Adventures in Disclosure:
A Look at the Legal Exploit Sales Market

Charlie Miller

Independent Security Evaluators

cmiller@securityevaluators.com

May 21, 2008

Who am I

- Principal Analyst, Independent Security Evaluators
- Previously, 5 years at National Security Agency (USA)
- PhD, University of Notre Dame
- Security Researcher
  - Find Bugs: iPhone, SecondLife, Safari, QuickTime...
  - Won CanSecWest Pwn2Own contest
  - Write papers, books; give talks, etc

Questions

- A security researcher discovers a vulnerability in a widely deployed application
  - What do they do with it?
  - What influences their decision?
- What is the impact of these answers on Internet security in general

Facts

- Zero Day Initiative (ZDI) offers approximately $5000 for high profile vulnerabilities
- iDefense Labs has offered various challenges including
  - $16-24k for each vulnerability found in applications such as Apache httpd, OpenSSH, Sendmail, IIS (Q2-Q3 2007)
  - $8-12k for email clients and servers (Q4 2007)
- In 2006, the U.S. Department of Homeland Security gave $1.24 million to Stanford and Coverity to hunt bugs in open source software

Agenda

- Why are researchers always causing trouble?
- All about disclosure
- So you don’t want to disclose?
- Case studies: adventures in (non)disclosure

Reasons you break things

- You are responsible for the system's security
- Someone hired you to test the security of a system
- You are a researcher
- Proving utility of new analysis technique
- Raising your profile
- Someone says their product is unbreakable
- You have nothing better to do

Unbreakable

ORACLE

Can't break it.

Your business relies on information and a reliable place to keep it in. Eliminate the need for planned downtime and withstand any unplanned failure -- system failure, storage failure, site failure or human error, all with Oracle9i.

Can't break in.

Oracle's security is fully proven, having been approved by 14 independent security evaluations. Only Oracle9i provides you with the security and encryption you need to protect your data in storage and transmission.

You can't afford to wait! Get your **FREE** Oracle9i eKit and build an unbreakable business today:

- **See** the Oracle9i iSeminar on how to deliver 24x7 reliability.
- **Try** the demonstrations that prove Oracle9i's unique technology.
- **Download** free Oracle9i software.
- **Read** business and technical white papers on safeguarding your data.
- **Learn** how Oracle Consulting can build an unbreakable business.

Get your FREE eKit now by clicking on the link at the right.

Oracle9i. Unbreakable.

I'm a new user

Get your FREE eKit Now!

I already have an account

Username

Password

Sign In

Lost your password? Click here

All about disclosure

- No disclosure
- Full disclosure
- Responsible disclosure

No disclosure

- Can mean a few things
  - Don’t tell anyone
  - Just sit on it
  - Tell your friends
  - Sell information to interested third party

No disclosure (cont.)

- Pros
  - Little chance of legal action
  - Requires little work - easy
  - Possible financial gain
- Cons
  - Consumers may not be protected
    - Fails the “grandmother rule”

Full disclosure

- Reveal information without previously contacting vendor
  - Post on mailing list
  - Give talk at conference
- Vendors really hate this!

Full disclosure (cont.)

- Pros
  - Vendors tend to react quickly to this information
  - Trivial to do
  - Can raise your profile - for good or bad
- Cons
  - Puts consumers at risk until patch is developed
  - Can provide recipe for bad guys

Responsible disclosure

- Contact vendor with vulnerability details
- Wait for vendor to develop patch, fix, or new version of product
- Coordinate release of vulnerability information

Responsible disclosure (cont.)

- Pros:
  - Consumers are protected at all times
  - Can develop good relationship with vendor
- Cons:
  - Vendor may not be cooperative
  - Vendor may not understand the severity of the vulnerability
  - Vendor may not develop patch in a timely manner
    - Oracle has taken over two years to patch

When responsible disclosure is a bad idea

- You want the vendor to work quickly

ZDI-CAN-226	Symantec	High	2007-09-14, 195 days ago
ZDI-CAN-211	Microsoft	High	2007-07-20, 251 days ago
ZDI-CAN-206	Hewlett-Packard	High	2007-07-17, 254 days ago
ZDI-CAN-224	Oracle / PeopleSoft	High	2007-07-13, 258 days ago
ZDI-CAN-222	Motorola	High	2007-07-10, 261 days ago
ZDI-CAN-200	IBM	High	2007-05-22, 310 days ago
ZDI-CAN-185	Hewlett-Packard	High	2007-05-22, 310 days ago
ZDI-CAN-174	Symantec	High	2007-05-22, 310 days ago
ZDI-CAN-186	Microsoft	High	2007-03-29, 364 days ago
ZDI-CAN-177	Hewlett-Packard	High	2007-03-19, 374 days ago
ZDI-CAN-175	Microsoft	High	2007-03-19, 374 days ago
ZDI-CAN-165	Novell	High	2007-03-09, 384 days ago
ZDI-CAN-160	Oracle / PeopleSoft	High	2007-01-29, 423 days ago
ZDI-CAN-105	Hewlett-Packard	High	2006-10-10, 534 days ago
ZDI-CAN-103	Microsoft	High	2006-09-14, 560 days ago
ZDI-CAN-088	Computer Associates	High	2006-09-12, 562 days ago
ZDI-CAN-063	Computer Associates	High	2006-09-12, 562 days ago

- You fear legal prosecution
  - http://www.securityfocus.com/columnists/466/4

The system is broken

- Responsible disclosure
  - Get credit for your discovery (hopefully)
  - Must convince the company there is a bug
  - Typically, wait for company to fix the bug at their pace
  - Worst case, the company threatens to sue you or you could face possible criminal action

The system is broken (cont.)

- No disclosure
  - You don’t get credit for discovering it (publish a hash...)
  - You possibly get lots of money
    - See my new kitchen, bathroom
  - You don’t get sued
  - You don’t have to deal with companies

So you don’t want to disclose...

- 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

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
Vista Remote	$200,000	Unnamed contractor
a “real good” exploit	over $100,000	Official from SNOsoft research team
Flash or PDF exploit	$75,000	Price I brokered with contractor
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 (mostly)
- 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?
  - Scenario: Sell an OpenSSH exploit used by terrorist to attack nuclear reactor systems... Welcome to gitmo!
- 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, Immunity Security Inc.

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

WabiSabiLabi

- Its a buyer's market...

Code	Time to live	Title	System	Offer type	Last bid	
ZD-00000223	5d 6h 7m	AbleDating	Web application	Auction Buy now at	0€ 0 bid(s) 300€	info
ZD-00000222	5d 6h 7m	phpFoX	Web application	Auction Buy now at	0€ 0 bid(s) 300€	info
ZD-00000220	5d 6h 7m	Camfrog	Windows Vista	Auction	0€ 0 bid(s)	info
ZD-00000218	5d 6h 7m	PHP-Nuke	Web application	Auction	0€ 0 bid(s)	info
ZD-00000199	5d 6h 7m	Avaya	Windows Server 2003	Auction Buy now at	0€ 0 bid(s) 500€	info
ZD-00000190	5d 6h 7m	phpShop #2	PHP	Auction Buy now at	0€ 0 bid(s) 1,000€	info
ZD-00000183	5d 6h 7m	CA ARCserve Backup for Laptops & Desktops	Windows XP	Auction Buy now at	0€ 0 bid(s) 900€	info
ZD-00000117	5d 6h 7m	Phpauction	Windows Server 2003	Auction	0€ 0 bid(s)	info
ZD-00000077	5d 6h 7m	GemStone	Linux	Auction	0€ 0 bid(s)	info
ZD-00000072	5d 6h 7m	DWebPro	Windows Server 2003	Auction	0€ 0 bid(s)	info
ZD-00000065	5d 6h 7m	Weird Solutions BOOTPTurbo	Windows XP	Auction Buy exclusively at	0€ 0 bid(s) 500€	info
ZD-00000031	5d 6h 7m	ElectroServer	Linux	Auction	0€ 0 bid(s)	info
ZD-00000029	5d 6h 7m	3Com FTP server	Windows XP	Auction	0€ 0 bid(s)	info
ZD-00000017	8d 6h 7m	MailEnable	Windows 2000	Auction Buy now at	0€ 0 bid(s) 500€	info

WabiSabiLabi statistics

- Total received submissions for evaluation from July 2007 to date: 223
- Total vulnerabilities accepted and listed to the marketplace : 81
- Vulnerabilities sold: 32

More statistics (Euros)

- Average sale price: 1821
- Median sale price: 650
- Minimum sale price: 100
- Maximum sale price: 5100
- 13 unique buyers
- 97% of auctions had only one bidder

Who visits this site?

- 10. SAP
- 9. Verisign
- 8. Oracle
- 7. US Army
- 6. F-Secure
- 5. Symantec
- 4. Veritas
- 3. IBM
- 2. Microsoft
- 1. Cisco

Case studies

Case Study #1 - Samba

- Samba is an open source set of programs that impliments Server Message Block (SMB) / Common Internet File System (CIFS) protocol for UNIX systems.
- Used for interoperability of Unix and Windows systems
- Has a history of bugs
- I found one such bug in the Summer of 2005

What's all the fuss about

```
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))
```

This bugs is a...

- Remote, pre authentication, root exploit against Unix systems running it
- Any reasonable network wouldn’t allow these ports through a firewall
- Would be useful once inside a network

Timeline

6/2005 ⟷ 5/2007

Timeline

Discovered 6/2005

Timeline

Discovered 6/2005

6/2005

5/2007

Timeline

Discovered 6/2005

Submitted for review - 11/7/05

6/2005

5/2007

Timeline

Timeline

Discovered 6/2005

Submitted for review - 11/7/05

Approved for release - 7/27/06

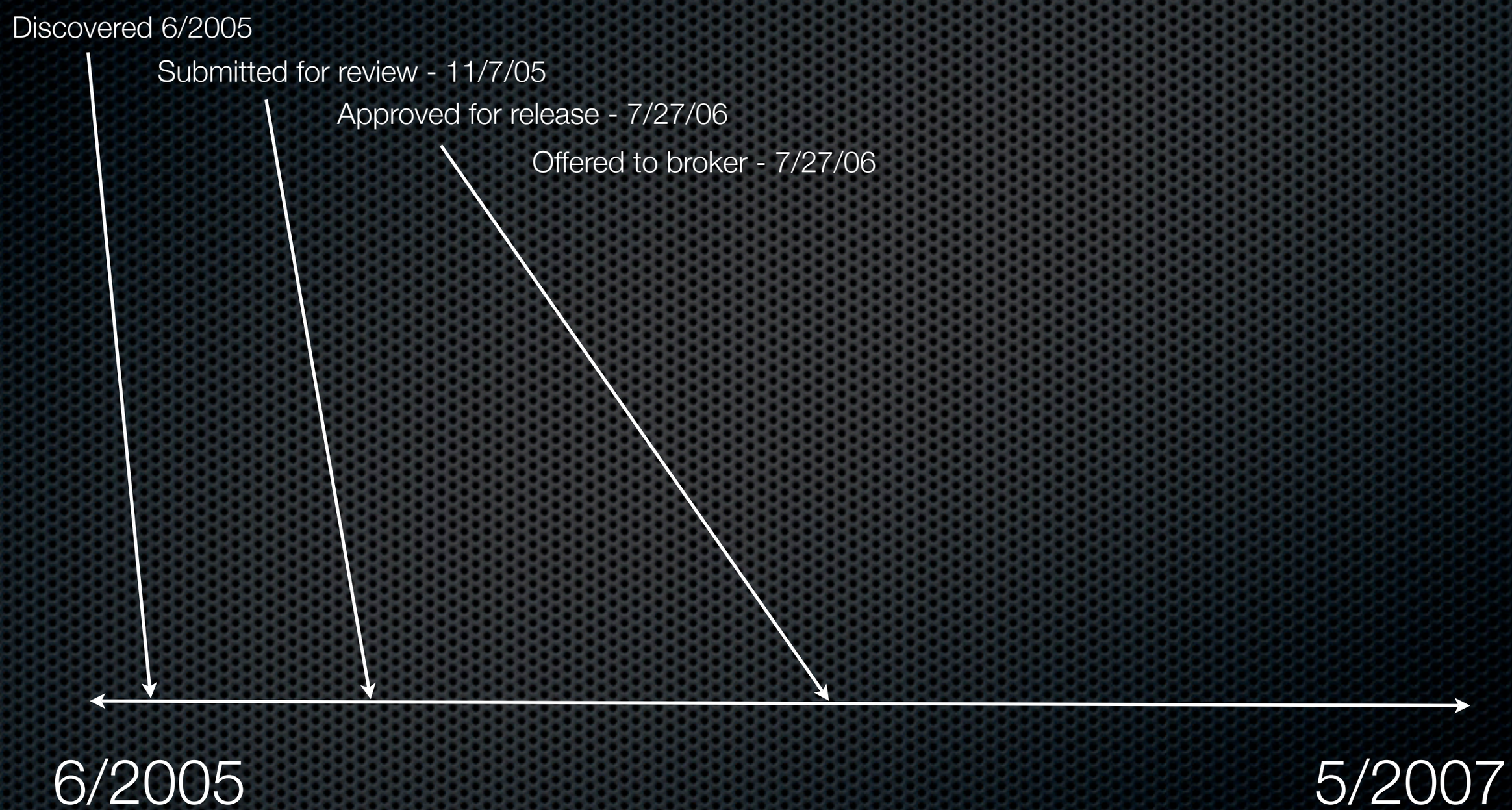
6/2005

5/2007

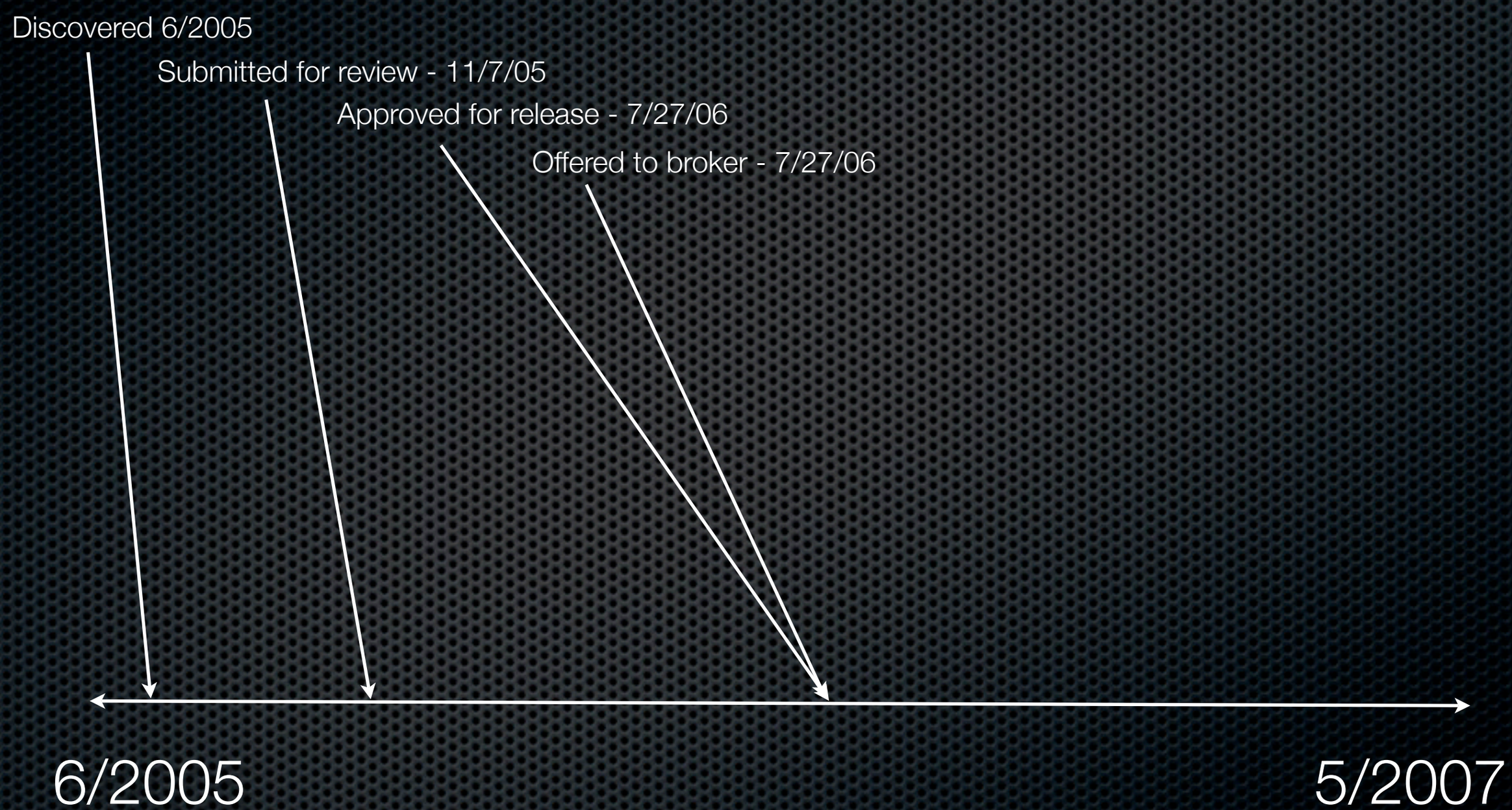
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
6/2005
5/2007

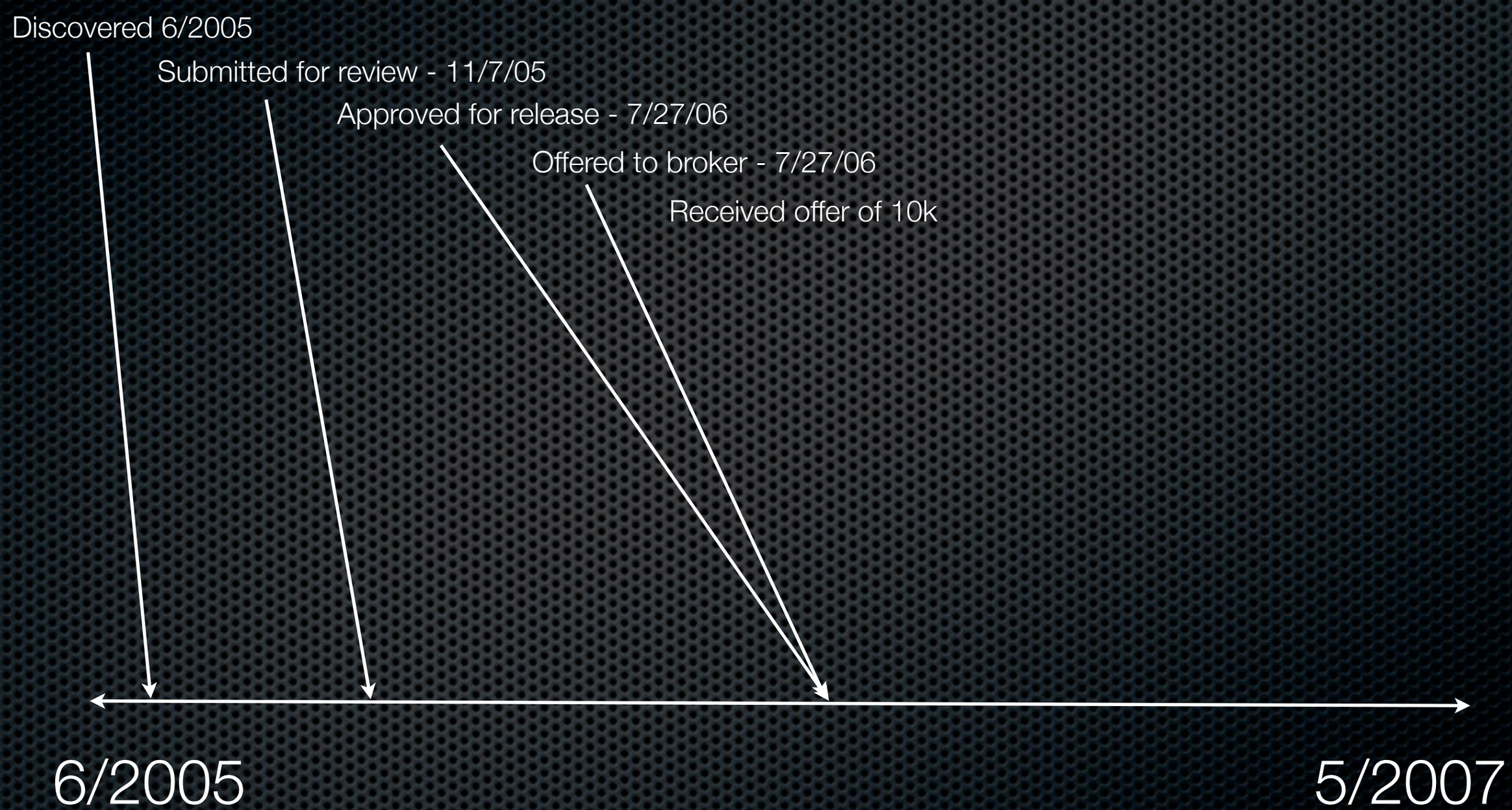
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
6/2005
5/2007

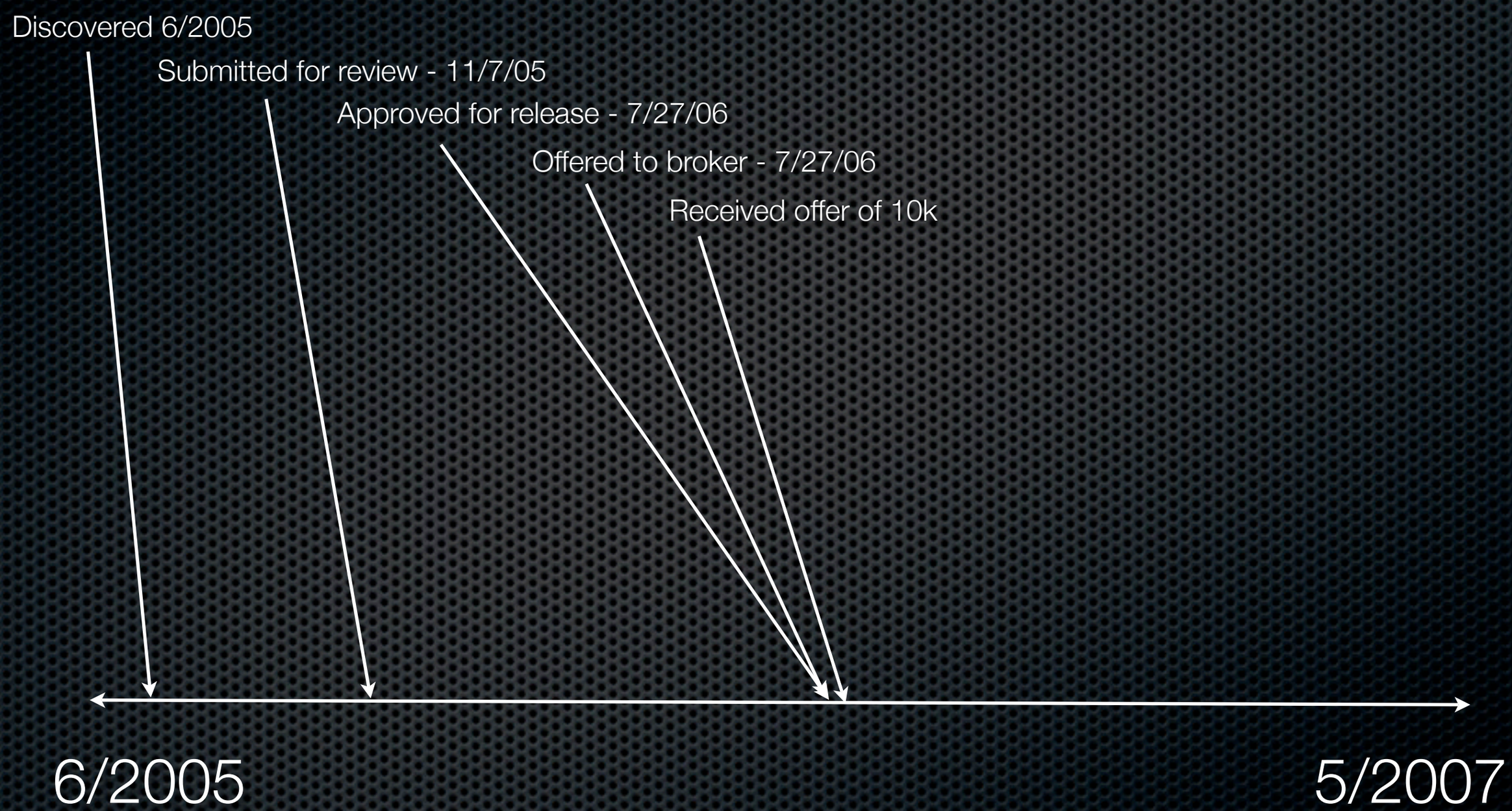
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
6/2005
5/2007

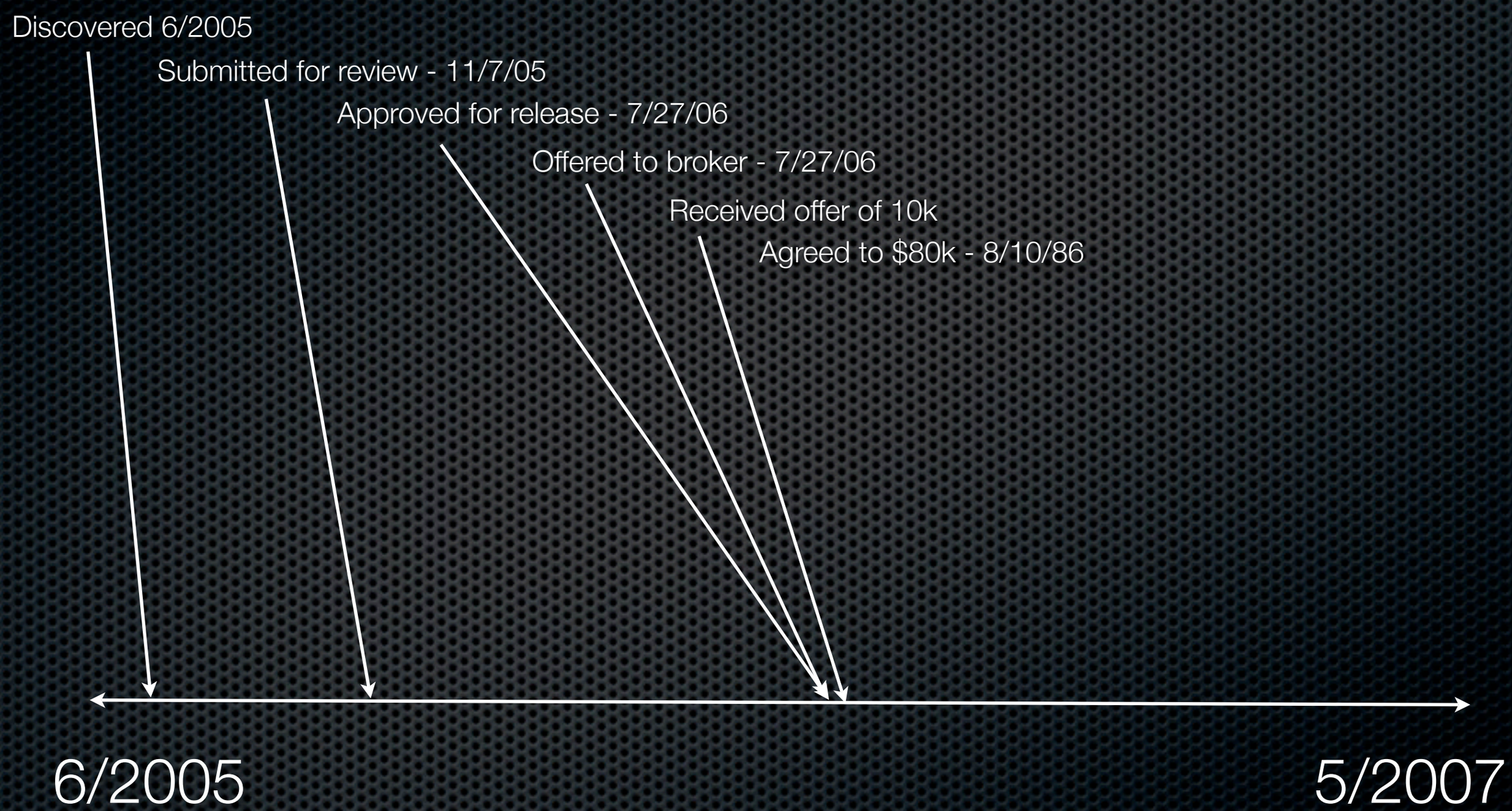
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
6/2005
5/2007

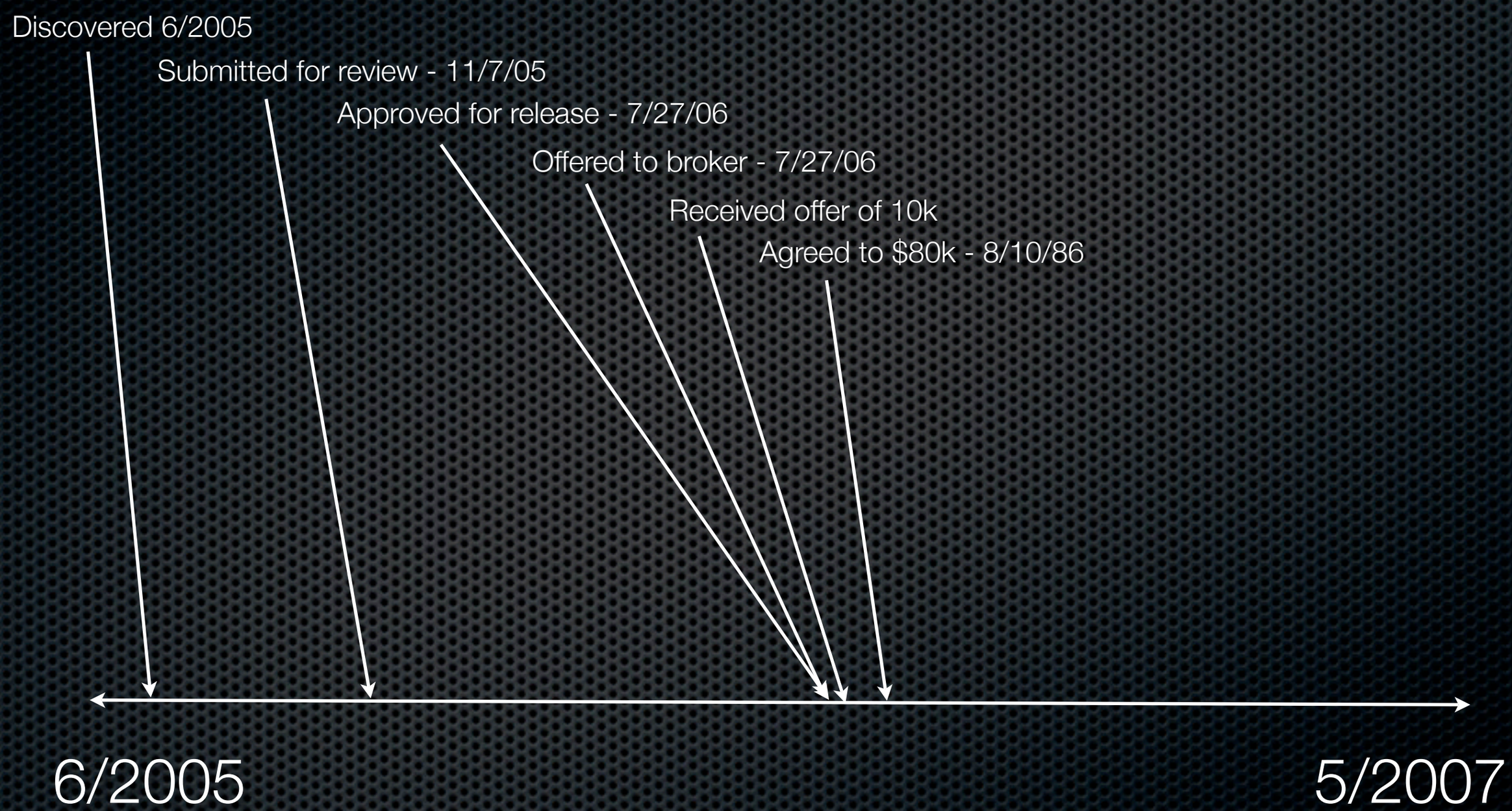
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
6/2005
5/2007

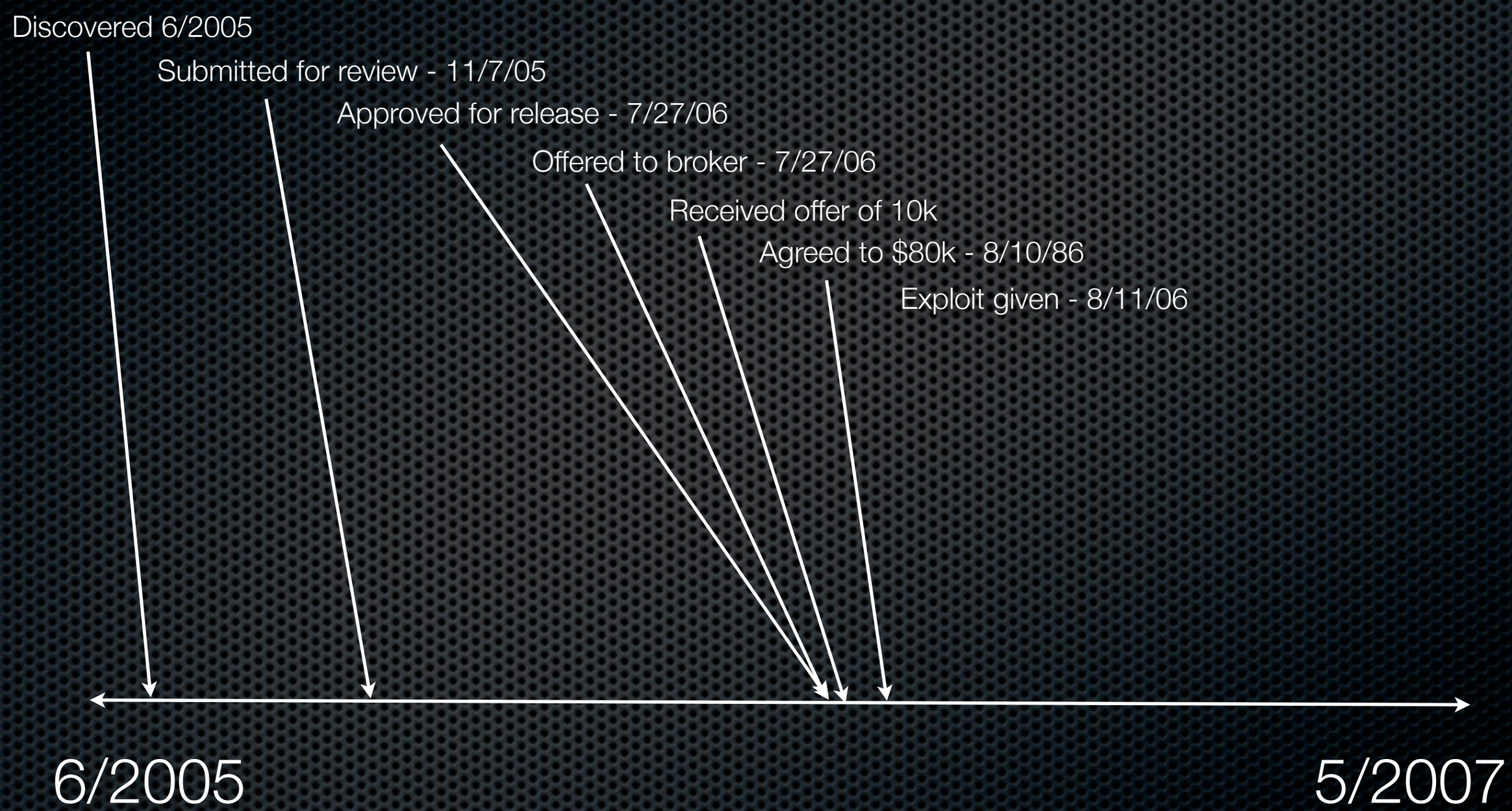
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
6/2005
5/2007

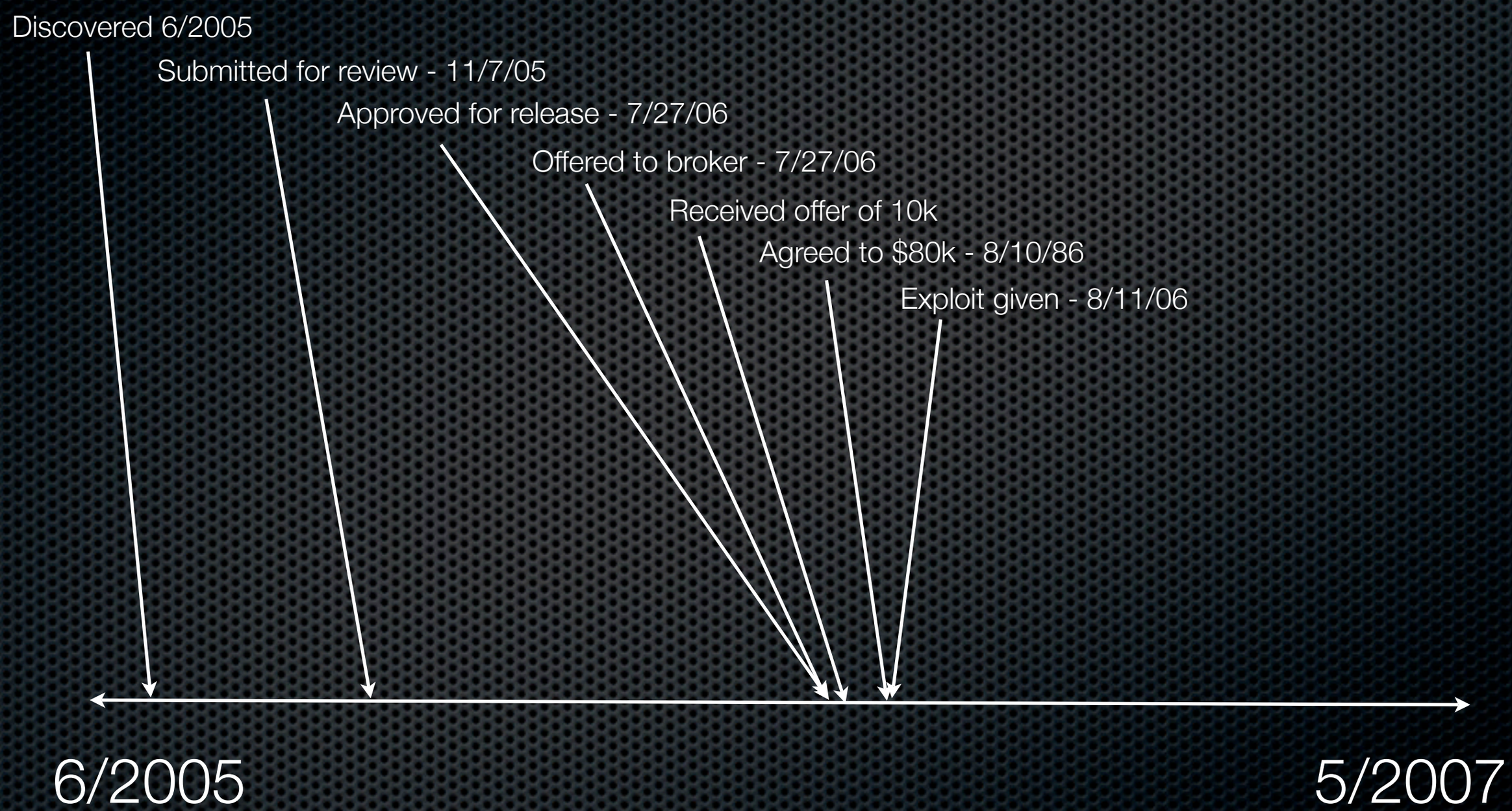
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
6/2005
5/2007

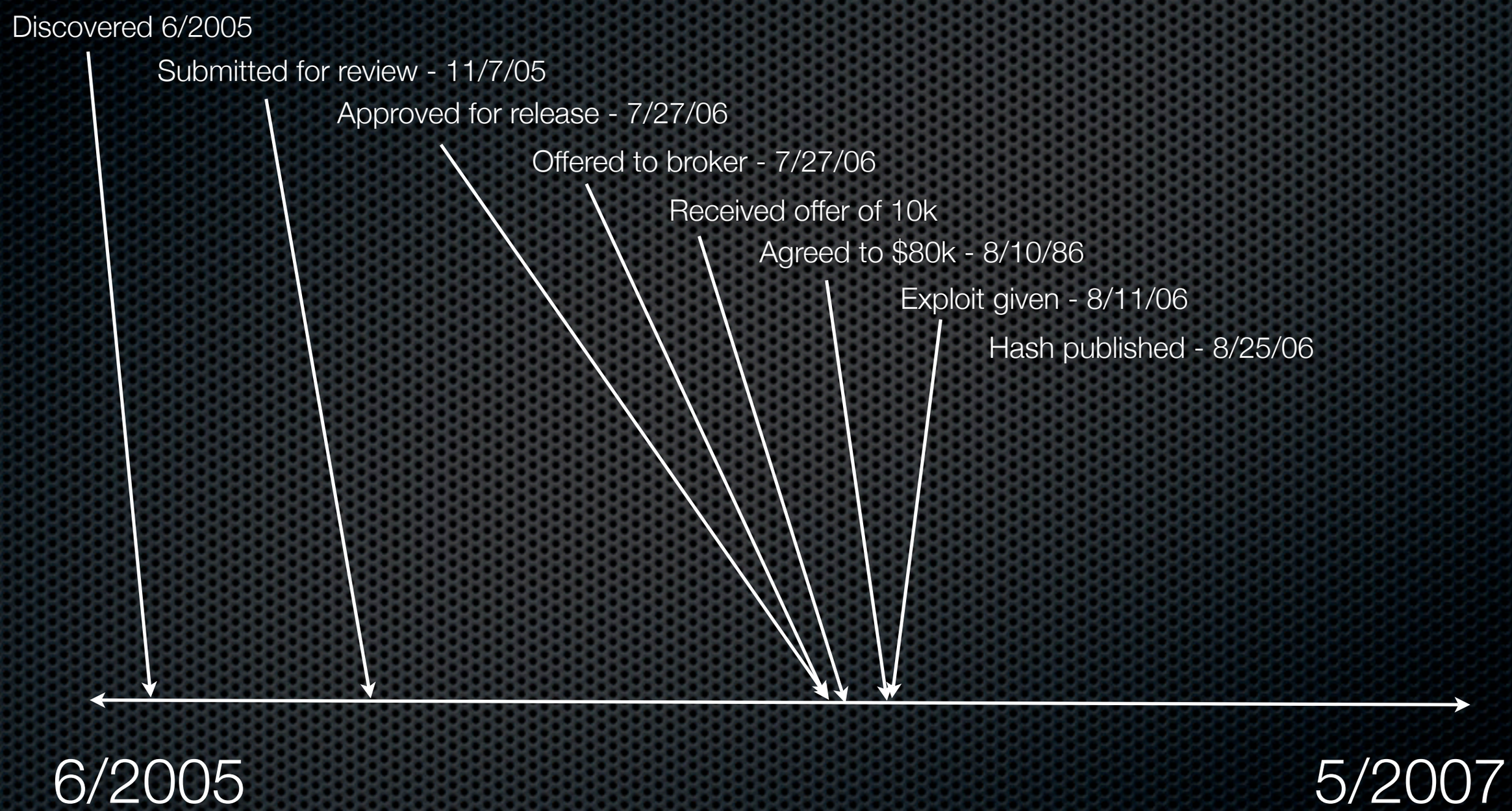
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
6/2005
5/2007

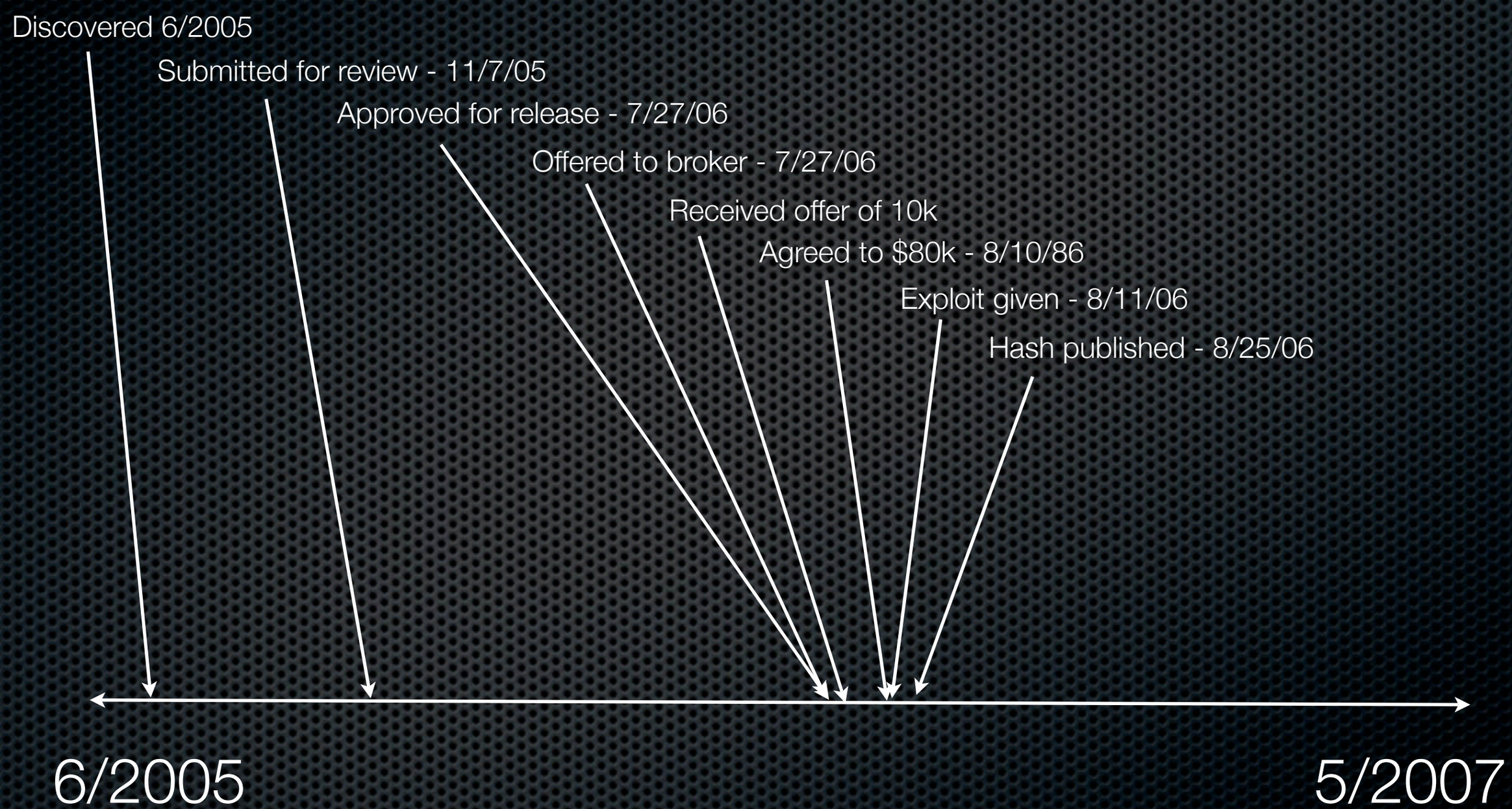
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
6/2005
5/2007

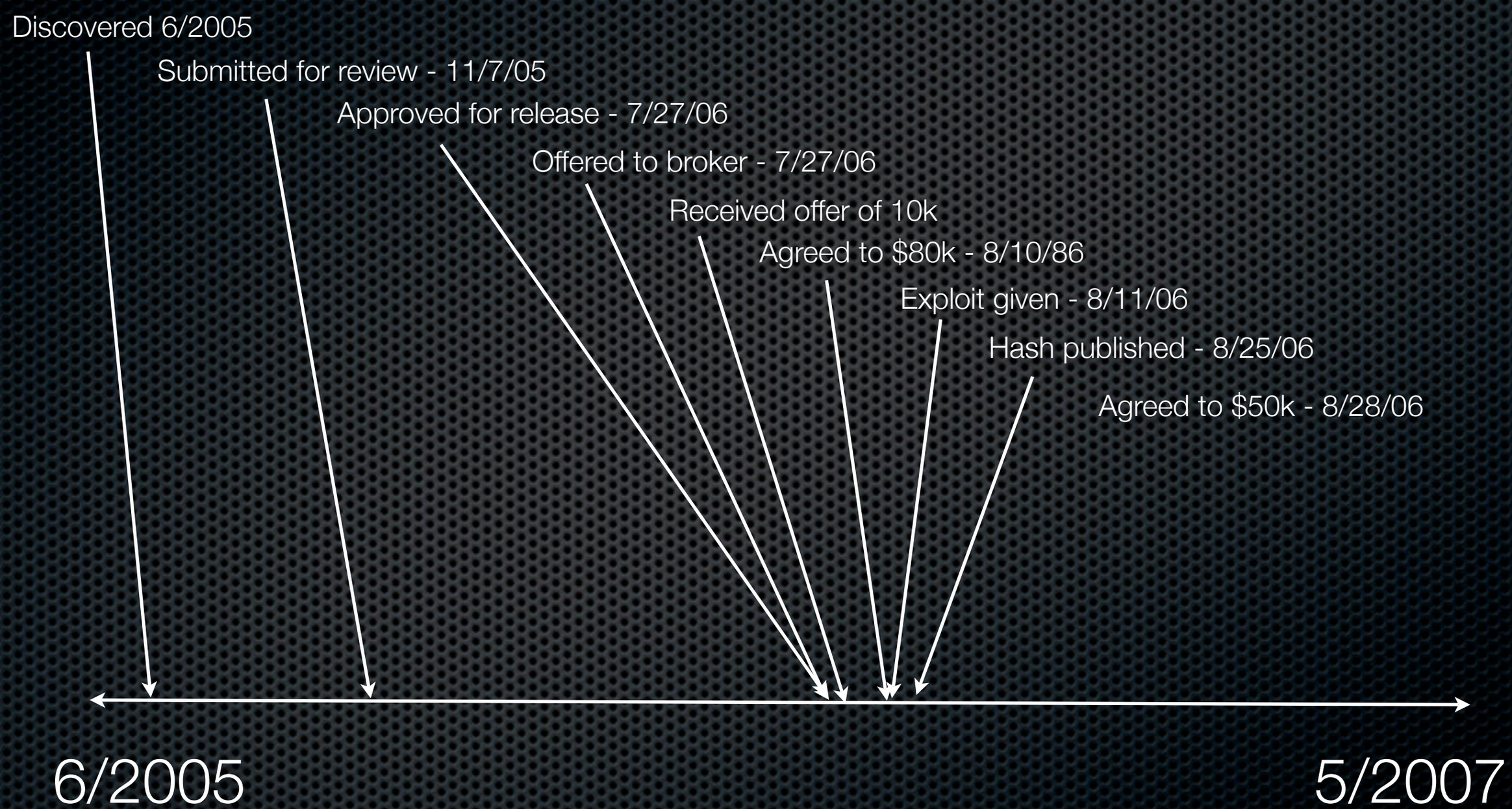
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
6/2005
5/2007

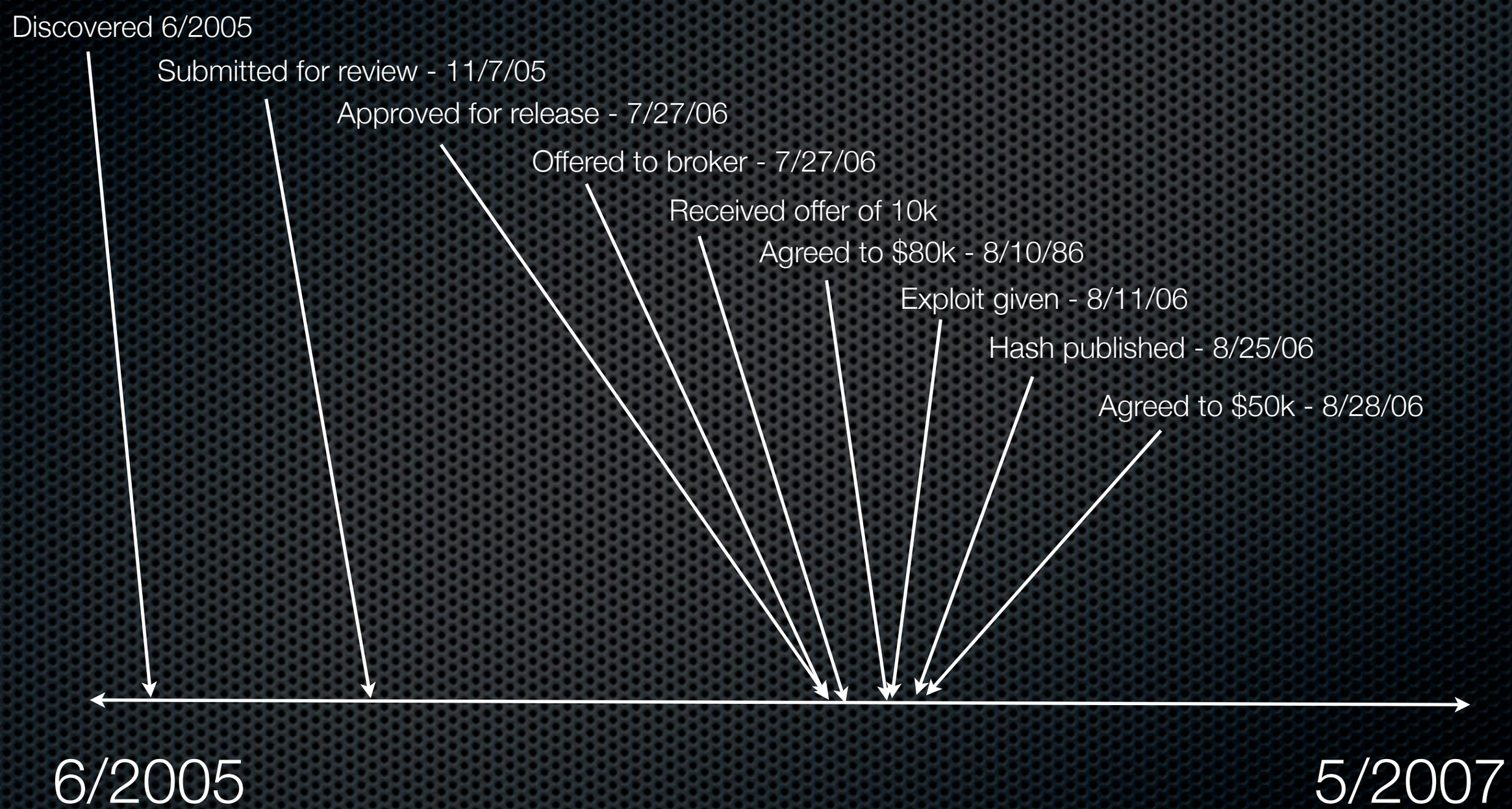
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
6/2005
5/2007

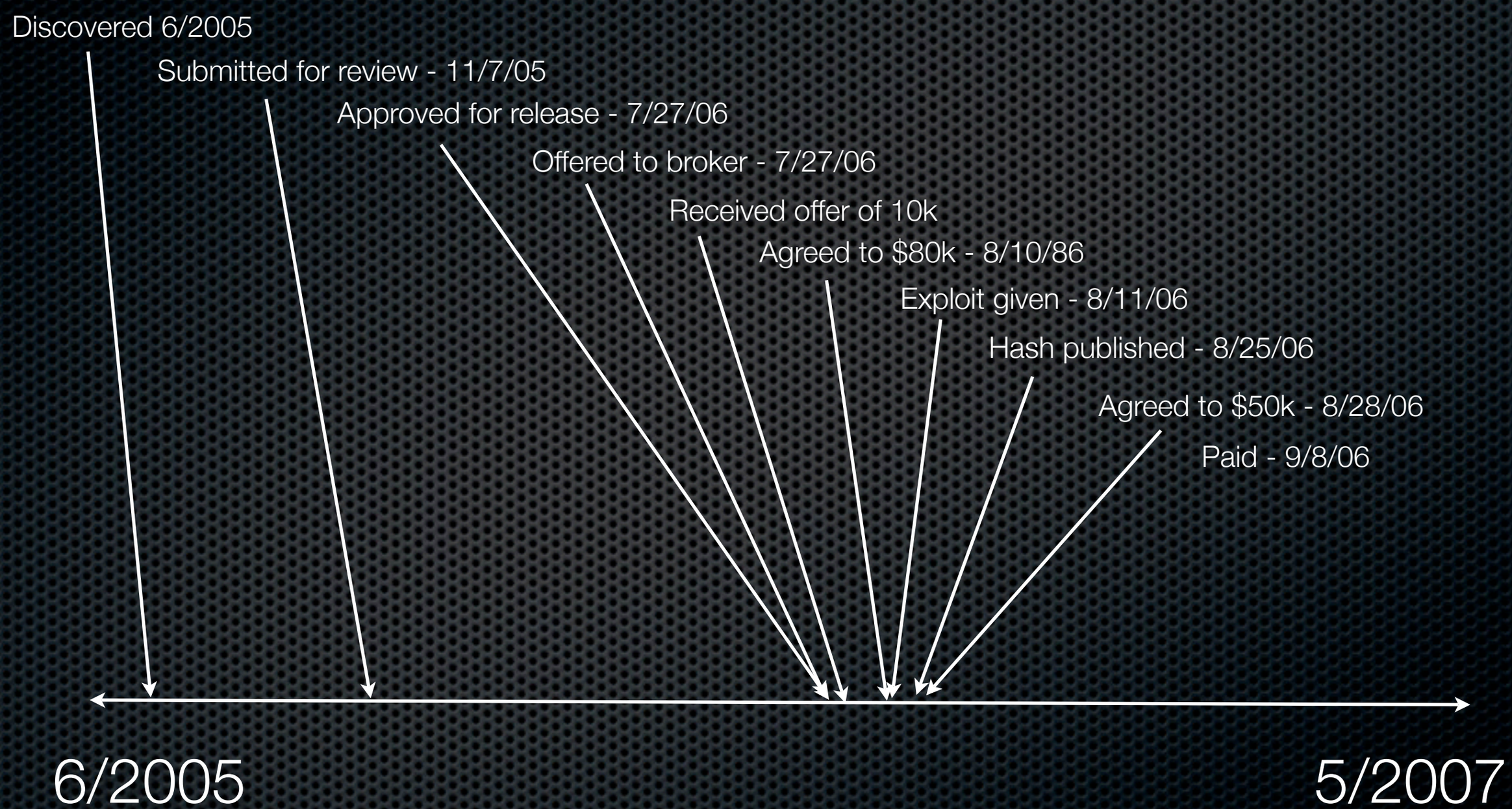
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
Agreed to $50k - 8/28/06
6/2005
5/2007

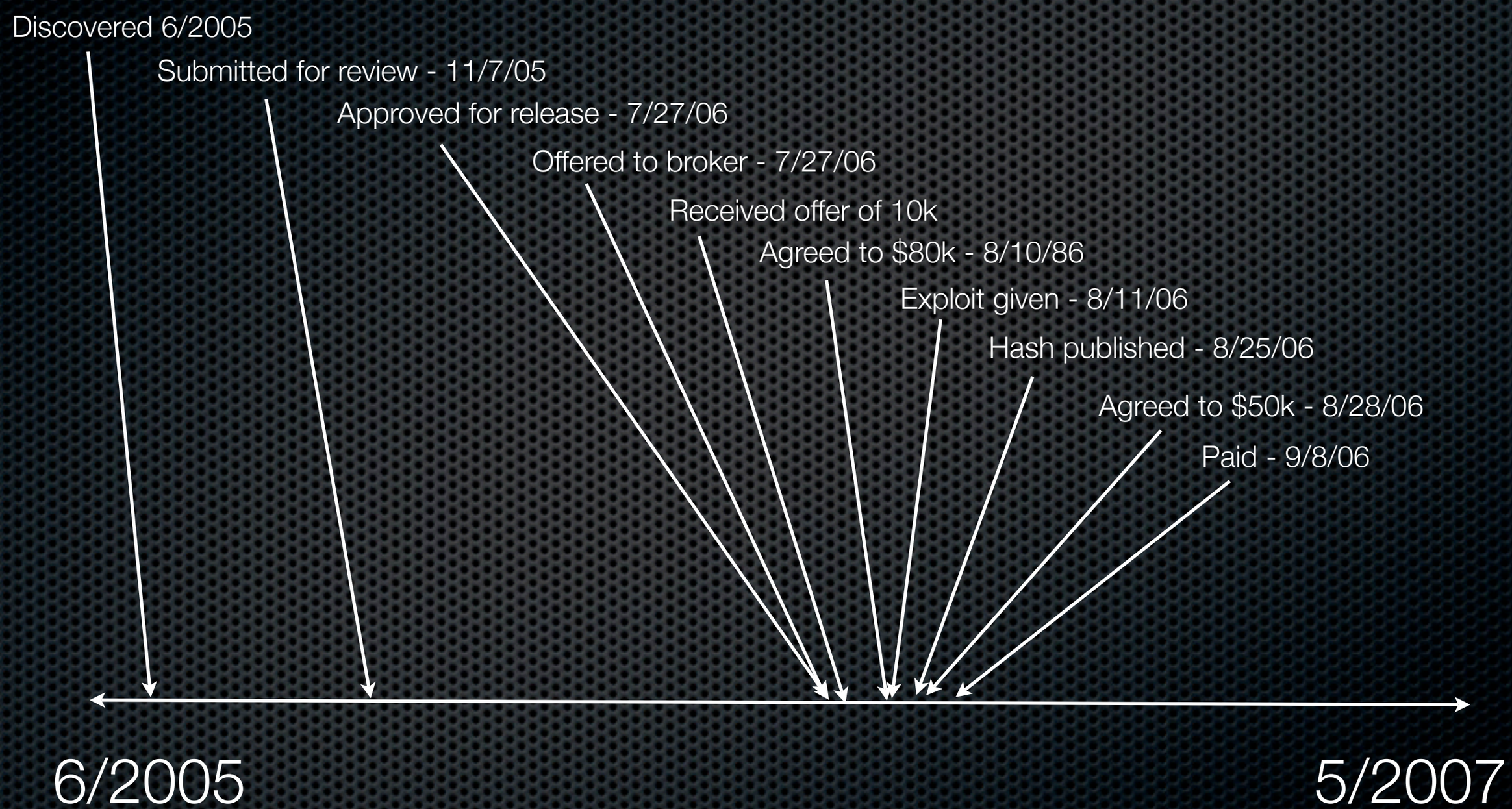
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
Agreed to $50k - 8/28/06
6/2005
5/2007

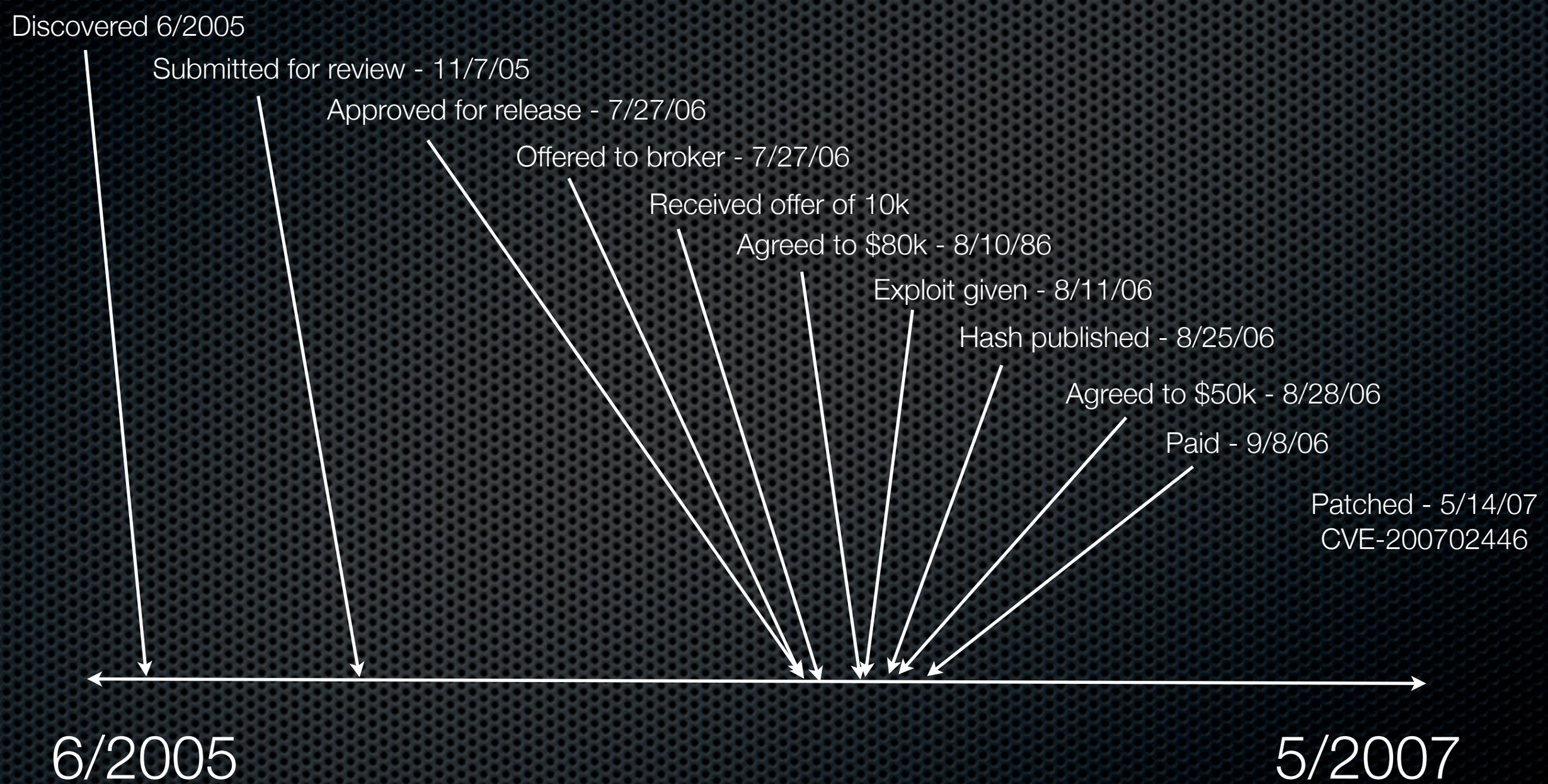
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
Agreed to $50k - 8/28/06
Paid - 9/8/06
6/2005
5/2007

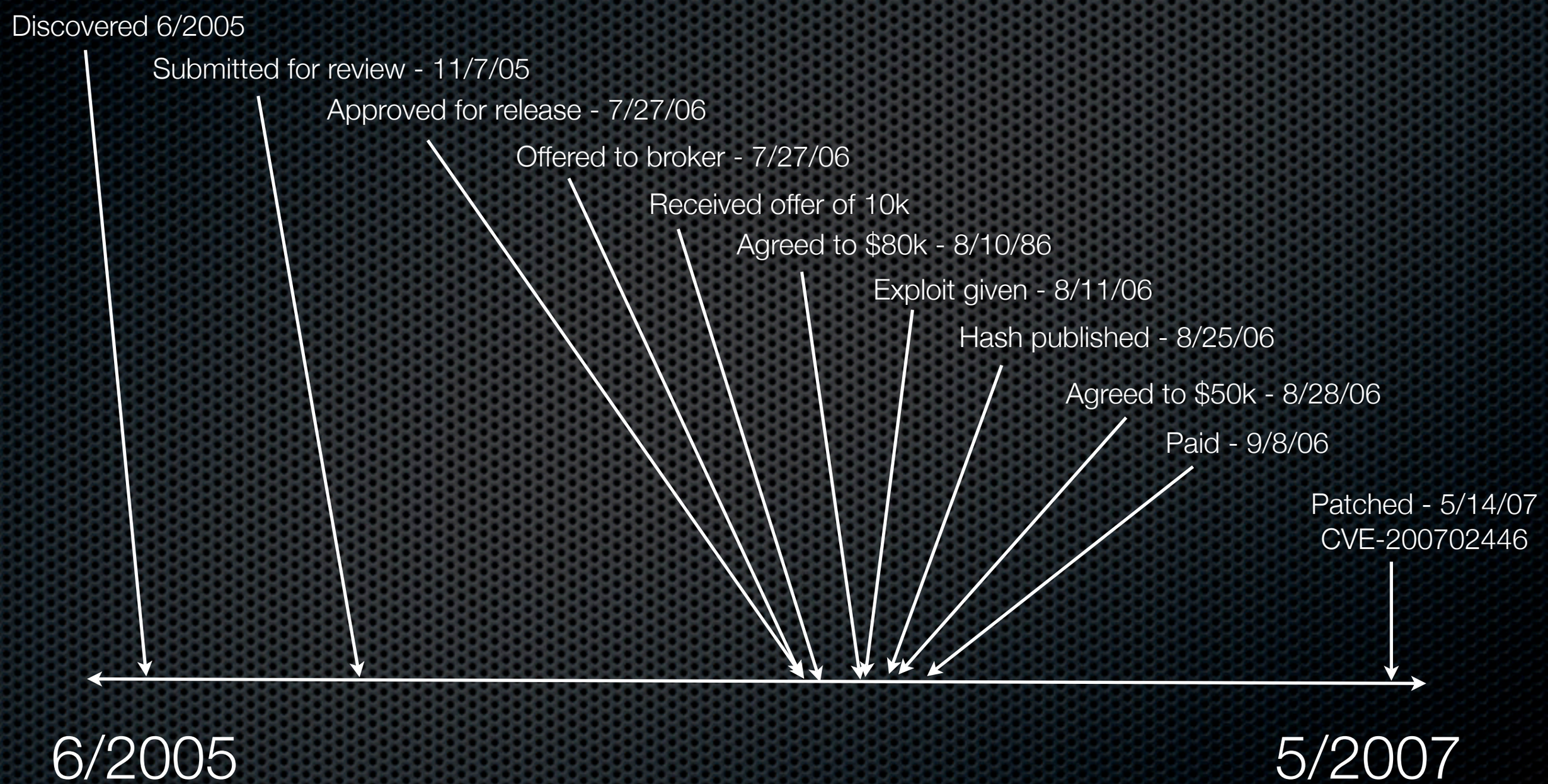
Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
Agreed to $50k - 8/28/06
Paid - 9/8/06
6/2005
5/2007

Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
Agreed to $50k - 8/28/06
Paid - 9/8/06
Patched - 5/14/07
CVE-200702446
6/2005
5/2007

Timeline


Discovered 6/2005
Submitted for review - 11/7/05
Approved for release - 7/27/06
Offered to broker - 7/27/06
Received offer of 10k
Agreed to $80k - 8/10/86
Exploit given - 8/11/06
Hash published - 8/25/06
Agreed to $50k - 8/28/06
Paid - 9/8/06
Patched - 5/14/07
CVE-200702446
6/2005
5/2007

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

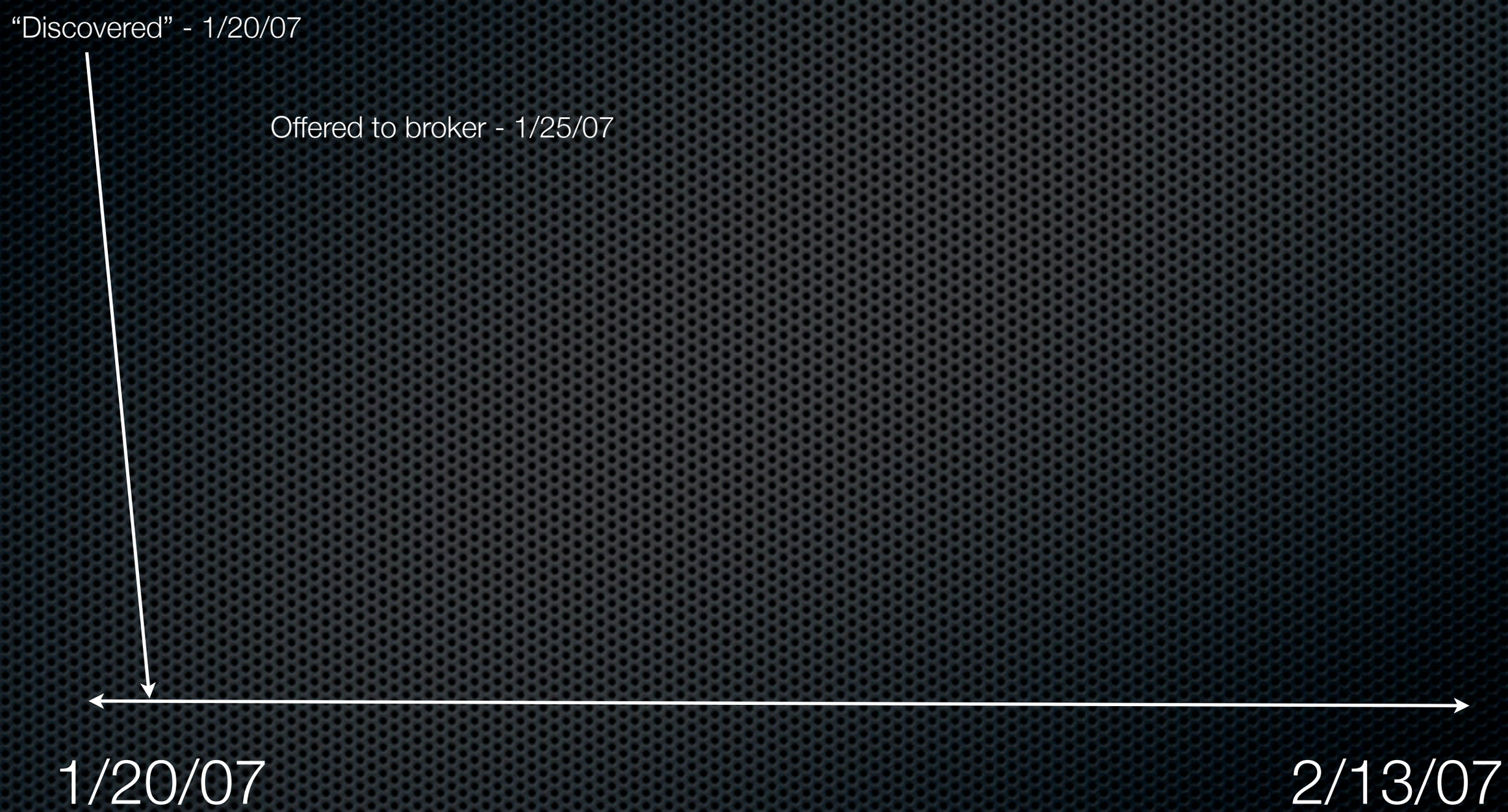
Timeline

“Discovered” - 1/20/07

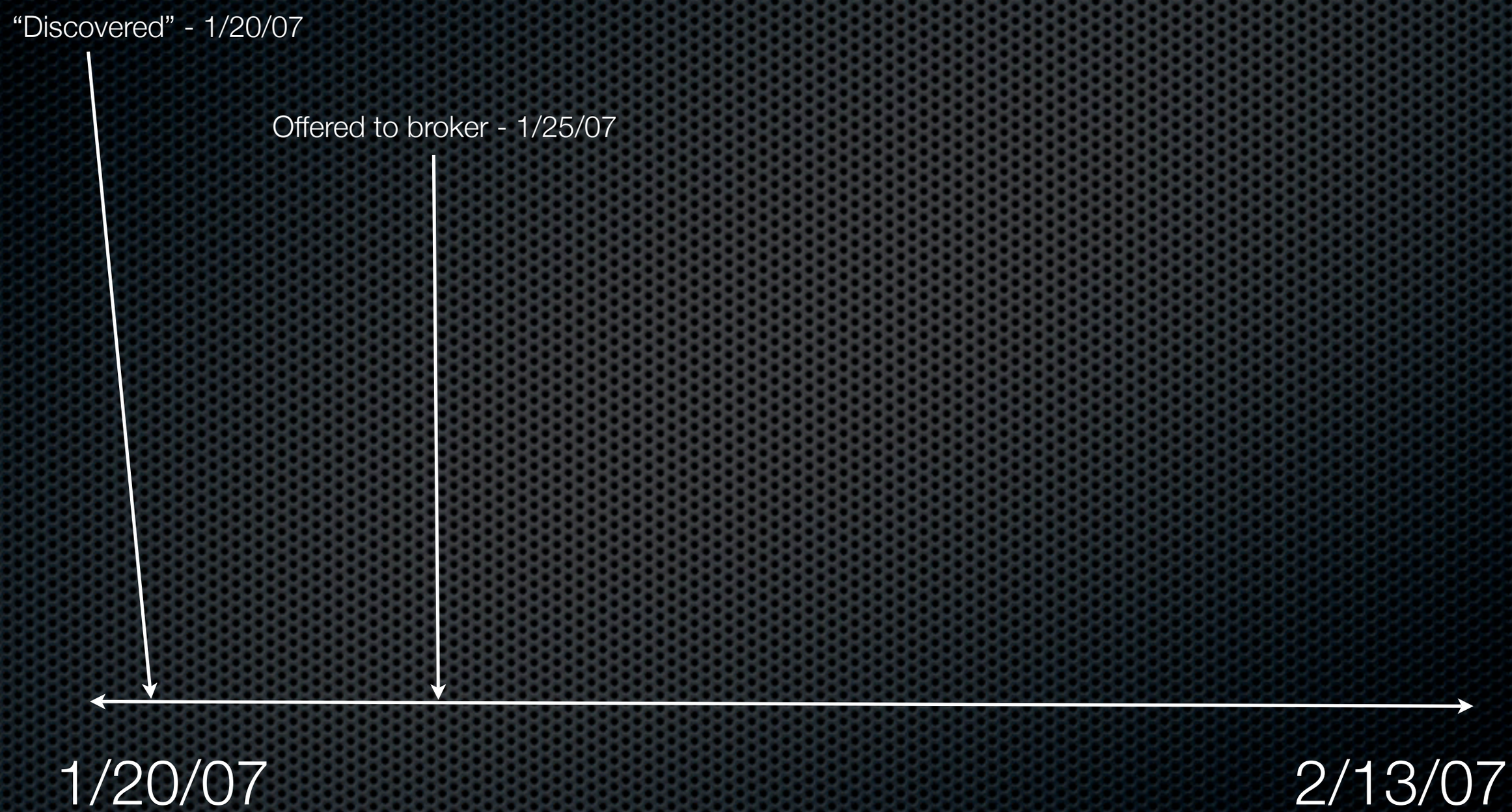
1/20/07 ⟷ 2/13/07

Timeline

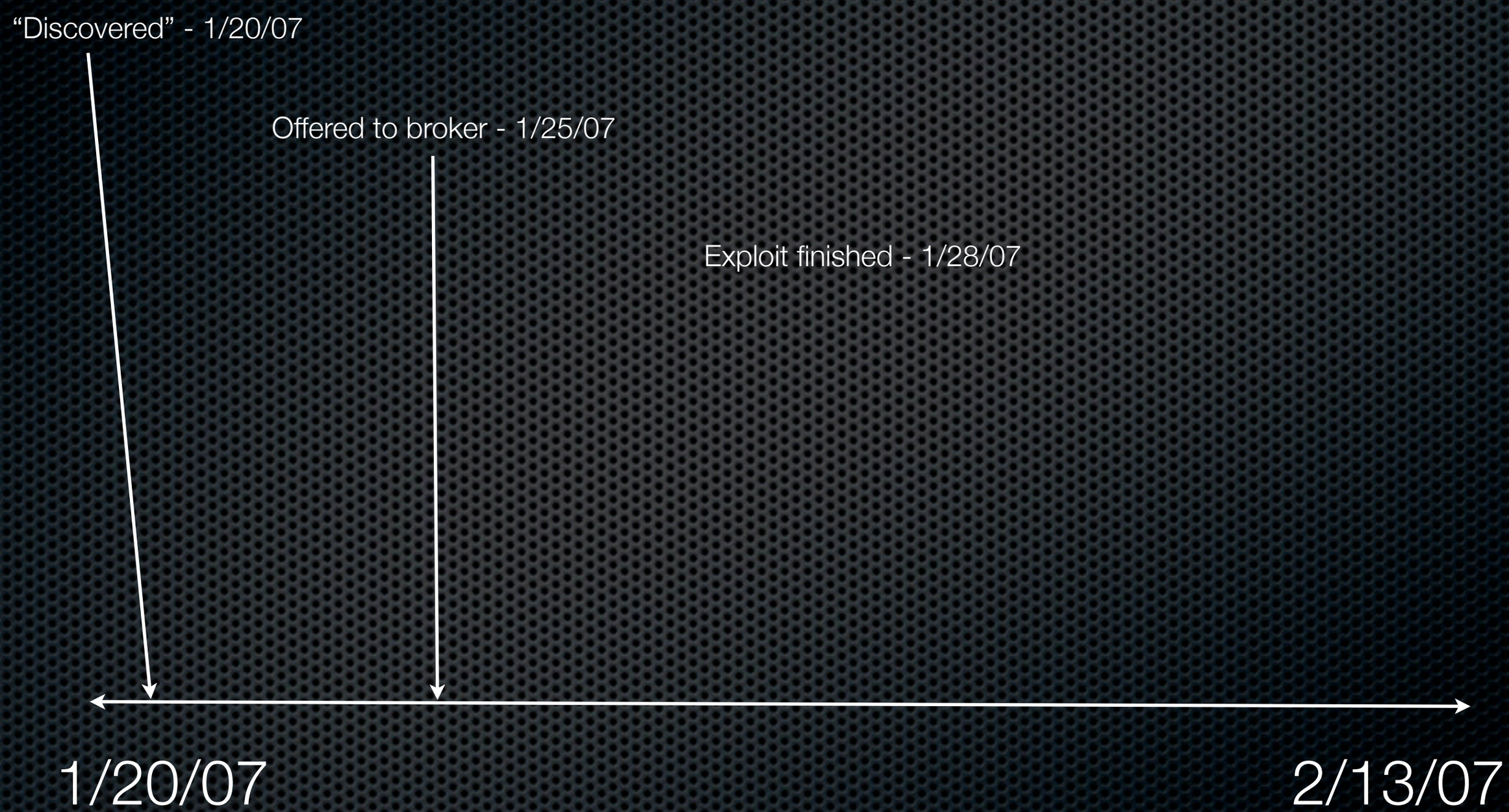
Timeline



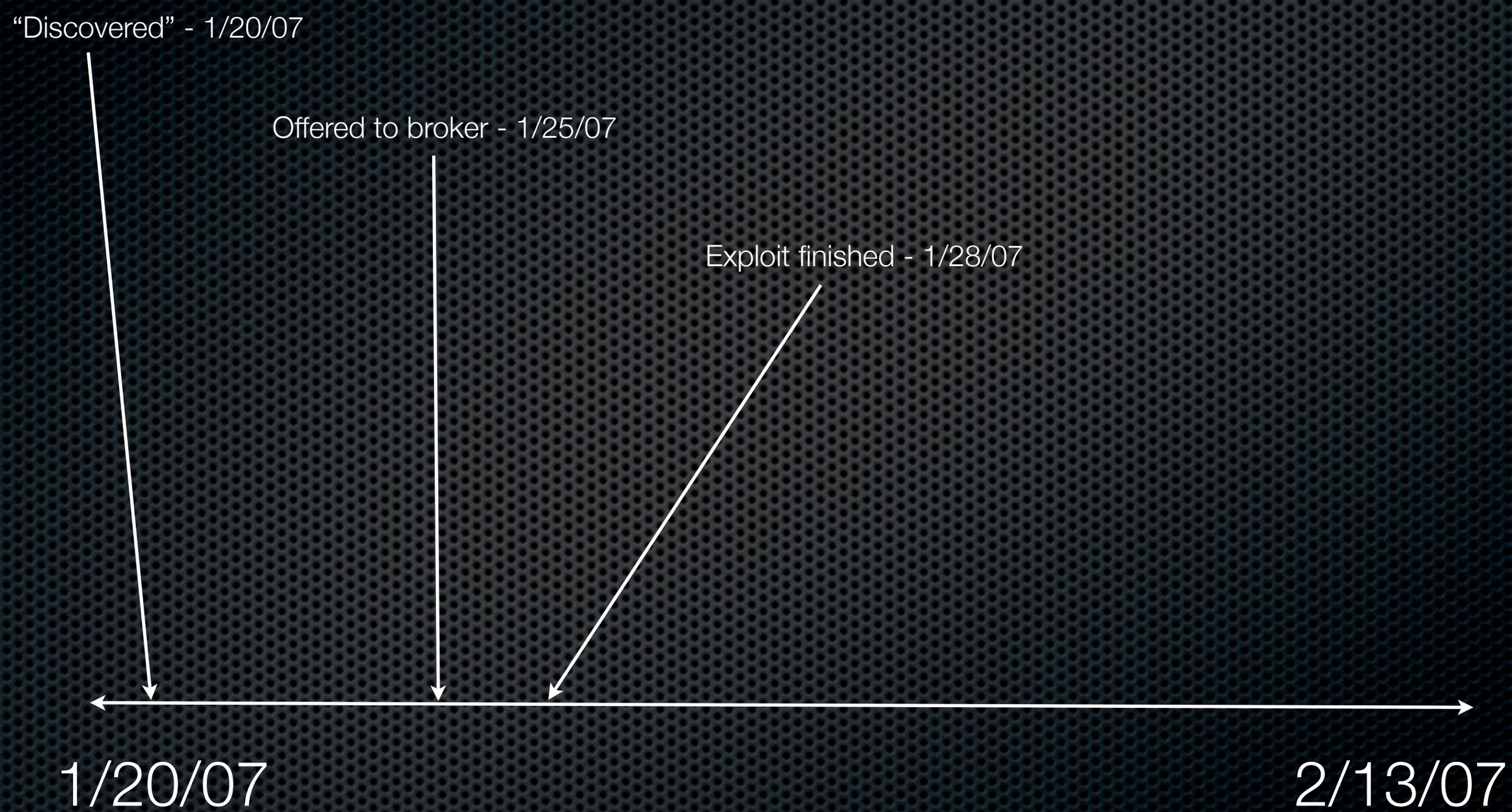
Timeline



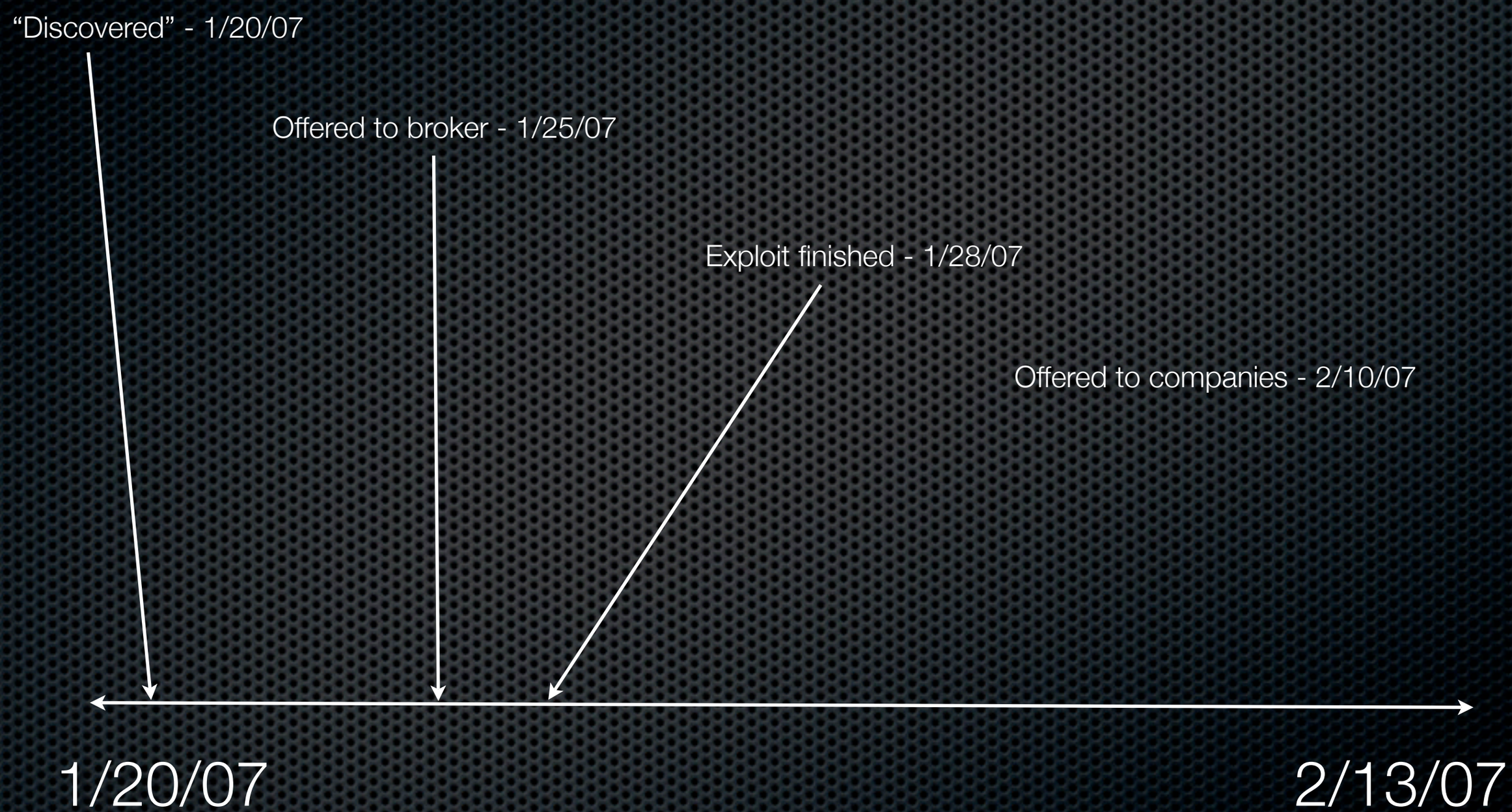
Timeline


"Discovered" - 1/20/07
Offered to broker - 1/25/07
Exploit finished - 1/28/07
1/20/07
2/13/07

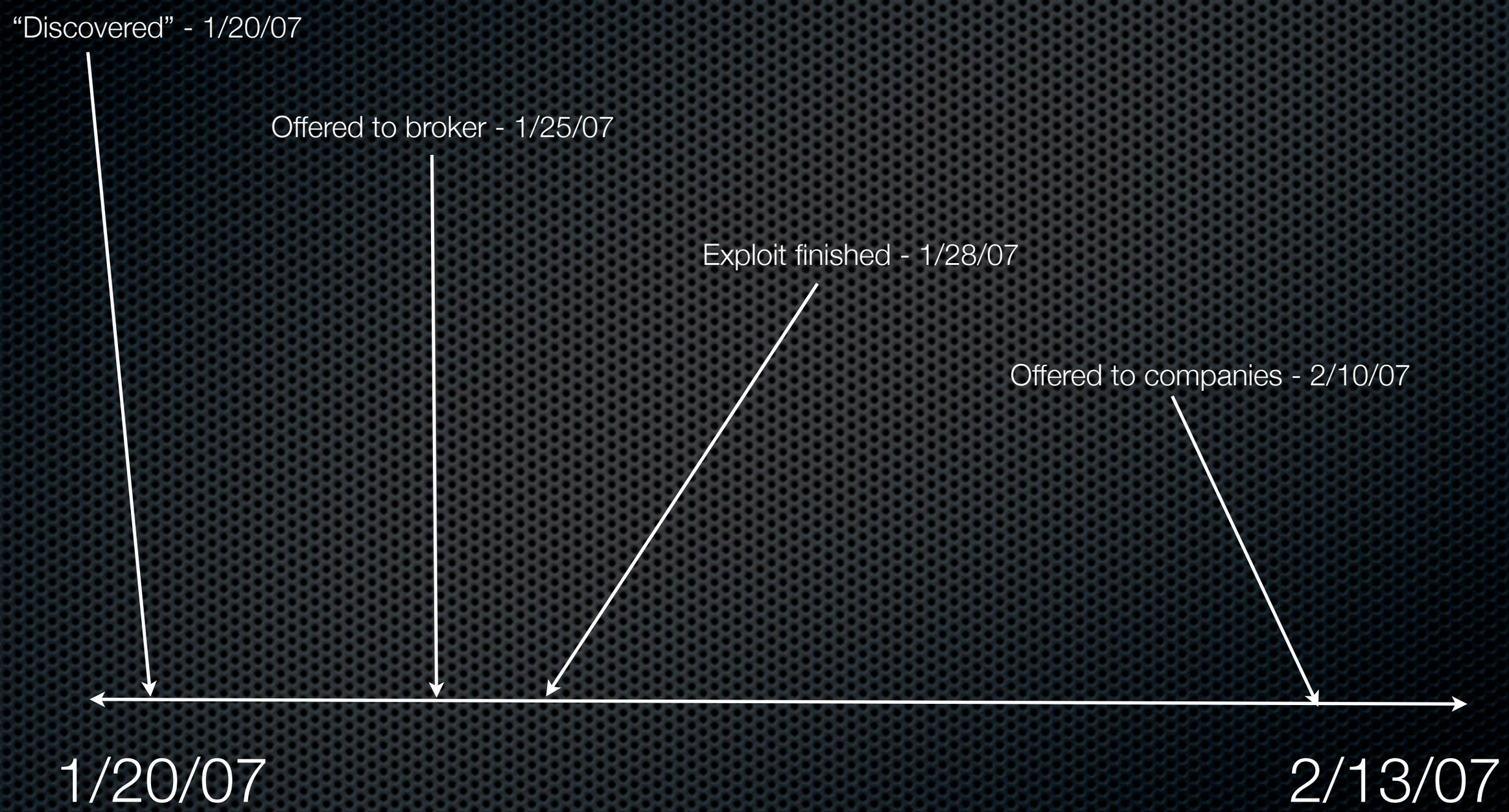
Timeline


"Discovered" - 1/20/07
Offered to broker - 1/25/07
Exploit finished - 1/28/07
1/20/07
2/13/07

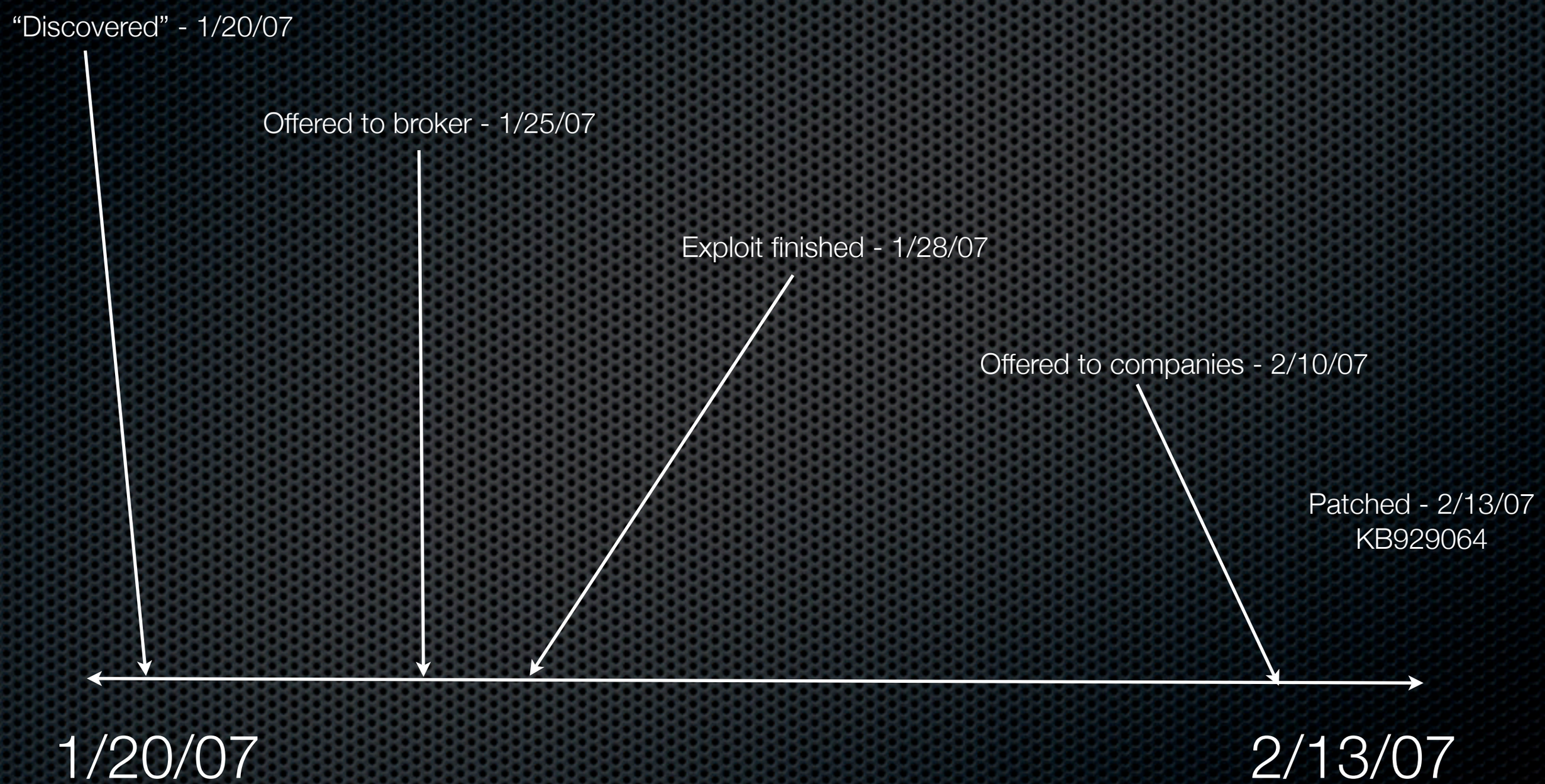
Timeline


"Discovered" - 1/20/07
Offered to broker - 1/25/07
Exploit finished - 1/28/07
Offered to companies - 2/10/07
1/20/07
2/13/07

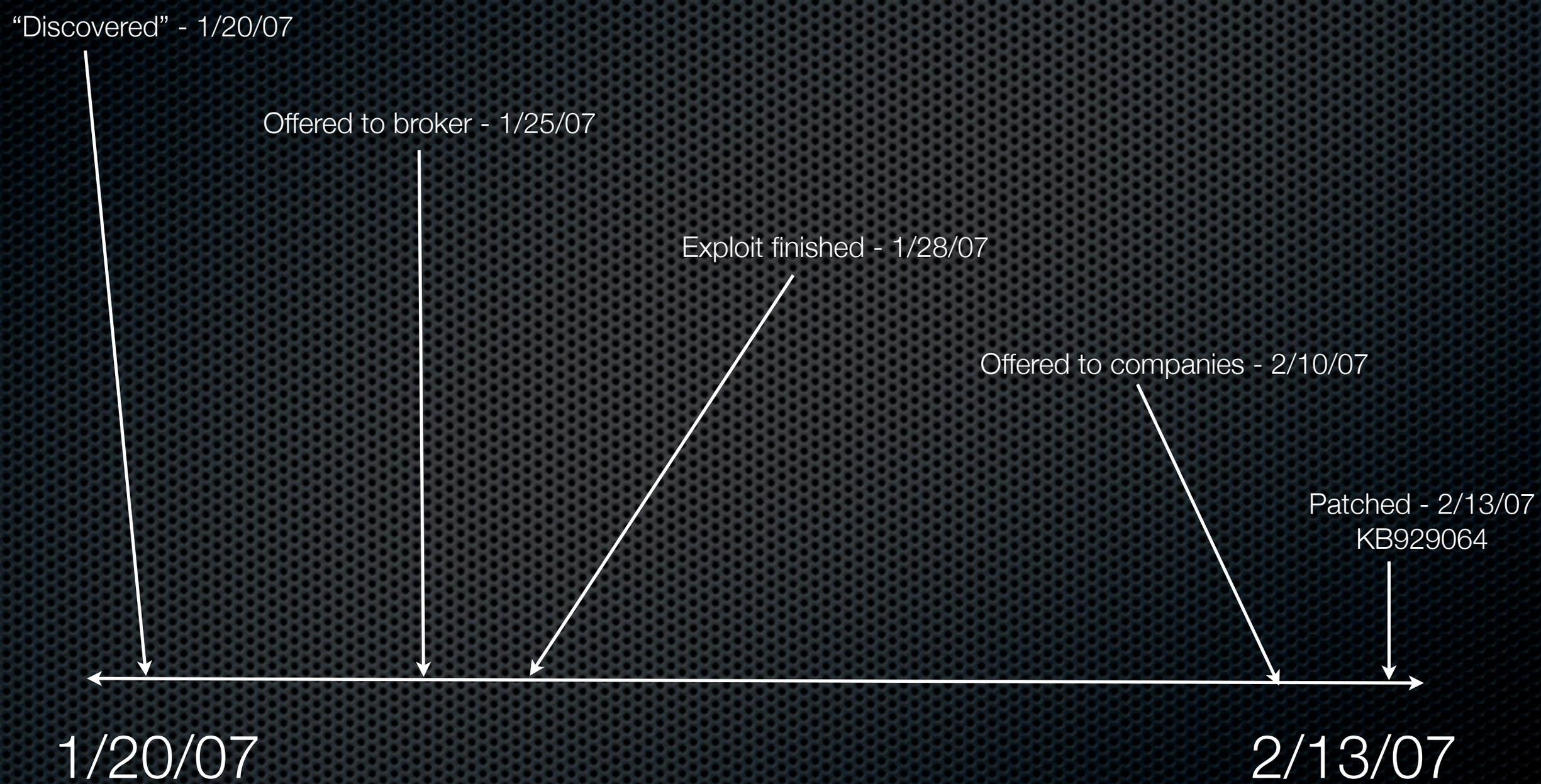
Timeline


"Discovered" - 1/20/07
Offered to broker - 1/25/07
Exploit finished - 1/28/07
Offered to companies - 2/10/07
1/20/07
2/13/07

Timeline


"Discovered" - 1/20/07
Offered to broker - 1/25/07
Exploit finished - 1/28/07
Offered to companies - 2/10/07
Patched - 2/13/07
KB929064
1/20/07
2/13/07

Timeline


"Discovered" - 1/20/07
Offered to broker - 1/25/07
Exploit finished - 1/28/07
Offered to companies - 2/10/07
Patched - 2/13/07
KB929064
1/20/07
2/13/07

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

Conclusions

- No TTP leaves researchers vulnerable to losing their vulnerability information
- Time sensitivity compounds problems
- Some solutions exist but implementation remains far off
- 0-days exist
- vulnerabilities ***are*** rediscovered!
- The implication of “high end” vulnerability sales is that the Internet is a less safe place - *vendors need to pay researchers!*

Final Thoughts

- We need to make responsible disclosure easier and more pleasant
- We need to reward researchers for their work
- The community needs to make it so that responsible disclosure is the preferred method by any measurement
  - Not the method researchers have to make sacrifices to use

Final Final Thought

- Samba story revisited
  - If the anonymous researcher had been offered $80,000 for his Samba bug, instead of (an estimated) $5000 + disclosure, would he have taken it?
- Researchers shouldn’t be put in this position
- Internet security shouldn’t depend on the results of 19 year old Eastern Europeans earning $8000/year making this decision...

Questions?

- Please contact me at: cmiller@securityevaulators.com