“I Honorably Assure You: It is Secure”

Hacking in the Far East

Paul S. Ziegler / HITB2012KL

Introduction

Introduction

In 60 seconds or less

Paul Sebastian **Ziegler**


Pentester

Cross-Site Scripting

Paul Sebastian Ziegler

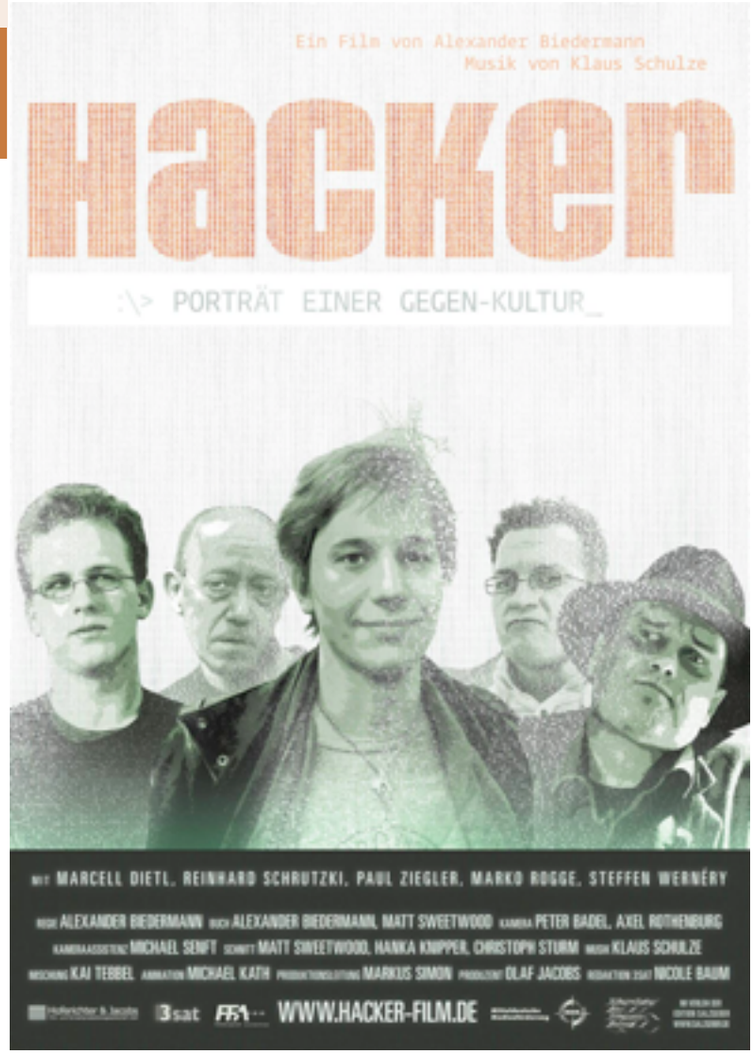
Cross-Site Scripting (XSS) ist die Schwachstelle in Webanwendungen schlechthin. Wie kaum eine andere Technik kombiniert diese Technik einfache Methoden und Ansätze zu letztendlich verheerenden Angriffen. Jedoch ist das Wissen um diese Schwachstelle und die damit verbundenen Angriffe derzeitig lediglich Sicherheitsexperten vorbehalten. Es existieren zwar umfangreiche Berichte und Dokumentationen, aber diese können zumeist nur von Insidern verstanden werden. Der normale Programmierer oder Nutzer, der sich mit Cross-Site Scripting auseinandersetzen muss, bleibt in der Regel außen vor.
Dieses TecFeed ist bemüht, das zu ändern. In einfachen Schritten führt Sie der Autor in das komplexe Thema ein. Sie werden lernen, was Cross-Site Scripting ist und wie man mit seiner Hilfe Webanwendungen angreifen kann. Nach der Lektüre dieses TecFeeds werden Sie in der Lage sein, Schwachstellen zu erkennen und zu beheben.

O'REILLY®

INHALT

TecFeeds

www.tecfeeds.de



LOKALES

Sonnabend/Sonntag, 22./23. Dezember 2007 · Nr. 299

Kein System ist absolut sicher

20-jähriger Hacker gibt Einblick in seine Welt – Die größte Schwachstelle ist der Mensch

Tokyo


Asia

Wednesday, October 10, 12

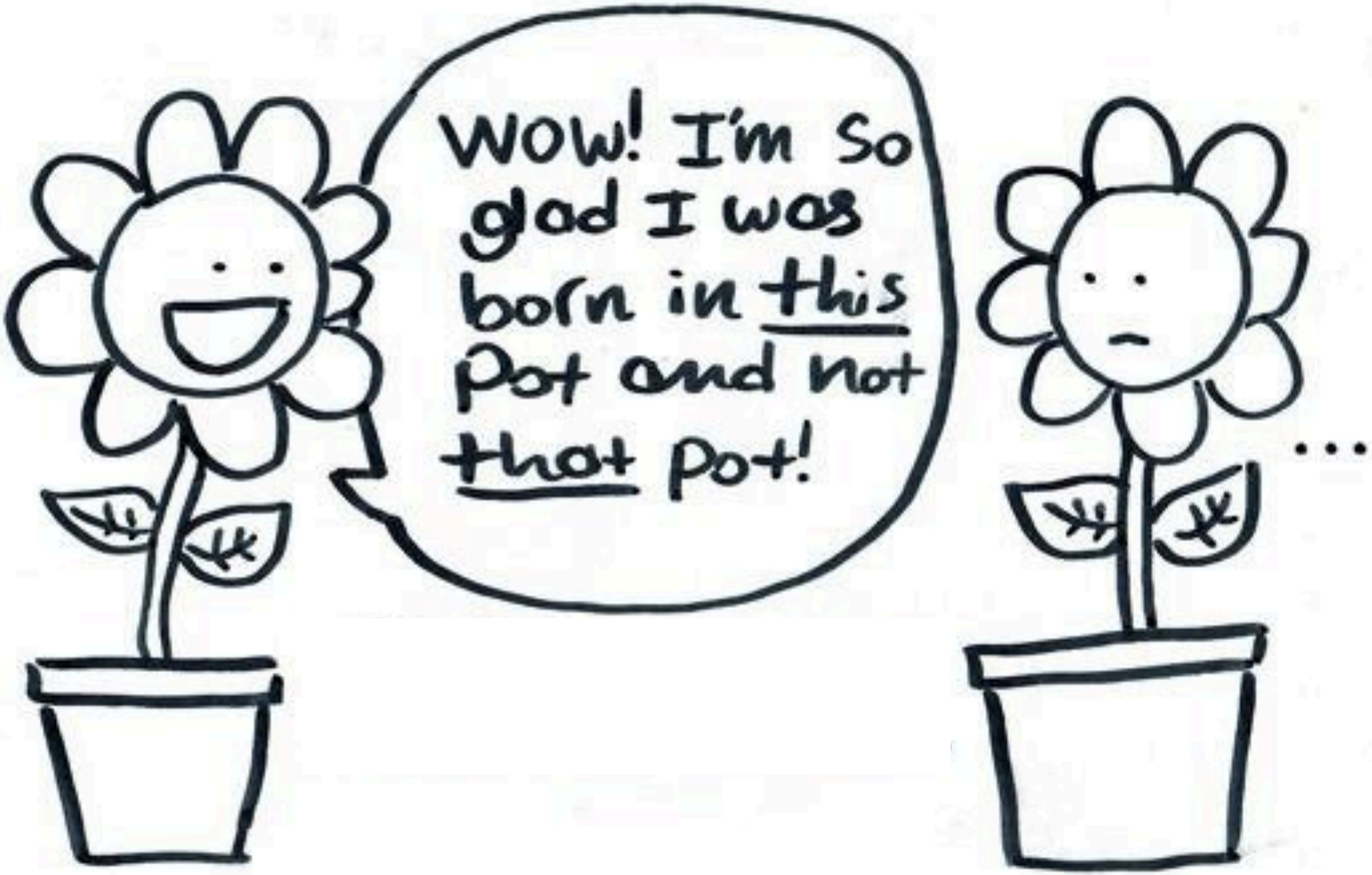
Anything else?

Ask!

Feeling stalkerish?

http://observed.de

Before we begin


Wow! I'm so glad I was born in this pot and not that pot!
...

Less of this

Hate

Well then...

Three Wise Monkeys

See No Evil

See No Evil

Hear No Evil

See No Evil

Hear No Evil

Speak No Evil

Wednesday, October 10, 12


I read your email


I read your email


I read your email


Bring My Cup
I read your email


Bring My Cup
I read your email


Bring My Cup
I read your email

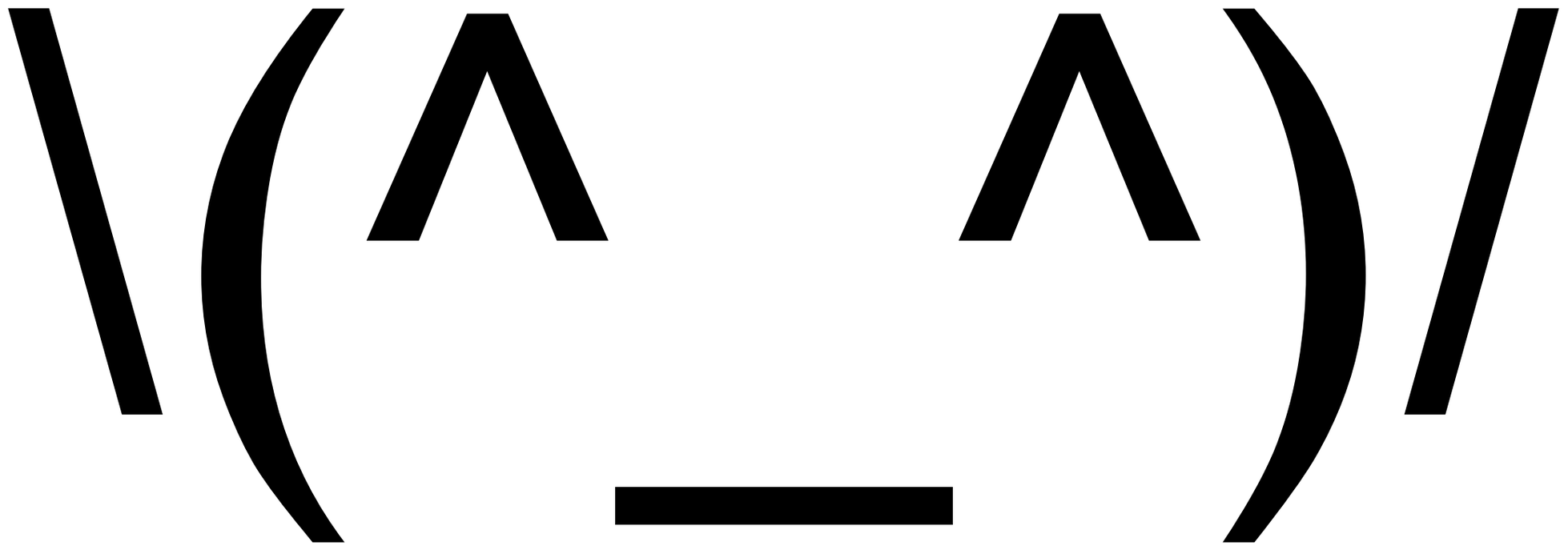

Bring My Cup
I read your email


Bring My Cup
I read your email


Bring My Cup
ハッカー


“Hacker”
ハッカー

“I humbly apologize, but I must ask you to kindly leave this establishment.”



Exploitation Vector:

Invest your time into intelligence gathering or exploitation - not covert operation.

The Invisibility Cloak

NINJAS

There are four in this picture.

Amazon.com: Cloak of Invisi

www.amazon.com/Harry-Potter-883516-Cloak-Invisibility/dp/B00421A5FS

amazon

Reflare's Amazon.com | Today's Deals | Gift Cards | Help

Shop by Department | Search | Toys & Games | Go | Hello, Reflare Your Account | Join Prime | 0 Cart | Wish List

Toys & Games | Best Sellers | New Releases | Preschool Toys | Boys' Toys | Girls' Toys | Games & Puzzles | Hobby, Models & Trains | Toys Outlet

Click for larger image and other views

Share your own related images

Cloak of Invisibility

by Harry Potter

(6 customer reviews) | Like (18)

List Price: $395.00

Price: $389.00 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $6.00 (2%)

Only 2 left in stock (more on the way).

Ships from and sold by **Amazon.com**. Gift-wrap available.

Want it delivered Tuesday, October 9? Order it in the next 11 hours and 6 minutes, and choose **One-Day Shipping** at checkout. Details

3 new from $389.00

Hot New Toys for Fall

New

Shop a wide selection of all-new toys from top brands for kids of all ages. Learn more

Quantity: 1

Yes, I want **FREE Two-Day Shipping** with Amazon Prime

Add to Cart

or

Sign in to turn on 1-Click ordering.

Add to Wish List

More Buying Choices

SwordsandSw... Add to Cart
$389.00 + $11.00 shipping

Comic Book Culture Add to Cart
$416.95 + Free Shipping

3 new from $389.00

Have one to sell? Sell on Amazon

Share

Product Features

- Officially licensed
- Made from authentic materials true to the movie
- Screen accurate
- Hand finished silk screened design, no two are alike
- Heavy velvet cloak with silk lining

25 of 47 people found the following review helpful

★☆☆☆☆ **A Bit Disappointed.**, March 4, 2011

By **Austin Jennings** - See all my reviews

= Durability: ★★★★☆ **= Fun:** ★★☆☆☆ **= Educational:** ★☆☆☆☆

This review is from: Cloak of Invisibility (Toy)

Well, it didn't work. Otherwise nice looking, but... well, I'd prefer no one be able to see it at all.

Help other customers find the most helpful reviews

Was this review helpful to you? Yes No

Report abuse | Permalink

Comment

Invisible Cloak You Say?

- Obliterates badge requirements (even better when talking on a cellphone in English)
- Reduces random police ID checks from once a month to never
- Lets you get away with virtually any social violation

Works differently in South Korea

Honor Cloak

- Gets you service in restaurants as a foreigner
- Triples native's willingness to communicate in English / Japanese / Signs
- Strangers will walk you to the location you search for and randomly carry your stuff instead of running away or screaming
- Taxi acquisition time reduced to less than 60 seconds

Honor Cloak

- Taxi drivers actually drop you off at your door instead of kicking you out at the nearest intersection
- In short: If you're a foreign male, putting on a suit in Korea teleports you into a different country

Swarm Effect


Let us praise the Lord
and His grace
都要齐声赞美主的恩惠
共に　主の恵みを賛美せよ
파더스드림
중보기도
훈련학교

Class Effect

The three classes of foreigners

The three classes of foreigners

Military

The three classes of foreigners

Military

English Teachers

The three classes of foreigners

Military

English Teachers

Business

The three classes of foreigners

Military

English Teachers

Business

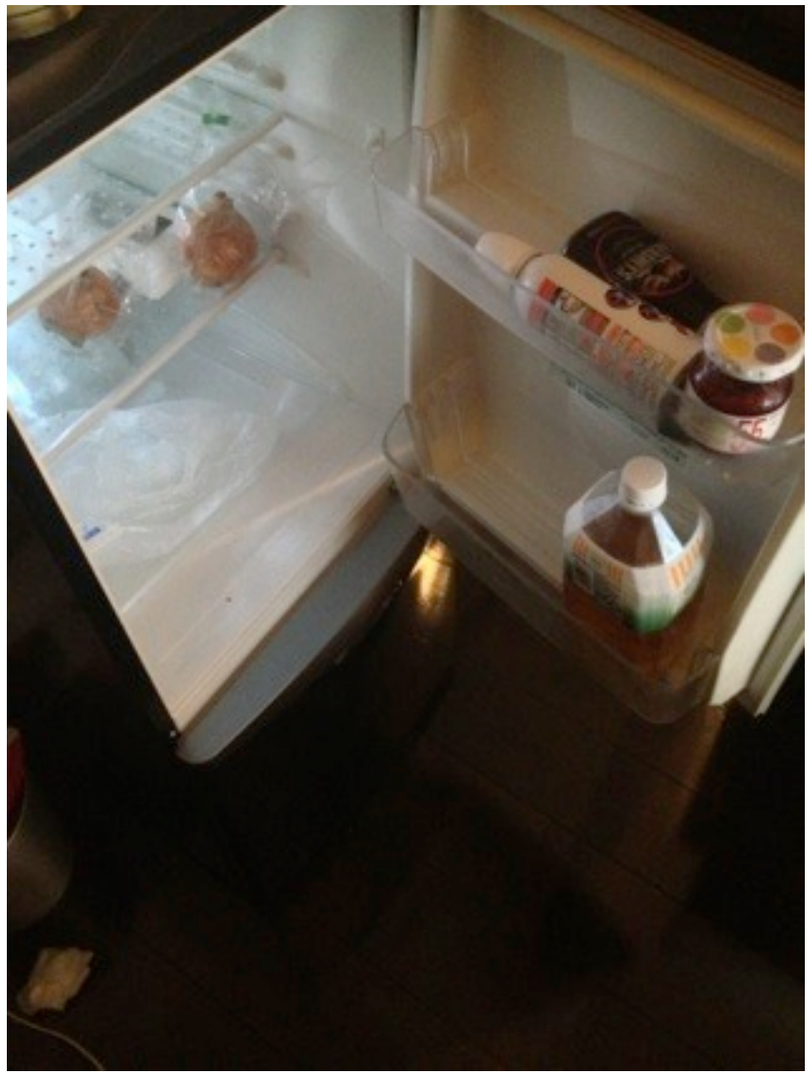
Also Works in Hong Kong

"Hey, look - it's another banker!"

Exploitation Vector

If all else fails, use the “dumb foreigner” card.

Home Insecurity



“Apartment”

“Mansion”

“Apartment”

- Cheap (rent & construction)
- Wood and Paper
- Not guaranteed to withstand a strong earthquake
- The concept of security just doesn’t apply

Wednesday, October 10, 12

Wednesday, October 10, 12

Wednesday, October 10, 12

Wednesday, October 10, 12

Wednesday, October 10, 12

Wednesday, October 10, 12

Wednesday, October 10, 12

"To prevent crime, you are prohibited by national law to create a copy of your key."

-- AMMS Estate Rental Agreement (2008)


MISTER MINIT

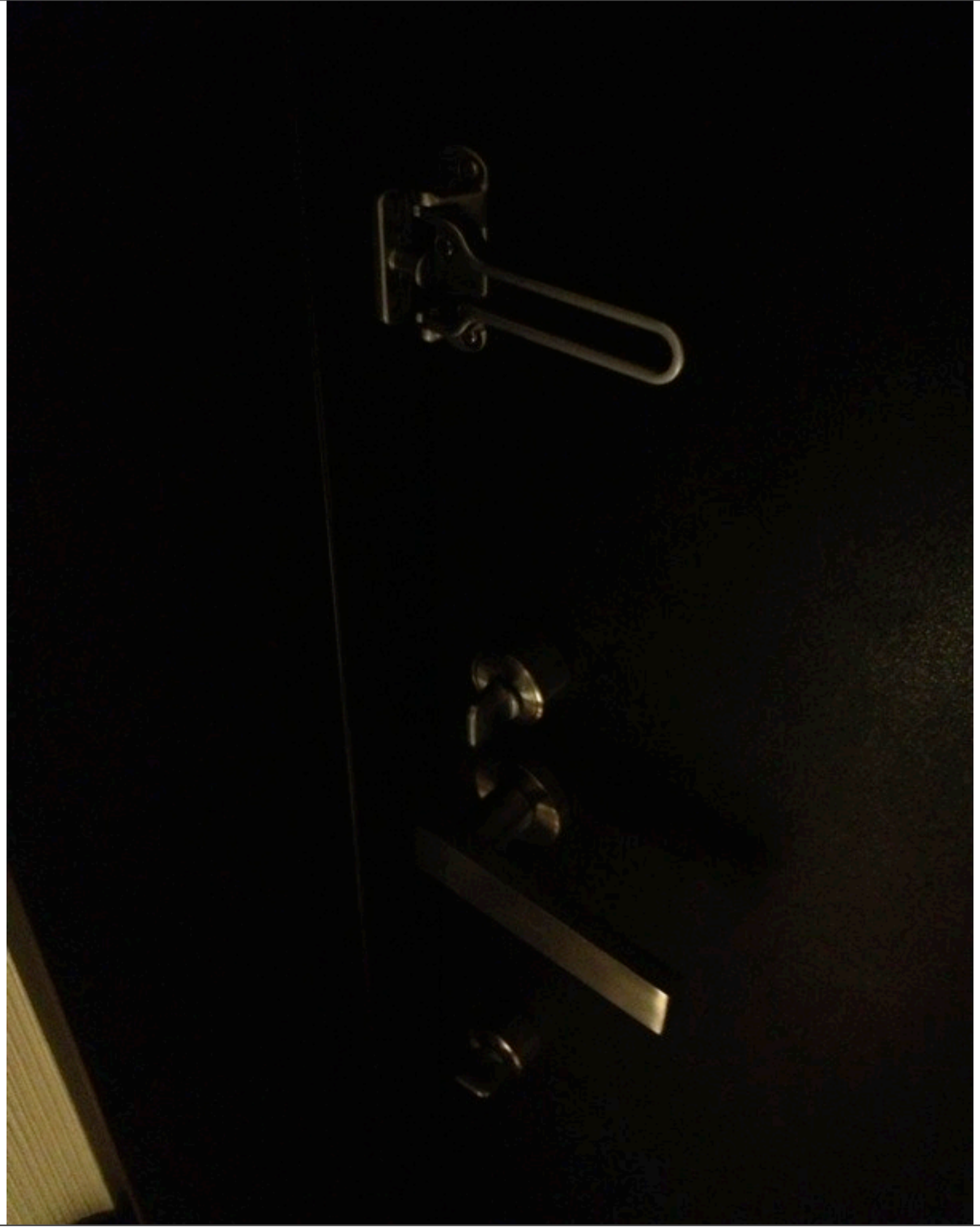

MISTER MINIT
Key Cutting


MISTER MINIT
SMART SHOE REPAIR
EXPRESS
MISTER MINIT
EXPRESS

“Mansion”

- You’ll need to sell a kidney to afford one
- Sturdy construction
- Earthquake resistant
- Central lock
- (Often) Including security services


警報音
停止
復旧
火災
確認
非常
メニュー
終了
防犯
戻
NAIS
通話

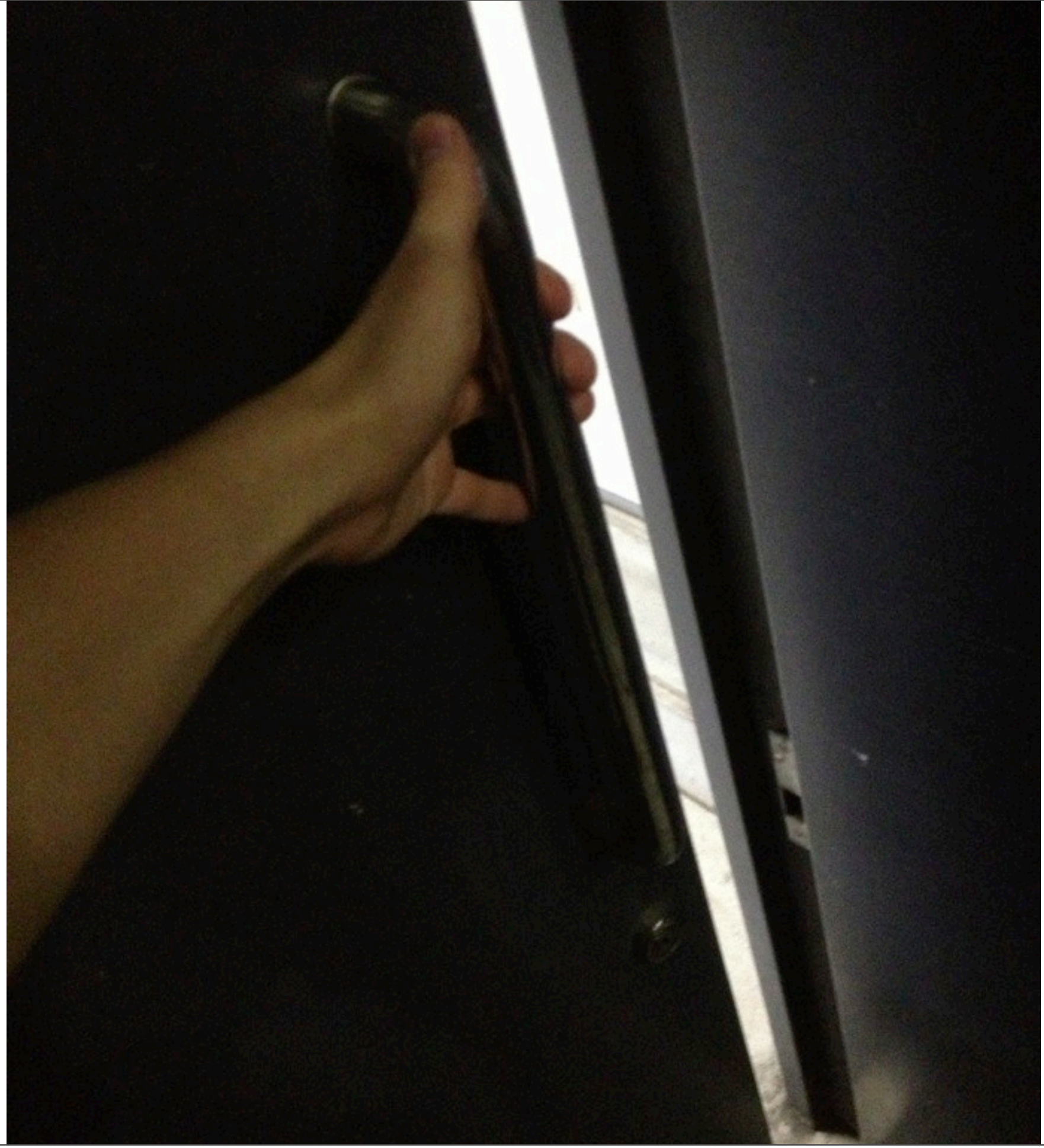


Wednesday, October 10, 12


操作手順 ①訪問先の室番号を押してください
②室番号を確認して呼出ボタンを押してください
室番号をまちがえたときは#ボタンを押して初めから操作してください
使用中のランプが点灯している時は呼び出しできません 消えるまでしばらくお待ちください
管理室は＊＋呼出

Safe!

Wednesday, October 10, 12



Damn it!


警報音
停止
復旧
火災
確認
非常
メニュー
終了
防犯
戻
NAIS
通話


808
705

Reducing Lock Efficiency to basically zero

-

In 4 easy steps

Entropy:

20^8

1. Legally prohibit mail locks with more than 3 digit combinations

Entropy:

20^3

2. Legally force all locks to open in a clockwise-clockwise-clockwise-counterclockwise pattern

Entropy:

1000

3. Legally force the first two digits of the combination to be the same

Entropy:

100

4. Don't integrate a separate opening crank, but simply open once the correct combination is entered

Time per attempt:

1.5 seconds

50% unlock chance

75 Seconds

100% unlock chance

150 Seconds

Jumping to Korea...


Emergency Power DC9V
1
2
3
4
Suspension
5
Auto
6
Manual
7
Release
8
Mute
9
*
Start
End
0
Lock
#
Change
Setting
DIGITAL DOOR LOCK SYSTEM
Mitre

Entropy:

10^8

Well, albeit not a law, most locks only take up to 4 digits...

Entropy:

10^4

And the majority of them are not wired to any monitoring...

Or block you out after numerous attempts...

Time per attempt:

0.85 seconds

50% unlock chance

66 Minutes

38 Seconds

100% unlock chance

133 Minutes

16 Seconds

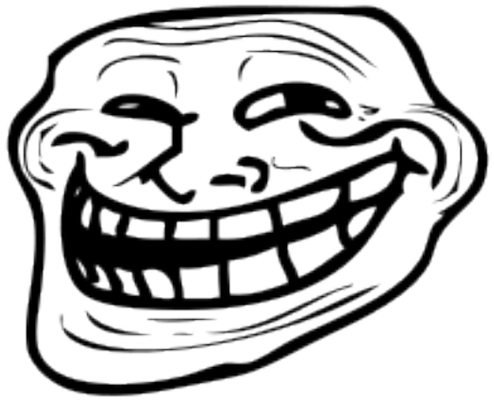

Emergency Power DC9V
1
2
3
4
5
6
Suspension
Auto
Manual
7
8
9
Release
Mute
*
0
#
Start
End
Lock
Change
Setting
DIGITAL DOOR LOCK SYSTEM
Mitre


DIGITAL DOOR LOCK SYSTEM
Mitre

+


GUANGYUN
N9605 46B24RS

=



Counter Exploitation:

Work from the assumption that if someone wants to get into your place - they will.

Corporate Insecurity

“Lifetime Employment”

- Get a mediocre wage
- Guaranteed mediocre raises
- You can not be fired or laid off
- If you survive to retirement, the company pays you around 75% of your last wage until you die
- If you die, it pays your spouse until their death

“Bonus”

- Officially rewards good work
- Unofficially often dependent on overtime
- Can contribute up to 50% to annual wage
- Easy tool to keep employees in line

Don’t fuck up

Don’t fuck up

Requires Action

Make a judgement call that could potentially save the company a lot and seems very clear.

Incur a small loss

Make a judgement call that could potentially save the company a lot and seems very clear.

Incur a small loss

You fucked up.

Pedantically stick to protocol even though it is wrong for the current case and cost the company millions.

Pedantically stick to protocol even though it is wrong for the current case and cost the company millions.

Promotion secured.

Also, don't work too fast and stay until I am to secure that bonus.

Also, don't work too fast and stay until I am to secure that bonus.

(Alternatively become a contractor.)

Example A

1) Run nmap on customer network

1) Run nmap on customer network

2) Find Windows NT4 box

1) Run nmap on customer network

2) Find Windows NT4 box

3) Find IRC server running on NT4 box

1) Run nmap on customer network
2) Find Windows NT4 box
3) Find IRC server running on NT4 box
4) Find it runs on port 31337

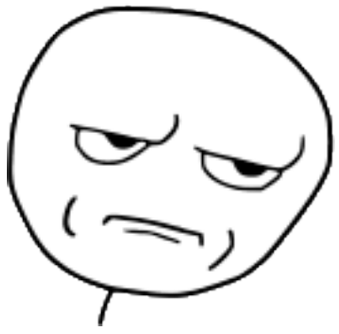
1) Run nmap on customer network
2) Find Windows NT4 box
3) Find IRC server running on NT4 box
4) Find it runs on port 31337

How do you react?

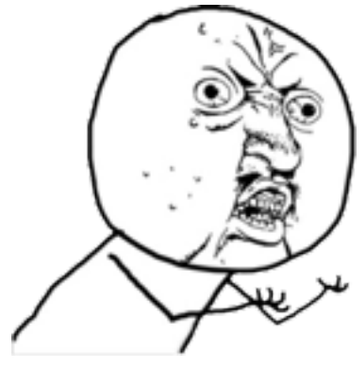
“We’ll check into it.”

2 Weeks Pass

"We have decided against shutting down or altering the affected machine..."

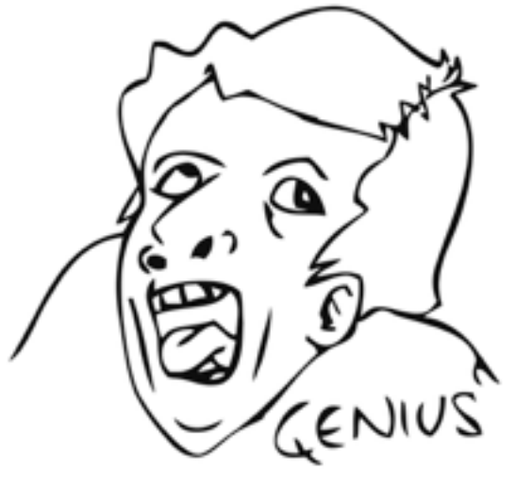


“Because the guy who set it up no longer works here...”



“And we have no idea what it does...”

"But it might be important, so we'll just leave it running."



Checklist

- ☑ I didn't touch it
- ☑ It is not obviously horribly broken from a middle management PoV
- ☑ If we get hacked, someone else "did it"
- ☑ I still get my raise and keep my job

Example B

Setting

Client operates an SaaS API that integrates into their dashboard.

Japanese company integrates their product with it.

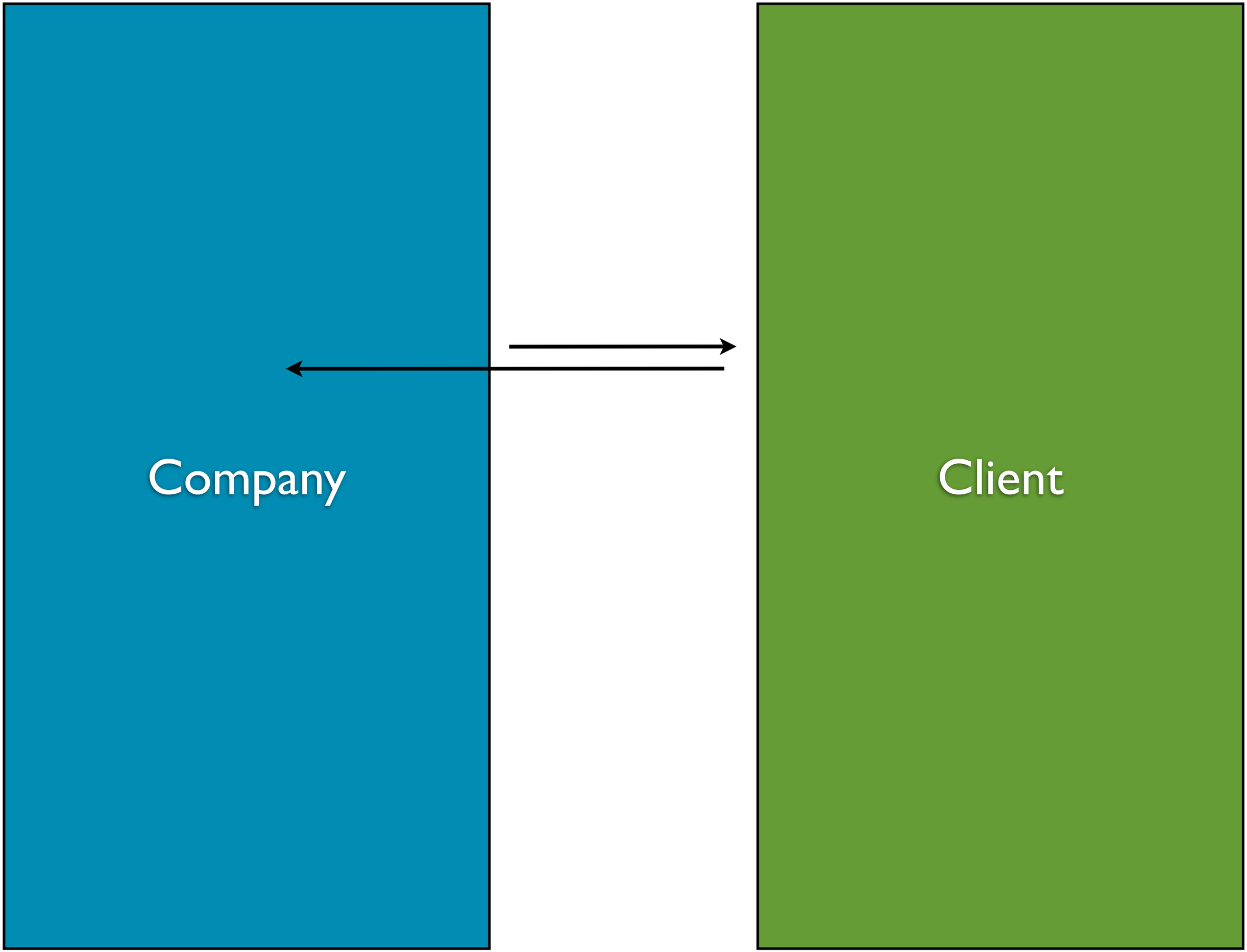
If the API isn't called for 24 hours, an error message is displayed.

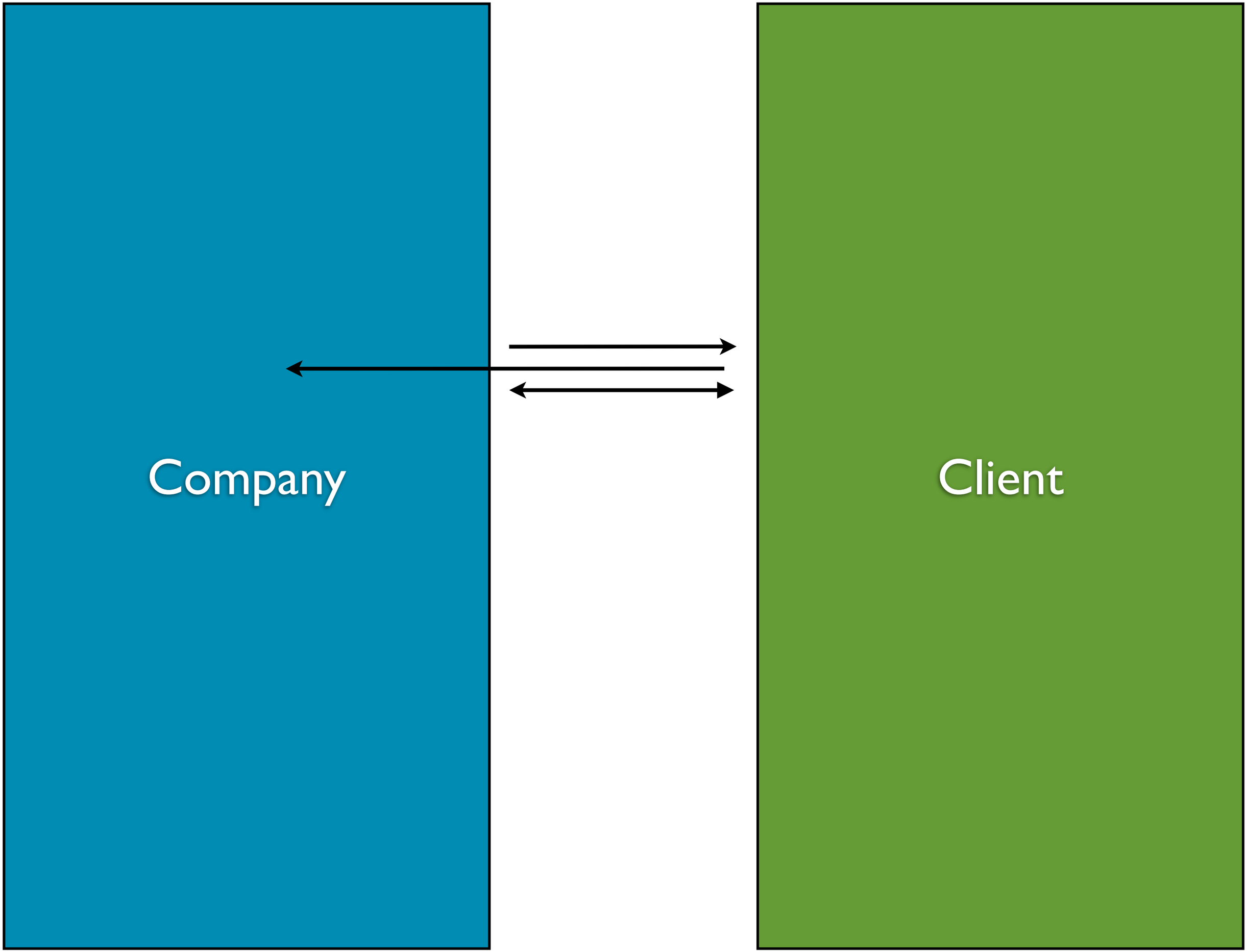
Of 25 possible causes, number 22 names "there may be issues with your encryption certificate".

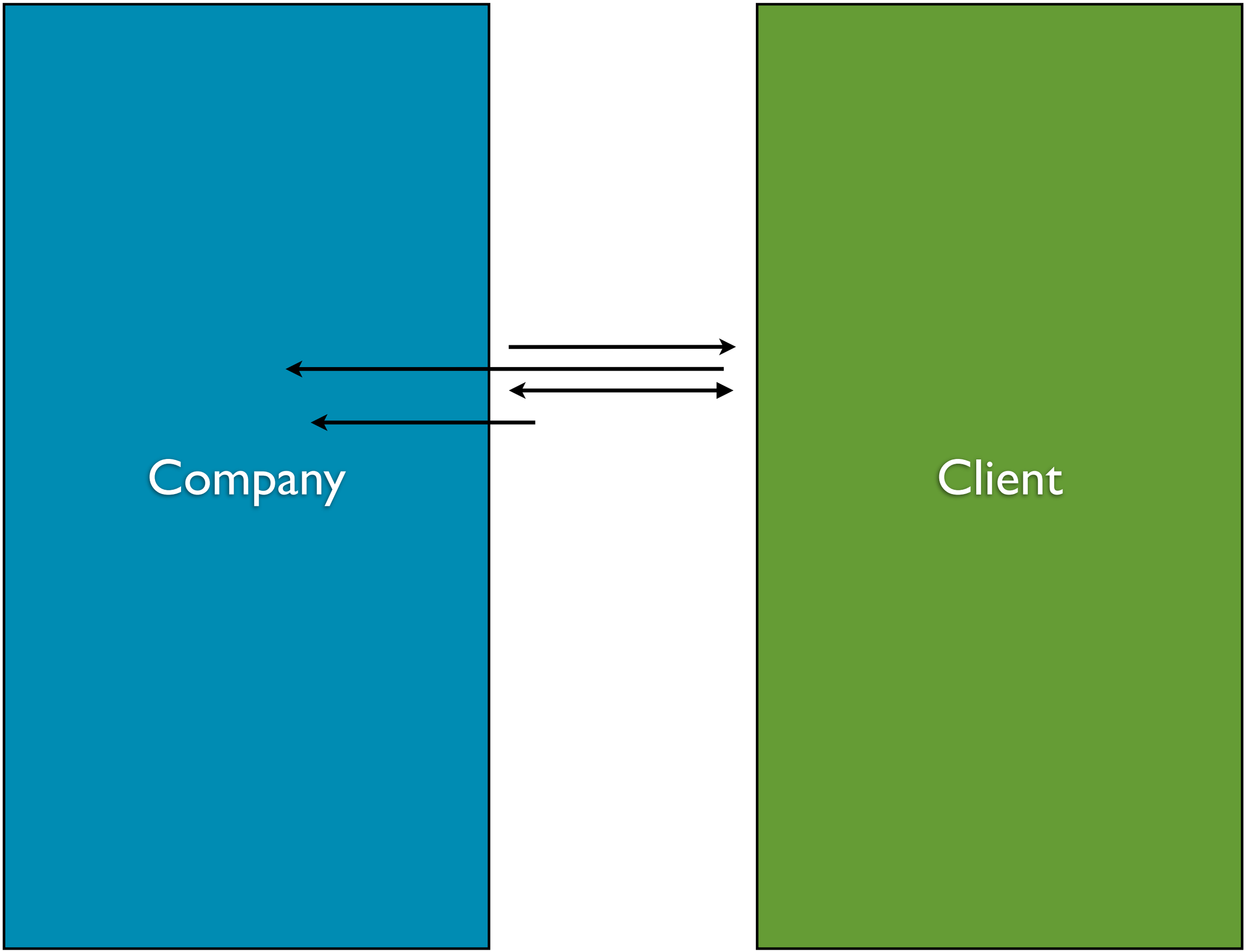
What do you do?

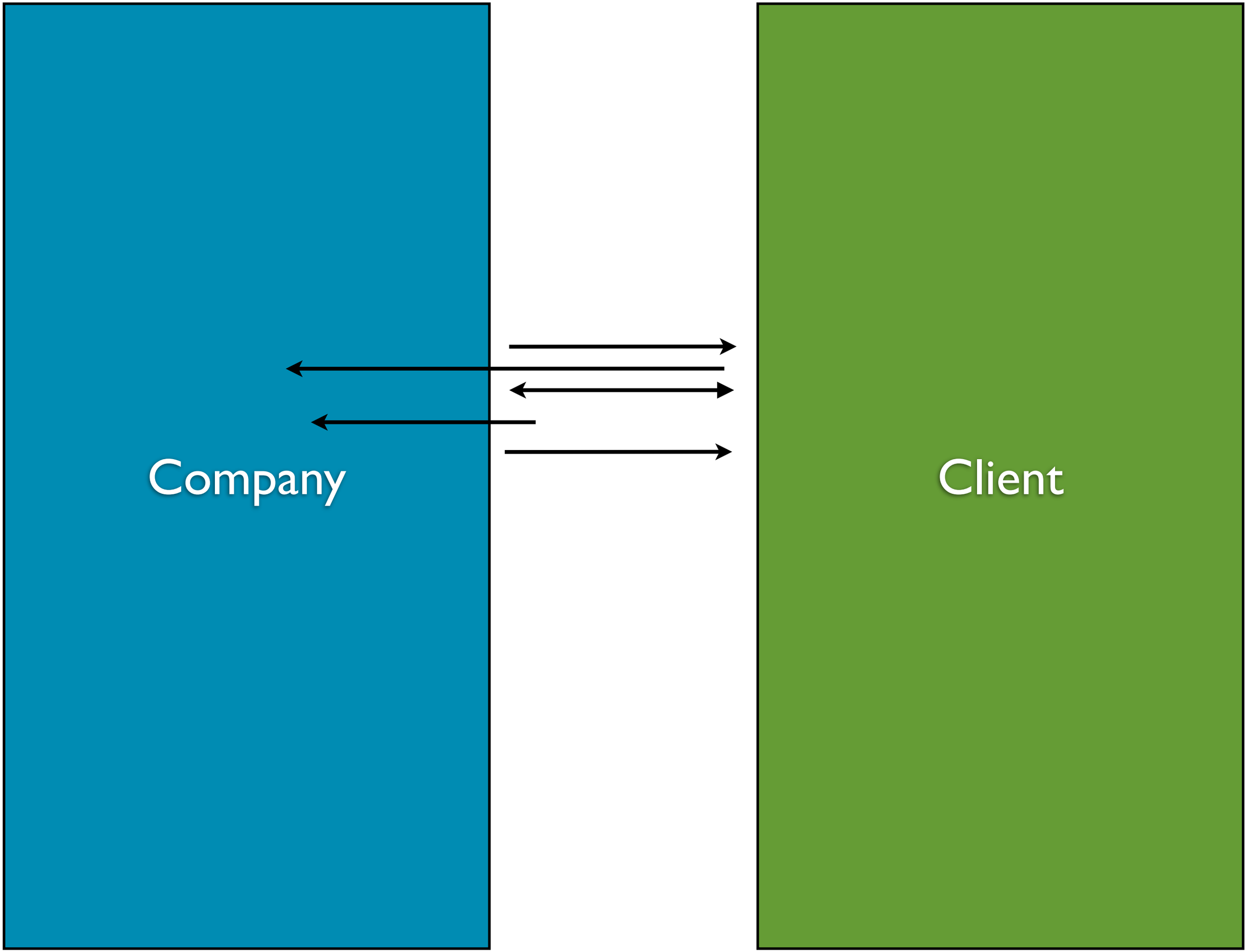
Company

Client

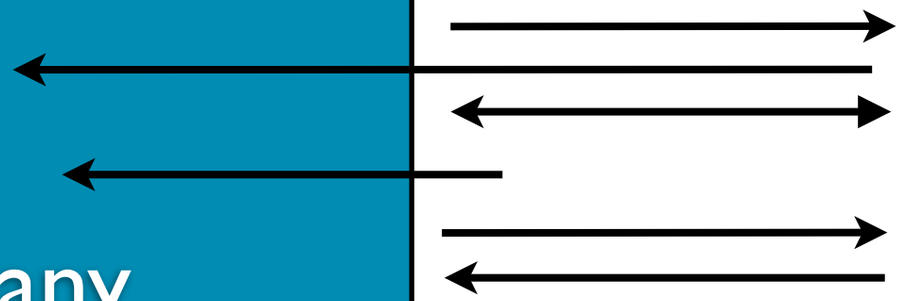

Company
Client


Company
Client


Company
Client


Company
Client

Company

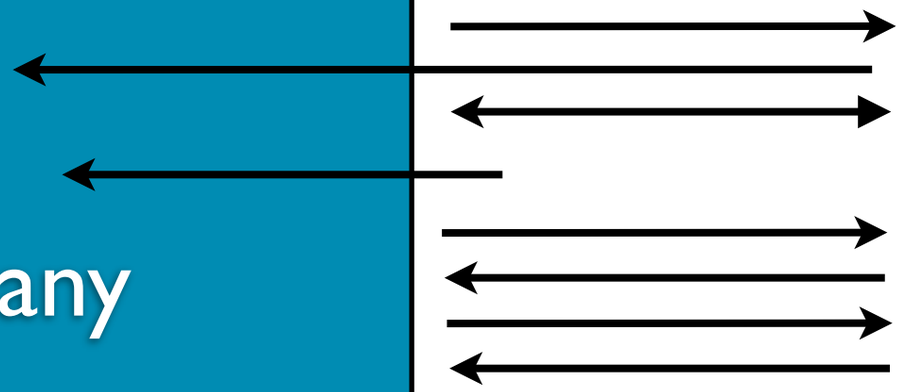


Client

Company

Client

Company

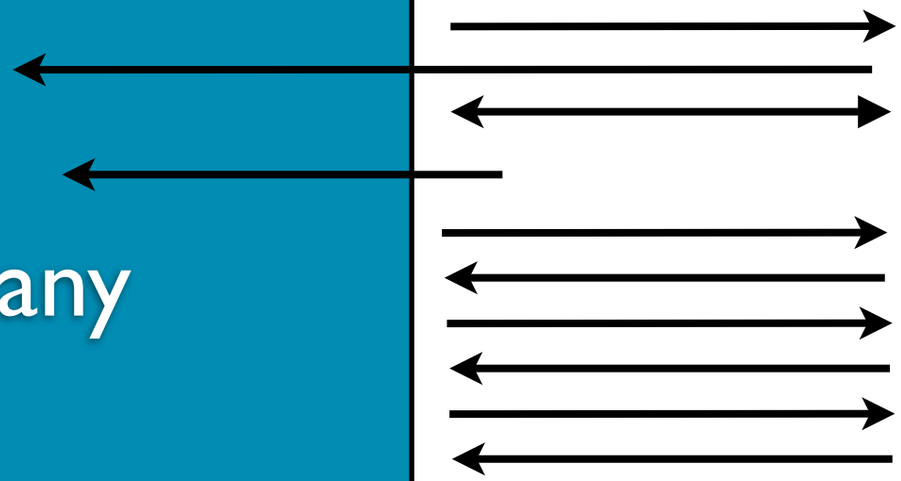


Client

Company

Client

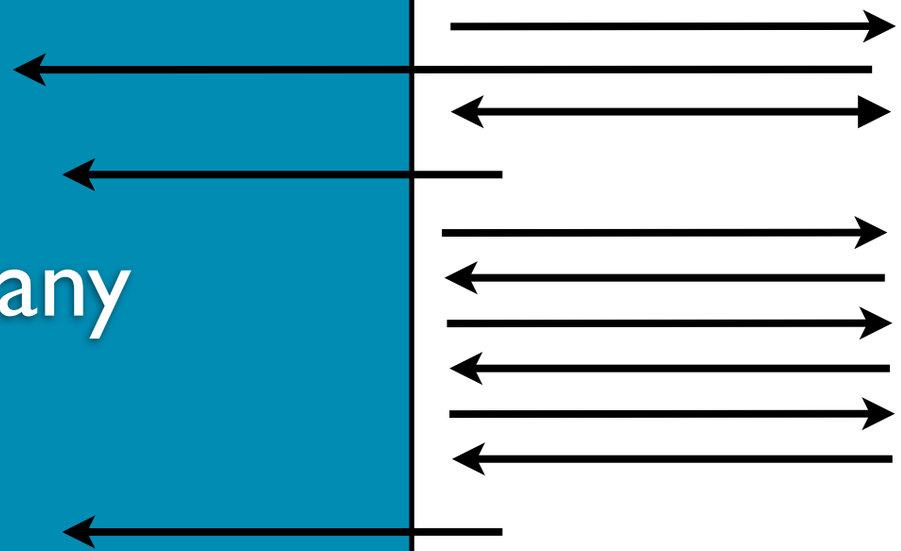
Company



Client

Company

Client



Company

Client

?

Solution?

2 months in, I suggested the client removed the SSL warning, then call the company and say they fixed the problem.

Product was launched within 24 hours.

Checklist

- ☑ It says it may be the certificate
- ☑ I didn't put my neck out and escalated it
- ☑ No one put their neck out
- ☑ The entire operation delayed launch by 2 months and cost hundreds of thousands of dollars
- ☑ Client took responsibility
- ☑ I still get my raise and keep my job

Exploitation Vectors

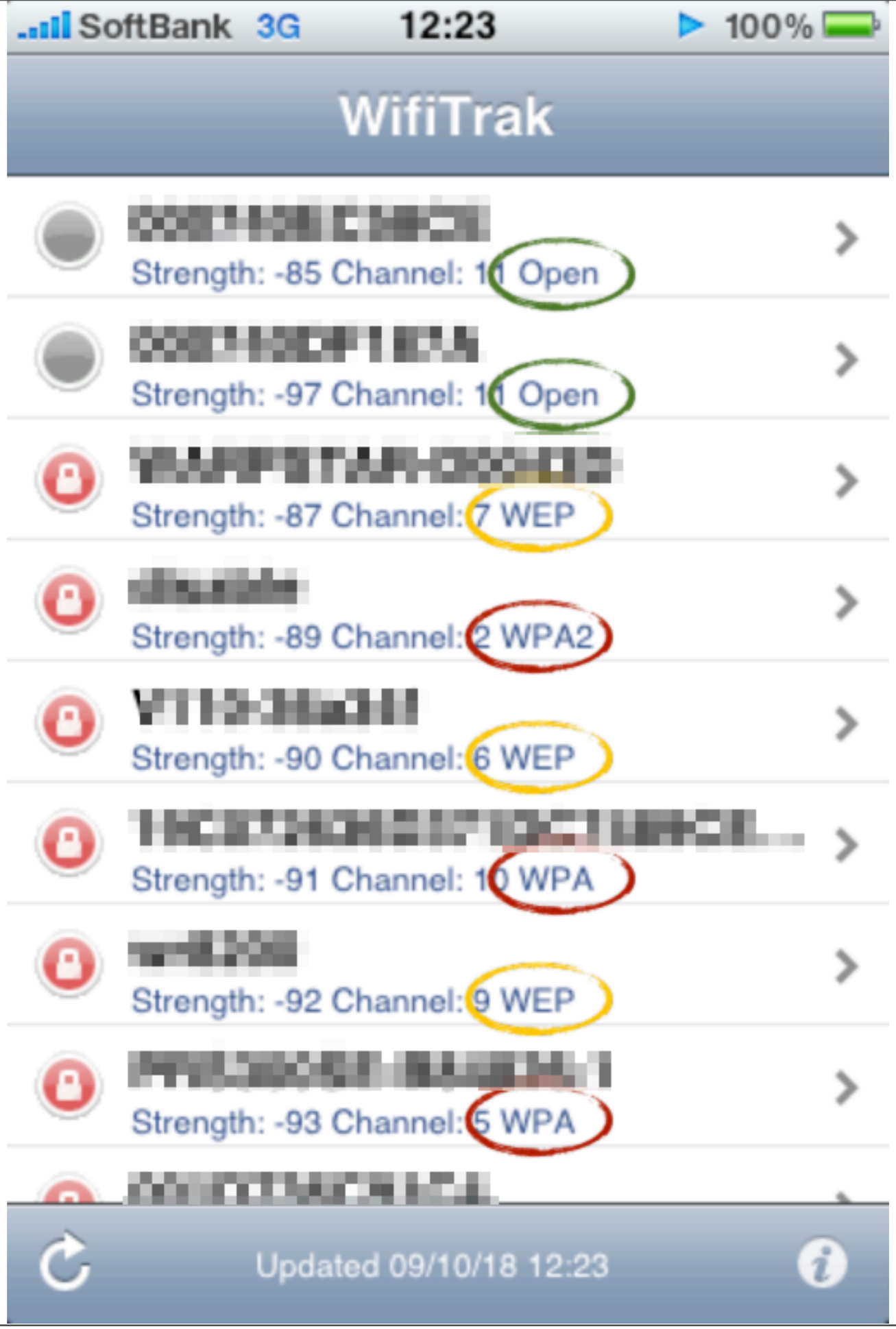
1) Stuff won't be fixed.

2) Create a responsibility setting and no one disturbs you.

"I am here on behalf of *unreachable high ranking manager*.

Will YOU be responsible when he finds out you disturbed my work?"

Wires? Where we're going we don't need wires!


SoftBank 3G
12:23
100%
WifiTrak
Strength: -85 Channel: 11 Open
Strength: -97 Channel: 11 Open
Strength: -87 Channel: 7 WEP
Strength: -89 Channel: 2 WPA2
Strength: -90 Channel: 6 WEP
Strength: -91 Channel: 10 WPA
Strength: -92 Channel: 9 WEP
Strength: -93 Channel: 5 WPA
Updated 09/10/18 12:23

SoftBank

au by KDDI

Cellphone hotspots

NTT DoCoMo

Access filtered by a mix of Mac Address and User-Agent sent to Gateway

Absolutely Secure

However Korea takes the Cake here

KOR... 15:48 71 %

WifiTrak

THEMARIUM
Strength: -70 Channel: 6 Open

ZIO
Strength: -78 Channel: 6 Open

iptime
Strength: -78 Channel: 1 Open

unicorn
Strength: -78 Channel: 11 Open

hpsetup
Strength: -82 Channel: 6 Open

anygate
Strength: -85 Channel: 1 Open

anygate
Strength: -85 Channel: 6 Open

unicorn
Strength: -87 Channel: 11 Open

Unicorn

Updated 09/12/06 15:48

Exploitation Vector:

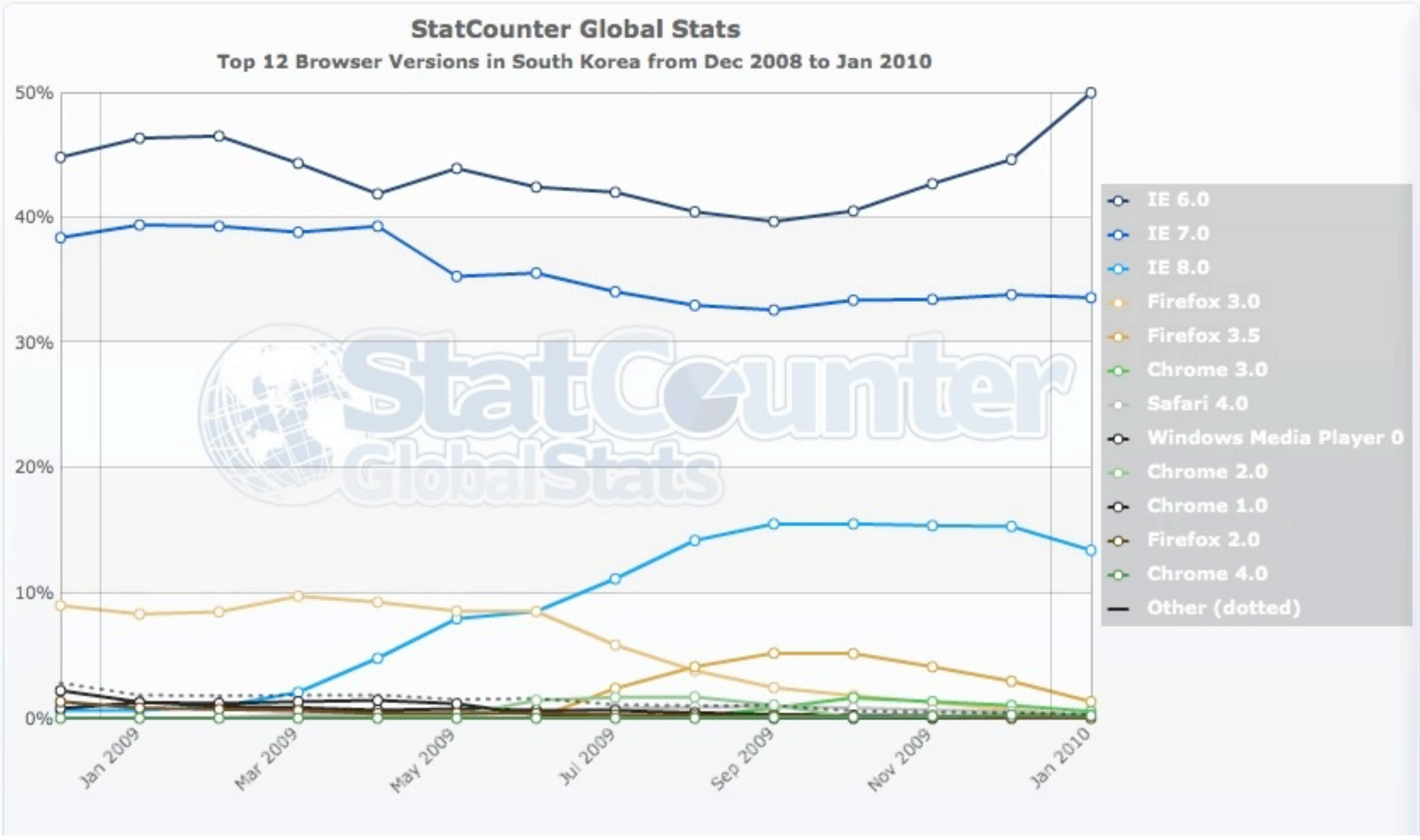
Yeah, gee, I wonder what anyone could ever do with anonymous open internet access.

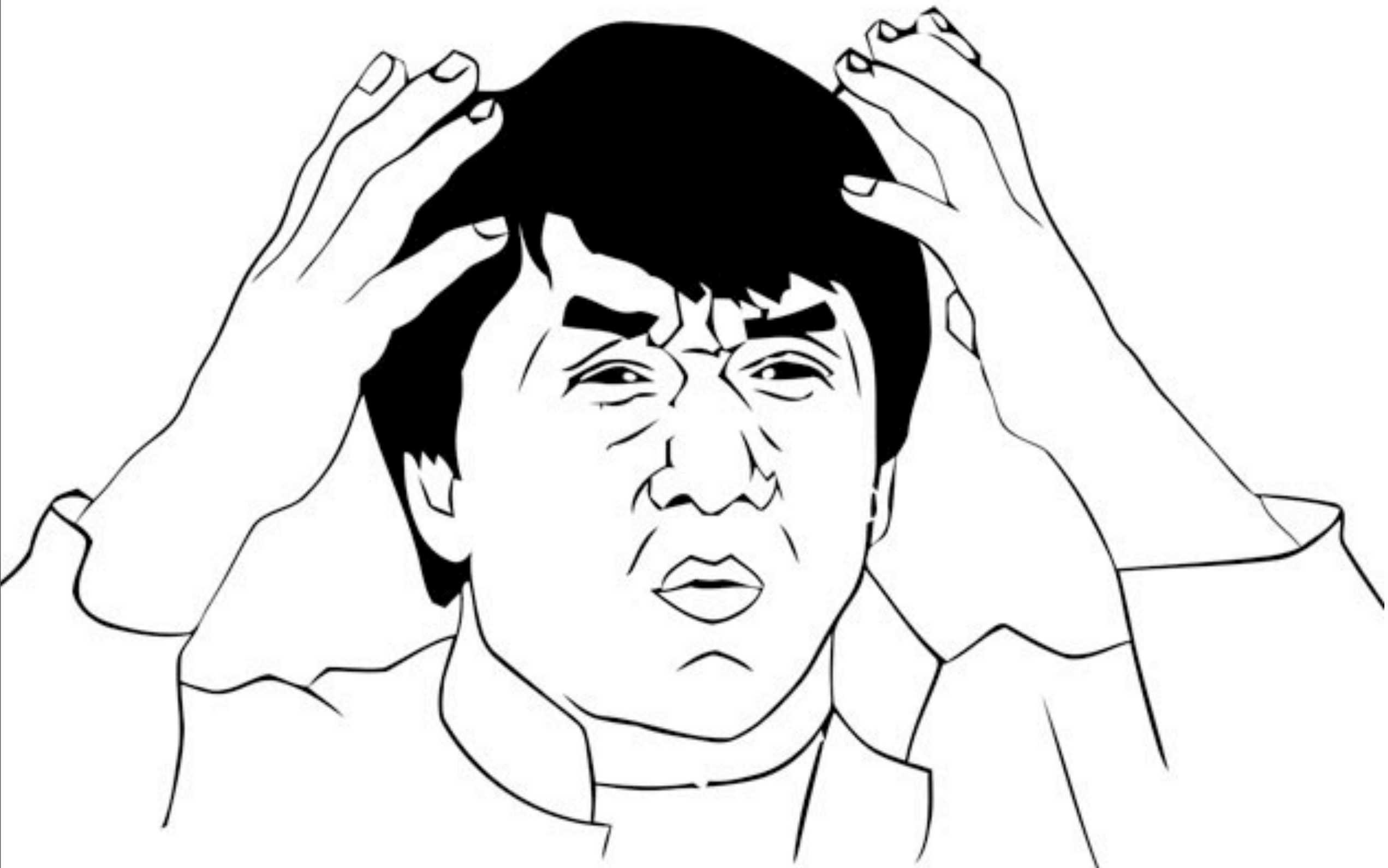
Speaking of Korea

Taking all guesses - what's the browser market share for IE in Korea.

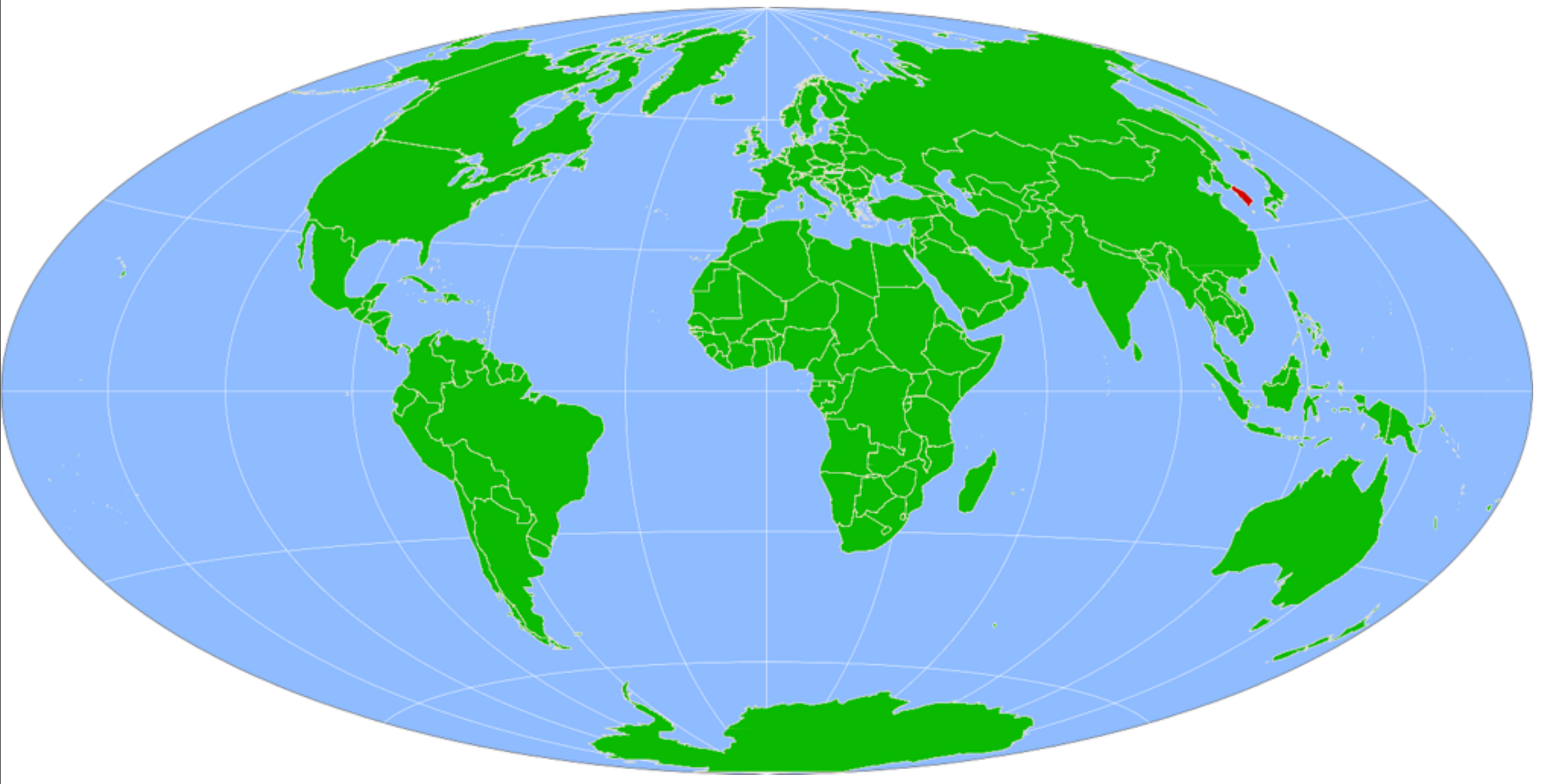
97%

Ninety-Seven-Percent


StatCounter Global Stats
Top 12 Browser Versions in South Korea from Dec 2008 to Jan 2010
50%
40%
30%
20%
10%
0%
Jan 2009
Mar 2009
May 2009
Jul 2009
Sep 2009
Nov 2009
Jan 2010
IE 6.0
IE 7.0
IE 8.0
Firefox 3.0
Firefox 3.5
Chrome 3.0
Safari 4.0
Windows Media Player 0
Chrome 2.0
Chrome 1.0
Firefox 2.0
Chrome 4.0
Other (dotted)



Adaption of SSL



SEED

- Published in 1998 by the Korean Information Security Agency
- 128-bit Block Cypher
- Alternative to SSL
- Required for online banking, online shopping, government transactions, etc
- Works as an ActiveX plugin compatible with some IE and Windows versions

Effects

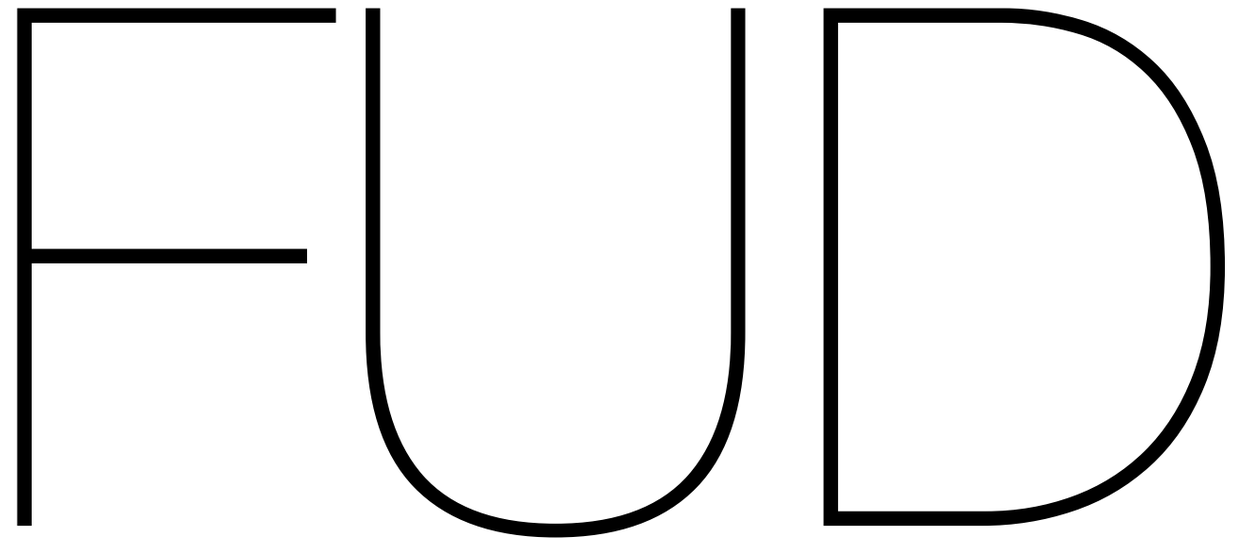
- Extremely slow adaption to new Windows versions
- Alternative browsers and OSs are virtually useless
- Also integrated with most cellphones (the iPhone was the first non-Korean cellphone sold)
- Very poor understanding of SSL

Many SEED variations allow for user identification, leading to a low perceived need for security.

Many SEED variations allow for user identification, leading to a low perceived need for security.

More on this later...

Exploitation Vector



Oppan SEED Style

Too-Near Field

Communication


PRESTO


Suica


oyster™


八達通
OCTOPUS


Edy No. 0123 4567 8901 2345
Edy


mo
mo
PASMO


ELECTRONIC USE ONLY
Suica
view
Suica
view
CARD
4542
MONTH/YEAR
05/14
VISA


AQUOS
TV

Why?

- Used virtually everywhere
- Always carried on body
- Automatically recharged or charged to phone bill (loose and/or high limits)
- Accepted by lots of online stores
- Stores your purchase history and reveals it without authentication


SONY
FeliCa
ACTIVE

SFCard Viewer

¥11,670

関連サイト　メニュー

利用年月日	入場駅	出場駅	残額	メモ
2006/12/29	JR東 [redacted]		¥11,670	精算
2006/12/29	JR東 [redacted]	JR東 [redacted]	¥12,070	
2006/12/23	JR東 [redacted]	JR東 [redacted]	¥12,230	
2006/12/23	JR東 [redacted]	JR東 [redacted]	¥12,390	
2006/12/23	JR東 [redacted]	JR東 [redacted]	¥12,540	
2006/12/18	JR東 [redacted]	JR東 [redacted]	¥12,700	
2006/12/18	JR東 [redacted]	JR東 [redacted]	¥12,910	
2006/12/17	東モノ [redacted]		¥13,200	磁気券購入
2006/12/16	東モノ [redacted]	東モノ [redacted]	¥13,700	
2006/12/11	JR東 [redacted]	JR東 [redacted]	¥14,170	
2006/12/03	東モノ [redacted]		¥14,820	磁気券購入
2006/12/02	東モノ [redacted]	東モノ [redacted]	¥15,320	
2006/12/01	JR東 [redacted]	JR東 [redacted]	¥15,790	
2006/11/30	JR東 [redacted]	JR東 [redacted]	¥16,000	
2006/11/26	JR東 [redacted]	JR東 [redacted]	¥16,160	
2006/11/11	神新 [redacted]	神新 [redacted]	¥16,350	
2006/11/11	[redacted]		¥16,670	物販
2006/11/11	JR西 [redacted]		¥16,806	ｶｰﾄﾞﾁｬｰｼﾞ
2006/11/11	東モノ [redacted]	東モノ [redacted]	¥6,806	
2006/11/11	JR東 [redacted]	JR東 [redacted]	¥7,276	

- [x] Location Tracking
- [x] Purchase Tracking


SO
WHERE DID YOU GET OFF THE TRAIN?
memegenerator.net

You need to have an account established before paying through Jibun Bank.

Edy

You can pay by “Osaifu-Keitai” and Edy card

※You need to register Edy service in your cellphone before using “Osaifu-Keitai”.

※You need to have an IC card reader/writer “PaSoRi” and install the software, " EdyViewer", on your PC before using Edy card if your PC doesn't have FeliCa port.

※Please note that this service is not available from 2:00AM to 7:00AM on the 3rd Wednesday of every month because of maintenance.

※Edy payment service “Osaifu-Keitai” of Softbank cellphone will be started from June in 2007.

Payment flow

1. Choose Convenience Store / ATM / Internet Banking / Edy as a payment method on either the payment selection page or the order confirmation

- ☑ Location Tracking
- ☑ Purchase Tracking
- ☑ Buying stuff on other people's tab

- ☑ Location Tracking
- ☑ Purchase Tracking
- ☑ ~~Buying stuff on other people's tab~~

But Paul, Felica Cards only work across millimeters.

You couldn't possibly get that close to a person with a reader without them noticing!

You, sir or ma'am, have obviously never seen the Tokyo morning rush-hour.


The doors are closing.
Take the next train, please.

- ☑ Location Tracking
- ☑ Purchase Tracking
- ☑ Buying stuff on other people's tab

Top 3 Hit List

#3 Airport Security

Wednesday, October 10, 12


ARINC Airport Systems
SelfServ
Copyright © 2003 ARINC AIRPORT SYSTEMS
Tulsa, Oklahoma, USA
All Rights Reserved ARINC Incorporated.
パスポート
PASSPORT
カード
CARD
レシート
RECEIPT

#2 Ultra Secure JavaScript

File Edit View History Bookmarks Tools Help

http://192.168.0.1/Basic/Index.s

Google

基本設定 高度な設定 システム設定 ステータス

ステータスセンター インターネット接続設定 無線LAN設定 LAN側設定

WN-GDN/R のステータスセンター

インターネット

「IPアドレス手動設定接続」に設定されています。
インターネットにIPアドレス 192.168.10.2 で接続中です。

インターネット接続設定

無線LAN

無線LANは、5チャンネルで利用可能ですが、セキュリティが無いために危険な状態です。
すぐに無線LAN設定ボタンをクリックして暗号化設定を行ってください。

無線LAN設定

困ったときには ? をクリックしてください。

Done 1337 0.3 MB / 17 MB 0.1 MB / 48.8 MB

I-O DATA Draft-n Wireless Broadband Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.1/Basic/Index.s

Google

基本設定 高度な設定 システム設定 ステータス

ステータスセンター インターネット接続設定 無線LAN設定 LAN側設定

WN-GDN/R のステータスセンター

インターネット

「IPアドレス手動設定接続」に設定されています。
インターネットにIPアドレス 192.168.10.2 で接続中です。

インターネット接続設定

無線LAN

無線LANは、5チャンネルで利用可能ですが、セキュリティが無いために危険な状態です。
すぐに[無線LAN設定]ボタンをクリックして暗号化設定を行ってください。

無線LAN設定

困ったときには ? をクリックしてください。

Done 1337 0.3 MB / 17 MB 0.1 MB / 48.8 MB

about:blank - Chart of I-O DATA Draft-n Wireless Broadband Router - Mozilla Firefox

```
                page_load();
            }
        //]]>

</script>

<!-- InstanceBeginEditable name="Scripts" -->

<script type="text/javascript" src="md5.js">
</script>

<script type="text/javascript">
        //<![CDATA[
        function page_load()
        {
                /* Detect browsers that cannot handle XML methods. */
                if (!document.getElementsByTagName || !((document.implementation &&
document.implementation.createDocument) || window.ActiveXObject)) {
                        alert ("このWEBブラウザは対応していないため、設定画面を表示することができません。対応のWEBブラ
ウザで設定画面を開いてください。");
                        return;
                }
                /* For debugging on a local client. */
                if ("" != "") {
                        hide_all_ssi_tr();
                }

                var password = "uaspb2Lm";
                if(password == "")
                {
                        send_login();
                }
                else
                {
                        document.getElementById("wrapper").style.display = "block";
                        document.getElementById("footer_container").style.display = "block";
                }

                //document.forms.myform.password.focus();
        }
        function data_ready(xml)
        {
                var status = xml.getElementData("login");
                if (status) {
                        if (status == "timeout") {
                                alert("このセッションは時間切れになりました。");
                                location.replace ('/');
                        } else if (status == "error") {
                                alert("パスワードが間違っています。もう一度入力してください。");
                                location.replace ('/');
                        } else {
                                location.replace (status);
```

k k3b k3bsetup kab2kabc kaccess kaddprinterwizard kaffeine kanjipad kapplymousetheme kasbar kasumi kbd_mode kbdrate kbookmarkmerger kbuildsycoca kbxutil kcminit kcminit_startup

I-O DATA Draft-n Wireless Broadband Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.1/Basic/Index.s

Google

基本設定 高度な設定 システム設定 ステータス

ステータスセンター インターネット接続設定 無線LAN設定 LAN構設定

WN-GDN/R のステータスセンター

インターネット

「IPアドレス手動設定接続」に設定されています。
インターネットにIPアドレス192.168.10.2で接続中です。

インターネット接続設定

無線LAN

無線LANは、5チャンネルで利用可能ですが、セキュリティが無いために危険な状態です。
すぐに[無線LAN設定]ボタンをクリックして暗号化設定を行ってください。

無線LAN設定

困ったときに

Done 1337 0.3 MB / 17 MB 0.1 MB / 48.8 MB

about:blank - Chart of I-O DATA Draft-n Wireless Broadband Router - Mozilla Firefox

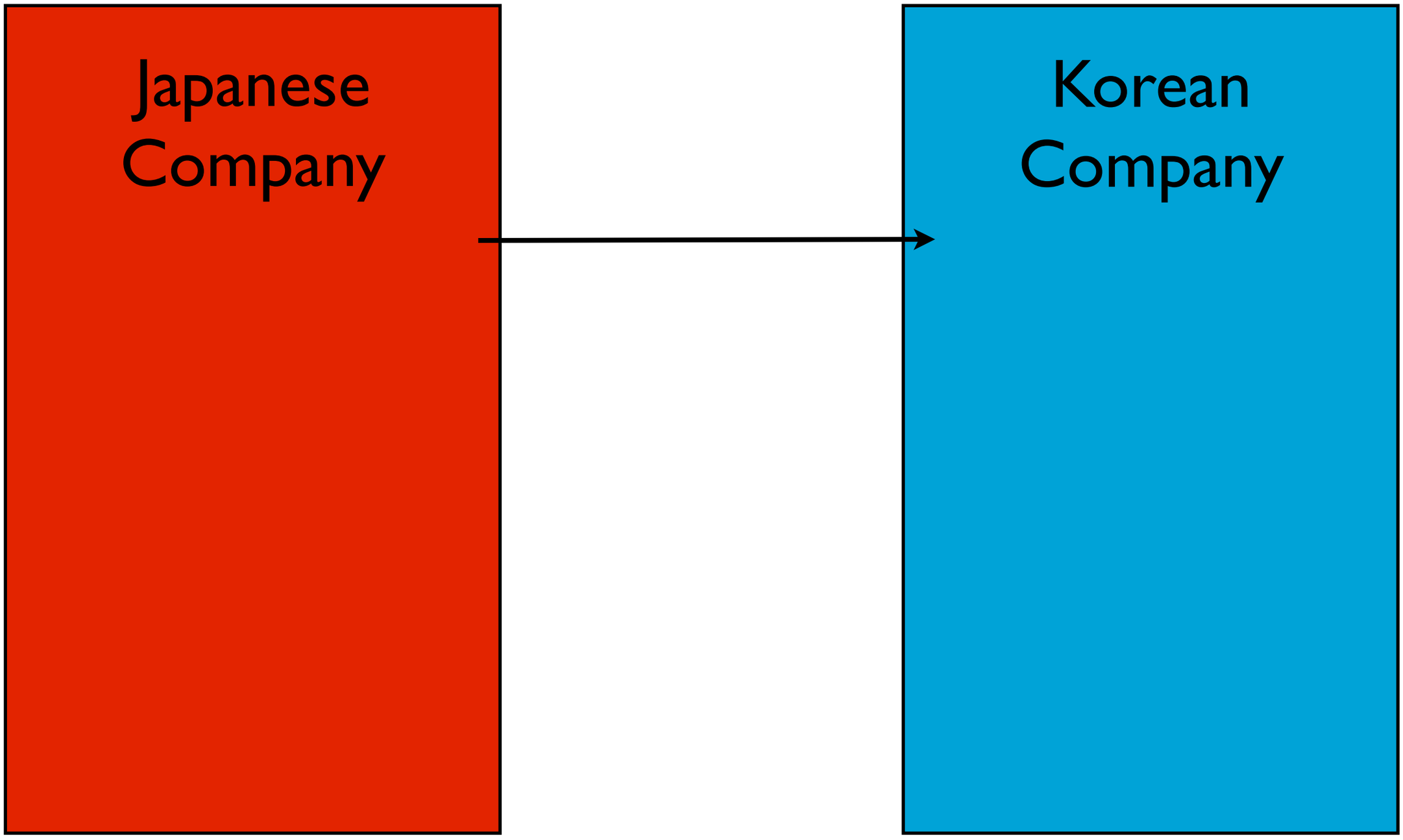
```
                page_load();
            }
        //]]>

</script>

<!-- InstanceBeginEditable name="Scripts" -->

<script type="text/javascript" src="md5.js">
</script>

<script type="text/javascript">
        //<![CDATA[
        function page_load()
        {
                /* Detect browsers that cannot handle XML methods. */
                if (!document.getElementsByTagName || !((document.implementation &&
document.implementation.createDocument) || window.ActiveXObject)) {
                        alert ("このWEBブラウザは対応していないため、設定画面を表示することができません。対応のWEBブラ
ウザで設定画面を開いてください。");
                        return;
                }
                /* For debugging on a local client. */
                if ("" != "") {
                        hide_all_ssi_tr();
                }

                var password = "uaspb2Lm";
                if(password == "")
                {
                        send_login();
                }
                else
                {
                        document.getElementById("wrapper").style.display = "block";
                        document.getElementById("footer_container").style.display = "block";
                }

                //document.forms.myform.password.focus();
        }
        function data_ready(xml)
        {
                var status = xml.getElementData("login");
                if (status) {
                        if (status == "timeout") {
                                alert("このセッションは時間切れになりました。");
                                location.replace ('/');
                        } else if (status == "error") {
                                alert("パスワードが間違っています。もう一度入力してください。");
                                location.replace ('/');
                        } else {
                                location.replace (status);
```

k3b k3bsetup kab2kabc kaccess kaddprinterwizard kaffeine kanjipad kapplymousetheme kasbar kasumi kbd_mode kbdrate kbookmarkmerger kbuildsycoca kbxutil kcminit kcminit_startup

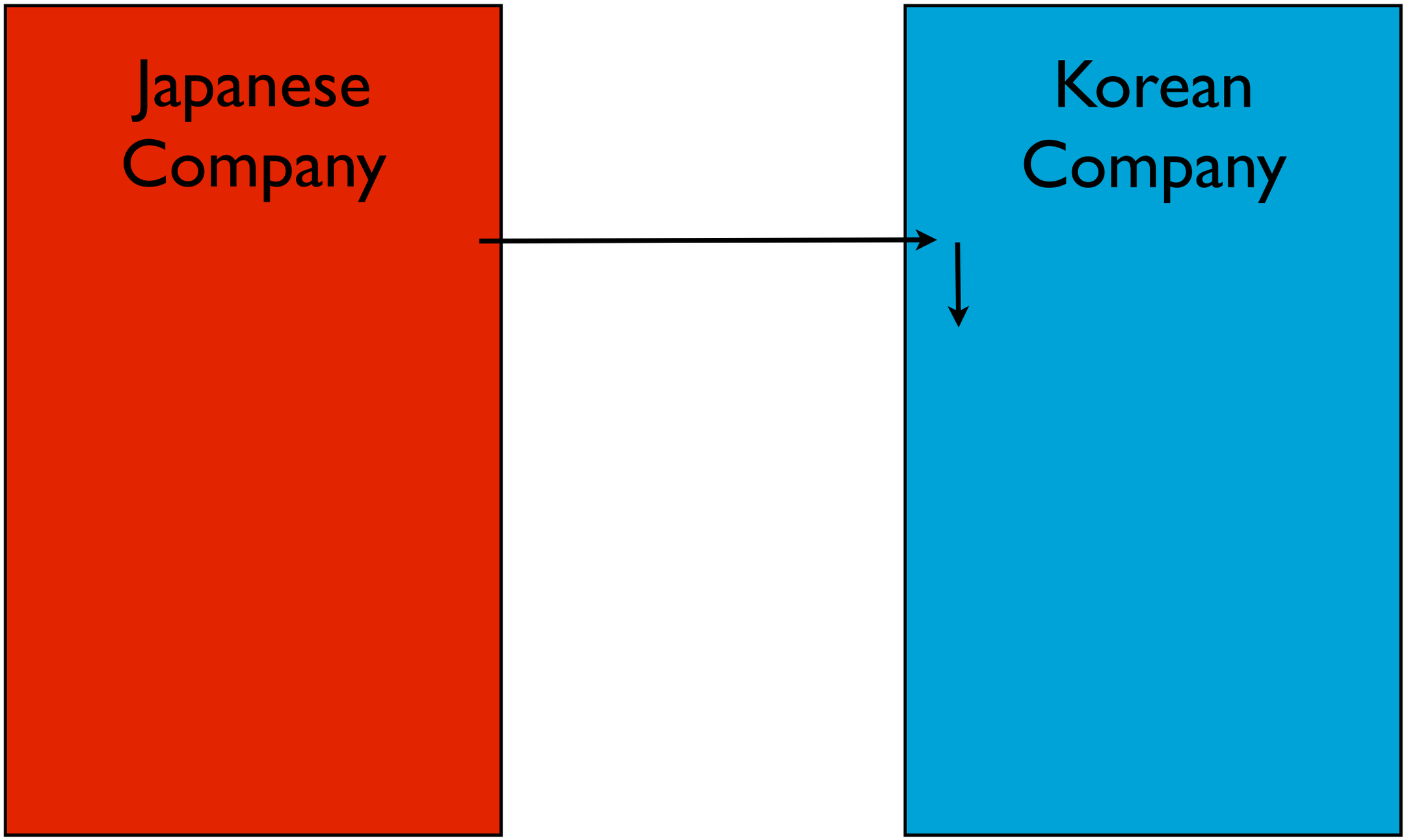
#1 Korean-Japanese Web Development

(The Grand Finale)

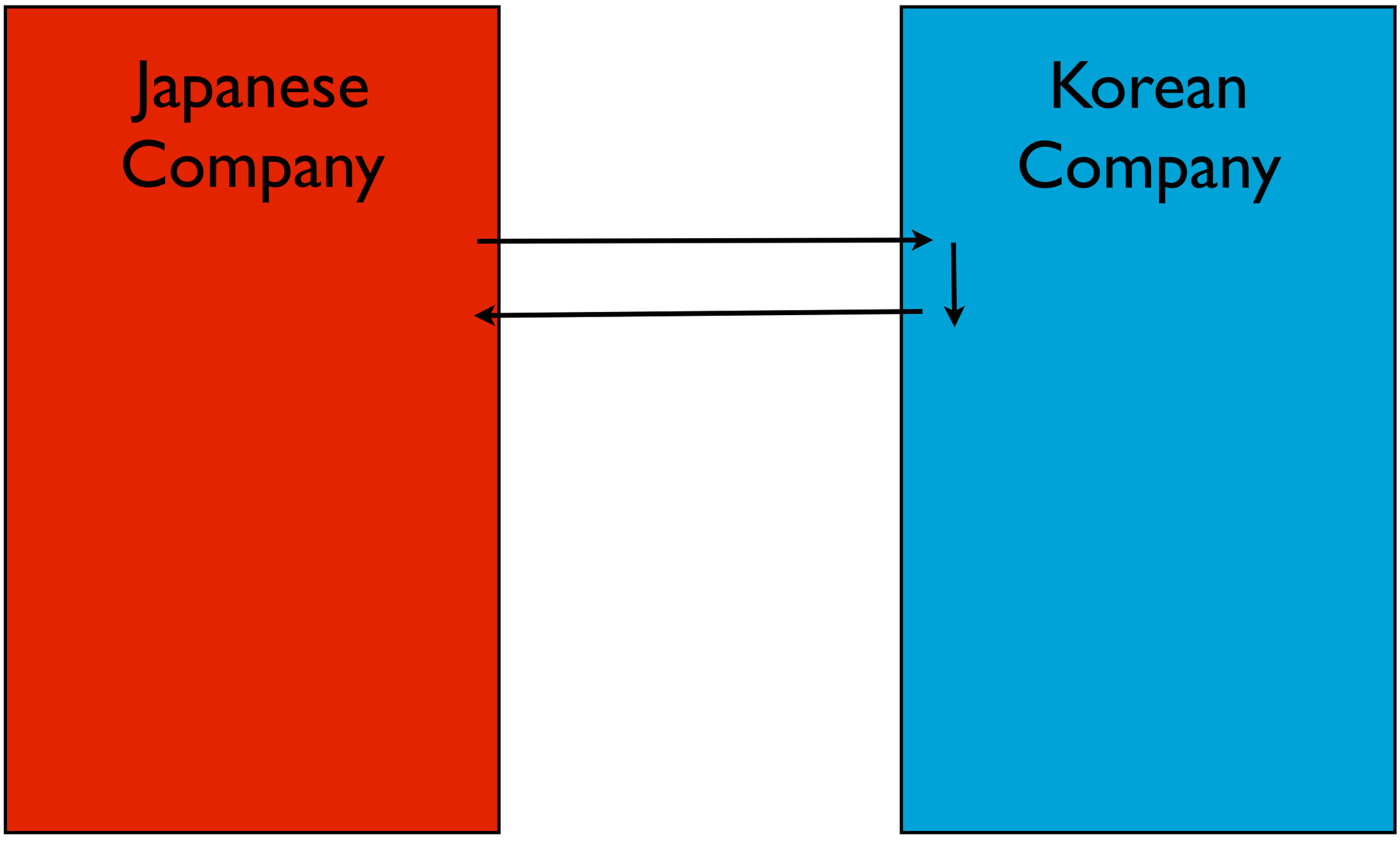
Setting



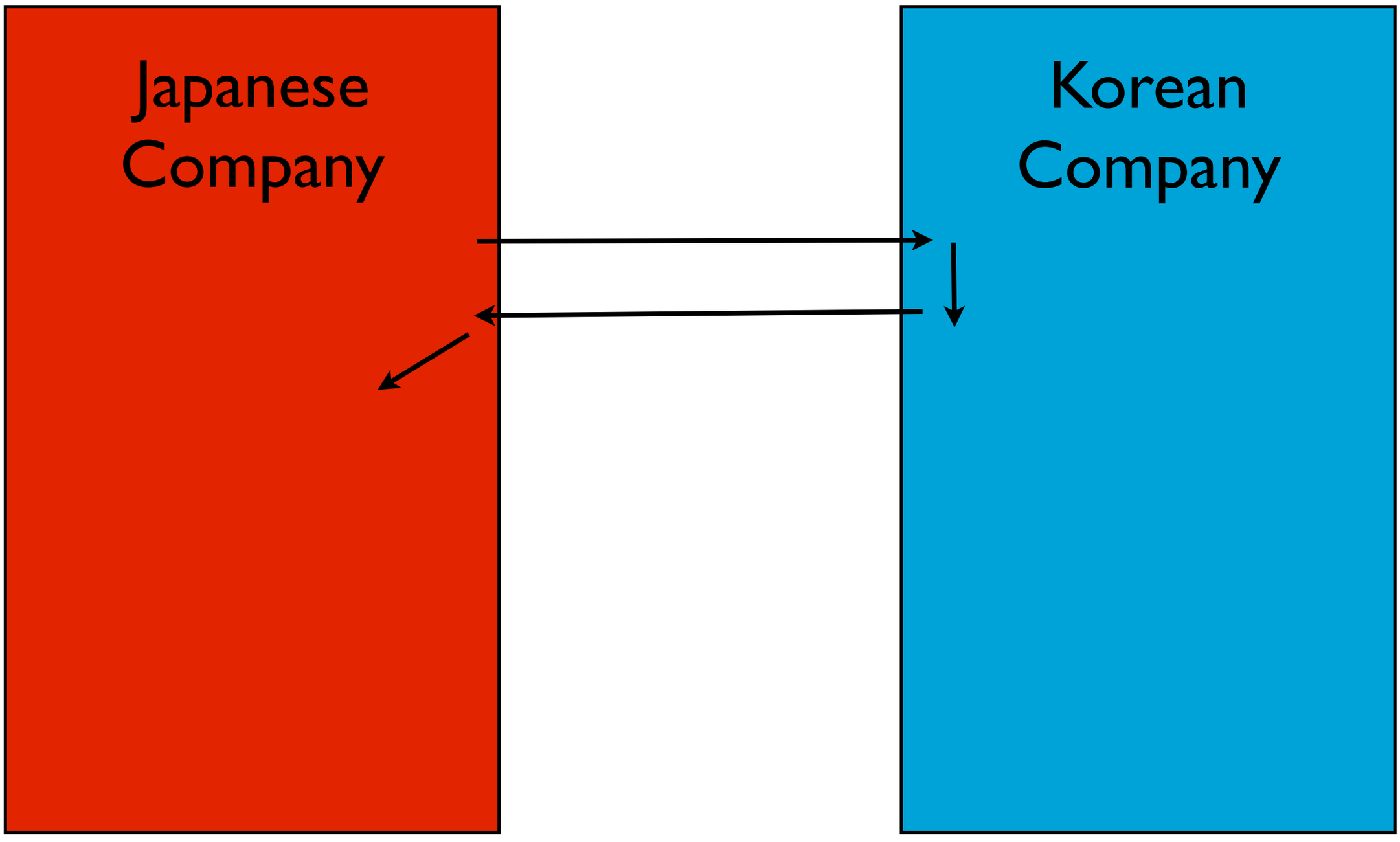
Setting



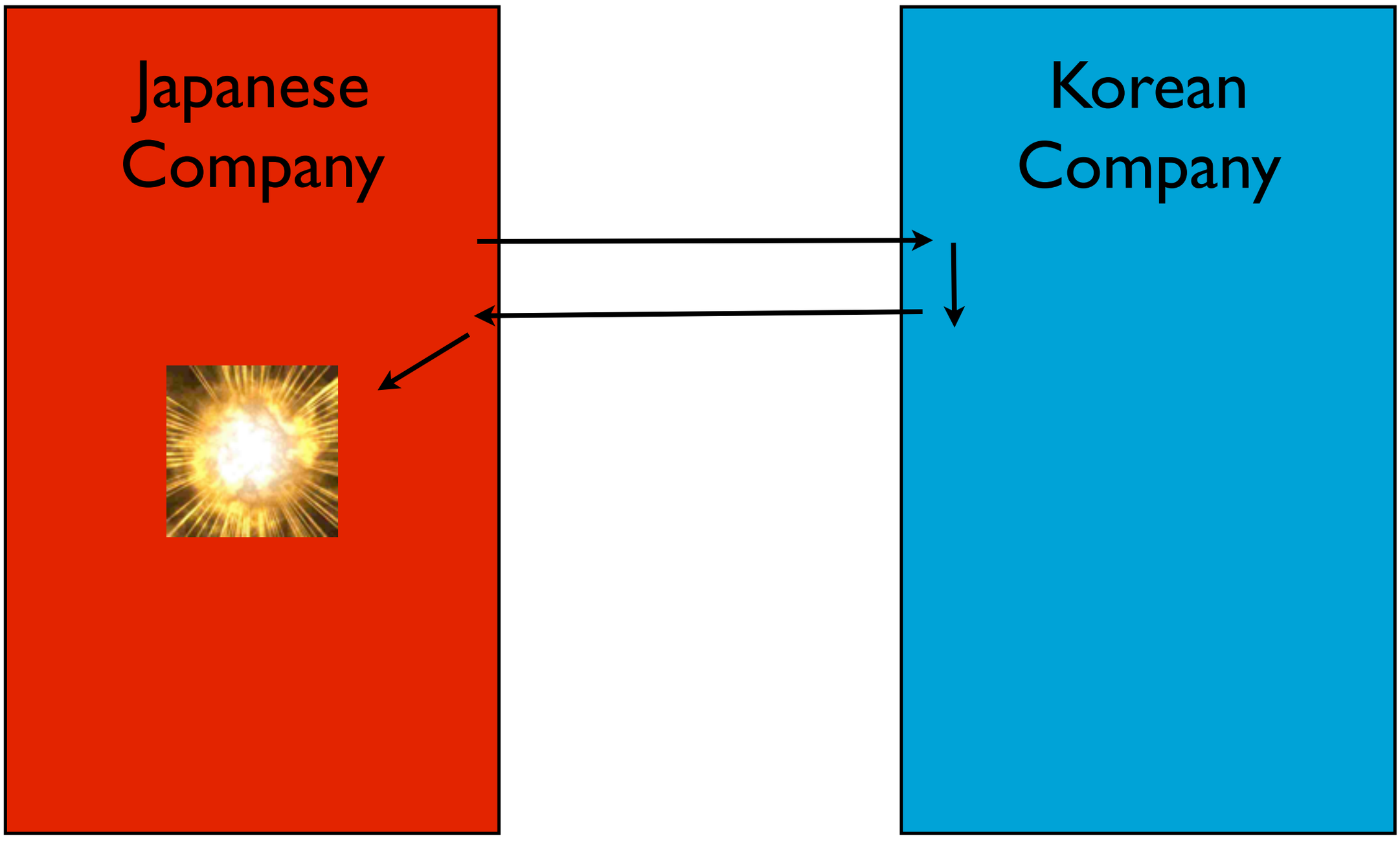
Setting



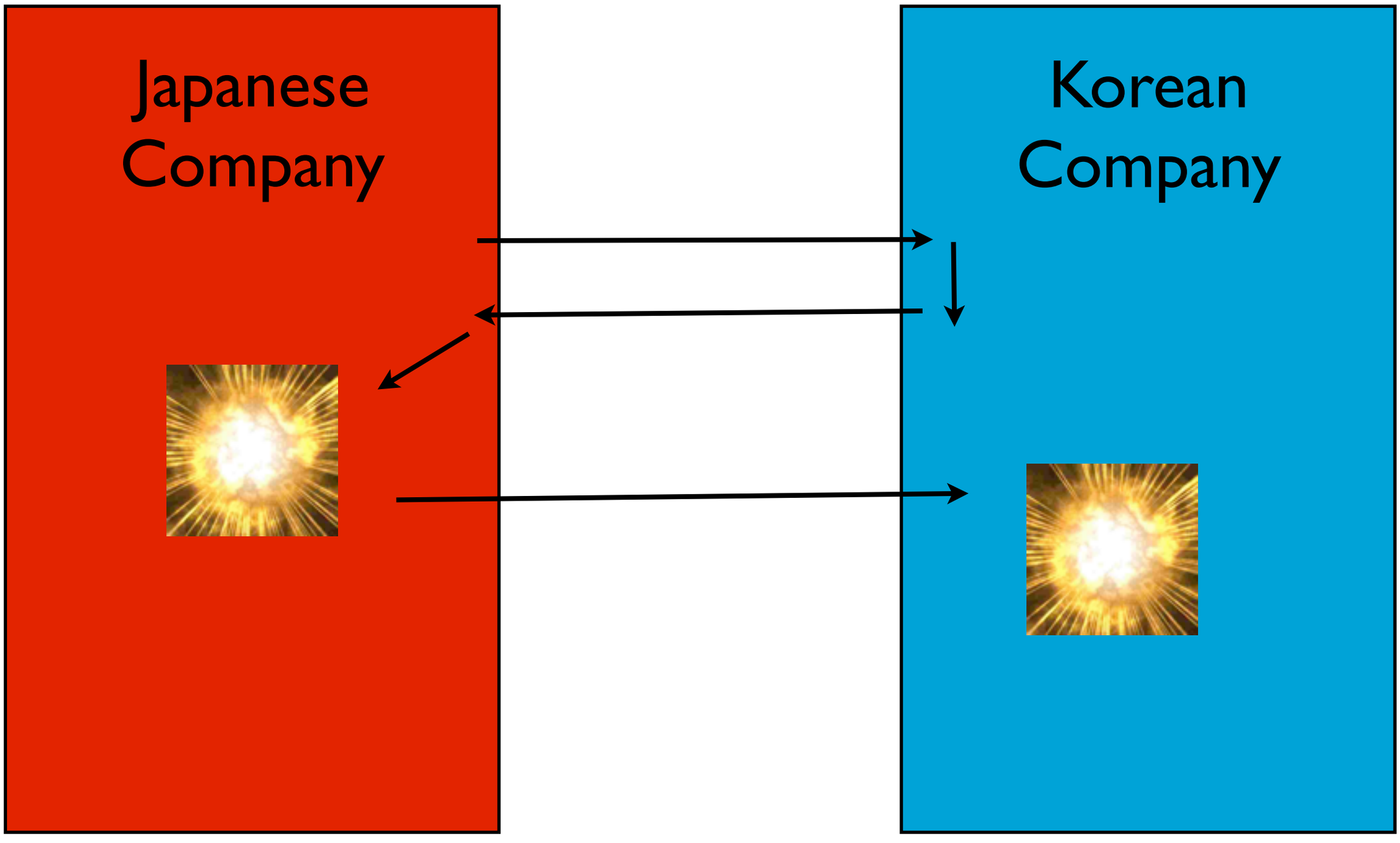
Setting



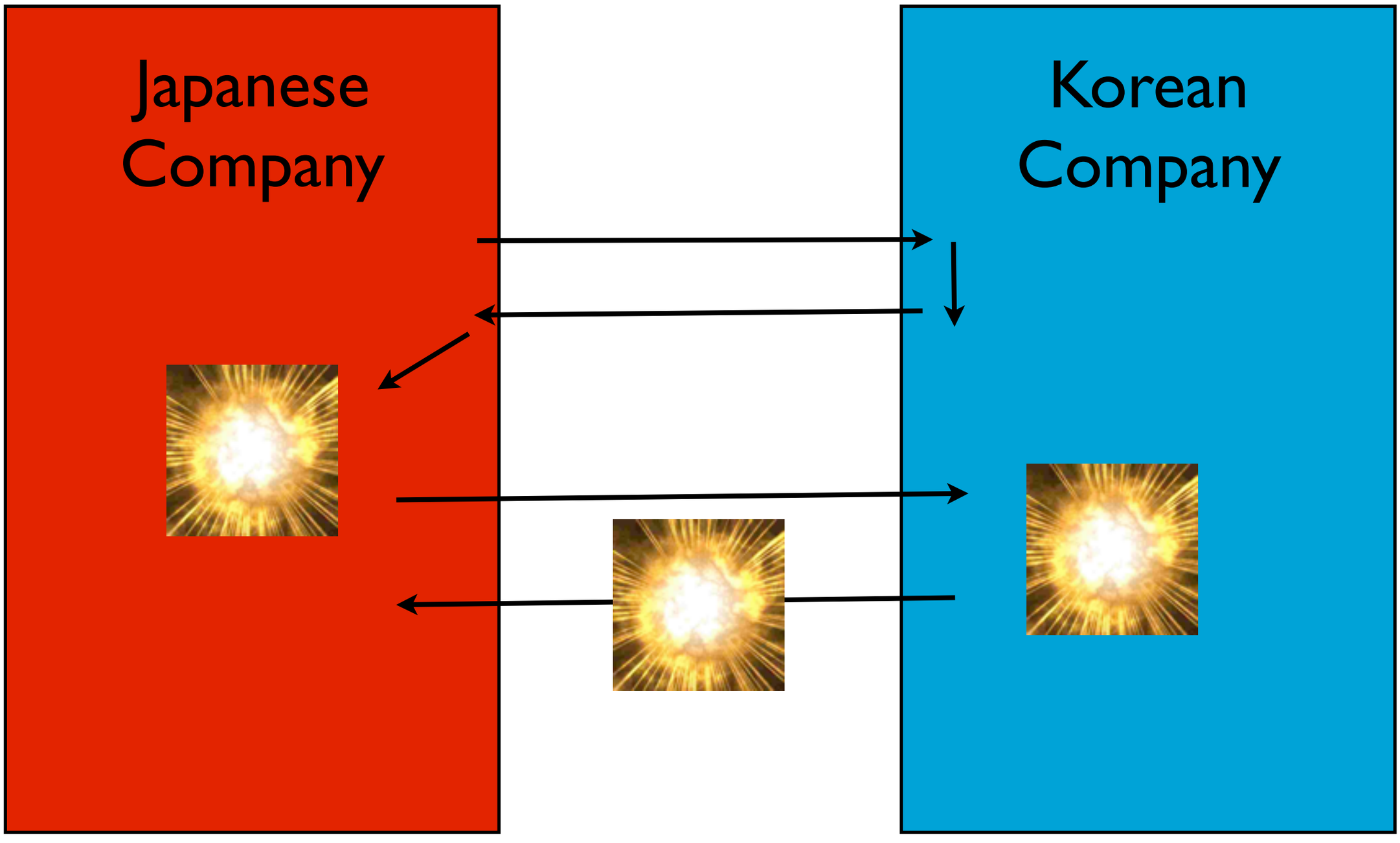
Setting



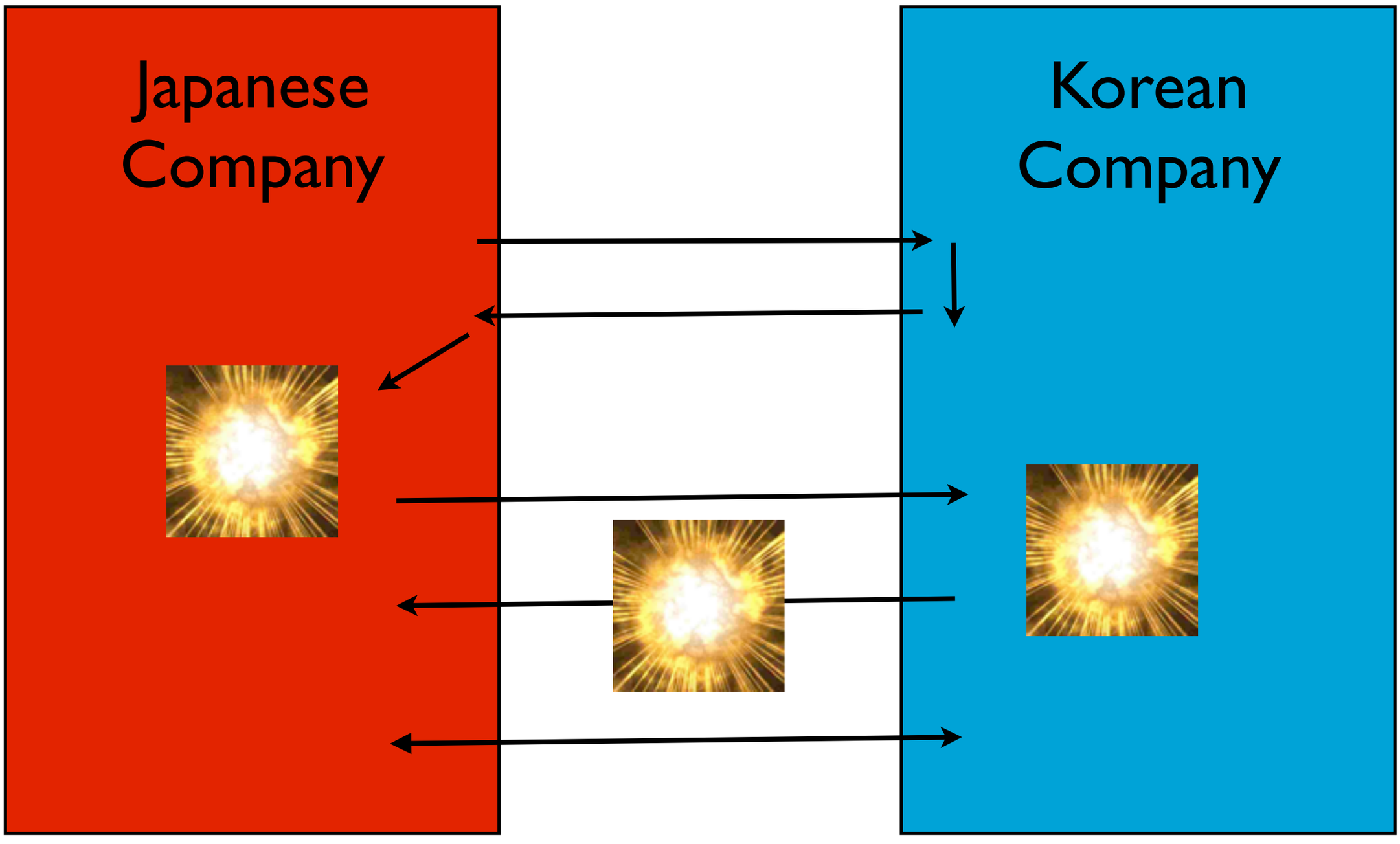
Setting



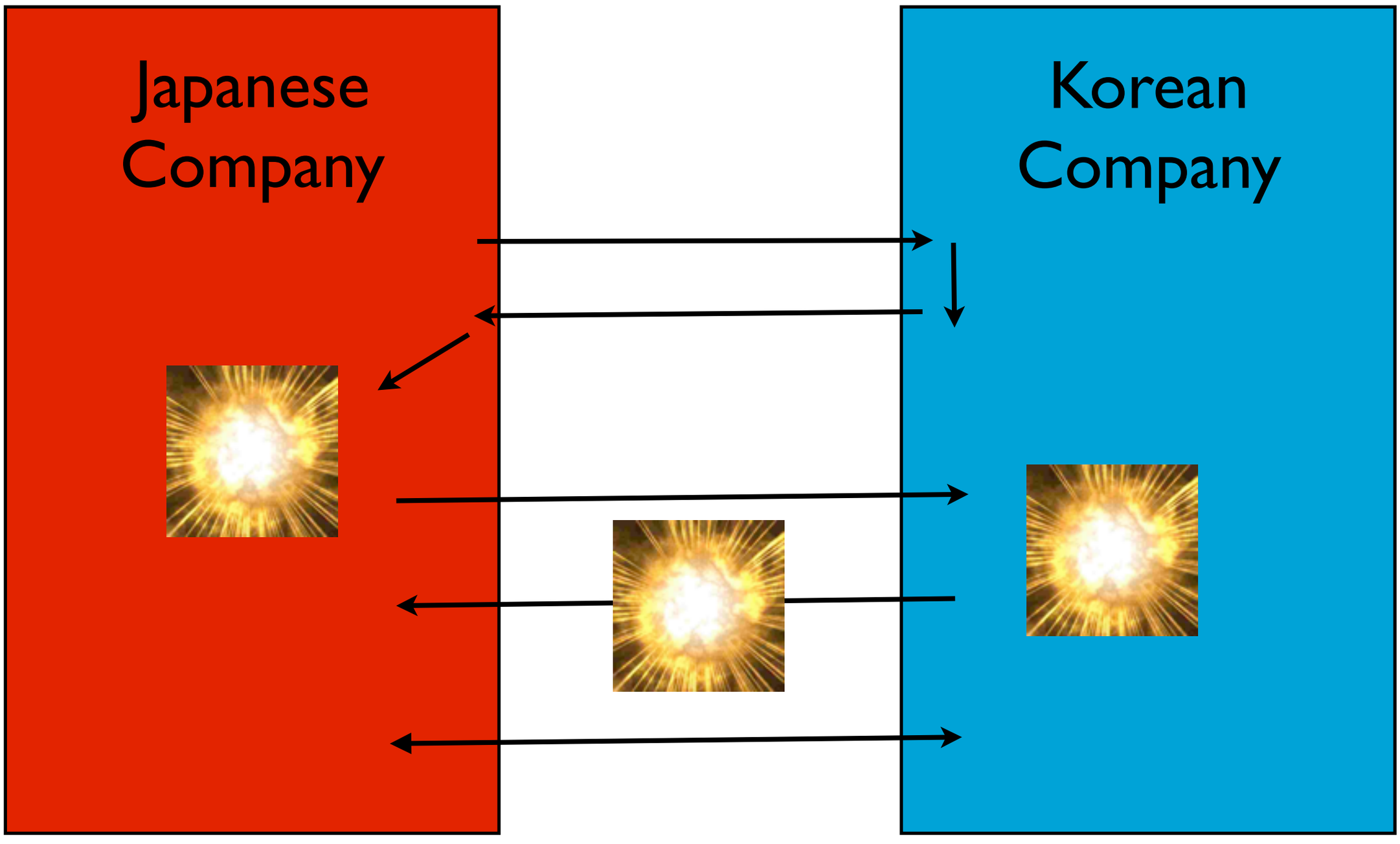
Setting



Setting



Setting



Critical Flaws

- Users not being logged in if name contains special characters
- Too quick session timeout annoying potential users
- Dislike colors
- Annoying SSL error
- Credit Card numbers stored in plain text

Non-Critical Flaws

- SQL Injection on Login Form
- 207 counts of XSS
- Admin console “secured” by JavaScript

Non-Critical Flaws

- SQL Injection on Login Form
- 207 counts of XSS
- Admin console "secured" by JavaScript

"We can launch with those. No one would check that."

SSL


SSL

Are we screwed?

Yes.

\<°_°>/

Questions?

Attribution

- Slide 7 - apple 94
- Slide 8 - paukrus
- Slide 13 - Unknown. If you're the artist, drop me a line and I'll buy you a beer.
- Slide 14 - PSY
- Slide 16 - Anderson Mancini
- Slide 37 - Warner Brothers
- Slide 48 - diloz
- Slide 49 - Martijn Booister
- Slide 55 - Disney
- Slide 96 - Milre
- Slide 174 - PSY
- Slide 188 - d0b33

Thank you for listening!