The Legitimate Vulnerability Market:
The Secretive World of 0-Day Exploit Sales

Charles Miller

Principal Security Analyst

Independent Security Evaluators

June 7, 2007

cmiller@securityevaluators.com

Agenda

- Introduction
- Obstacles faced by researchers
- Potential solutions
- Case studies
- Implications to Internet security
- Conclusions

Why am I here

- Question 1:
  - § iDefense Labs is offering $16-24k for each vulnerability found in applications such as Apache httpd, OpenSSH, Sendmail, IIS
  - § Is this a good deal for researchers?
- Question 2:
  - § In 2006, the U.S. Department of Homeland Security gave $1.24 million to Stanford and Coverity to hunt bugs in open source software
  - § Is this the best use of money to find vulnerabilities?
- What do the answers to these questions mean for Internet security in general?

Introduction

- Vulnerabilities have been bought and sold for many years
- A few programs exist which pay researchers for vulnerability information:
  - § Zero Day Initiative (TippingPoint)
  - § Vulnerability Contributor Program (iDefense)
  - § Exploit Acquisition Program (SNOsoft)
- Some companies sell tools or packages containing 0-day exploits
  - § Ultimate 0day Exploits Pack (Argeniss)
  - § VulnDisco Pack (GLEG)
  - § Canvas (IMMUNITY)
- How can a researcher get paid a fair value in the legal vulnerability market?

Obstacles faced

Time sensitivity

- Vulnerability information is only valuable when it is not widely known
- A patch can make it worthless
- Other technologies, SElinux, /GS flag, other patches, newer versions can reduce the value
- Researcher doesn't have knowledge of when these things will occur (except "Patch Tuesday")
- Therefore, researchers must be able to locate a buyer and complete a sale quickly

No pricing transparency

Vulnerability/Exploit	Value	Source
“Some exploits”	$200,000 - $250,000	A government official referring to what “some people” pay
a “real good” exploit	over $100,000	Official from SNOsoft research team
Vista exploit	$50,000	Raimund Genes, Trend Micro
“Weaponized exploit”	$20,000-$30,000	David Maynor, SecureWorks
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks
WMF exploit	$4000	Alexander Gostev, Kaspersky
Microsoft Excel	> $1200	Ebay auction site
Mozilla	$500	Mozilla bug bounty program

Difficulty finding buyers

- No public marketplace
- Must contact many potential buyers
- Companies do not advertise that they buy vulnerabilities
- Good luck contacting the government
- Perhaps vendors should buy this information...

Checking the buyer

- How does the researcher verify that a buyer is legitimate, i.e. not a terrorist or criminal?
- Need trusted third parties

Value cannot be demonstrated without loss

- Once the vulnerability is shown to a potential buyer, why should they pay for it?
- Demonstrating via exploit is no better
- Giving too much vague information can reveal the vulnerability
  - § Version
  - § Authentication
  - § Stability
- Typically, buyers require seeing the exploit/ vulnerability information before they send payment (or even make an offer)

Exclusivity

- How does the researcher guarantee exclusivity of rights?
- “Sometimes we get burnt, sometimes not” - Dave Aitel

Solutions

Small steps

- Post a hash of the exploit
- “Mutually assured destruction”
- Proving the exploit exists
  - § can be done in person

Market place solutions

- Of the 5 market types suggested by Bohme in “Vulnerability Markets”, only one
  - § Doesn’t require vendor initiation and
  - § Has immediate incentive for researcher
- Exploit derivatives
  - § Contracts which pay based on whether vulnerability events occur
  - § Researchers benefit with “insider” knowledge
  - § Advantage: no exploits need to actually be sold.
  - § Disadvantage: unclear how much researchers could make.
  - § Requires a TTP

Direct auction

- Sell exploit to the highest bidder(s)
- Has been tried via Ebay
- Could use “reputational” system
- Could offer escrow services
- Visibility into pricing and vulnerability information is obtained
- Drawbacks: legality, exclusivity

Case studies

Case Study #1 - Samba

- Summer of 2005, I discovered a remote vulnerability in Samba - a common Linux server:


```
static BOOL lsa_io_trans_names(const char *desc, LSA_TRANS_NAME_ENUM2 *trn, prs_struct *ps, int
depth)
{
...
        if(!prs_uint32("num_entries     ", ps, depth, &trn->num_entries))
...
        if (trn->ptr_trans_names != 0) {
                if(!prs_uint32("num_entries2    ", ps, depth, &trn->num_entries2))
                        return False;
....
                if (UNMARSHALLING(ps)) {
                        if ((trn->name = PRS_ALLOC_MEM(ps, LSA_TRANS_NAME2, trn->num_entries)) ==
NULL) {
                                return False;
...
                }

                for (i = 0; i < trn->num_entries2; i++) {
...

                        if(!lsa_io_trans_name2(t, &trn->name[i], ps, depth))
```

Timeline

6/2005

5/2007

Timeline

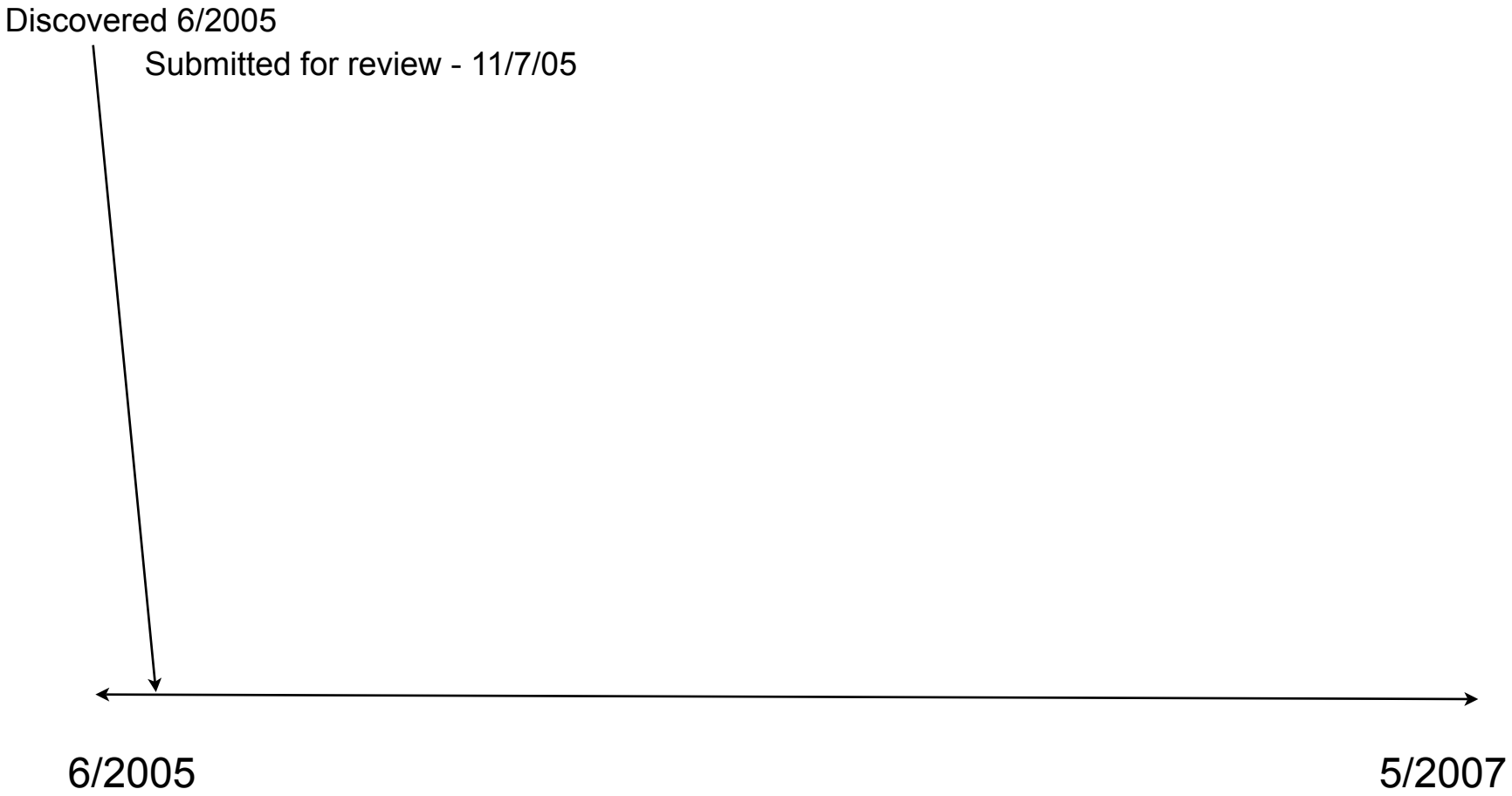
Discovered 6/2005

6/2005

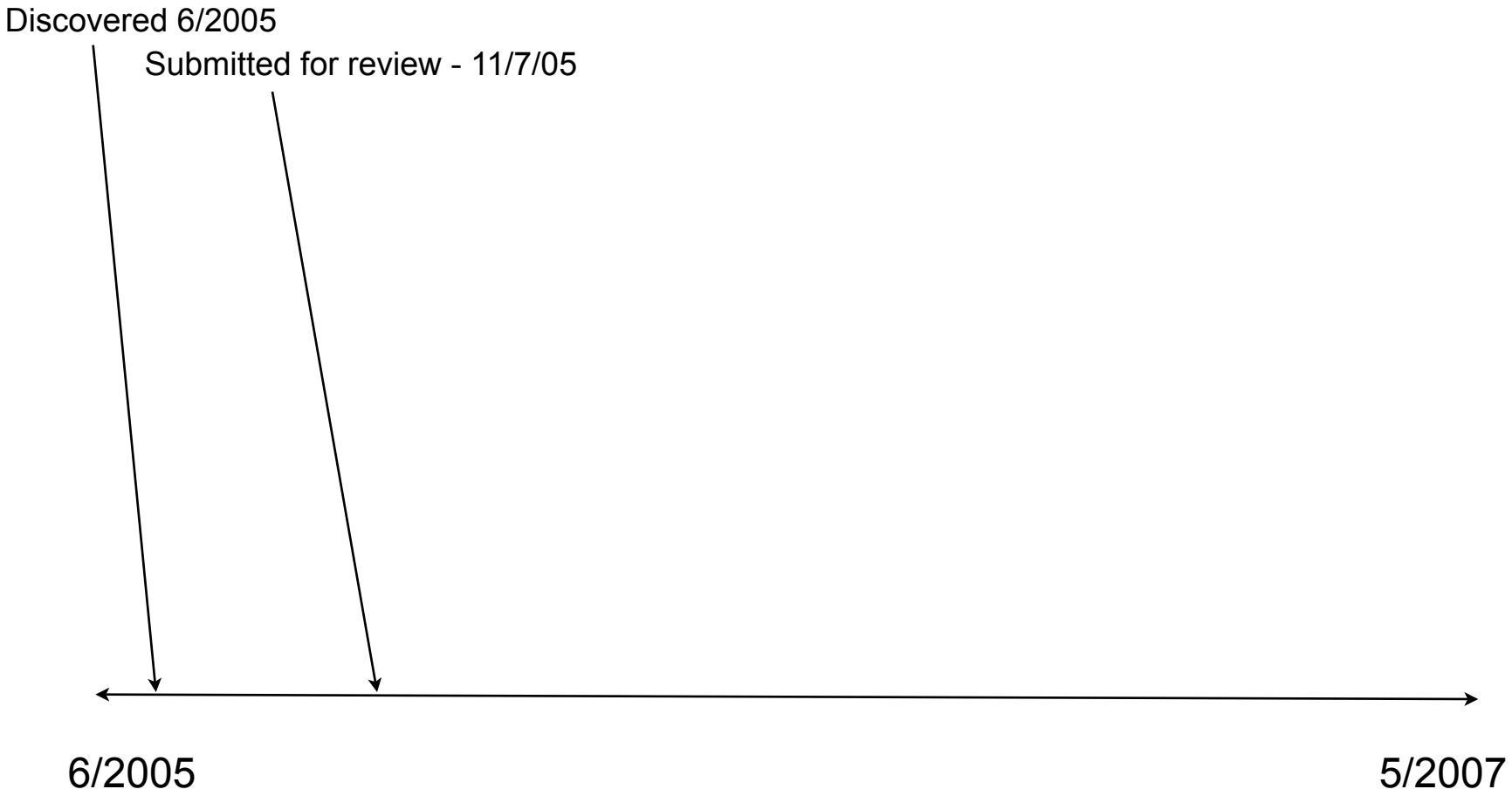
5/2007

Timeline

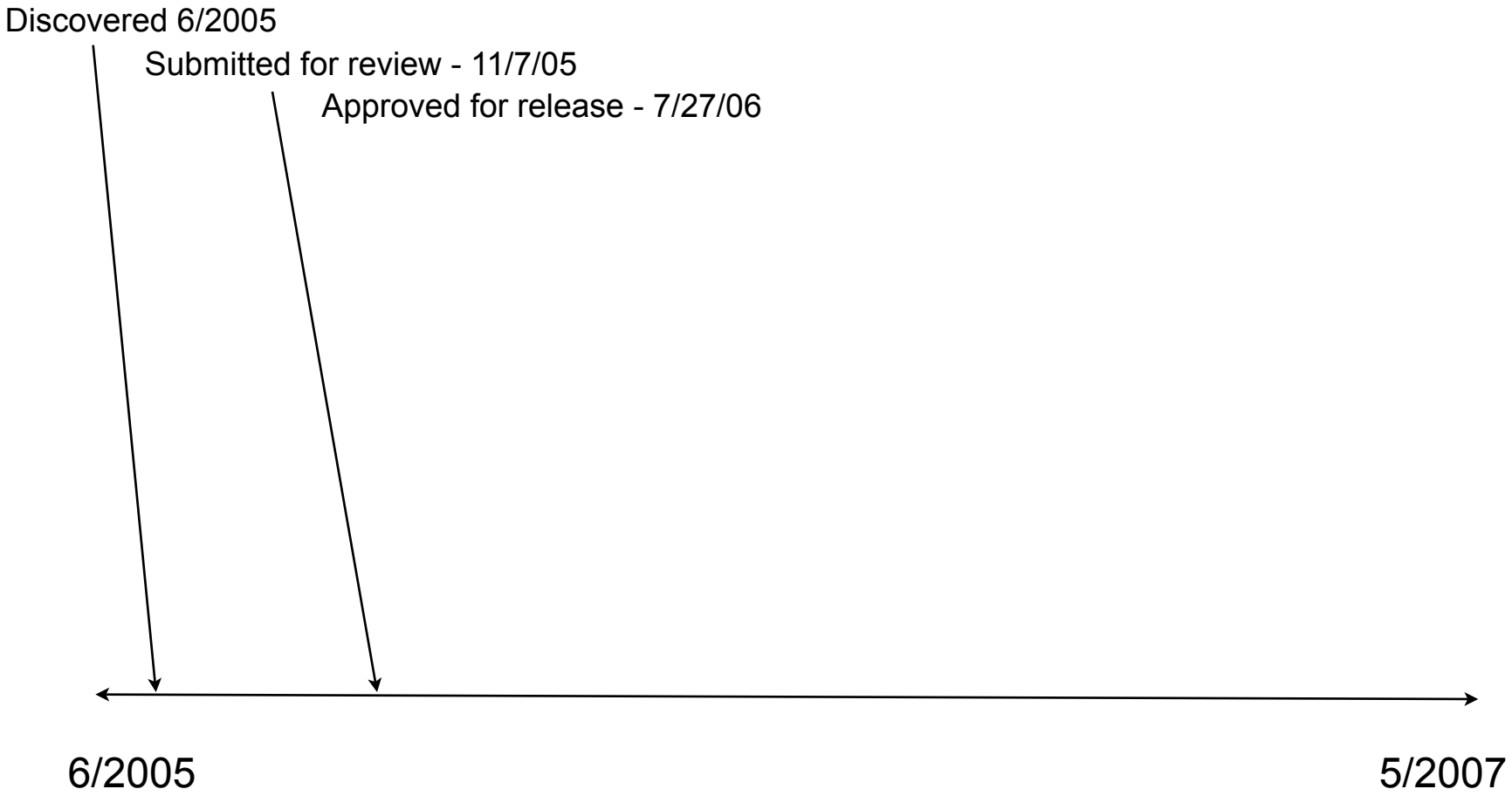
Timeline



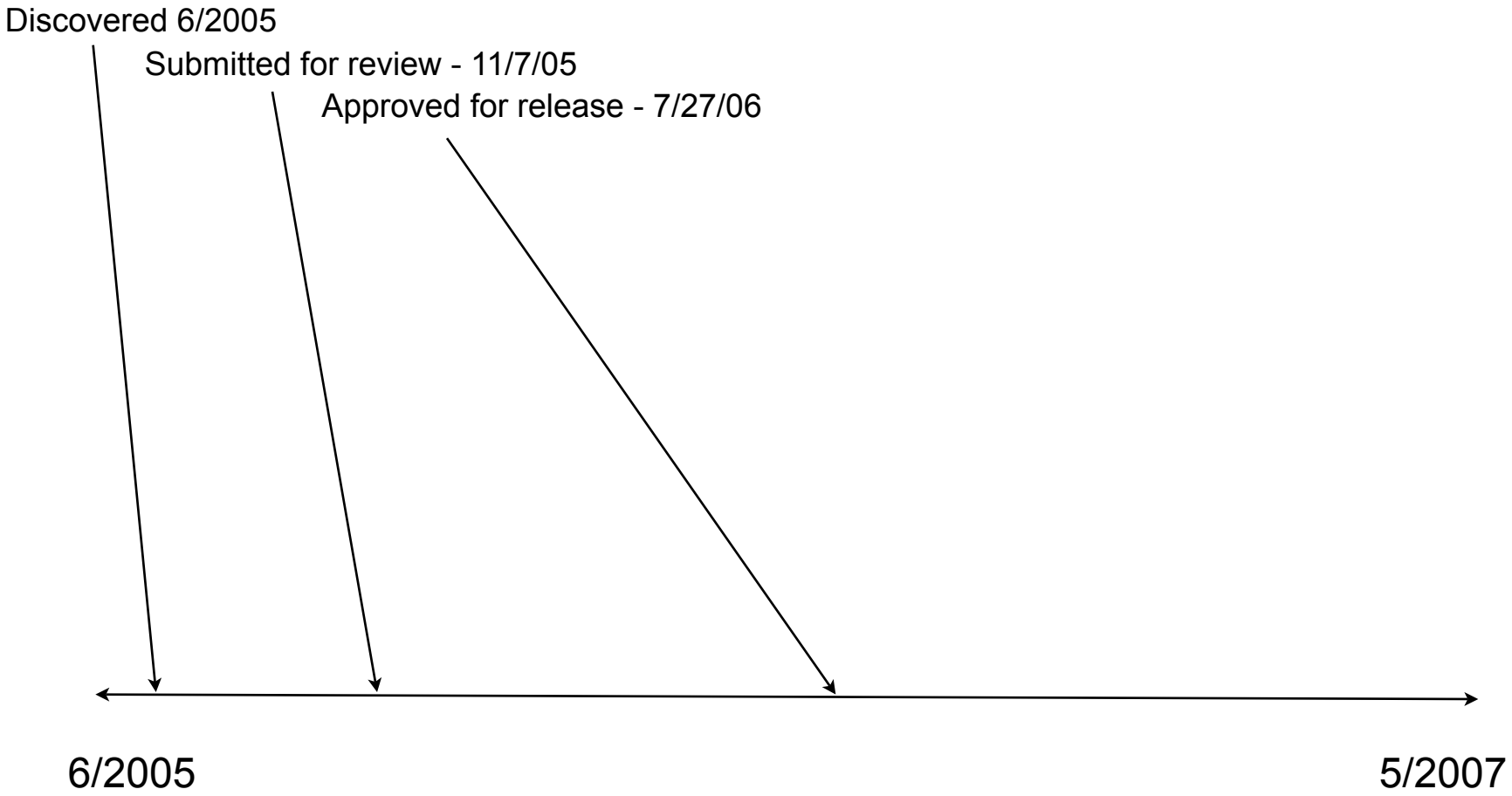
Timeline



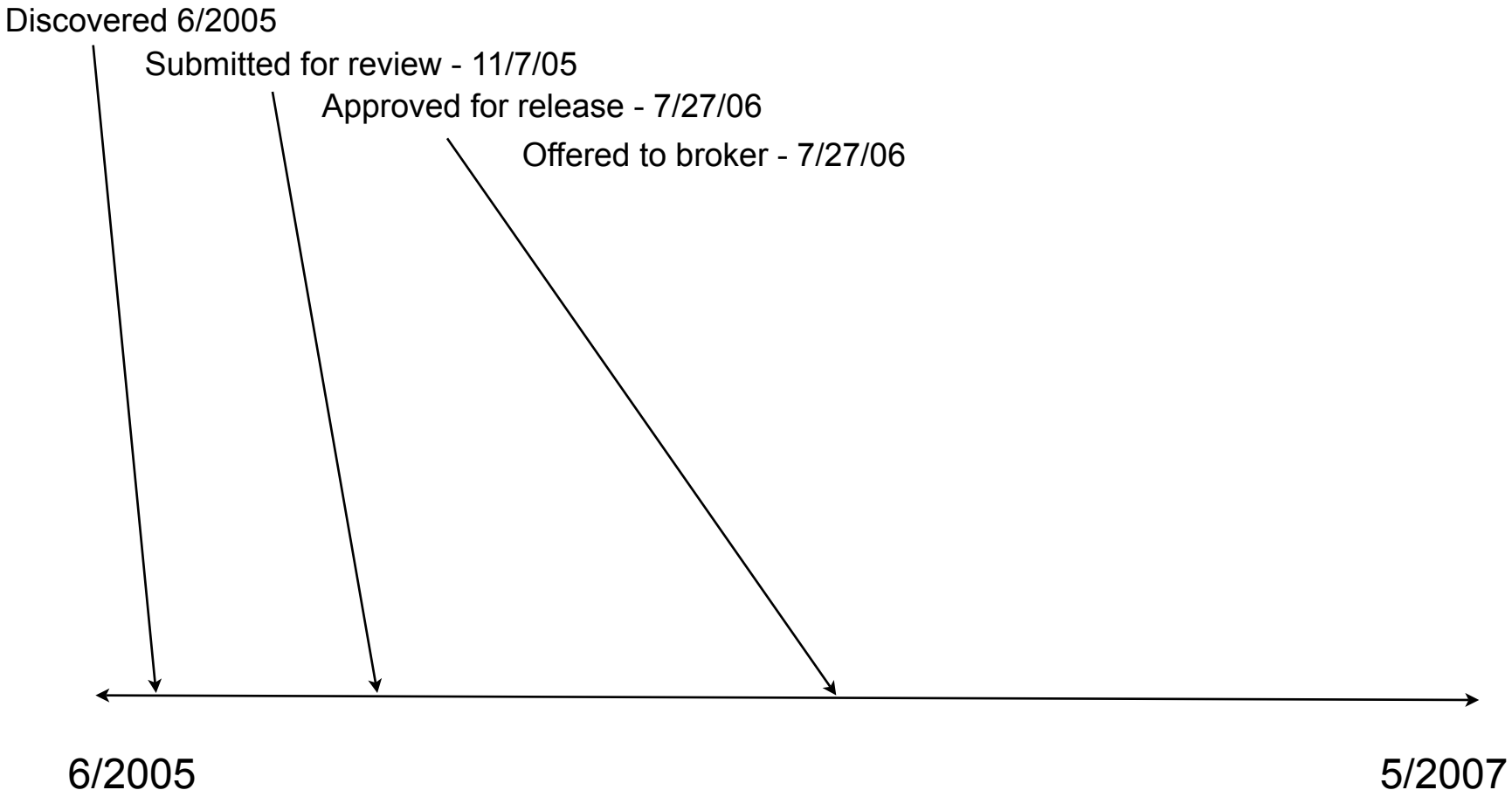
Timeline



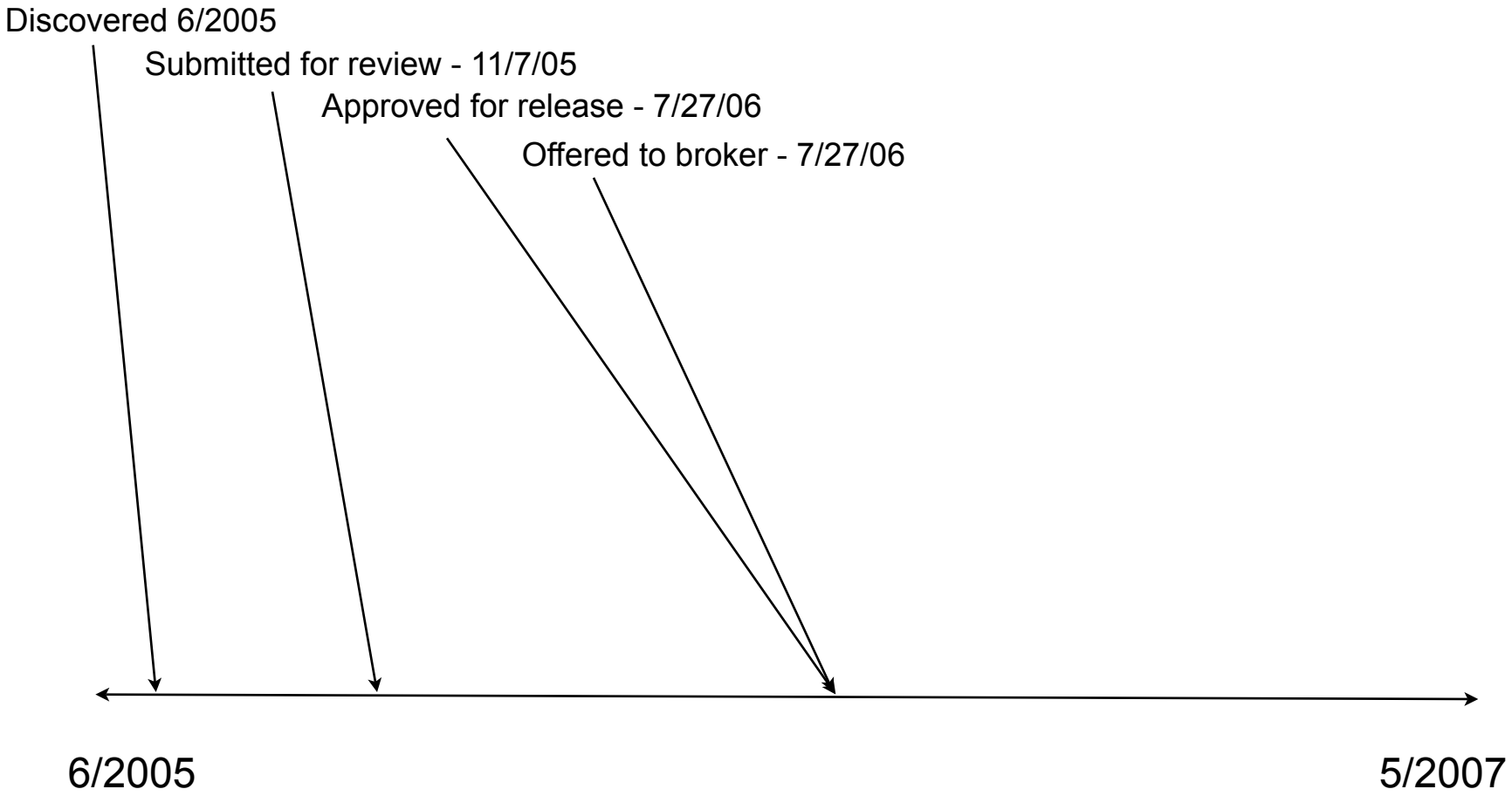
Timeline



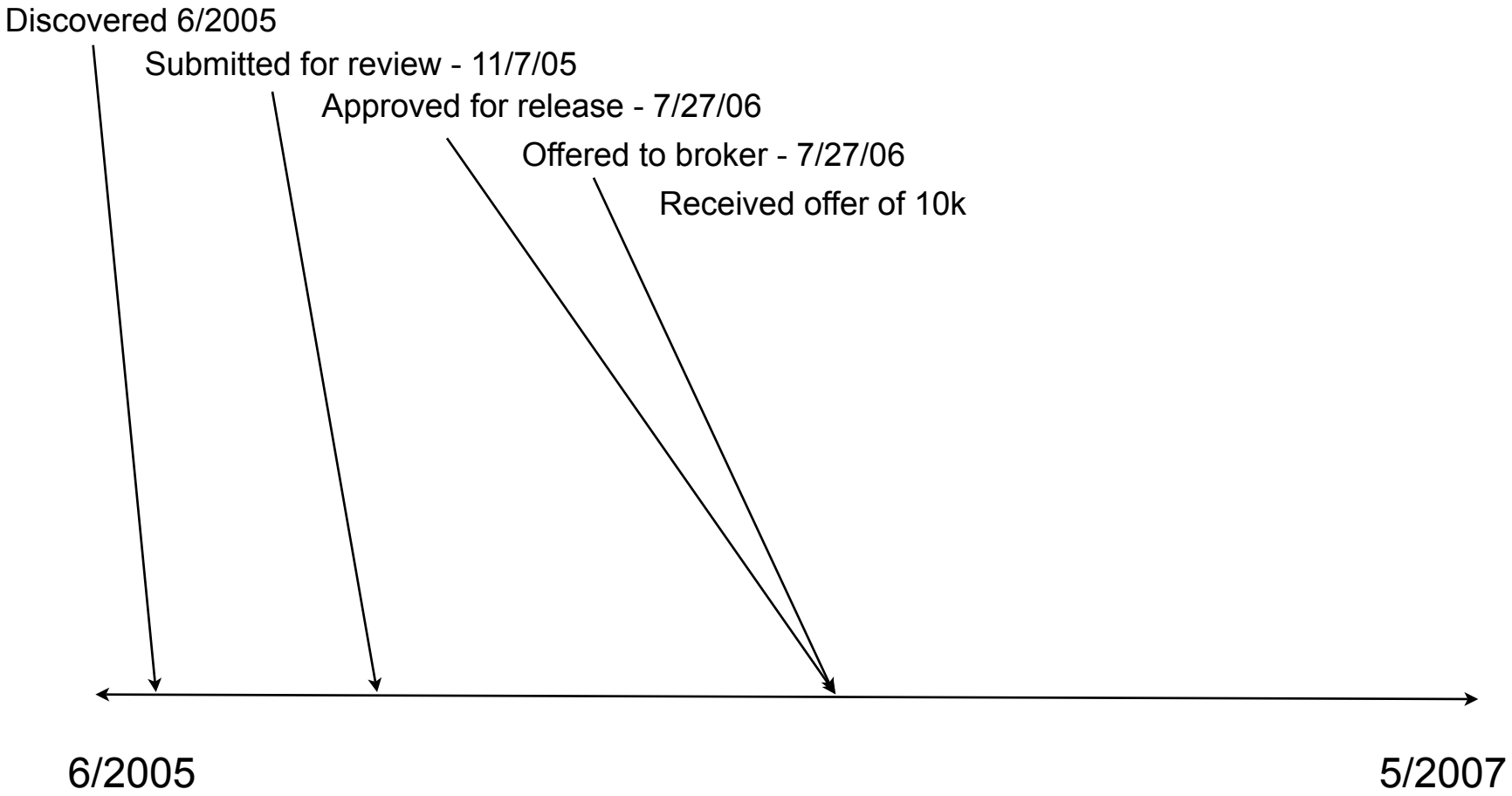
Timeline



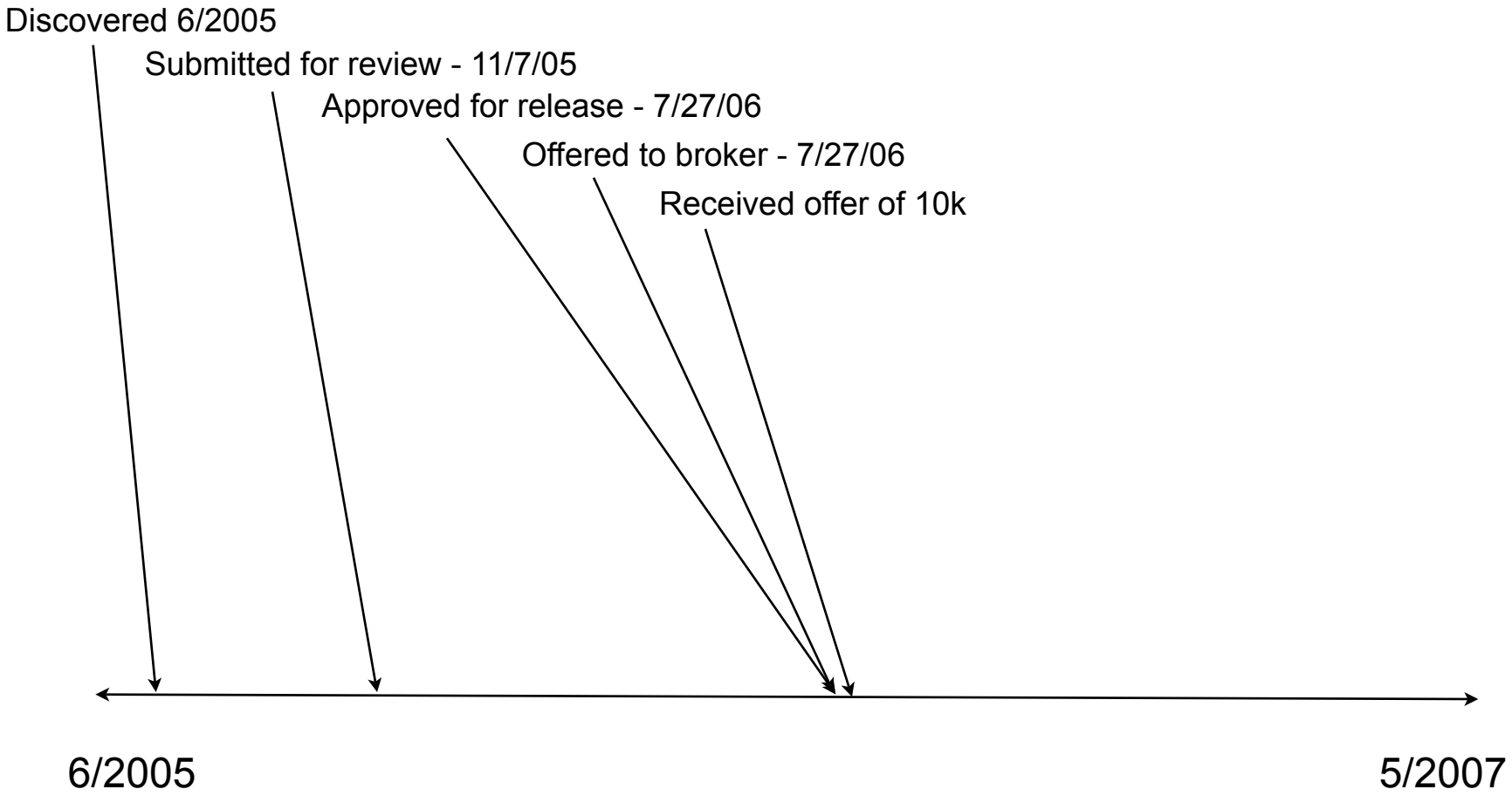
Timeline



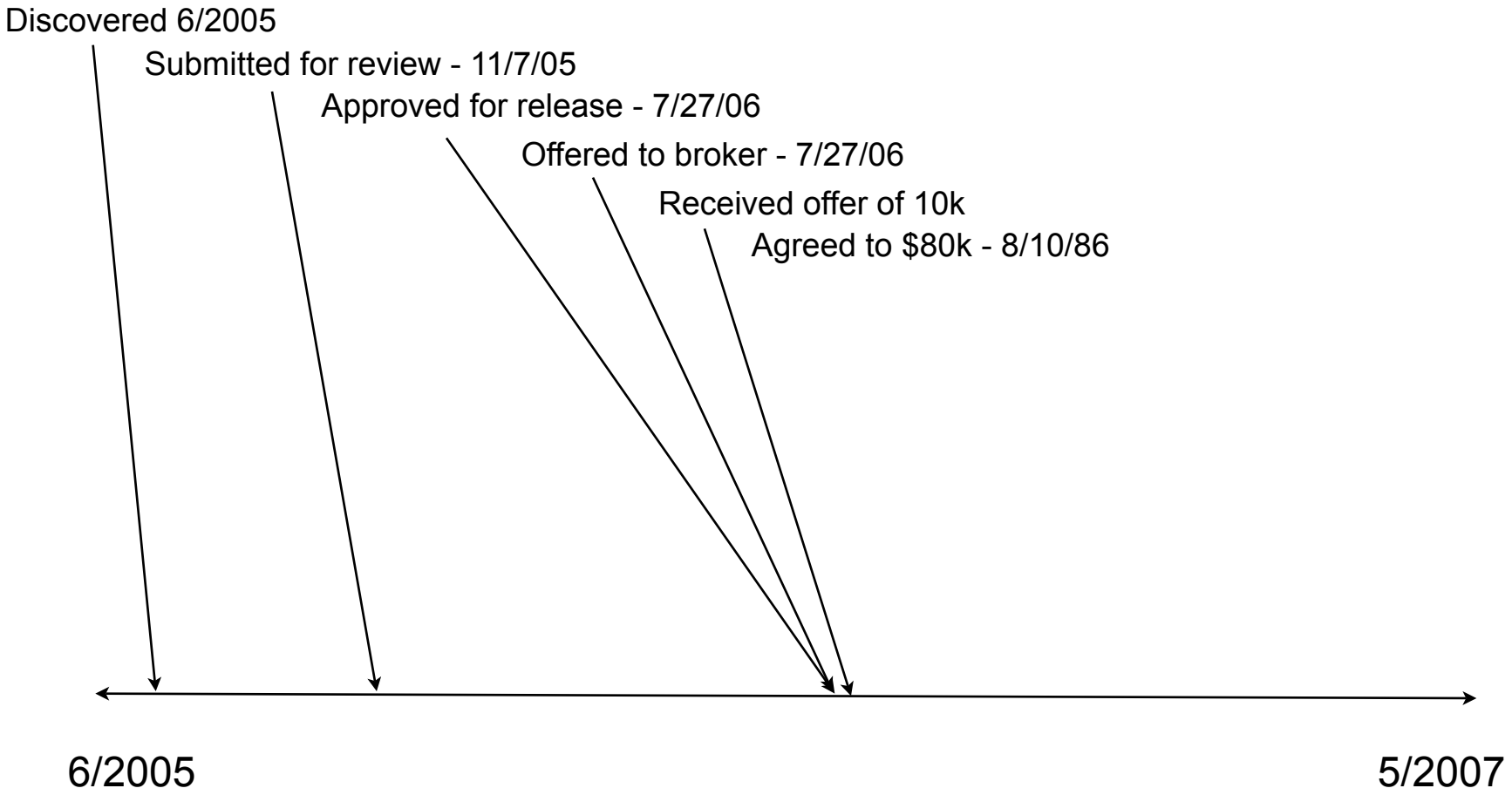
Timeline



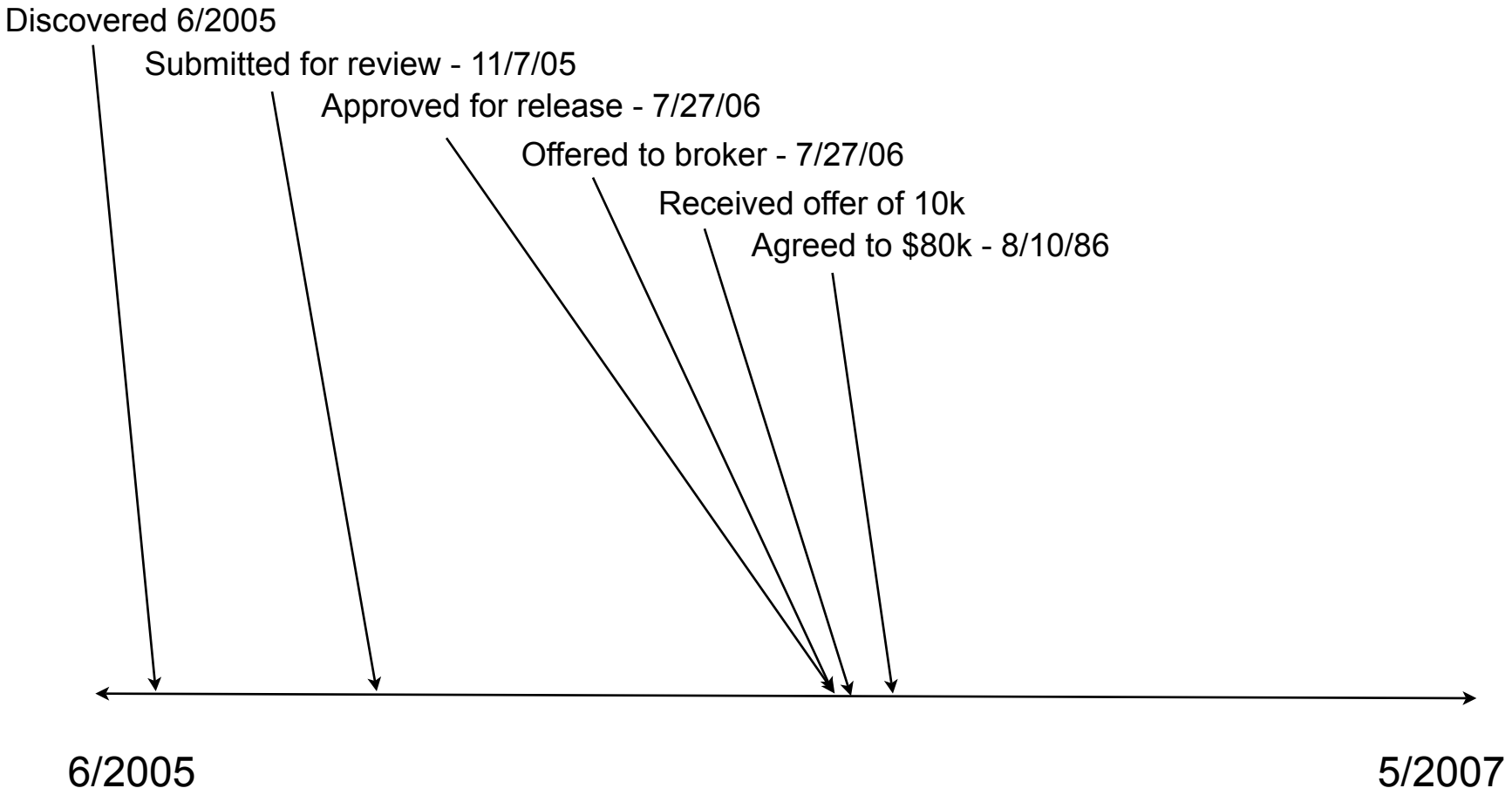
Timeline



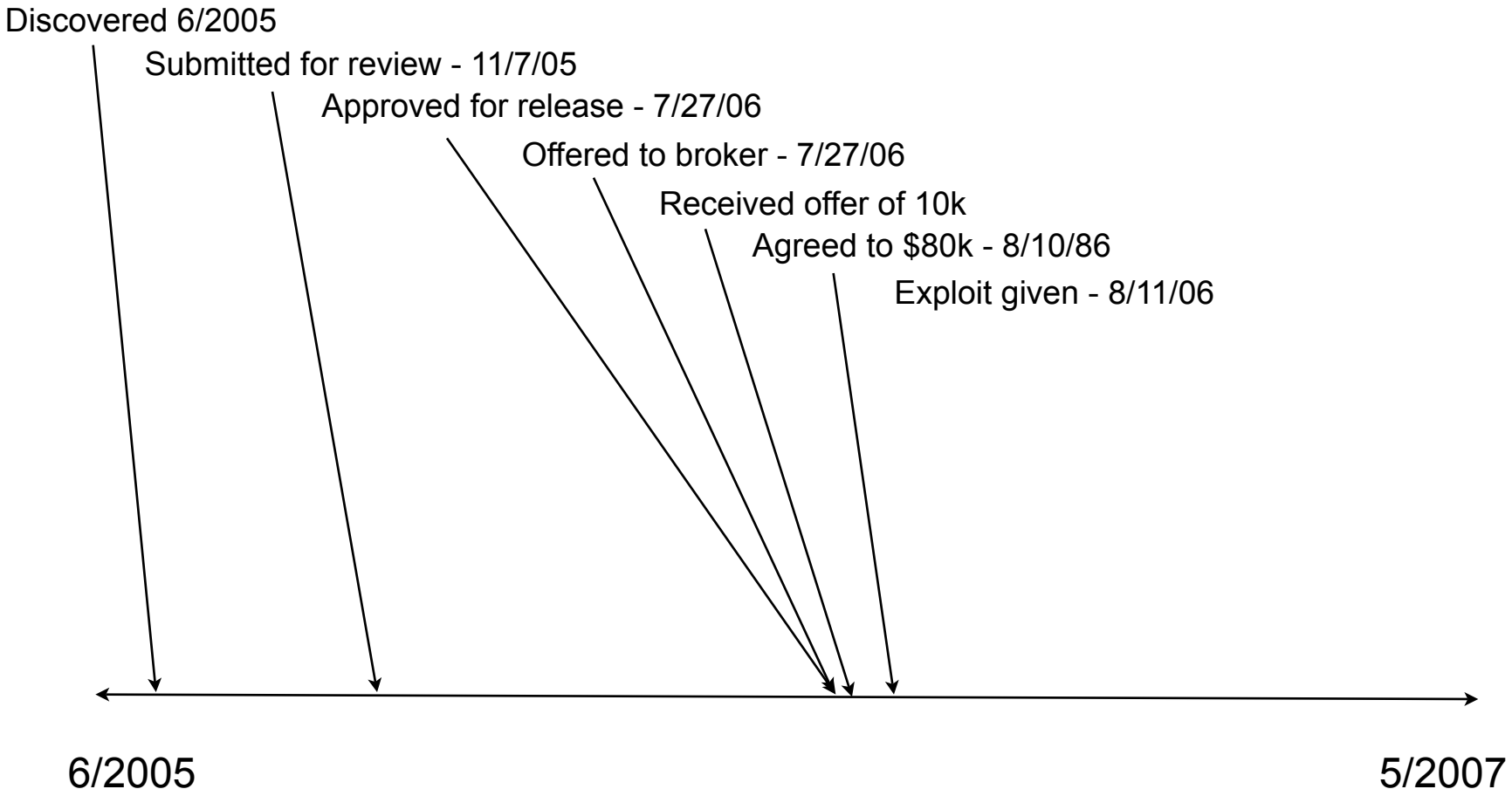
Timeline



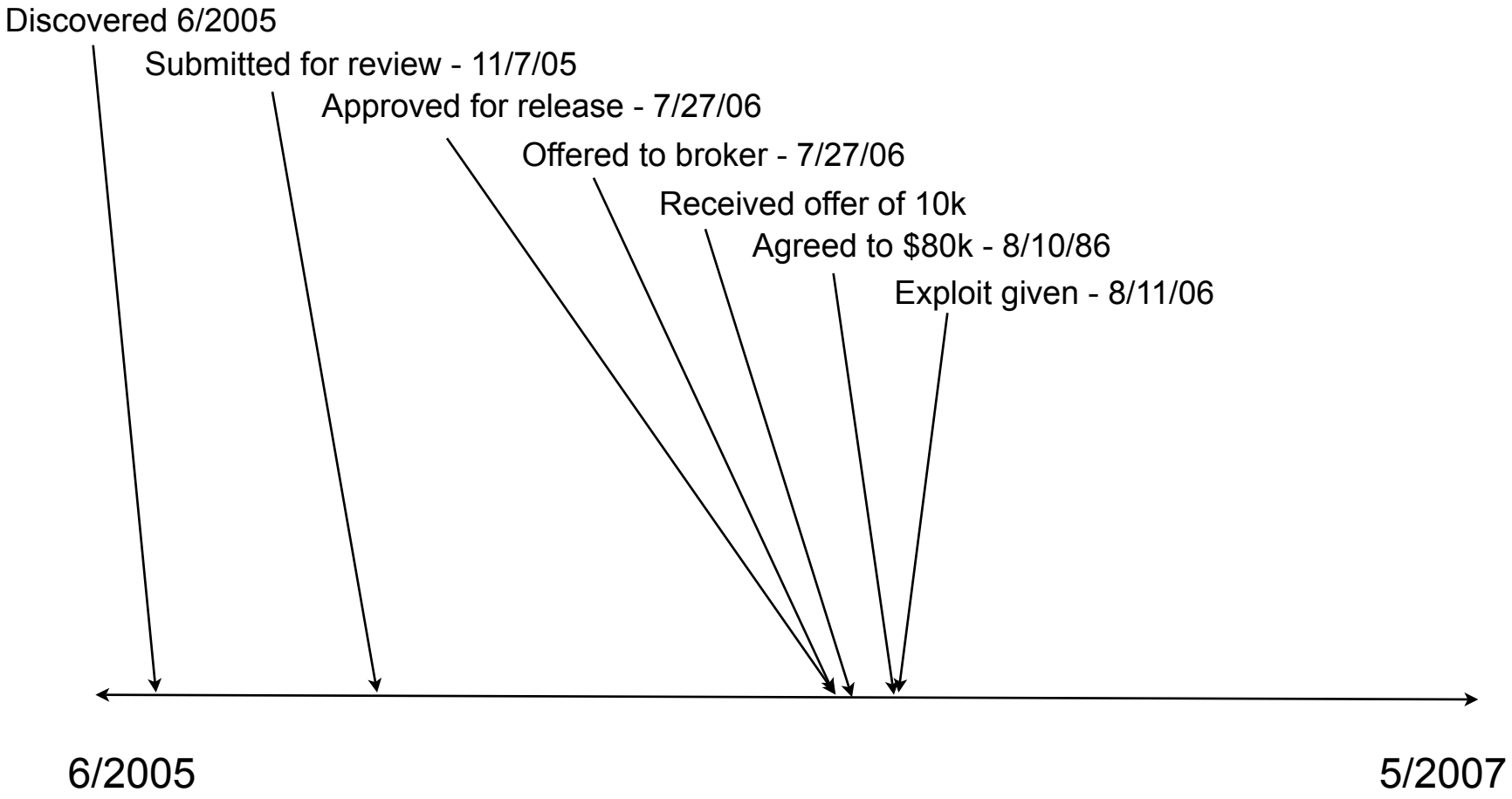
Timeline



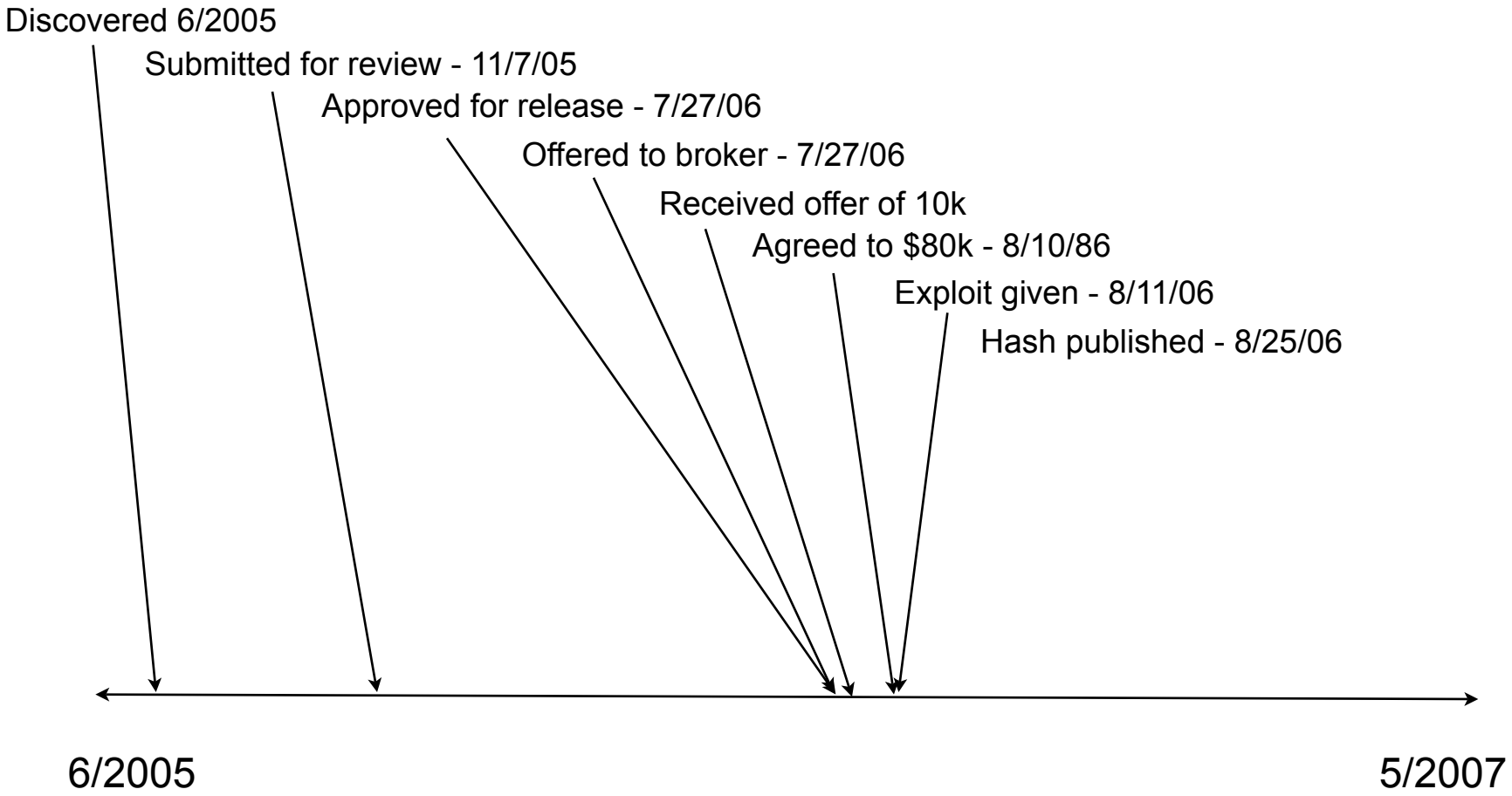
Timeline



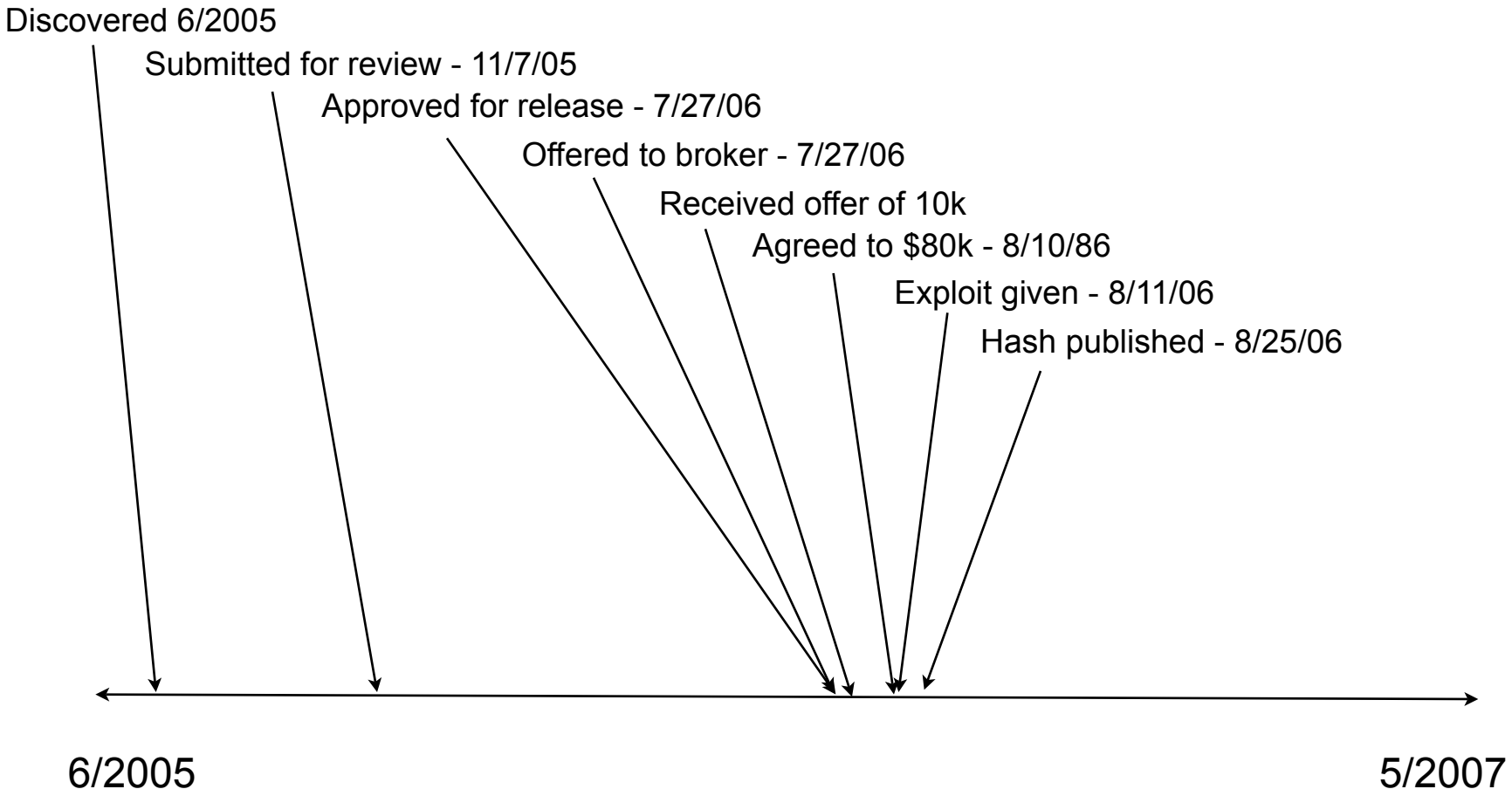
Timeline



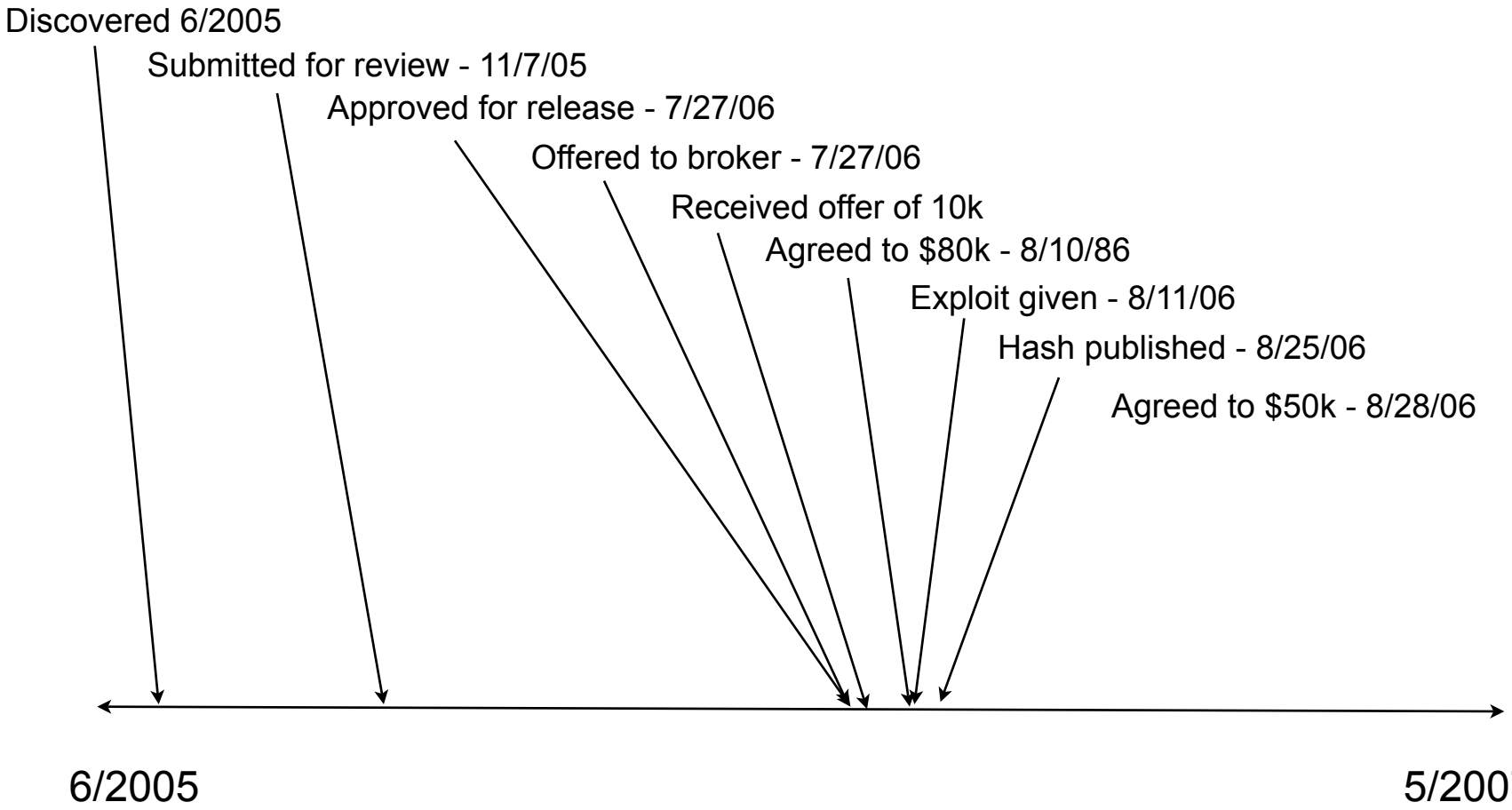
Timeline



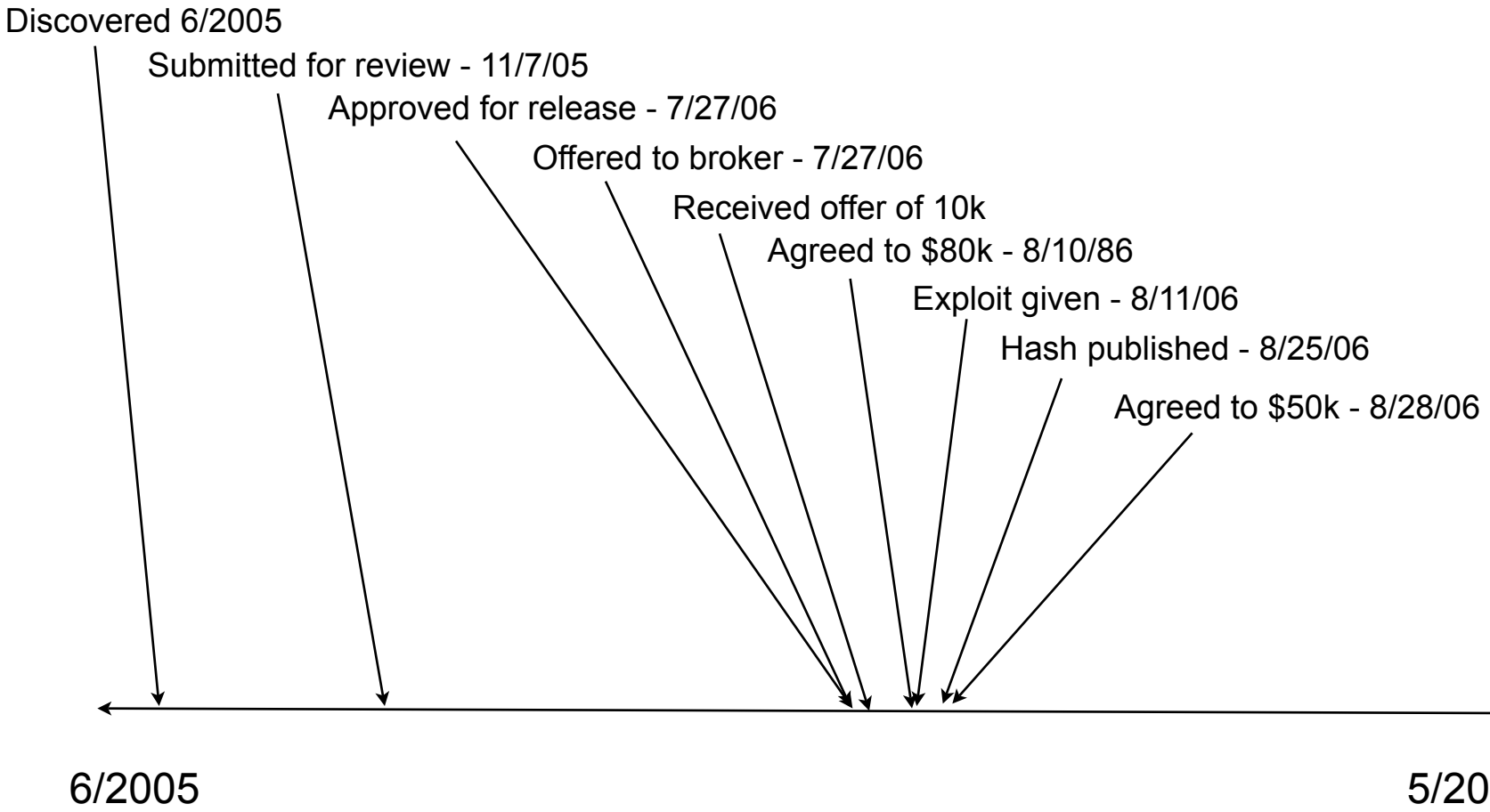
Timeline



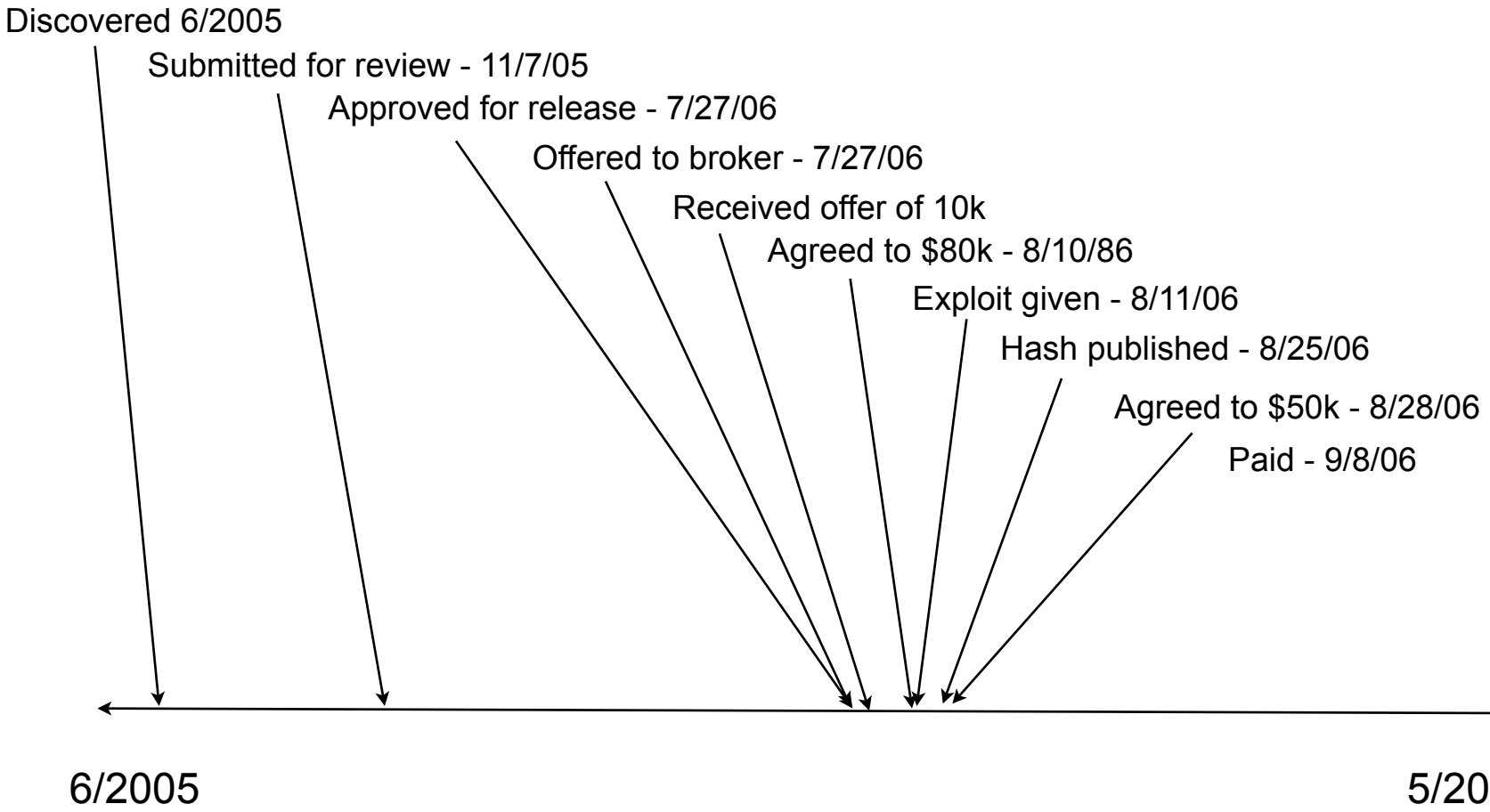
Timeline



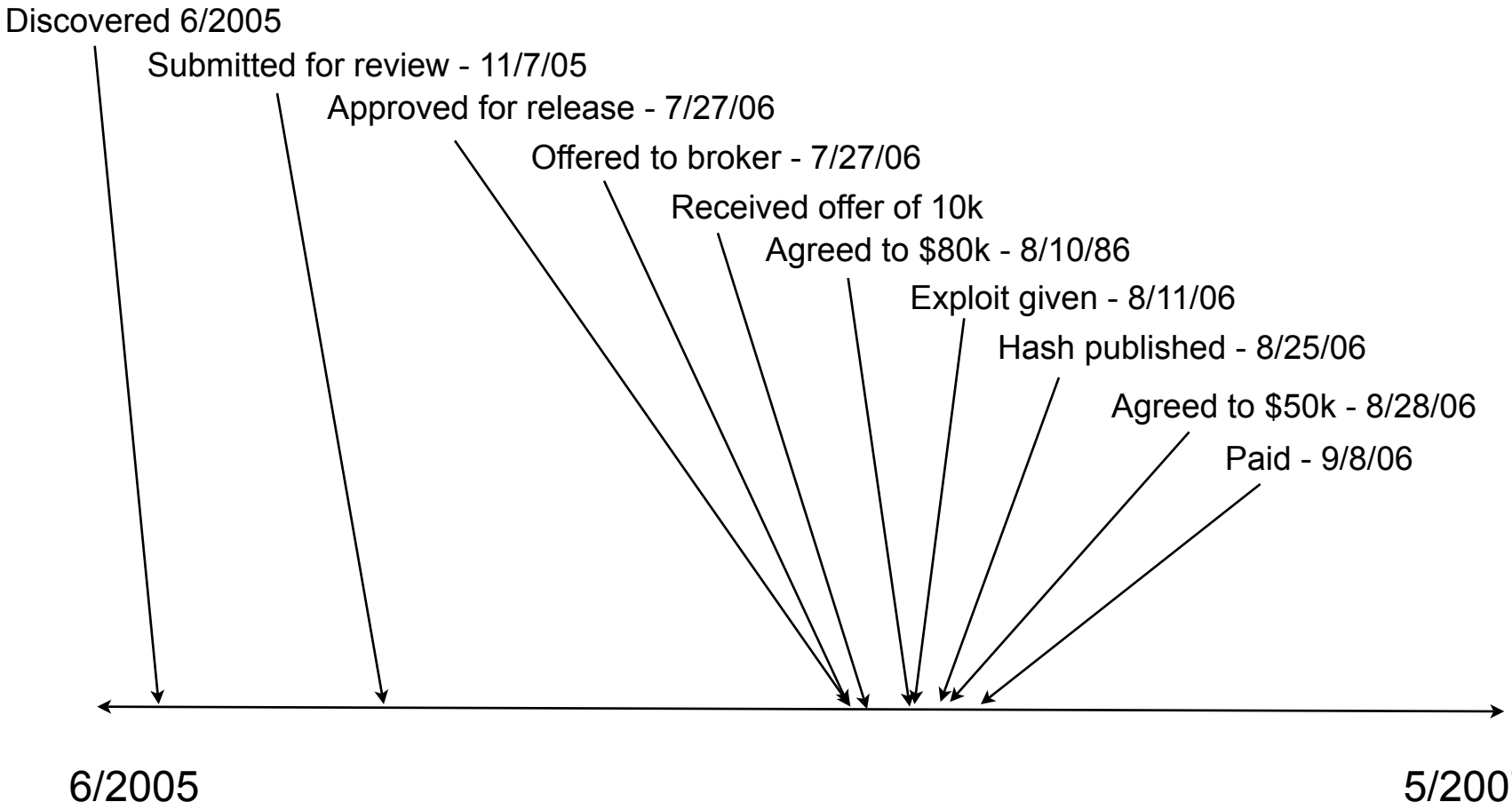
Timeline



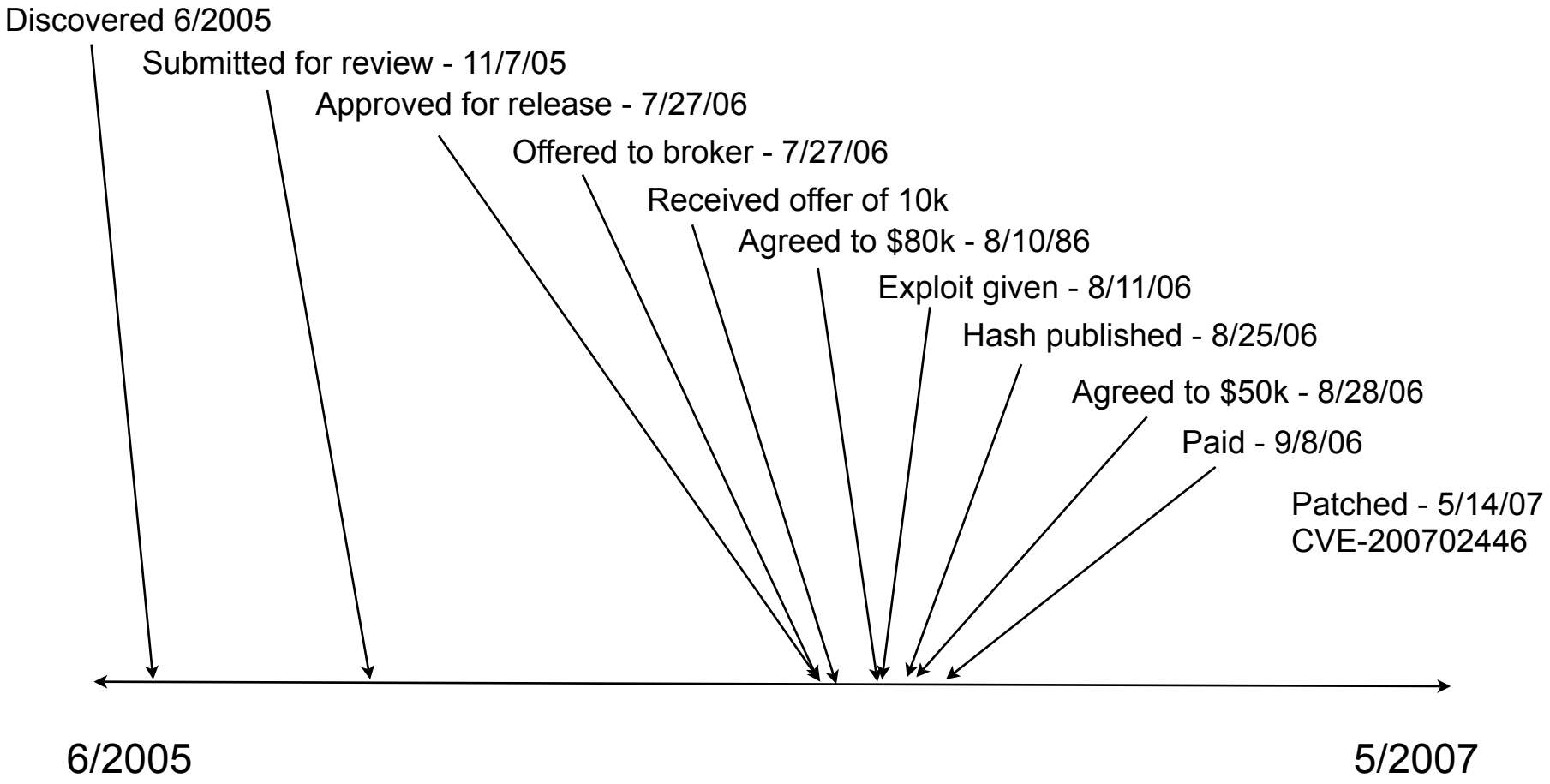
Timeline



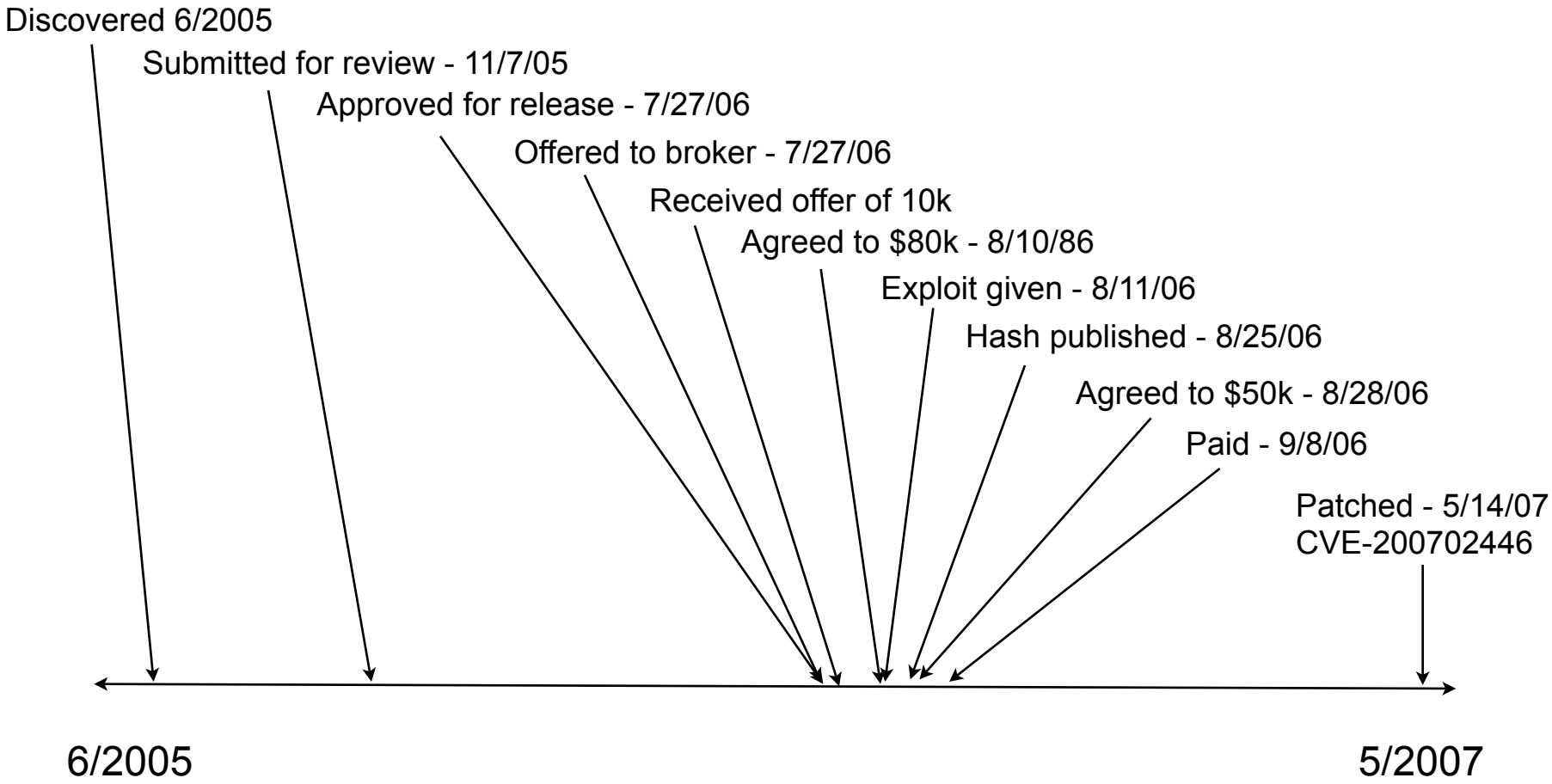
Timeline



Timeline



Timeline



Hashing for verification

```
echo "Charlie Miller found a vulnerability in Samba in the function
lsa_io_trans_names where trn->num_entries and trn->num_entries2 are
of different sizes." | md5sum
        e9a4f234e0f5d3e587c3d27e709b7eda  -
```

[Full-disclosure] Security researcher

From: asdfasf (*zerodayinithotmail.com*)
Date: Fri Aug 25 2006 - 09:01:39 CDT

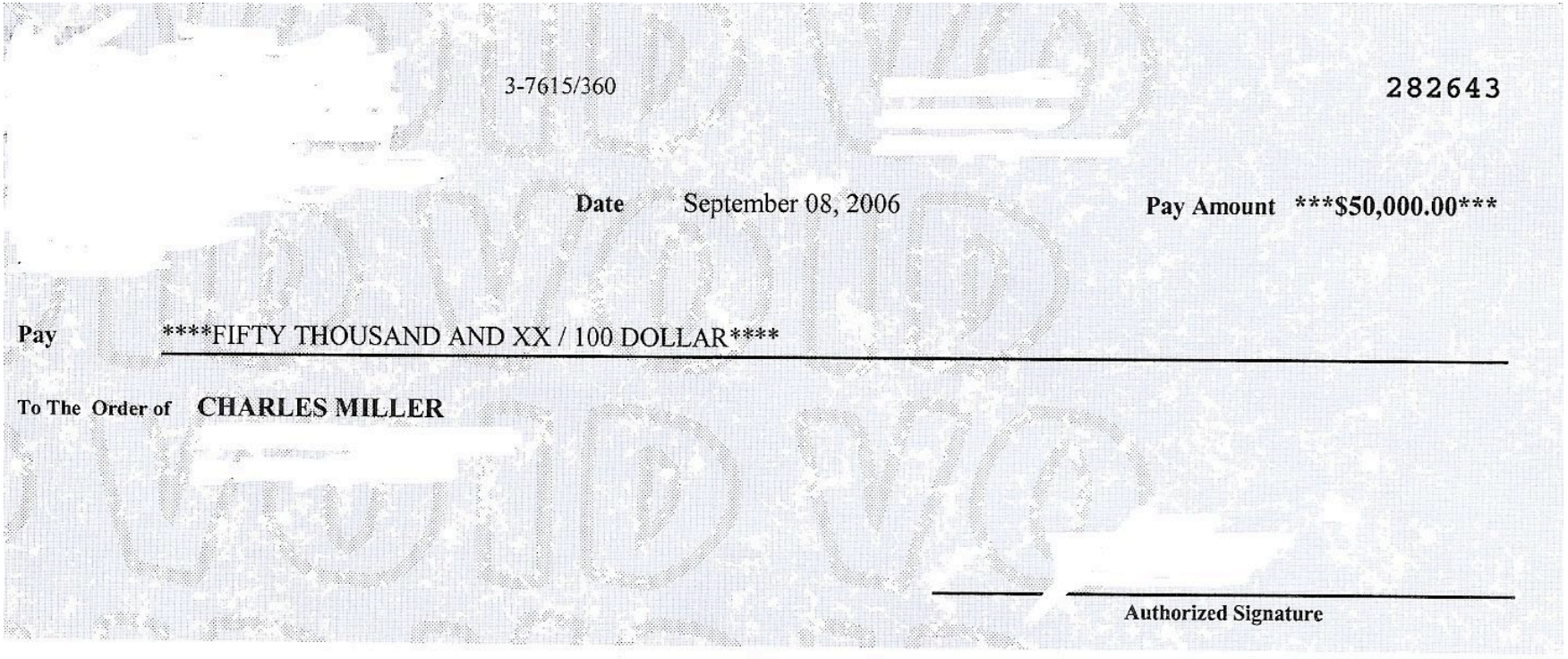
Messages sorted by: [date] [thread] [subject] [author]

I'm looking for a security researcher named "Gobbles". If anyone could send me his contact information I would appreciate it.

sadf
e9a4f234e0f5d3e587c3d27e709b7eda

_____
Full-Disclosure - We believe in it.
Charter: http://lists.grok.org.uk/full-disclosure-charter.html
Hosted and sponsored by Secunia - http://secunia.com/

The result



3-7615/360 282643

Date September 08, 2006 Pay Amount ***$50,000.00***

Pay ****FIFTY THOUSAND AND XX / 100 DOLLAR****

To The Order of CHARLES MILLER

Authorized Signature

Summary of Bug #1

- Due to no centralized place of contact, information sat for 5 months
- The government is slow....
- Had no idea of a fair market value
- Forced to give 10% to broker
- Only found broker due to personal contacts
- Sale helped by personal contacts
- Exploit given before any payment or signed contract
- *Sale occurred despite the market*

Case Study #2: Powerpoint

- Approached by friend to help him sell a 0-day Microsoft Powerpoint vulnerability
- This time, not so lucky

Timeline

1/20/07

2/13/07

Timeline

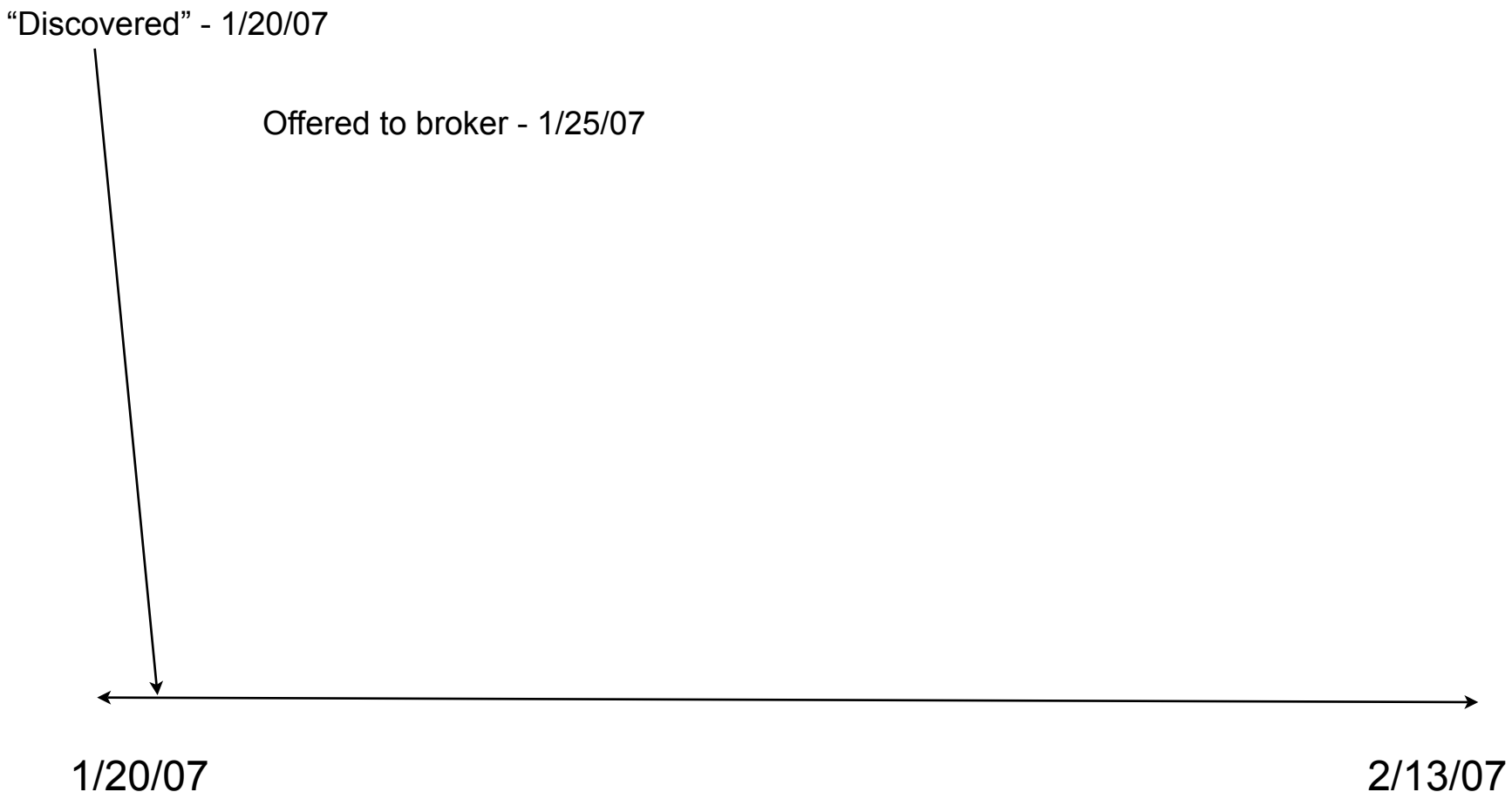
“Discovered” - 1/20/07

1/20/07

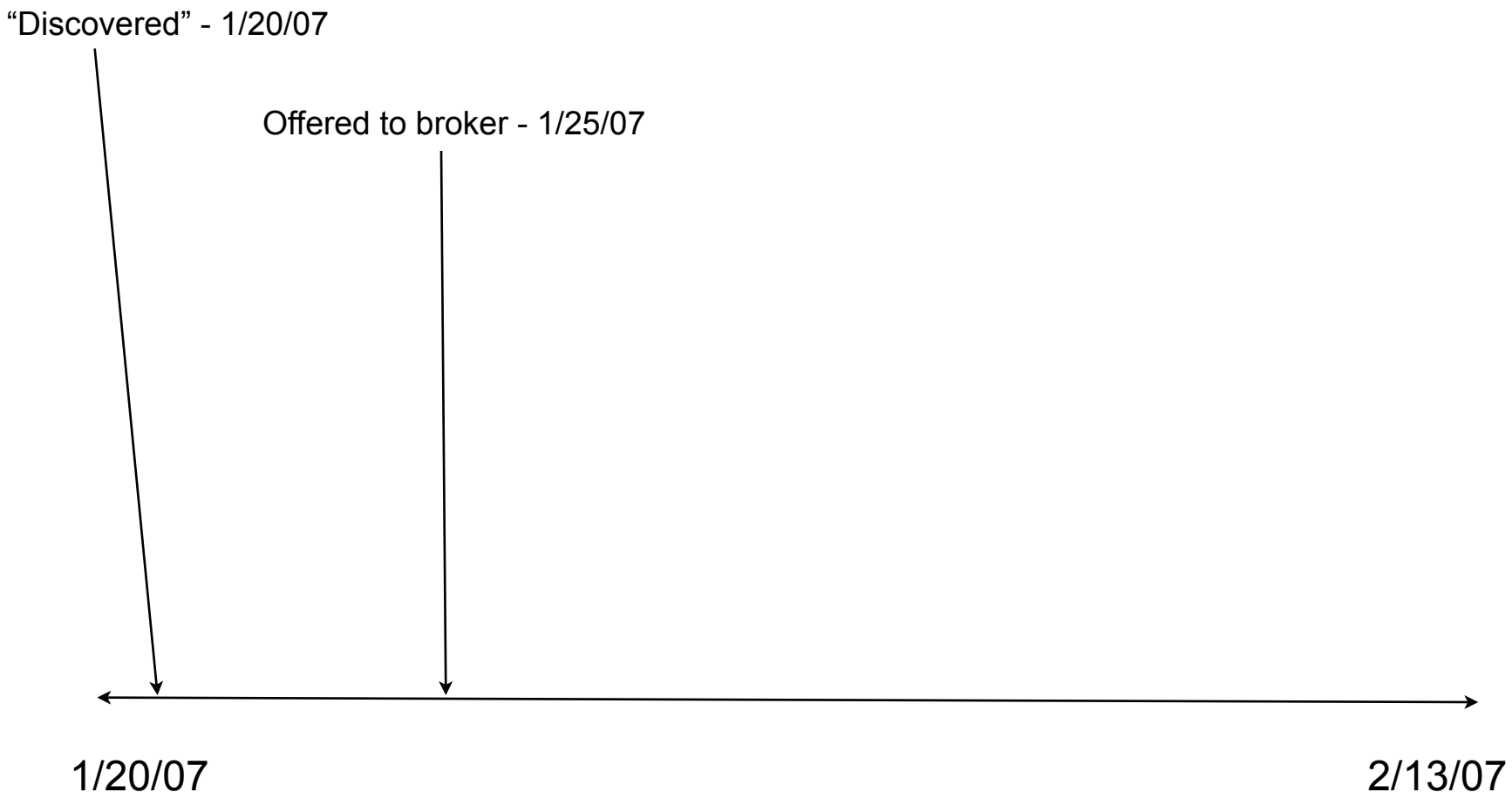
2/13/07

Timeline

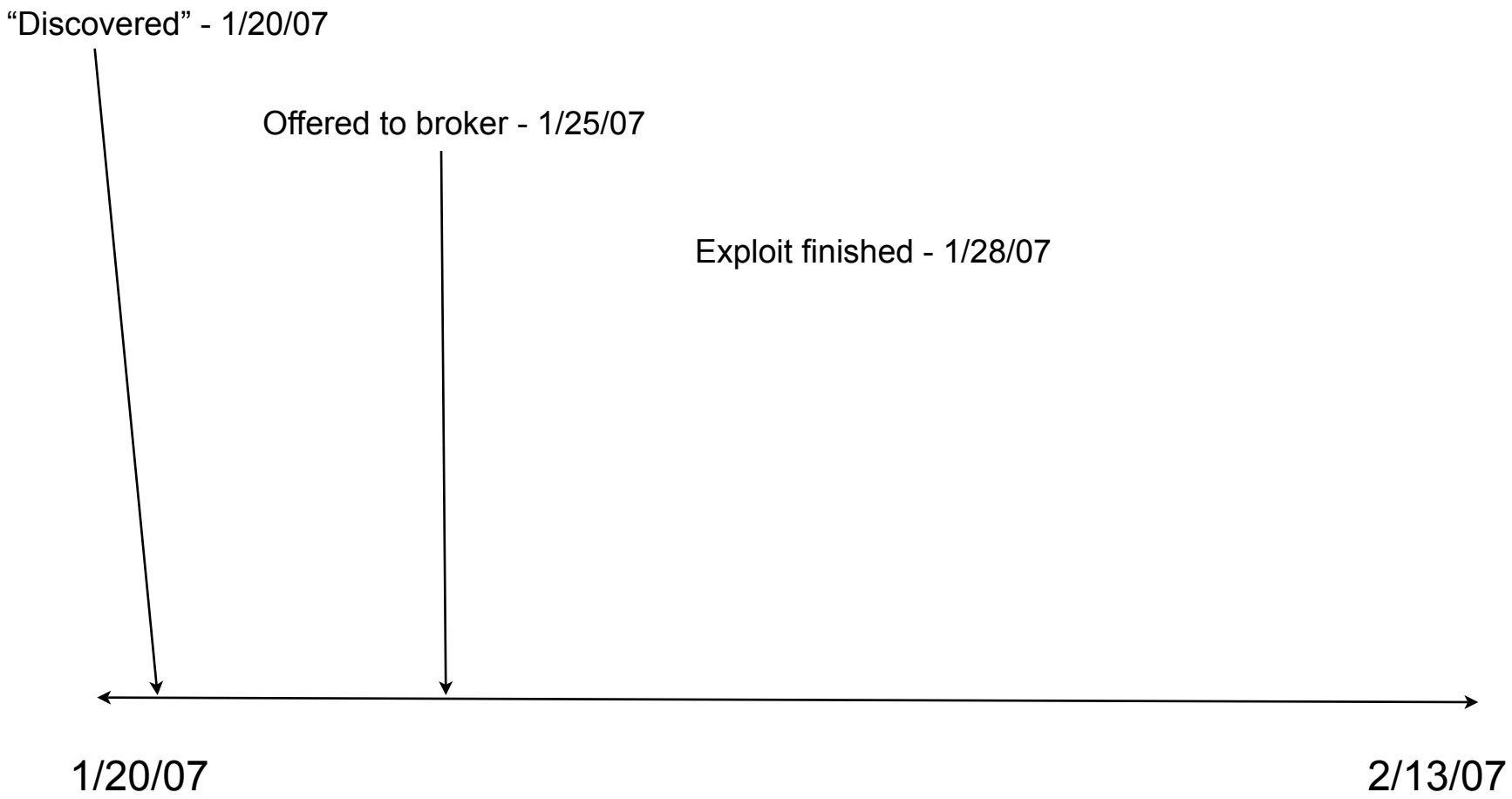
Timeline



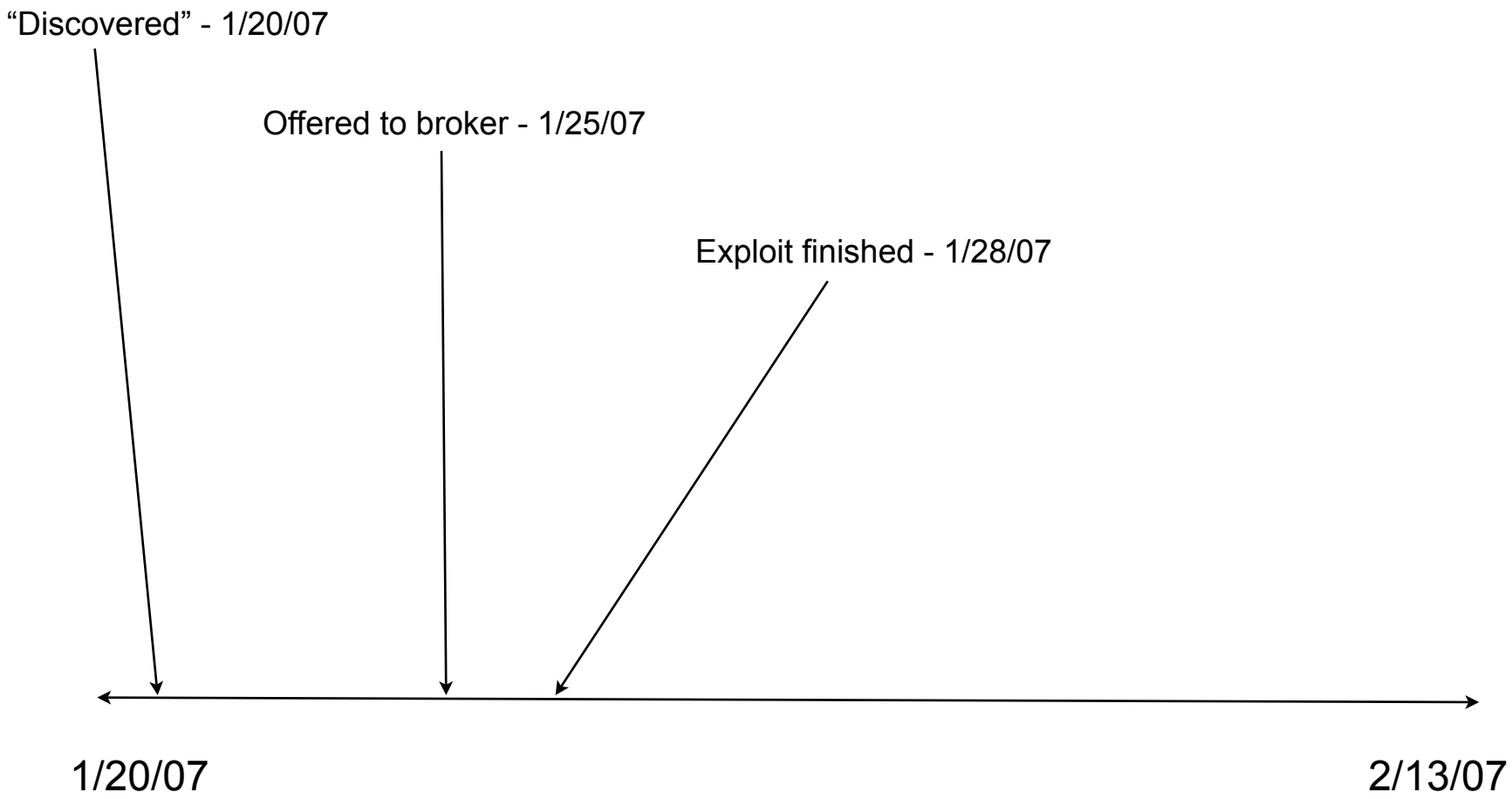
Timeline



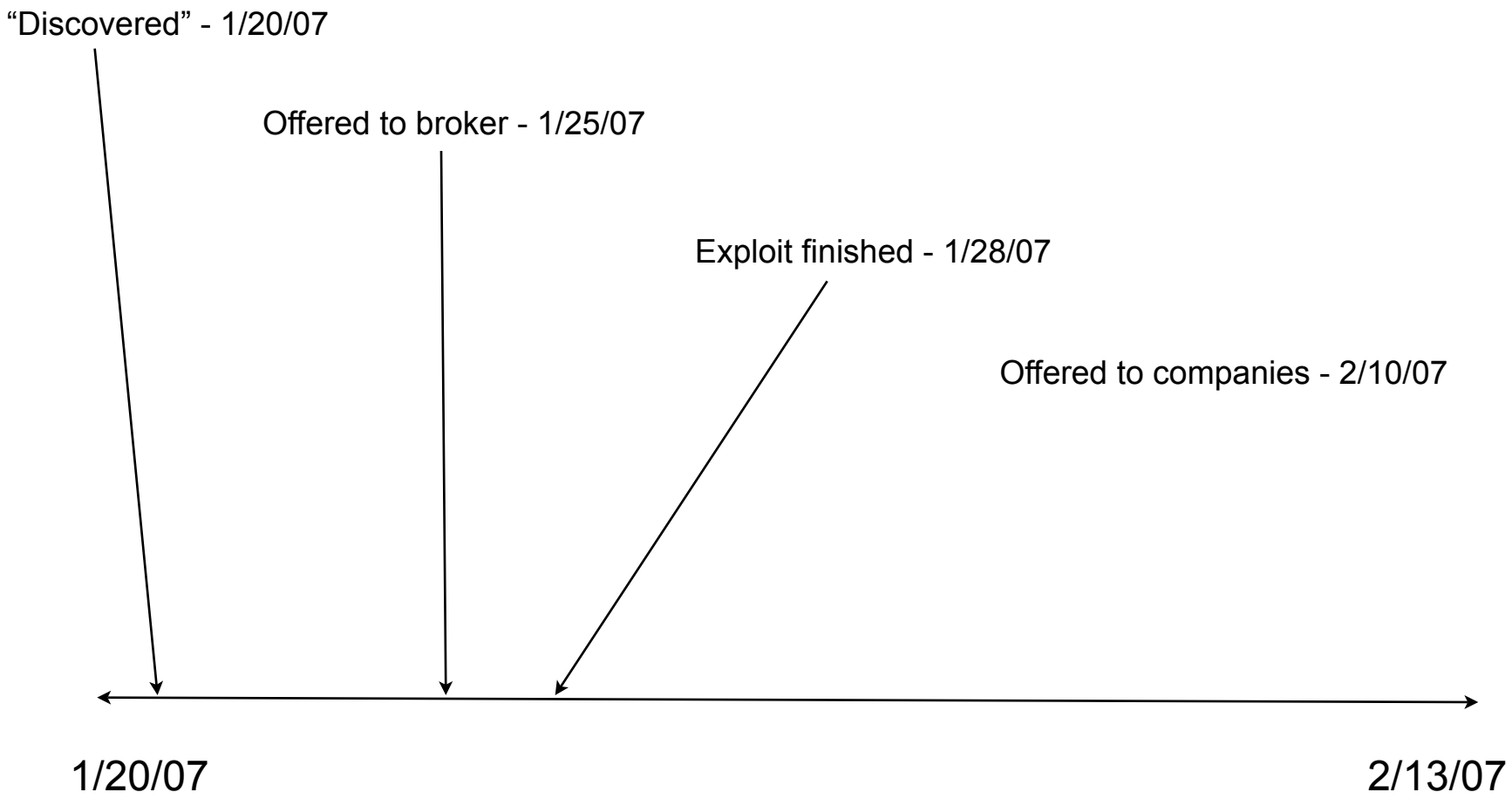
Timeline



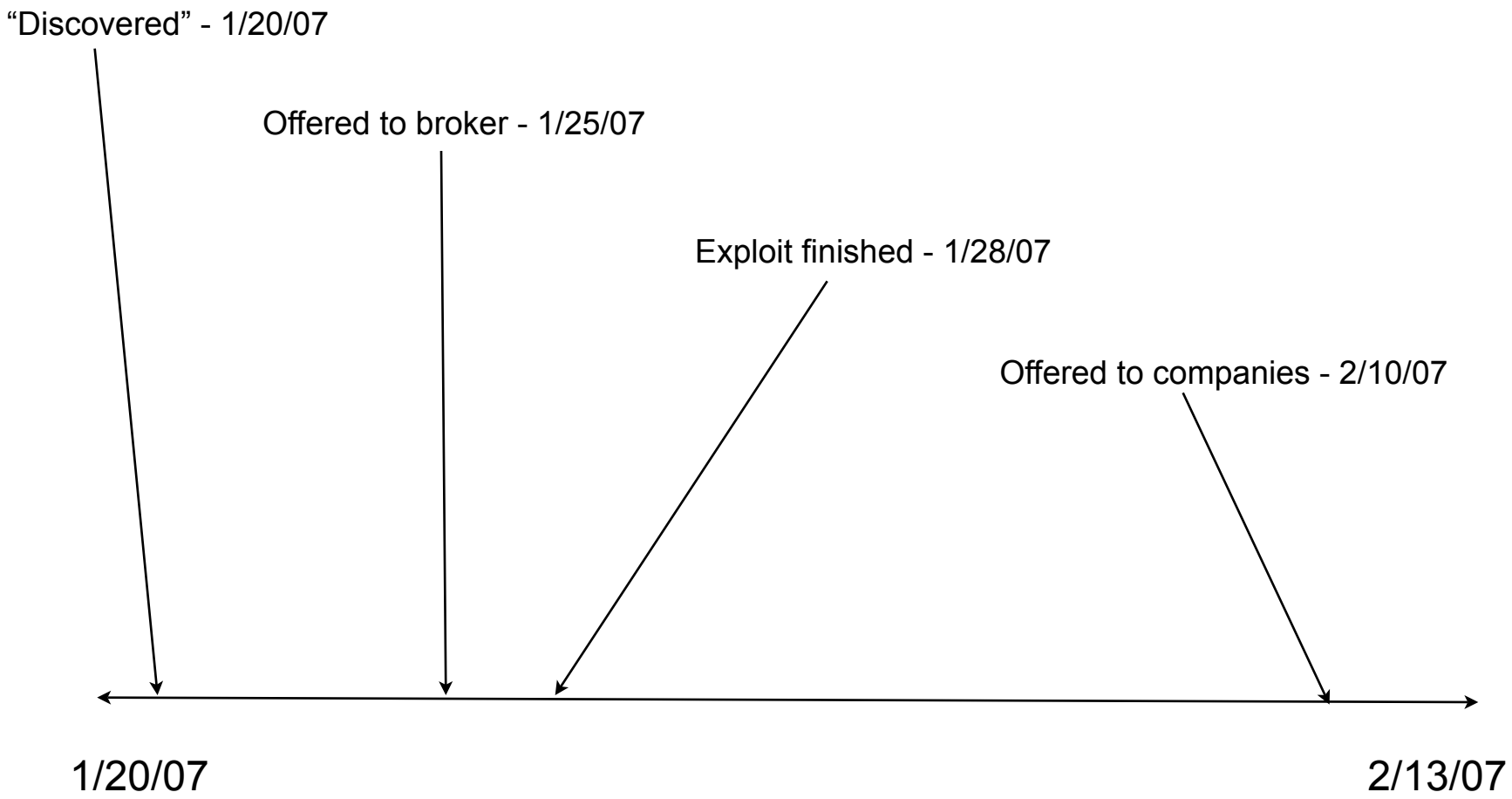
Timeline



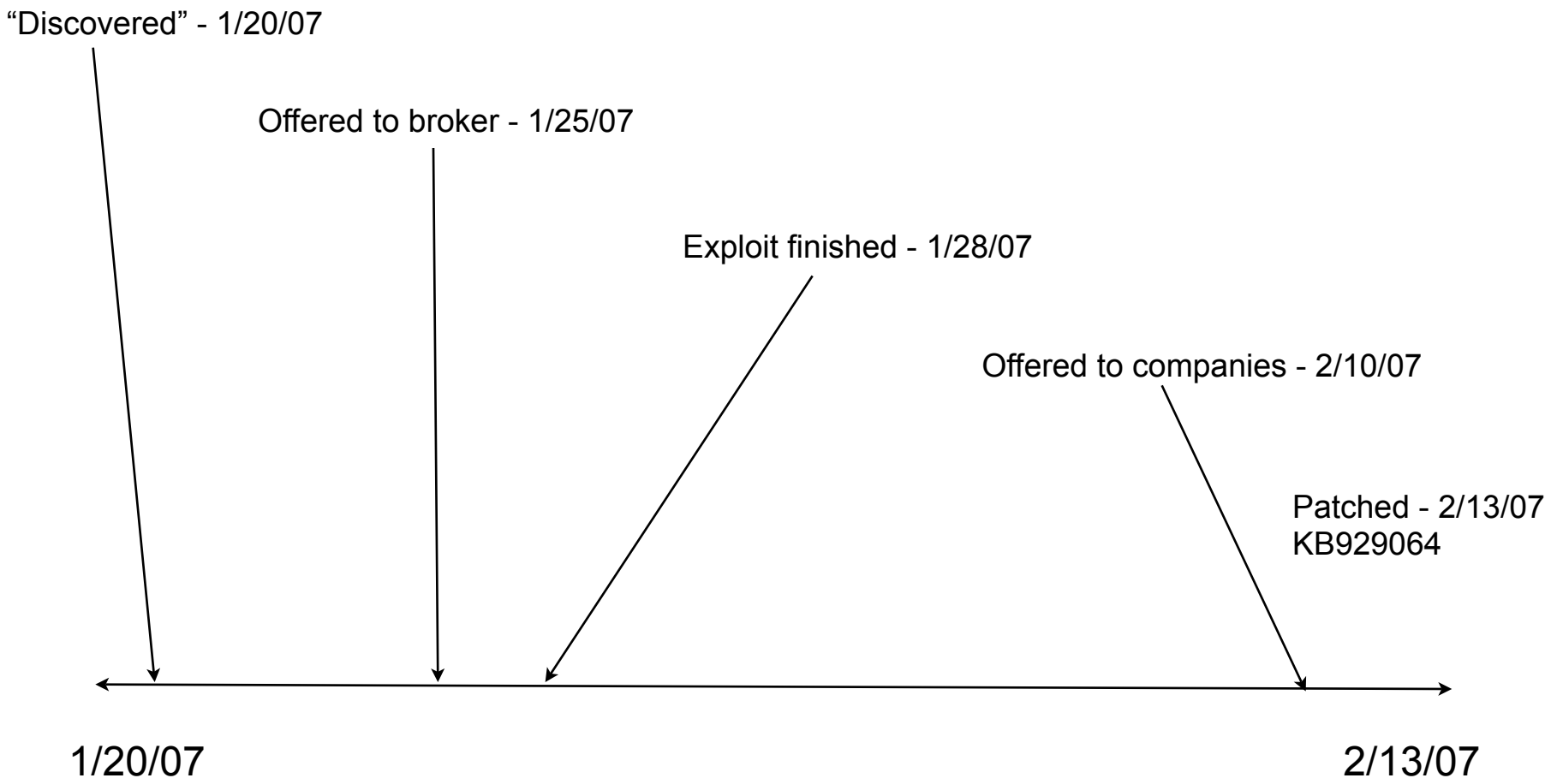
Timeline



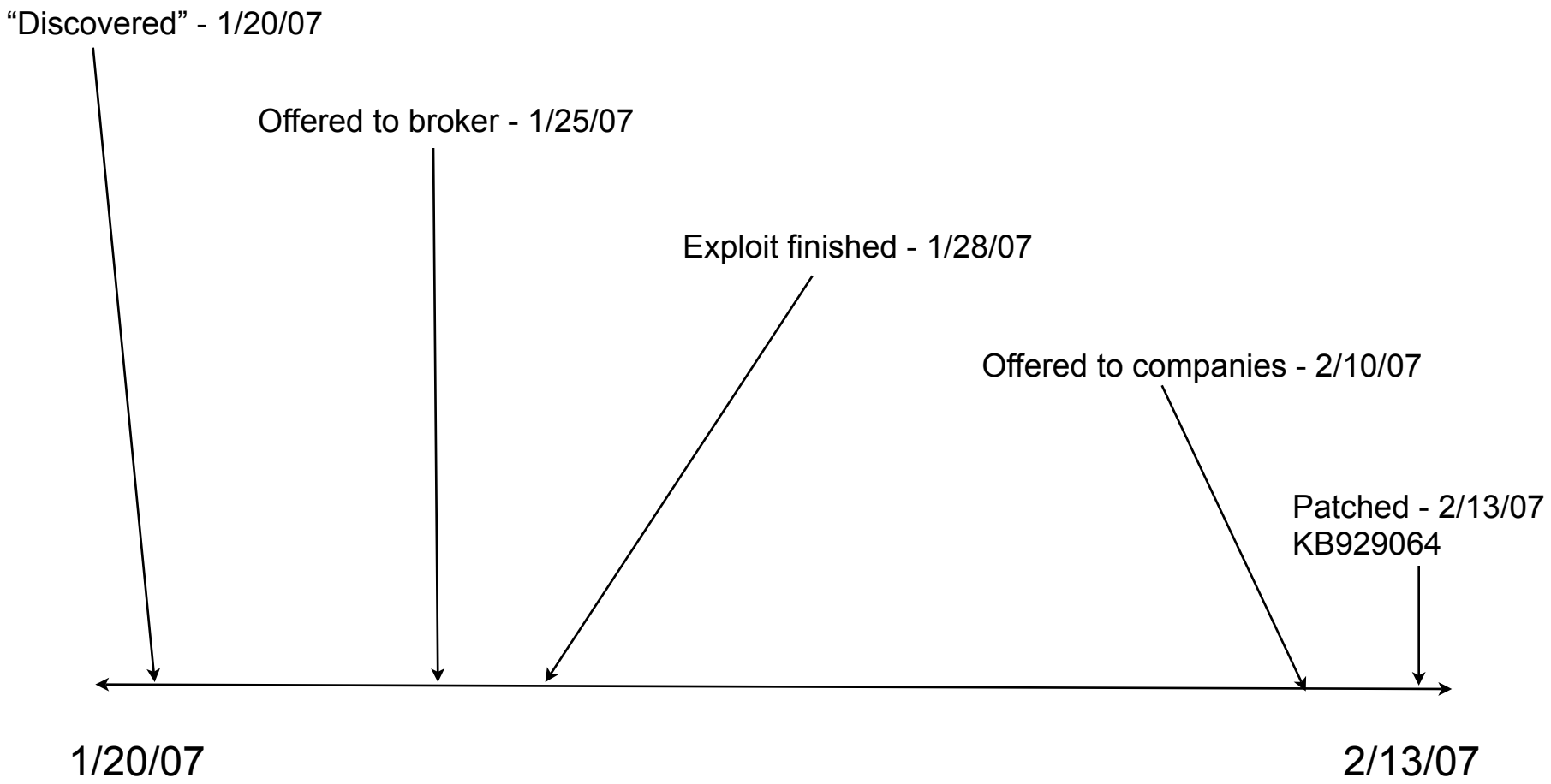
Timeline



Timeline



Timeline



Value

- I felt it was worth $20k
- I received offers as low as $5k
- I negotiated with a company from $8k up to $12k

Summary of Bug #2

- Lack of transparency meant pricing was basically arbitrary
- Lack of speed finding a buyer ruined sale
  - § The negotiation with the final company went quickly but started too late
- Sale could not proceed without shared personal contacts
- Exploit was to be sent before payment

Implications to Internet Security

- Summarizing
  - § Researchers forced to act in secret
  - § Buyers that pay the most (by a factor of 10) for vulnerability information do not release it to the vendor
  - § Vendors do not pay researchers
- Therefore
  - § Researchers have an economic incentive not to inform vendor or anyone who will
  - § “Privileged” parties are aware of vulnerability information months or years ahead of the vendor - and public.
  - § Researchers not motivated to find vulnerabilities

Conclusions

- Secrecy of market hurts security researchers
- Difficult to:
  - § Find a buyer
  - § Determine price
  - § Prove value of vulnerability/exploit
  - § Exchange goods for money
- No TTP leaves researchers vulnerable to losing their vulnerability information
- Time sensitivity compounds problems
- Some solutions exist but implementation remains far off
- Vulnerabilities ***are*** rediscovered!
- The implication of “high end” vulnerability sales is that the Internet is a less safe place - *vendors need to pay researchers!*

Questions?

- Please contact me at: cmiller@securityevaulators.com