SAMUEL KEELEY / 2017-10-05 / MACSYSADMIN 2017

Securing the Sysadmin

SAMUEL KEELEY / 2017-10-05 / MACSYSADMIN 2017

Securing the MacSysAdmin

SAMUEL KEELEY / 2017-10-05 / MACSYSADMIN 2017

Security for the Mac Admin #1

SAMUEL KEELEY / 2017-10-05 / MACSYSADMIN 2017

Practical Security for the Mac Admin #1

WHAT AM I REALLY TALKING ABOUT?

THINGS I WISH SOMEONE HAD MADE ME THINK ABOUT LONG AGO

MAY BE A TALE OF BEST PRACTICES, BUT FOR THIS SPECIAL AUDIENCE

YOU!

Ponder this!

- What access does a "standard user" have in your organization?

- What access do *you* have as a sysadmin?

You are the target.
Defend yourself.

FROM MICHAEL MANN DIRECTOR OF HEAT, COLLATERAL AND THE INSIDER

CHRIS HEMSWORTH

blackhat

YOU ARE NO LONGER IN CONTROL

LEGENDARY PICTURES AND UNIVERSAL PICTURES PRESENT A LEGENDARY PICTURES/FORWARD PASS PRODUCTION A MICHAEL MANN FILM CHRIS HEMSWORTH "BLACKHAT" TANG WEI VIOLA DAVIS RITCHIE COSTER HOLT McCALLANY YORICK VAN WAGENINGEN AND WANG LEEHOM MUSIC BY HARRY GREGSON-WILLIAMS ATTICUS ROSS COSTUME DESIGNER COLLEEN ATWOOD VISUAL EFFECTS SUPERVISORS JOHN NELSON PHILIP BRENNAN FILM EDITORS JOE WALKER ACE STEPHEN RIVKIN ACE JEREMIAH O'DRISCOLL MAKO KAMITSUNA PRODUCTION DESIGNER GUY HENDRIX DYAS DIRECTOR OF PHOTOGRAPHY STUART DRYBURGH ASC EXECUTIVE PRODUCERS ERIC McLEOD ALEX GARCIA PRODUCED BY THOMAS TULL p.g.a. MICHAEL MANN p.g.a. JON JASHNI p.g.a. STORY BY MICHAEL MANN AND MORGAN DAVIS FOEHL

LEGENDARY

MOTION PICTURE RATED R VIOLENCE AND BRIEF LANGUAGE

SCREENPLAY BY MORGAN DAVIS FOEHL AND MICHAEL MANN DIRECTED BY MICHAEL MANN

A UNIVERSAL RELEASE UNIVERSAL

JANUARY 16

Ponder this!

- What access does a "standard user" have in your organization?

- What access do *you* have as a sysadmin?

Access is key

- How could an attacker use the access of a Mac sysadmin to achieve success?
- Attackers target those with privileged access - that's you!

Access is key

- Sysadmins have especially useful access, useful to amplify or zone in attacks.
- Nobody is going to be perfectly safe, but thinking security for the long term is key.

Access is key

- An attacker with unlimited resources can certainly achieve goals, but reality imposes limits.
- Make it so expensive in time or effort that attackers don’t win.

A LITTLE GAME

Never have I ever...

Connected to an RDP/VNC session from another user's computer.

Never have I ever...

Connected to an RDP/VNC session from another user's computer... and left the credentials saved.

Never have I ever...

Used my own credentials for an application such as a JSS or printer's LDAP lookups.

Never have I ever...

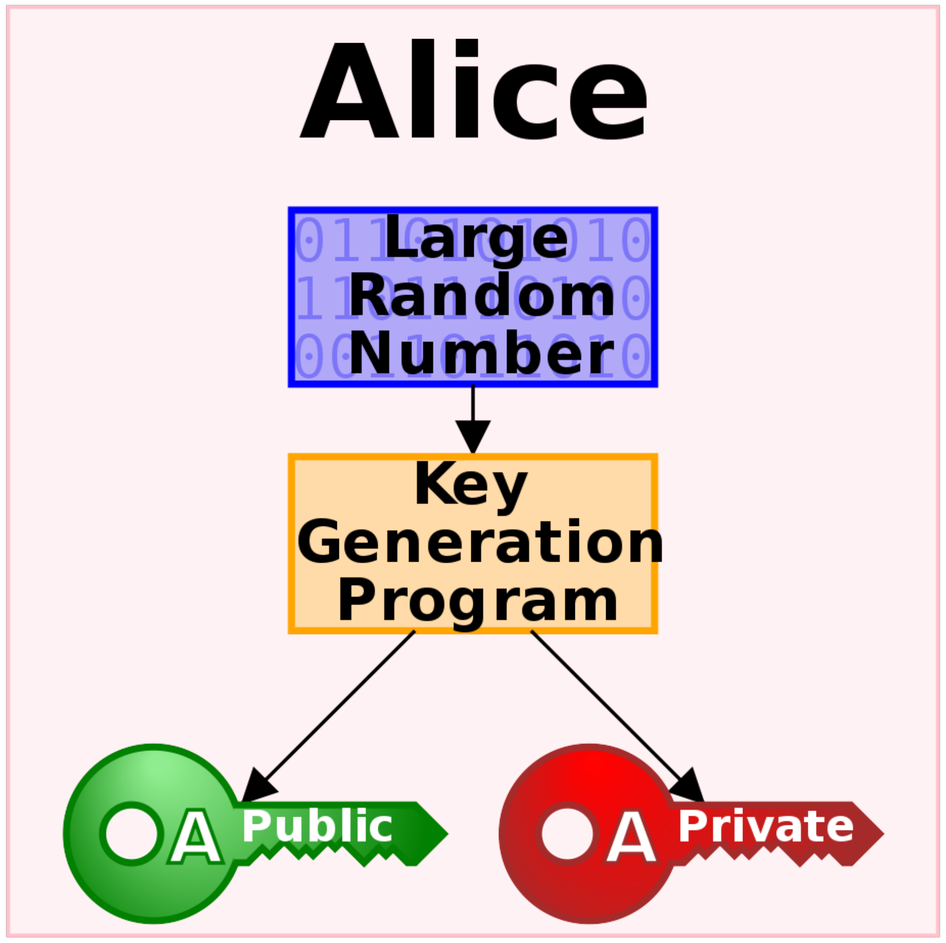
Used the same password for multiple applications.

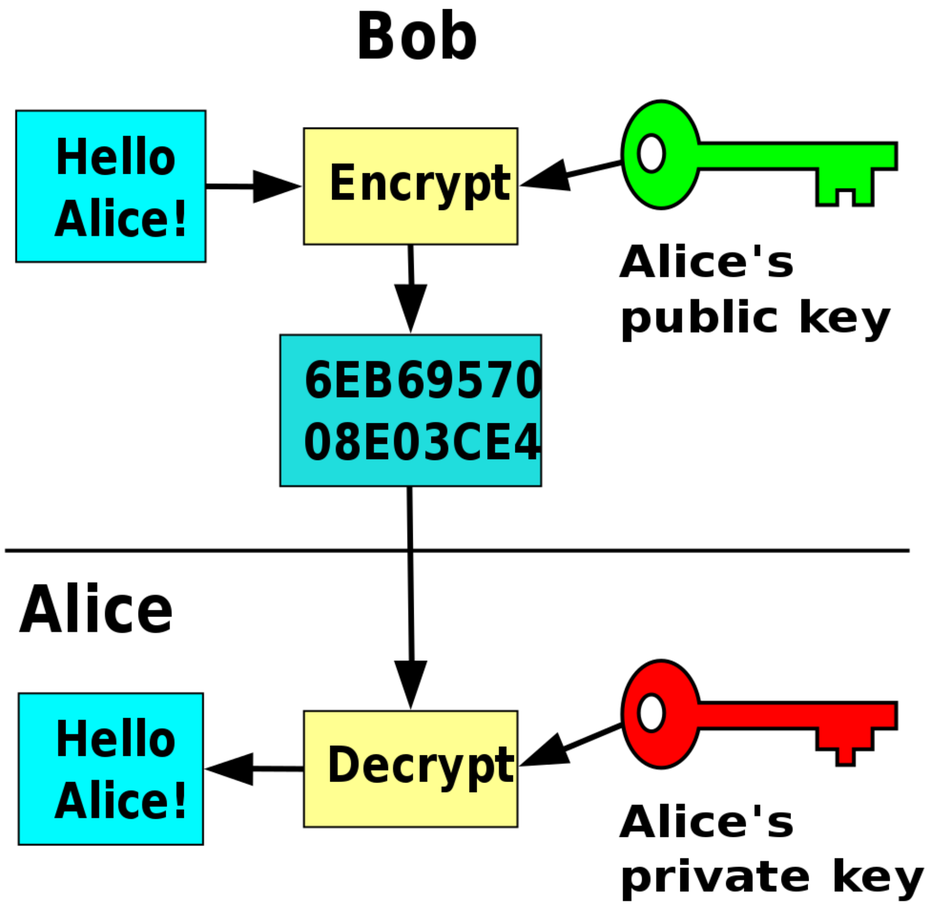
Never have I ever...

Submitted my password directly to an application.

All of these actions lead to the loss of control of one's credentials.

PASSWORDS VS. KEYS


Alice
Large Random Number
Key Generation Program
A
Public
A
Private


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Passwords

- Usually memorable
- Commonly short (64-128 bits)
- Password itself is the secret
- Submit the secret to the requestor
- Easily phishable
- Crackable
- No ability to verify single possession
- Can be intercepted by services

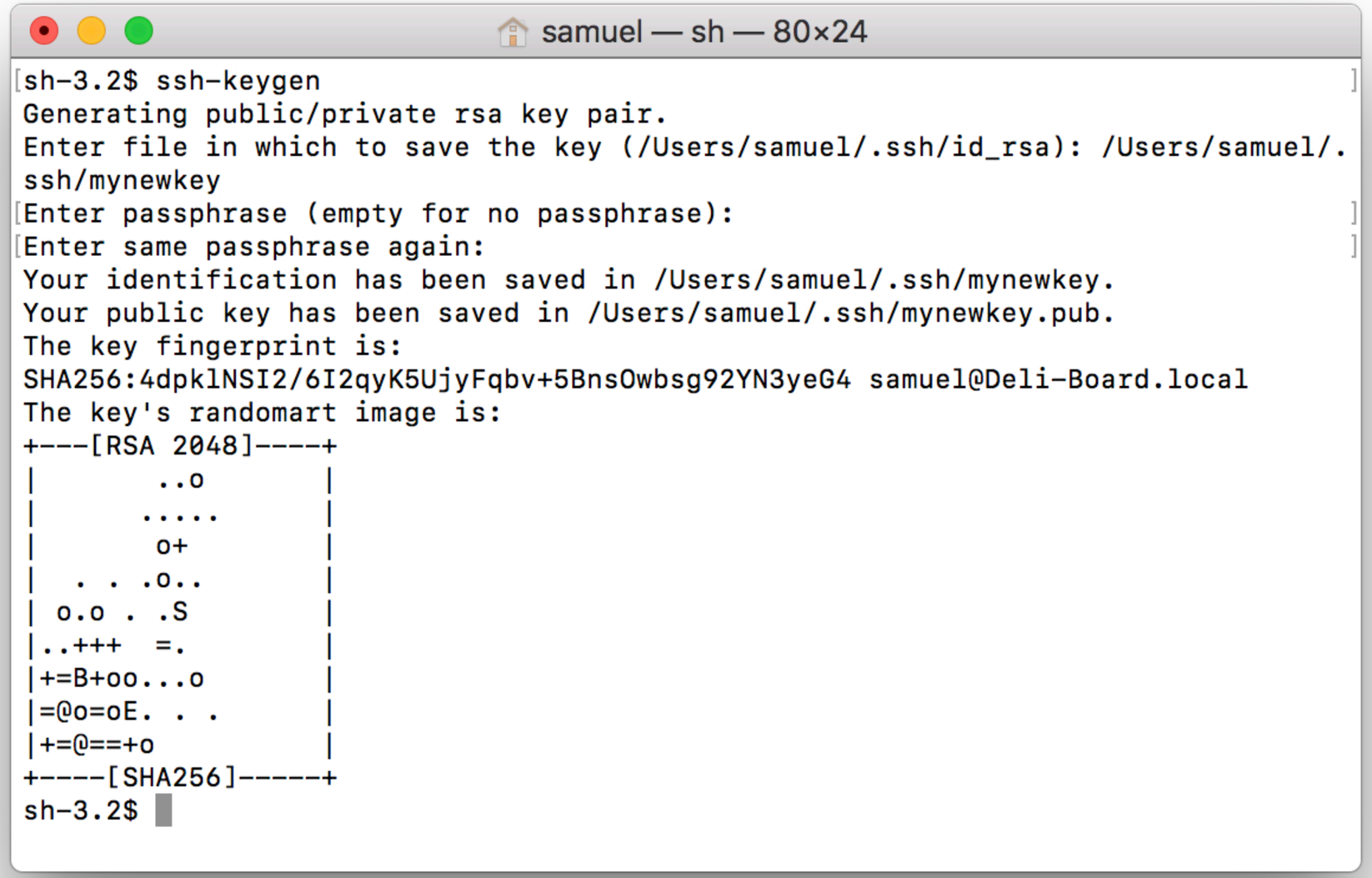
Keys

- Not memorable
- Long (at least 1024 bits)
- Private key is the secret
- Submit proof of private key control to requestor
- Hard or impossible to phish
- Effectively not crackable if strong (2048 bit+)
- Can be secured easily to keep non-stealable
- Can’t be intercepted by services*

** avoid SSH agent forwarding*

👎 PASSWORDS 👎

KEYS


samuel — sh — 80×24
sh-3.2$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/samuel/.ssh/id_rsa): /Users/samuel/.ssh/mynewkey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/samuel/.ssh/mynewkey.
Your public key has been saved in /Users/samuel/.ssh/mynewkey.pub.
The key fingerprint is:
SHA256:4dpklNSI2/6I2qyK5UjyFqbv+5BnsOwbsg92YN3yeG4 samuel@Deli-Board.local
The key's randomart image is:
+---[RSA 2048]----+
| ..o |
| ..... |
| o+ |
| . . .o.. |
| o.o . .S |
|..+++ =. |
|+=B+oo...o |
|=@o=oE. . . |
|+=@==+o |
+----[SHA256]-----+
sh-3.2$


samuel — sh — 80×24
sh-3.2$ cat /Users/samuel/.ssh/mynewkey.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8OU8mkPYC5nC+Qy33BOmc2JghdpdeiPxd7Fvu2vRS
cfqy9D4RJUlvMDHARVNZGXAN4NEJtBAsnZCJhSddGL1ybXv7SkXTS4Z5ERXGk8MKwxgyBnPMHBeg+CBY
u2U5IcrSsGjeT6jRkN5Fml2kcucyYKs4jKg2f1MuWOHxzPJQhPcFJ659JFXY4gXW3jfPme/4qyejxIlY
uoW0SB+byKNemmDJzUPr+tnRntt0a1m0iY/DmS/1gFToJ9G5/TWZFIUO4ei1/8Aqbmd7MsdzU4/qZBmK
B+O7wbsaNv/zakPvQzNy1cPv9K7PHoMyzhSeABjm6FMddJZNs+YdTYtWiNEJ samuel@Deli-Board.l
ocal
sh-3.2$

KEY SECURITY

Security Keys

(SMARTCARDS/PKCS#11 PROVIDERS/SMART TOKENS)

NO MO’ YOLO

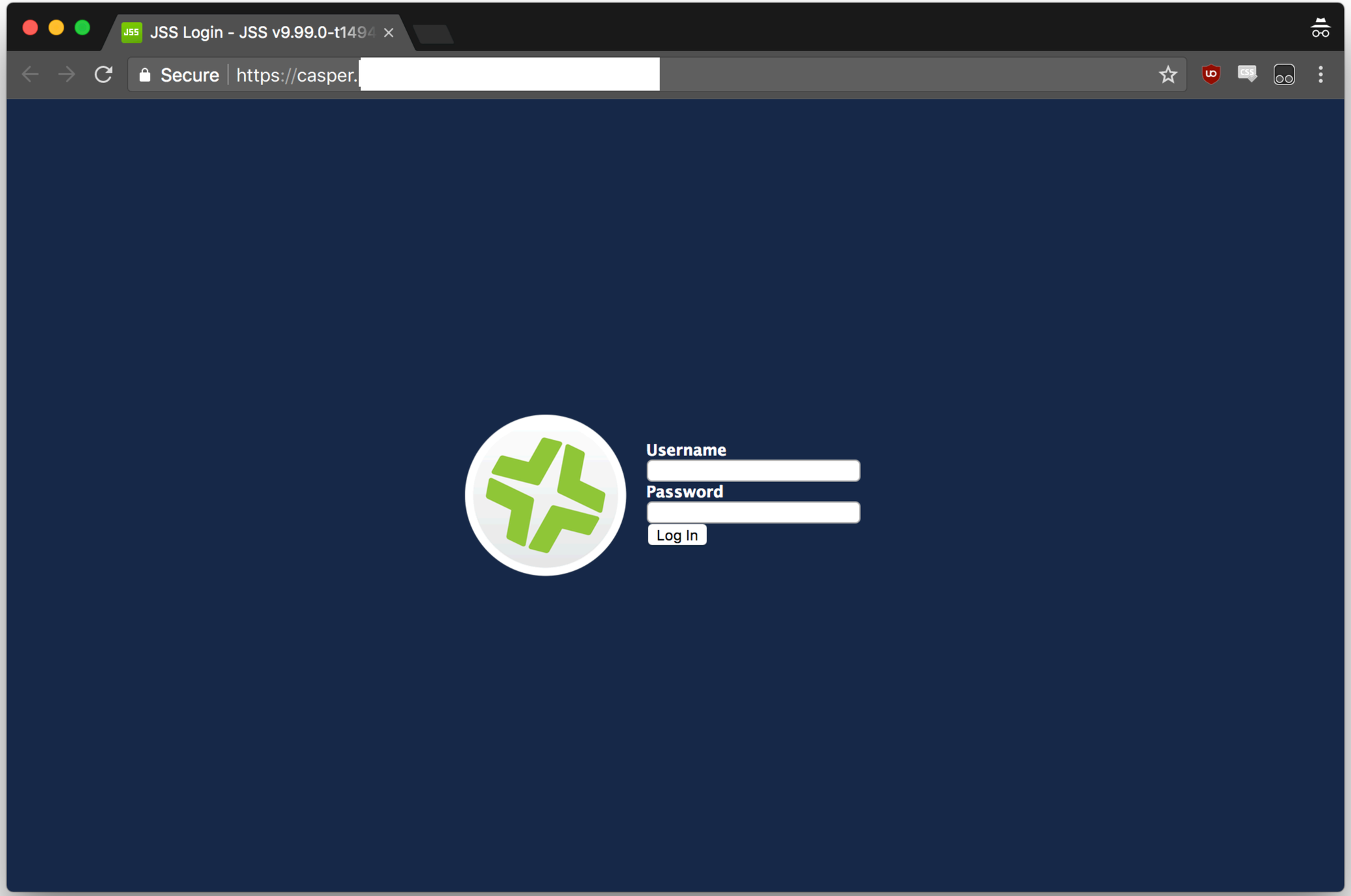
How many types actions can you take alone, without review or checks?

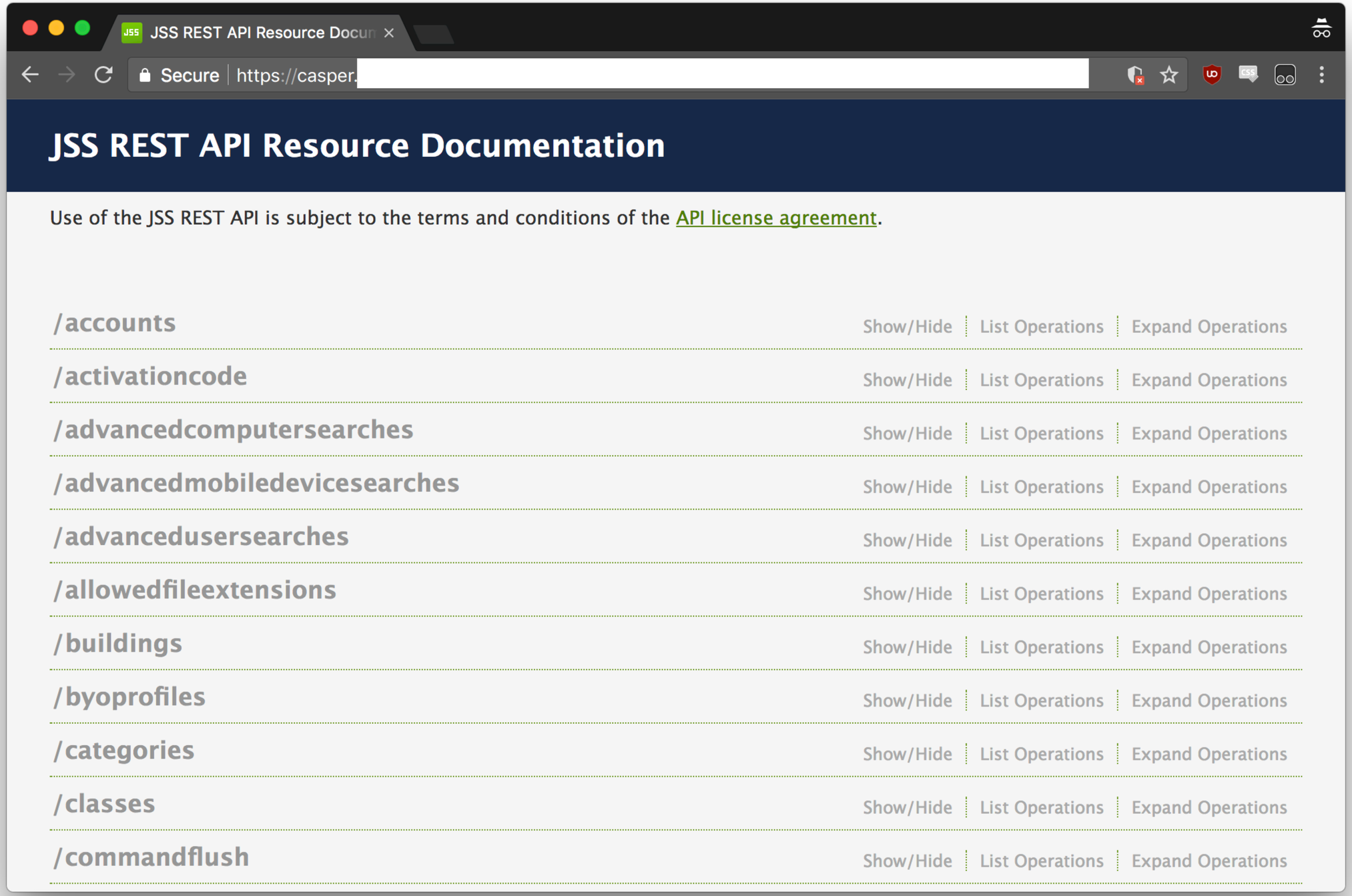
It takes two keys to launch a missile.

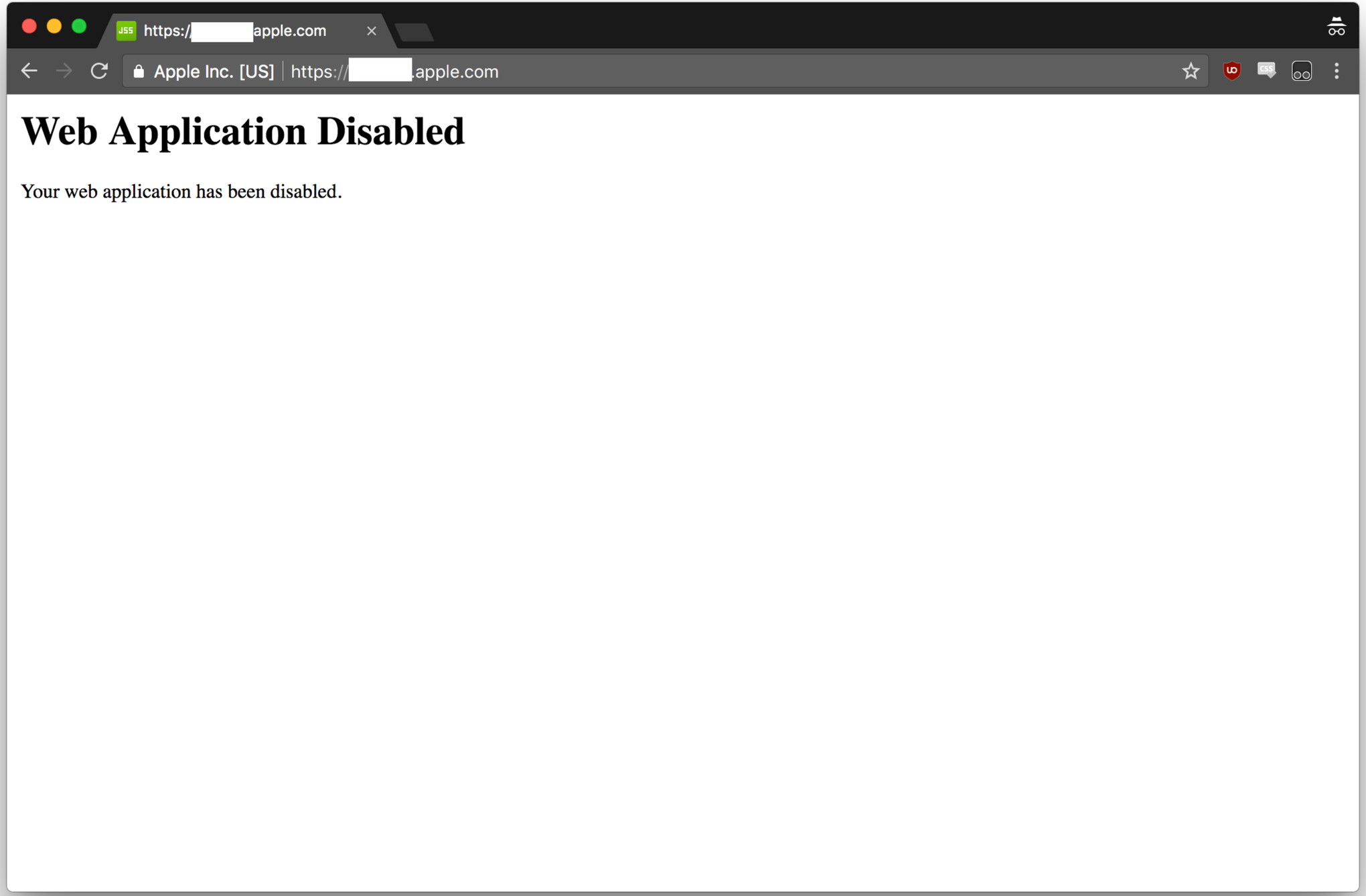
What would a missile look like to your organization?

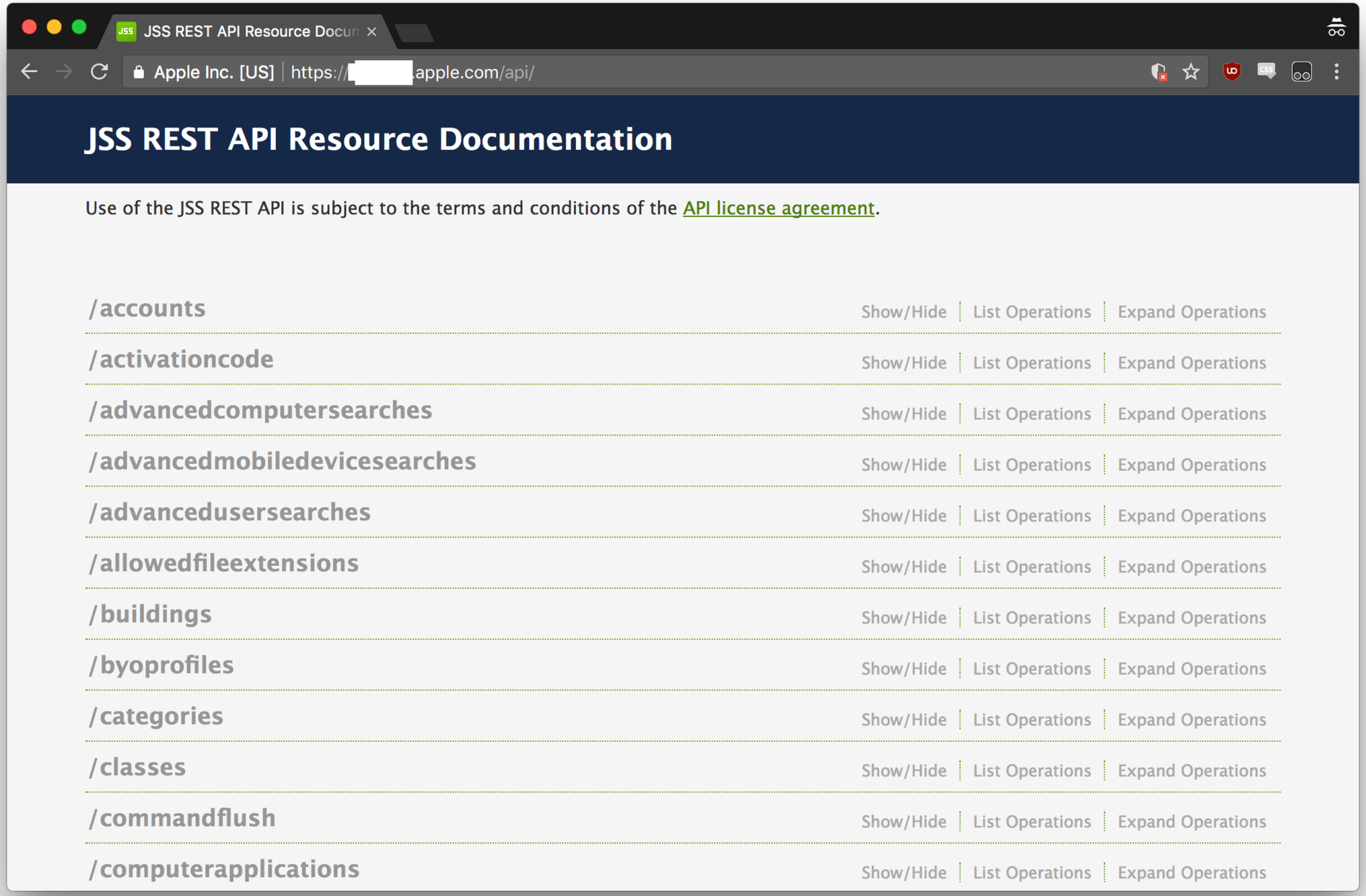
TO ØL S

JAMF


JSS Login - JSS v9.99.0-t1494
Secure
https://casper.
Username
Password
Log In


JSS REST API Resource Documentation
Use of the JSS REST API is subject to the terms and conditions of the API license agreement.
/accounts Show/Hide List Operations Expand Operations
/activationcode Show/Hide List Operations Expand Operations
/advancedcomputersearches Show/Hide List Operations Expand Operations
/advancedmobiledevicesearches Show/Hide List Operations Expand Operations
/advancedusersearches Show/Hide List Operations Expand Operations
/allowedfileextensions Show/Hide List Operations Expand Operations
/buildings Show/Hide List Operations Expand Operations
/byoprofiles Show/Hide List Operations Expand Operations
/categories Show/Hide List Operations Expand Operations
/classes Show/Hide List Operations Expand Operations
/commandflush Show/Hide List Operations Expand Operations


https:// apple.com
Apple Inc. [US] | https:// .apple.com
Web Application Disabled
Your web application has been disabled.


JSS REST API Resource Docun
Apple Inc. [US] | https://[redacted]apple.com/api/
JSS REST API Resource Documentation
Use of the JSS REST API is subject to the terms and conditions of the API license agreement.
/accounts Show/Hide | List Operations | Expand Operations
/activationcode Show/Hide | List Operations | Expand Operations
/advancedcomputersearches Show/Hide | List Operations | Expand Operations
/advancedmobiledevicesearches Show/Hide | List Operations | Expand Operations
/advancedusersearches Show/Hide | List Operations | Expand Operations
/allowedfileextensions Show/Hide | List Operations | Expand Operations
/buildings Show/Hide | List Operations | Expand Operations
/byoprofiles Show/Hide | List Operations | Expand Operations
/categories Show/Hide | List Operations | Expand Operations
/classes Show/Hide | List Operations | Expand Operations
/commandflush Show/Hide | List Operations | Expand Operations
/computerapplications Show/Hide | List Operations | Expand Operations

Jamf Pro

- Restrict web-facing API - you've probably opened it up for iOS MDM.
- Configure SAML based SSO using a secure provider with MFA.
  - OneLogin
  - Duo
  - Okta
  - Google Cloud Identity
- Consider programmatically making changes over API instead of GUI, based on code level changes and a testing server, while having no direct changes on the real JSS.

MUNKI/PUPPET/IMAGR/ DEPLOYSTUDIO/CHEF/ ANSIBLE/SALTSTACK/ AUTOPKG/ETC

Munki & Friends

MUNKI/PUPPET/IMAGR/
DEPLOYSTUDIO/CHEF/ANSIBLE/
SALTSTACK/AUTOPKG/ETC

- These tools can be controlled solely through text files, making version control through git easy.
- This allows code review, but further can be used to *enforce* code review.
- Used in conjunction with a product like GitHub or Phabricator, be sure that changes require at least two to act.
- Ensure that master pushes are blocked - merges must happen online.

PLEASE MIND THE SECURITY

???