Access Control and Privacy Policies (4)

Email: christian.urban at kcl.ac.uk Office: S1.27 (1st floor Strand Building) Slides: KEATS (also homework is there)

Unix-Style Access Control

- Q: "I am using Windows. Why should I care?" A: In Windows you have similar AC: administrators group (has complete control over the machine) authenticated users server operators power users network configuration operators
- Modern versions of Windows have more fine-grained AC than Unix; they do not have a setuid bit, but have runas (asks for a password).

Unix-Style Access Control

- Q: "I am using Windows. Why should I care?" A: In Windows you have similar AC: administrators group (has complete control over the machine) authenticated users server operators
 - power users network configuration operators
- Modern versions of Windows have more fine-grained AC than Unix; they do not have a setuid bit, but have runas (asks for a password).
- OS-provided access control can add to your security.

Network Applications: Privilege Separation



• the idea is make the attack surface smaller and mitigate the consequences of an attack

Shared Access Control



APP 04, King's College London, 16 October 2012 - p. 4/37

Lessons from Access Control

Not just restricted to Unix:

- if you have too many roles (i.e. too finegrained AC), then hierarchy is too complex you invite situations like...let's be root
- you can still abuse the system...

The idea is to trick a privileged person to do something on your behalf:

ort:

rm /tmp/*/*

The idea is to trick a privileged person to do something on your behalf:

• root: rm /tmp/*/*

> the shell behind the scenes: rm /tmp/dir1/file1 /tmp/dir1/file2 /tmp/dir2/file1 ...

this takes time

APP 04, King's College London, 16 October 2012 - p. 6/37

- 1 attacker (creates a fake passwd file)
 1 mkdir /tmp/a; cat > /tmp/a/passwd
- root (does the daily cleaning)
 rm /tmp/*/*

records that /tmp/a/passwd should be deleted, but does not do it yet

- attacker (meanwhile deletes the fake passwd file, and establishes a link to the real passwd file) rm /tmp/a/passwd; rmdir /tmp/a; ln -s /etc /tmp/a
- root now deletes the real passwd file

- 1 attacker (creates a fake passwd file) mkdir /tmp/a; cat > /tmp/a/passwd
- To prevent this kind of attack, you need additional policies (don't do such operations as root).

should be deleted, but does not do it yet

- attacker (meanwhile deletes the fake passwd file, and establishes a link to the real passwd file) rm /tmp/a/passwd; rmdir /tmp/a; ln -s /etc /tmp/a
- soot now deletes the real passwd file

Schneier Analysis

There is no absolutely secure system and security almost never comes for free.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

You might have the policy of not typing in your credit card online. Worthwhile or not?

You might have the policy of not typing in your credit card online. Worthwhile or not?

 What assets are you trying to protect? your credit card number

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets? With credit cards you loose a fixed amount £50. Amazon £50.

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?

Well, hackers steal credit cards from databases. They usually do not attack you individually.

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

None (?)

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

Internet shopping is convenient and sometimes cheaper.

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?
 Nol



A firewall is a piece of software that controls incoming and outgoing traffic according to some rules.

APP 04, King's College London, 16 October 2012 - p. 10/37

 What assets are you trying to protect? Whatever is behind the firewall (credit cards, passwords, blueprints, ...)

- What assets are you trying to protect?
- What are the risks to these assets? With a small online shop you are already at risk. Pentagon, definitely.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks? Well, at home so not much. Everywhere

else, if properly configurated then it does.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

There might be backdoors or bugs in the firewall, but generally they are secure. You choose to prevent certain traffic.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

Minimal to modest. Firewalls are part of free software. You need a knowledgeable person to set them up.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?
 Yes!

Google uses nowadays two-factor authentication. But it is an old(er) idea. It is used for example in Germany and Netherlands for online transactions.

127067 130002 132234 134544 134644 146040 147054 157704 157704 157704 157705 146041 167355	19155 121409 122594 1525748 1525748 1525748 152529 144006 142529 144007 144497 144497 144497 144497 144497 157146 154133 157583 157583 157583 157584 157584 157584 157584 157584 157584 157584 157584 157584 157584 157584 157588 15758 157588 1	119541 121590 123594 125595 125595 125255 125255 125250 140178 140150 152250 140160 152178 140600 152178 157960 157960	119739 121770 122986 1301224 130234 130234 130234 130234 130234 130231 140251 140251 150240 150240 150240 150240 150240 150240 150240	119914 121956 124179 124554 120554 120554 125586 140525 145923 154800 155800 1578000000000000000000000000000000000000	120000 122130 1202130 120254 1205254 1205264 1205204 120204 140664 140665 150215 150256 1502715 1502715 150256 150256 160256 160256 160256	120290 122217 129521 129523 129529 131199 129529 140502 140500 140502 140500 140500 159530 150430 150430 150430 160007 160007	120472 122482 134778 136645 136645 136645 136645 136615 136817 141134 1420459 147059 150562 150562 150569 160659	120671 122897 124952 127952 125421 125421 121614 1236115 141300 146241 147275 155442 155442 155443 155843 155843 155831	120882 122912 125125 127323 127323 1247323 1247323 1247323 1247323 124425 141645 141645 141645 141645 141645 141645 152619 152046 152646 152646 152646 152646 152646 152646 152646 152646 152646	121066 122066 122066 122066 122064 122064 120642 120654 141000 147018 150455 150750 150750 150750 150750	
Amember of otograp								cit	tibar	h	

I Knob			000 00	VB	I-Nr. C	101	TAN-Block	-Nr.	004
-	to beauten	n Six dava L	im-peakin	et vor dem 2	upit durch (Selfan Girdwe	ugte an siche	rer öbnön a	
		10734-54	#5#755	843566	561720	872954	548458	444778	-
	100000	#384.93	******	122724	899733	427775	658125	584437	A31054
	001100	ATIART	179633	120115	132450	424839	344570	772804	5790%3
10404	10000	Par299	967799	298213	825475	#32545	829985	047584	534888
	and here	#14177	454540	411785	463645	\$34847	184408	341439	442334
	1.11 Barriel	Tanana .	1241.73	******	\$48309	#13325	PADATT	662475	845324
-	1000.04	114040	TTANKS	A75273	642475	879375	106562	274484	854435
	44580.4	154415	15351.0	545673	137458	427245	666367	794223	11.55N
-	158915	110717	5445.79	149943	THREE	474557	ASTATE	823589	23444
	Taxana.	******	141447	140878	1212.01	421112	2188+8	\$75517	04828

Google uses nowadays two-factor authentication. But it is an old(er) idea. It is used for example in Germany and Netherlands for online transactions.

114165 119541 119730 119414 129898 12999 129498 121500 12770 121465 12939 12999 129556 129734 12988 124175 124154 12655 12978 12567 12012 124120 12455 12555 127067 129057 12025 12024 125564 125788 128655 127067 129057 12025 12024 12564 125788 128655	10422 10071 12008 121005 10482 12007 12012 12005 18770 12482 12005 12500 18770 12482 12723 12500 186945 12712 12723 127465 186945 125421 12653 129442 13600 11444 13720 12005	BONTAN PIN TAN PIN TAN PIN TAN PIN TAN PIN TAN PIN TAN Deutscher db OnlineBanking View of TAN Buck Nr. File Schemenser With Buck International Control Object and Control Object Tanking International Control Objec	Bank 2
120304 120309 122790 120977 120154 120294 120494 134564 134627 12020 125450 126869 126296 126299	120/05 120847 13420 134382 136817 138113 135406 138564	TBADAT A17559 287429 838743 845566 441730 572814 548458 4487	A MESAL
129823 140006 140178 540351 540525 140694 140572 142060 142257 142453 542715 542913 143096 143298	141134 141300 141643 141073 143469 143641 143825 144009	ANNEY STATES ANALY STATE 179413 420445 127938 429879 344583 7728	04 \$71045
144043 144487 144689 144683 145137 146475 146787 147084 147989 148190 148833 148889 149685 149586	147079 147273 147446 147618 149767 149939 150246 153455	125484 941908 042749 947799 298313 829479 832945 829482 8495	10 SILANS
150710 151146 152170 152306 152508 150715 152908 150961 154130 154329 154519 154690 154672 155049	150262 150442 153619 153790 155226 155430 155804 156370	0 798351 175845 282866 T28179 685545 468209 813328 945497 4824	/L BALIDA
157382 157583 157540 158343 158842 158214 159430 161386 161943 162134 162480 162728 162958 163298	159640 159840 160045 160462 160609 160901 104237 164575	C. 102746 001020 124400 129400 079275 82444 070276 064547 1942	E3 /15647
164661 165121 165466 165808 166426 166659 166557 167535 167000 150000 168109 168366 168654 168677	167151 167352 169053	Z 380046 259025 298257 548579 149941 T09085 878557 459494 8220	A7 545287
109230 109417 109669 109855 170831 170212 170395	a the sector	Lis schaften underseitig ein Moreneng der McZein coch imm diesen 1426 dische anternetisch einen teisen Feige 1426	duck poperands
Amember of enterpoop	CITIDANK	E PIN TAN PIN TAN PIN TAN PIN TAN PIN TAN PIN TAN	PIN TAN PIN 2

Or nowadays by SMS (restricts the validity of the numbers) or with a secure generator



 What assets are you trying to protect? Your bank account.

- What assets are you trying to protect?
- What are the risks to these assets? Nowadays pretty high risk.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks? It prevents problems when passwords are

stolen. Man-in-the-middle attacks still possible.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

Your mobile phone or credit card/pin might be stolen. SIM card becomes more valuable.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?
 Banks need to establish an infrastructure.
 For you it might be inconvenient.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?
 Yes!

Security Seals

According to Ross Anderson: "... is a tamper-indicating device designed to leave non-erasable, unambiguous evidence of unauthorized entry or tampering."



They also need some quite sophisticated policies (seal regiment).
Security Seals (2)

- at the Argonne National Laboratory they tested 244 different security seals
 - meantime to break the seals for a trained person: 100 s
 - including 19% that were used for safeguard of nuclear material
- Andrew Appel defeated all security seals which were supposed to keep voting machines safe



- The tamper-indicating tape can be lifted using a heat gun.
- The security screw cap can be removed using a screwdriver, then the serial-numbered top can be replaced (undamaged) onto a fresh (unnumbered) base.
- The wire seal can be defeated using a #4 wood screw.
- The plastic strap seal can be picked using a jeweler's screwdriver.

 What assets are you trying to protect? Voting machines, doors.

- What assets are you trying to protect?
- What are the risks to these assets? Casual thieves, insider attacks.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks? Needs a quite complicated security regiment.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

You might not notice tampering.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

The "hardware" is cheap, but indirect costs can be quite high.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?
 No! Though in some areas they work: airports,

swimming pools, ...

You might think it is a good idea to keep a security relevant algorithm or software secret.

 What assets are you trying to protect? Source code, an algorithm and things that depend on it

You might think it is a good idea to keep a security relevant algorithm or software secret.

- What assets are you trying to protect?
- What are the risks to these assets? Can be pretty high (Oystercards).

You might think it is a good idea to keep a security relevant algorithm or software secret.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks? Not really. The source code can be reverse engineered, stolen, coerced ...

You might think it is a good idea to keep a security relevant algorithm or software secret.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

You prevent scrutiny and independent advice. You also more likely than not to get it wrong.

You might think it is a good idea to keep a security relevant algorithm or software secret.

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
 No!

What are the security requirements of a voting system?

Integrity

- The outcome matches with the voters' intend.
- There might be gigantic sums at stake and need to be defended against.

- Integrity
- Ballot Secrecy

- Integrity
- Ballot Secrecy

- Nobody can find out how you voted.
- (Stronger) Even if you try, you cannot prove how you voted.

- Integrity
- Ballot Secrecy
- Voter Authentication
- Only authorised voters can vote up to the permitted number of votes.

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy
- Voter Authentication
- Enfranchisement

 Authorised voters should have the opportunity to vote.

What are the security requirements of a voting system?

- Integrity
- Ballot Secrecy
- Voter Authentication
- Enfranchisement
- Availability

 The voting system should accept all authorised votes and produce results in a timely manner.

Ballot Boxes



Problems with Voting

Integrity vs. Ballot Secrecy

Authentication vs. Enfranchisement

Problems with Voting

Integrity vs. Ballot Secrecy Authentication vs. Enfranchisement

Further constraints:

- costs
- accessibility
- convenience
- intelligibility

E-Voting

 The Netherlands between 1997 - 2006 had electronic voting machines (hacktivists had found: they can be hacked and also emitted radio signals revealing how you voted)

- Germany had used them in pilot studies

 (in 2007 a law suit has reached the highest court
 and it rejected electronic voting on the grounds
 of not being understandable by the general
 public)
- UK used optical scan voting systems in a few polls



- US used mechanical machines since the 30s, later punch cards, now DREs and optical scan voting machines (fantastic "ecosystem" for study)
- Estonia used in 2007 the Internet for national elections (there were earlier pilot studies in other countries)
- India uses e-voting devices since at least 2003 ("keep-it-simple" machines produced by a government owned company)
- South Africa used software for its tallying in the 1993 elections (when Nelson Mandela was elected) (they found the tallying software was rigged, but they were able to tally manually)

A Brief History of Voting

Athenians

- show of hands
- ballots on pieces of pottery
- different colours of stones
- "facebook"-like authorisation

problems with vote buying / no ballot privacy

 French Revolution and the US Constitution got things "started" with paper ballots (you first had to bring your own; later they were pre-printed by parties)

Ballot Boxes

Security policies involved with paper ballots:

- you need to check that the ballot box is empty at the start of the poll / no false bottom (to prevent ballot stuffing)
- you need to guard the ballot box during the poll until counting
- tallied by a team at the end of the poll (independent observers)





What can go wrong with paper ballots?

Paper Ballots

What can go wrong with paper ballots?



William M. Tweed, US Politician in 1860's "As long as I count the votes, what are you going to do about it?"

APP 04, King's College London, 16 October 2012 - p. 25/37

Paper Ballots

What can go wrong with paper ballots?

Chain Voting Attack

- you obtain a blank ballot and fill it out as you want
- you give it to a voter outside the polling station
- voter receives a new blank ballot
- voter submits prefilled ballot
- voter gives blank ballot to you, you give money
- 🧿 goto 1

Mechanical Voting Machines

• Lever Voting Machines (ca. 1930 - 1990)



Mechanical Voting Machines

- Lever Voting Machines (ca. 1930 1990)
- Punch Cards (ca. 1950 2000)





Electronic Voting Machines

DRES



Optical Scan



APP 04, King's College London, 16 October 2012 - p. 27/37

Electronic Voting Machines

DRES



Optical Scan

all are computers



APP 04, King's College London, 16 October 2012 - p. 27/37



Direct-recording electronic voting machines (votes are recorded for example memory cards) typically touchscreen machines usually no papertrail (hard to add: ballot secrecy)


The work by J. Alex Halderman:

- acquired a machine from an anonymous source
- the source code running the machine was tried to keep secret

The work by J. Alex Halderman:

- acquired a machine from an anonymous source
- the source code running the machine was tried to keep secret
- first reversed-engineered the machine (extremely tedious)
- could completely reboot the machine and even install a virus that infects other Diebold machines
- obtained also the source code for other machines

What could go wrong?

What could go wrong? Failure-in-depth.

What could go wrong? Failure-in-depth.

A non-obvious problem:

- you can nowadays get old machines, which still store old polls
- the paper ballot box needed to be secured during the voting until counting; e-voting machines need to be secured during the entire life-time

Paper Trail

Conclusion: Any electronic solution should have a paper trail.



Paper Trail

Conclusion: Any electronic solution should have a paper trail.



You still have to solve problems about Voter registration, voter authentification, guarding against tampering

E-Voting in India

Their underlying engineering principle is "keep-it-simple":



E-Voting in India

Their underlying engineering principle is "keep-it-simple":



Official claims: "perfect", "tamperproof", "no need for technical improvements", "infallible"

Lessons to be Learned

- keep a paper trail and design your system to keep this secure
- make the software open source (avoid security-by-obscurity))
- have a simple design in order to minimise the attack surface

The adventures of citizen Michael C. Robertson



APP 04, King's College London, 16 October 2012 - p. 34/37













Drawings: Koen Hottentot — Story: Rop Gonggrijp / Barry Wels — Color: Adam Swiecky — Translation: Jaap Weel