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)

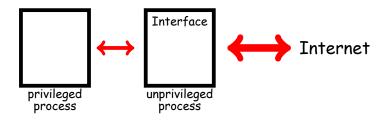
Unix-Style Access Control

- Q: "I am using Windows. Why should I care?" A: In Windows you have: 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; they do not have a setuid bit, but have runas (asks for a password).

Unix-Style Access Control

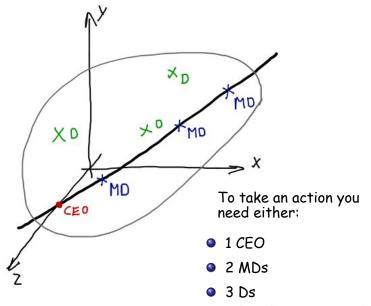
- Q: "I am using Windows. Why should I care?" A: In Windows you have: administrators group
 - (has complete control over the machine) authenticated users server operators power users
 - network configuration operators
- Modern versions of Windows have more fine-grained AC; they do not have a setuid bit, 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. 4/30

Lessons from Access Control

- 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

- 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

- Introduction of the passwork of the passwor
- To prevent this kind of attack, you need ri additional policies.

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
- soot now deletes the real passwd file

Schneier Analysis

- 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?

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

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 (?)

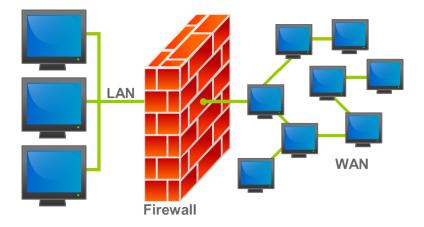
You might have the policy of not typing in your credit card online. Worthwhile or not?

- 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. 10/30

 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.

Arnomi	per of only	nat a							cit	libar	ık
164661 167535 189230	165121 167000	105400	105808	166426 168366 170021	168609	166557 168677 1777165	167151 169053	157352			
15/261 157282 161285	154133	1543254 157540 1572134	150343	154600 158042	1548/2 158214 167958	1500430	150640	155430 155843 157931	1000045 950245	1083402	
147884 150790 150564	147989 151145 154133	140160 152170 154120	5488233 1522306 1544540	548809 552528 152528	149085 152715 154872	149586 152508 155083	149787 150262 155295	140920 155442 155430	150246 153619 155814	153455 153793	
	144497	144689	144822	545527	146475	146787	147079	147272	547446	147613	
129023	140006	140170	540051	546625	140654	140072	141134	141300	141143	141073	
132224 134564	132529	135230	125450	105899	153324	136509	130725 136817	139112	135405	129554	
	150216	130438	130694	\$30,789	139307	131199	131580	131614	121793	102025	
127067	125768	125947	1201122	126306	126535	126723	120545	127153	127323	127495	
	121409	121590	121770	\$21956 \$24179	122139	122317	122482	122897	122912	123096	
	112105	110521	110730	110014	100000	100000	110472	120671	120802	121065	

004						00.000			
	we Shalls au	opte an siche	Inter Citaberte	witt such (Terr dam 2	its peaking	Lie dere D	the begaden	LASSE
	444778	548458	872954	961720	******	******	267529	#17569	195247
A31054	584437						438443	616205	195217
5770%3	772804							661268	AL7872
STAR	047584	829985						847706	125454
									MATLIN.
845324						1261/2	262994	LTING	******
854435							134669	201624	MODEL
1155N	794223							441100	
254842									
04828			e243.92 or Norteamp I						

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.

1642 1642 1542 1542 1542 1542 1542 1544 1542 1544 1542 1544 1545 1545 1	Deutsche Bank D Neut seid Contationnichtig TAN-Glock NV. 004	VS-Nr. 001 TAM	anking	nlineBan	db O	120882 121066 122912 122096 125125 125000 127323 127465 129653 129642 131790 132025	124953 127153 129421 131614	120472 122482 134778 136645 129226 131380	134531 136723 129569 131199	128535 128766 131907	1211856 1214179 1210306 1210504 1200709	119739 121770 123986 120132 120294 130594	121590 123794 125947 129225 120225	119105 121409 122594 122594 125768 129051 129051	127067
	PII 6449105 Balability 635050 900 164585 772886 579805 728 901 164587 972886 514886 728 901 164587 946876 514886 728 901 164507 946876 951488 728 901 164507 946876 951286 728 905 646647 778428 758970 728 728987 728 957 646467 928897 728 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 728847 7288477 7288477 7288477 728477 <td>122224 099723 679793 0 420464 121758 428999 5 421516 129758 428999 5 412159 65997 842945 8 412159 65969 41215 1 65566 648099 81215 1 56667 12568 42985 1 16982 72568 42985 1 16982 72568 42985 2</td> <td>438443 092594 433482 179433 04299 947799 556373 456945 282066 728795 134680 728945 134680 728945 134653 959456 294577 546579</td> <td>416205 423 661266 423 641705 PM 864751 57 137865 26 294624 23 609020 23 259425 24</td> <td>858279 44/472 325484 3855279 798338 385643 3252798 386643</td> <th>941643 141073 143825 144003 147466 147613 147466 160455 153619 153793 155804 156773 155804 156773 155804 156453</th> <td>1361151 141300 143641 1472751 140929 155442 155430 1558451 1558451</td> <td>141114 140489 147079 140787 15082 15028 150640 160699 167151</td> <td>1405/2 1432/88 146787 146686 152508 155049 15505000000000000000000000000000000000</td> <td>140604 143066 146475 149065 157715 154872 158214 168258 168099 168056</td> <td>140525 142913 145127 148809 152538 15268 15268 15268 15268 152625 16265 16265</td> <td>140351 142715 144823 148823 152366 154519 158343 162400 165808 169109</td> <td>140178 142453 144689 148180 152178 154329 157540 152134 165466 158003 199689</td> <td>142257 144497 147909 151146 154130 157580 167040 165121 167000 105417</td> <td>1298021 142060 144243 147054 150710 152564 157382 164864 167535 166854 167535</td>	122224 099723 679793 0 420464 121758 428999 5 421516 129758 428999 5 412159 65997 842945 8 412159 65969 41215 1 65566 648099 81215 1 56667 12568 42985 1 16982 72568 42985 1 16982 72568 42985 2	438443 092594 433482 179433 04299 947799 556373 456945 282066 728795 134680 728945 134680 728945 134653 959456 294577 546579	416205 423 661266 423 641705 PM 864751 57 137865 26 294624 23 609020 23 259425 24	858279 44/472 325484 3855279 798338 385643 3252798 386643	941643 141073 143825 144003 147466 147613 147466 160455 153619 153793 155804 156773 155804 156773 155804 156453	1361151 141300 143641 1472751 140929 155442 155430 1558451 1558451	141114 140489 147079 140787 15082 15028 150640 160699 167151	1405/2 1432/88 146787 146686 152508 155049 15505000000000000000000000000000000000	140604 143066 146475 149065 157715 154872 158214 168258 168099 168056	140525 142913 145127 148809 152538 15268 15268 15268 15268 152625 16265 16265	140351 142715 144823 148823 152366 154519 158343 162400 165808 169109	140178 142453 144689 148180 152178 154329 157540 152134 165466 158003 199689	142257 144497 147909 151146 154130 157580 167040 165121 167000 105417	1298021 142060 144243 147054 150710 152564 157382 164864 167535 166854 167535

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 become 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).

APP 04, King's College London, 16 October 2012 - p. 14/30

Security Seals (2)

- at the Argonne National Laboratory they tested 244 different security seals (including 19% that were used for safeguard of nuclear material)
 mean time to break the seals for a trained person: 100 s
- 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: airport,

swimming pool

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

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...

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, 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 voter intend.
- There might be gigantic sums at stake.

- 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

 Only authorised voters should be able to vote up to the permitted number of votes.

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 (it has been found that they could be hacked and emitted radio signals)
- Germany, had been used 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 50s, later punch cards, DREs and optical scan voting machines (fantastic "ecosystem" for research)
- Estonia used in 2007 the world's first Internet vote in national elections (there are earlier pilot studies)
- India, the biggest democracy 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 (Nelson Mandela) (they found the software was rigged, but they were able to manually tally)

A Brief History of Voting

Athenians

- show of hands
- ballots on pieces of pottery
- different colours of stones
- "facebook"-like autorisation
- French Revolution and the US Constitution got things "started" with paper ballots (you first had to bring your own, or later were pre-printed by the parties)



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. 24/30

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





APP 04, King's College London, 16 October 2012 - p. 26/30

The adventures of citizen Michael C. Robertson



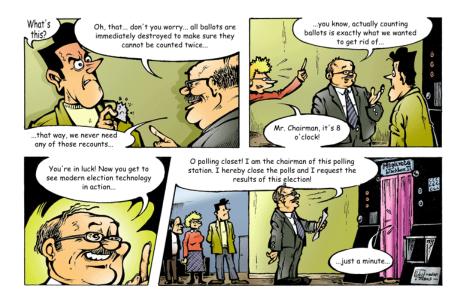
APP 04, King's College London, 16 October 2012 - p. 27/30













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