers	
Escap	pe character is '^]'.				
NetBS	SD/i386 (muon.mono.org) (pts/29)			OK Cancel	
logir	1: jw35				
	nt 1989-2005. PINE is a trademar	k of the University of Was	hington.		
HOST: ppsw-	lh.csi.cam.ac.uk USER: jw35 EN		, j		
^G Help					
`C Cancel	Ret Accept				

3	Authentication Required		<u>R</u>	Pidgin 🗙
User Name Passwore	A user name and password are being requested by http://mnementh.csi.cam.ac.uk. The site says: "Login with your Raven userid and password" e:	TY OF IDGE dge > Computing Service > Raven The web resource you re identify yourself [help - wh resource is provided by t wiki.csx.cam.ac.u If you are happy to be ide	Auth	Enter password for jw35@csi.cam.ac.uk/ Work (XMPP) Enter Password: Save password enticate to Kerberos
	Terminal	Nam	ne: jw35	
<u>File</u>			m: UXSUP.CSI	.CAM.AC.UK
	rpius jw35]\$ ssh wensum.csx.cam.a	c.uk A	rd:	
Password:	J	\$-		Connect to mnementh.csi.cam.ac.uk
	Terminal			
jw35@mn@	dit <u>V</u> iew <u>Terminal Tabs H</u> elp ementh:~\$ kinit d for jw35@UXSUP.CSI.CAM.AC.UK:	henticati d only er //rave	we finished ion. Do not disc nterit on web en.cam.ac.u) word by other	The server mnementh.csi.cam.ac.uk at Login with your Raven userid and password requires a username and password.
	Terminal	_ _ ×		Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> e	elp		User name:
Tryi	@mnementh:~\$ telnet mono.org ng 166.84.7.123 ected to mono.org. pe character is '^]'.			Password:
	SD/i386 (muon.mono.org) (pts/29)			🔁 ubuntu
Copyrigh	n: jw35 ht 1989-2005. PINE is a trademar		Washin	
HO <u>ST:</u> ppsw-	-lh.csi.cam.ac.uk USER: jw35 EN			Password
^G Help ^C Cancel	Ret Accept			

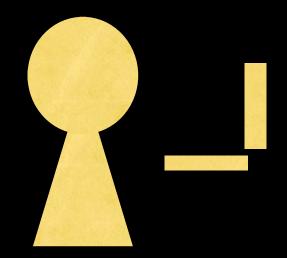
		help
	SITY OF Ra RIDGE	ven Authentication Service
University of Camb	ridge > Computing Service >	Raven
	The web resource you re	Authenticate to Kerberos
RAVEN	identify yourself [help - wh resource is provided by t wiki.csx.cam.ac.u if you are happy to be ide	Please type your Kerberos password
	User-id:	Name: jw35
	Password:	Realm: UXSUP.CSI.CAM.AC.UK
	🗆 override login o	Password:
	Submit	Cancel OK
Terminal	`	
<u>∨</u> iew <u>T</u> erminal Ta <u>b</u> s <u>H</u> elp		n you have finished hentication. Do not disclose
h:∼\$ kinit jw35@UXSUP.CSI.CAM.AC.UK:		▲ d only enter it on web //raven.cam.ac.uk/. ur password by other



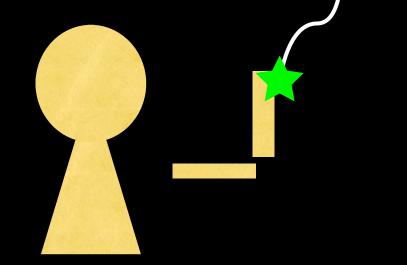












Where do we go from here?