how to attack a system

Daniel Jackson & Arvind Satyanaryan
what this nugget’s about

how to attack a system
strategies, from easiest to hardest

in practice
for typical system, any one of these may be enough
for a very secure system, may need several

why does this matter?
you can’t defend unless you know how to attack
#1 bribe insiders
how the strategy works

- find insider with privileges
- offer cash or blackmail asking to...
- plugin device grant access install malware
- you both get killed or jailed

45% of attacks are from insiders
$80 to bribe a cleaner to insert a USB key
blackmailing bank employees

Punjab National Bank insider and India CBI official (2018) blackmailed to run $1.8B SWIFT transactions
Edward Snowden

In 2013, released details of NSA programs still in undisclosed location in Moscow
sample defenses

principle of least privilege
don’t give people access they don’t need

happy organization
avoid angry employees

audit every operation
require login, with no account sharing

require dual approval
for critical actions
#2

social engineering
how the strategy works

collect info about insider

trick insider to...

run your code install malware
pretexting: the core of social engineering

from Catch Me If You Can (2002)
Frank Abagnale could write a check on toilet paper, drawn on the Confederate States Treasury, sign it “U.R. Hooked” and cash it at any bank in town, using a Hong Kong driver’s license for identification.

exploiting a major event

fake World Cup page
installed Chrome extension that recruits machine to bonnet
steals data, sends emails, mounts DOS attacks
infiltrating an army

Hamas attack on Israeli Army (2017)
World Cup app for Android
access to location, files, contacts, camera

https://www.independent.co.uk/news/world/middle-east/israel-world-cup-app-hamas-hack-
breaking into a security supplier

RSA SecurID two factor authentication generates keys at 60s intervals

phishing attack (2011) took over RSA machines obtained secret keys then attacked Lockheed Martin
breaking into a security supplier

payload
Flash object in Excel file, exploited zero-day vulnerability
installed code to administer RSA machines remotely
sample defenses

managed platforms
don’t let employees install code

train employees
to recognize phishing (not very successful)
to follow protocols (more successful)
#3 exploit policy holes
how the strategy works

- find a flaw in the system spec or policy
- devise a scenario to exploit it
- execute the scenario
an ingenious deposit fraud

bank protocol
many customers left account number blank
bank employee looked up number for them

what Abagnale did
took a slip and entered his account number
returned copies to pile

see: Frank Abagnale, *Catch Me If You Can*
Security Questions.
Select three security questions below. These questions will help us verify your identity should you forget your password.

Security Question: What was the name of your first pet?
Answer:

Security Question: What is your dream job?
Answer:

Security Question: In what city did your parents meet?
Answer:
and/or?

Sarah Palin  
2008 Vice Presidential Candidate

David Kernell

Yahoo policy
if forget password, can answer security questions instead!

what Kernell did
found Palin’s high school and birthdate on Wikipedia, then...

a subtle policy flaw

Boy, 9, accused of hacking into Fairfax schools' computer system

By Tom Jackman
Washington Post Staff Writer
Thursday, April 15, 2010

Are you smarter than a third-grader? Because the online education system used by the Fairfax County public schools apparently is not.

Police say a 9-year-old McLean boy hacked into the Blackboard Learning System used by the county school system to change teachers' and staff members' passwords, change or delete course content, and change course enrollment. One of the victims was Fairfax Superintendent Jack D. Dale, according to an affidavit filed by a Fairfax detective in Fairfax Circuit Court this week.

---

policy

student can access own files
teacher can add class members & change their passwords
superintendent can do anything

what if student gets teacher password?
add superintendent to class
change superintendent password
wreak havoc...

http://www.washingtonpost.com/wp-dyn/content/article/2010/04/14/AR2010041404159.html
interacting policies

hacker's strategy:

- call Amazon
  - ask to add credit card to account
  - provide name, address, email
- call Amazon
  - ask to add email address
  - provide name, address, a credit card
- login to Amazon
  - access list of credit cards
  - see last four digits of each
- call Apple
  - can't answer security question
  - they take address + last four digits of credit card

outcome

hacker deleted all his data, including photos of 1 year old
tweeted racist & homophobic remarks

Matt Honan
Writer, Wired Magazine

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
sample defenses

careful policy design
make goals, threats, policies explicit & review

be conservative
short expirations for tokens
multi-stage login for critical actions

defense in depth
assume your defenses will fail
#4 exploit bugs in code
how the strategy works

1. find a bug by fuzzing or code review
2. devise a scenario to exploit it
3. execute the scenario
tough times for Facebook

Facebook Security Breach Exposes Accounts of 50 Million Users

New York Times, Sept 28, 2018

How can I see what my profile looks like to other people?

This feature is currently disabled.

You can see what your profile looks like to other people by using the **View As** tool.

To use **View As**:

1. Go to your profile and click ⋮ to the bottom right corner of your cover photo.
2. Click **View As...** in the dropdown menu.
3. You’ll see what your profile looks to the public. To see how your profile appears to a specific person, like a friend or coworker, click **View as Specific Person**, type their name and press enter.
what went wrong

three nasty bugs
(1) when running “view as”, video uploader appears (should not)
(2) when activated, uploader generates sign-on token (should not)
(3) token generated was for user being simulated, not this user (ouch!)

markets for vulnerabilities

ZERODIUM Payout Ranges*

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape

*All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

https://www.zerodium.com/program.html
asymmetrical warfare

codebase with 1m bugs

attacker finds 1 bug in 1k hours

developer spend 10m hours finds & fixes 10k bugs

did it escape?
probability that attacker’s bug was fixed = 1%

from Ross Anderson, Security Engineering
sample defenses

architectural design
small trusted base: limit scope of compromise

best technology practices
TLS for connections, salted passwords, etc

use platform features
template escaping for XSS, form tokens for CSRF, etc

code quality
coding standards, review & test

apply patches
for platform vulnerabilities
#5 corrupt the pipeline
how the strategy works

1. find a hole in development pipeline
2. insert a tool that creates a backdoor, e.g.
3. exploit backdoor
Reflections on Trusting Trust (1984)
Ken Thompson Turing Award talk

XcodeGhost (2015)
slow networks in China: local copies popular
4,000 infected apps, including WeChat (FireEye)
inserted backdoor and disabled
Snowden leaked Sandia/CIA Xcode notes

for Thompson talk, see: https://dl.acm.org/citation.cfm?id=358210
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America’s technology supply chain, according to extensive interviews with government and corporate sources.
sample defenses

safe sources
know where your compiler came from

minimize dependences
don’t use that cool library

hope for the best
and pray...