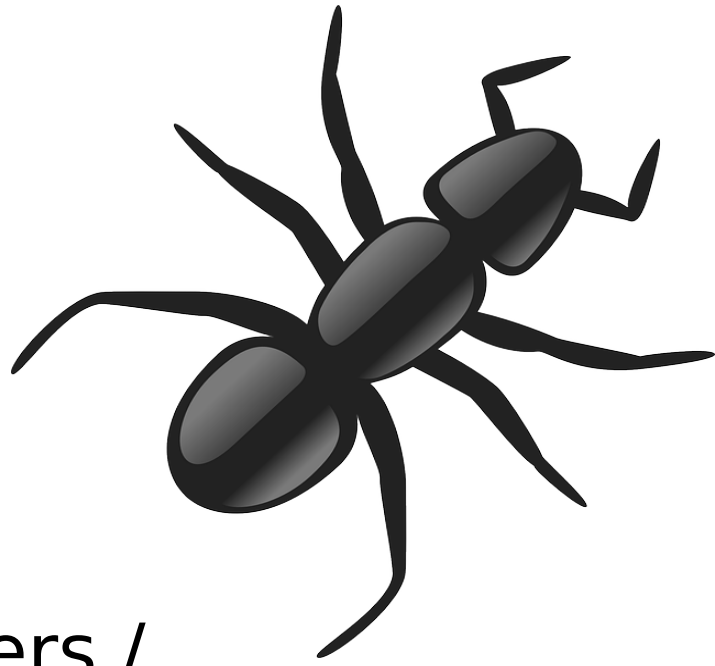
When the Internet Bleeded

Anant Shrivastava
(@anantshri)
for
RootConf 2014

Topic of Discussion

- Various SSL/TLS related issues in public
  - Heartbleed
  - GNUTLS Bug
  - Apple Bug
  - Lucky13
  - BEAST
  - CRIME
- What it means for Developers / Administrators.



Ref : Pixabay.com

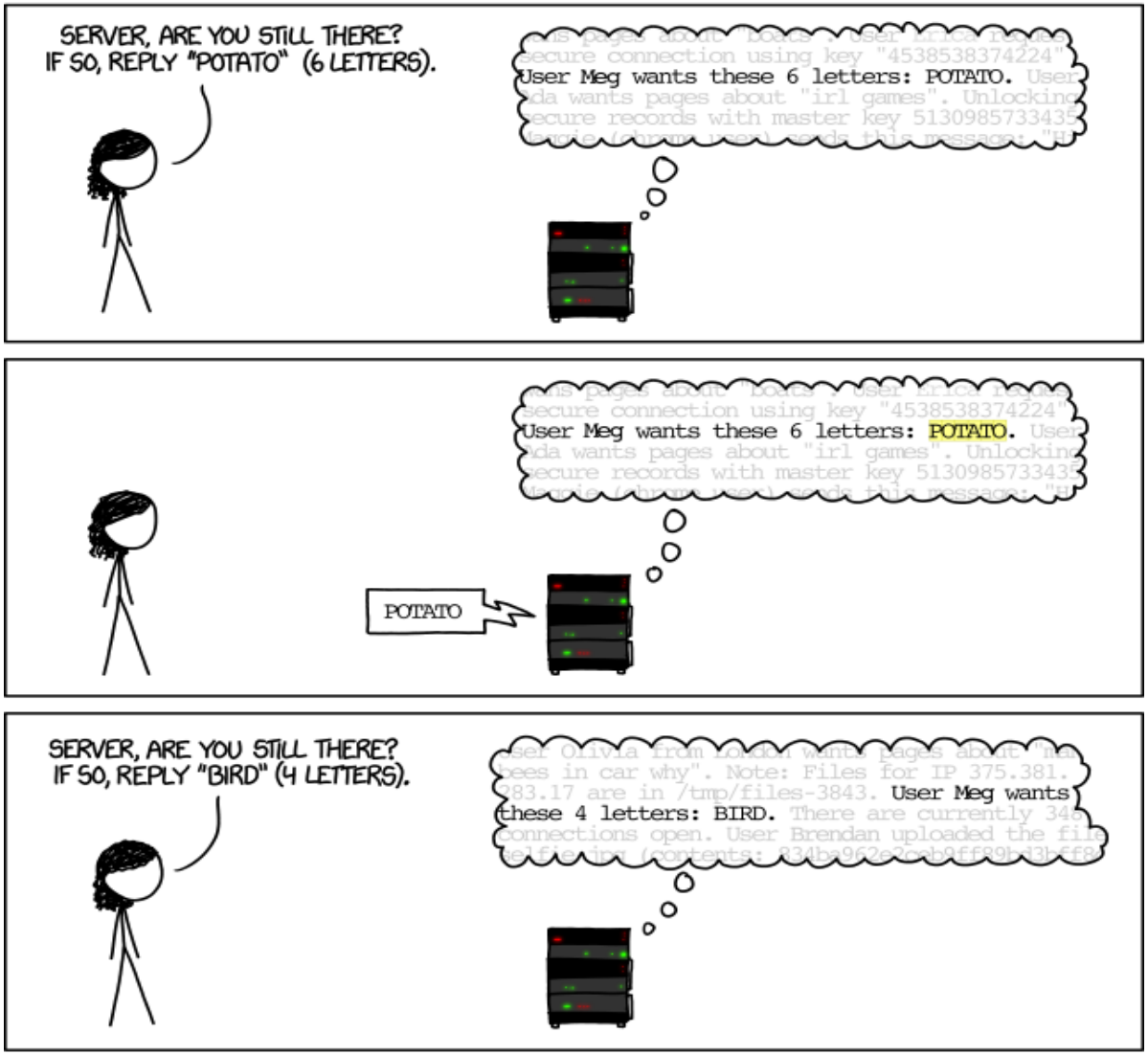
GIST of Security

“Most of the Security protocols are broken“

- SSL == inSecure Socket Layer

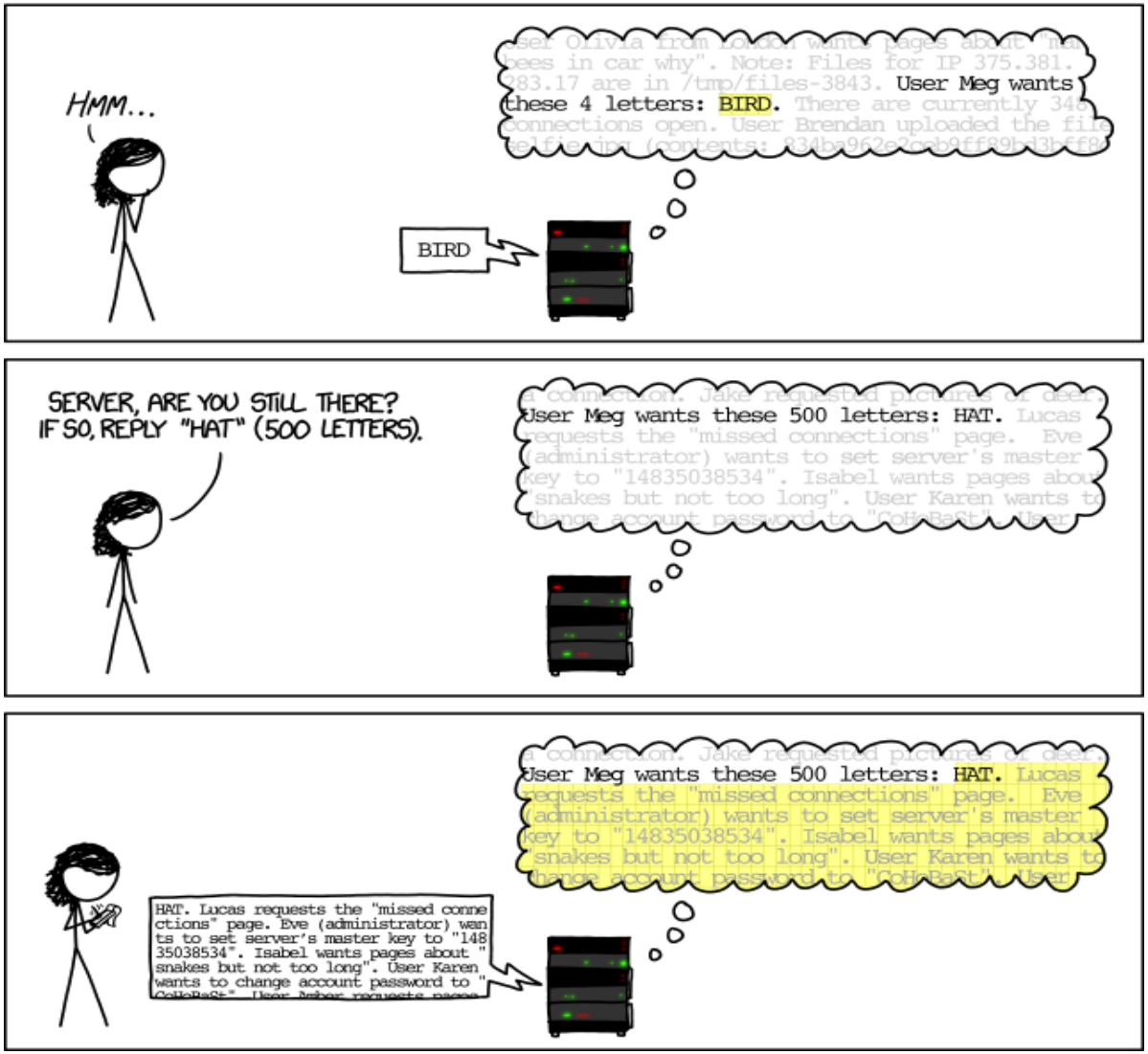
1000 Feet view of TLS / SSL Bugs

HeartBleed (Openssl Bug)



Ref : XKCD.com

HeartBleed (Openssl Bug)



Ref : XKCD.com

GOTO FAIL : GNU TLS / Apple

```
if (result < 0)
  {
    gnutls_assert ();
    goto cleanup;
    goto fail;
  }

result =

if (result < 0)
  {
    gnutls_assert ();
    goto cleanup;
    goto fail;
  }

result =
```

```
. . .
hashOut.data = hashes + SSL_MD5_DIGEST_LEN;
hashOut.length = SSL_SHA1_DIGEST_LEN;
if ((err = SSLFreeBuffer(&hashCtx)) != 0)
    goto fail;
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;  /* MISTAKE! THIS LINE SHOULD NOT BE HERE */
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(...);
. . .
```

- Functions which verifies x509 certificates. Invalid certificates can be passed off as genuine, even though they're invalid.

- GNUTLS Details : http://blog.existentialize.com/the-story-of-the-gnutls-bug.html
- Apple : https://www.imperialviolet.org/2014/02/22/applebug.html
- Test yourself : https://gotofail.com/

BEAST’s LUCKY13 CRIME

- BEAST (CBC Ciphers)
  - Allows retrial of encrypted data by key guess based on block based ciphers.
- CRIME (compressed connection / SPDY)
  - Exploit compression to extract data
- LUCKY13
  - cryptographic timing attack
- RC4
  - (http://blog.cryptographyengineering.com/2013/03/attack-of-week-rc4-is-kind-of-broken-in.html)

Status Quo

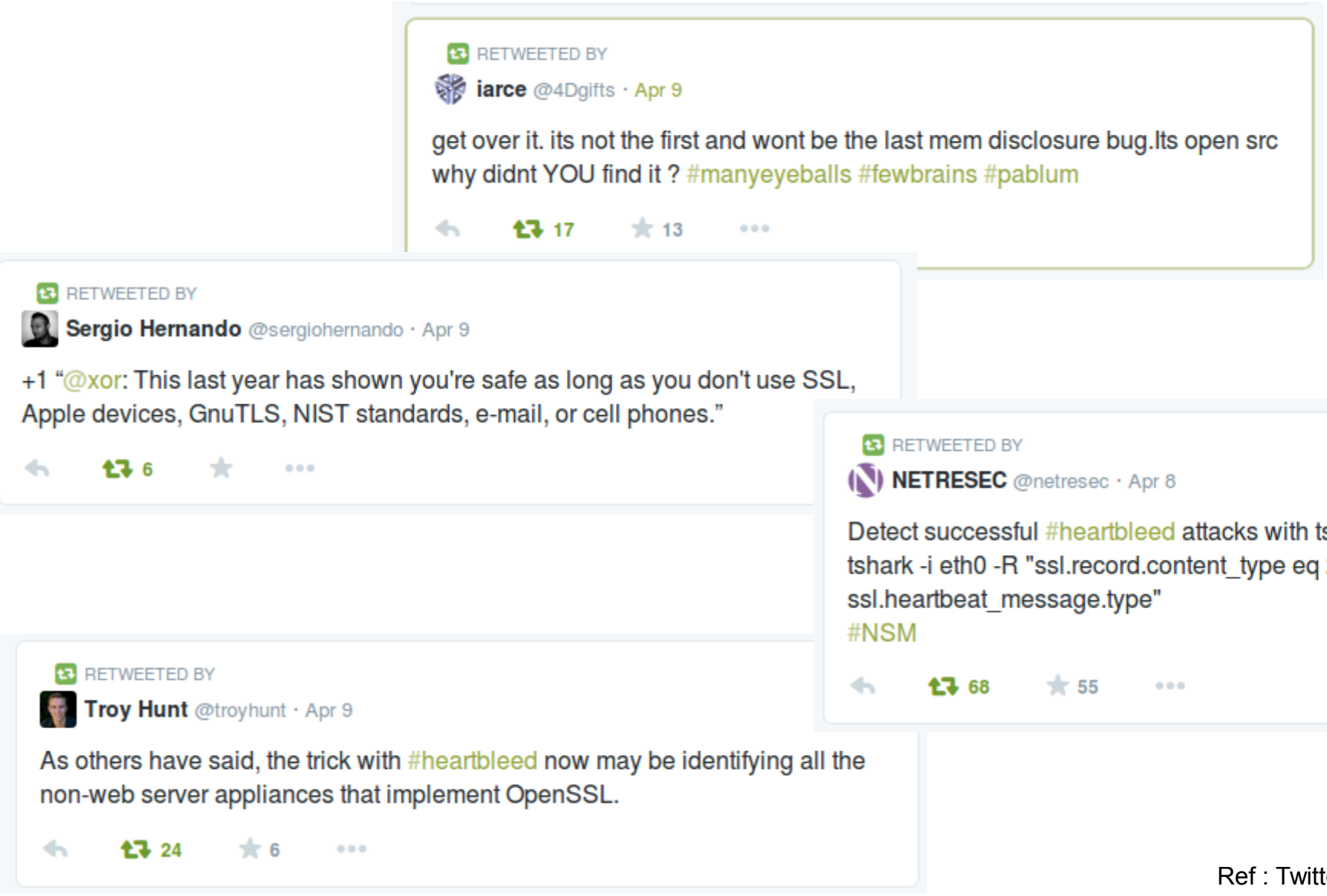
- SSL 3.0 / TLS 1.0 is broken at nearly all algorithm / protection level either reasonable exploits or conceptual exploitation available.

- Catch 22 : If you protect against BEAST you are vulnerable to LUCKY13 and vice-versa

Lets Understand Heartbleed

- Massive Effect over INTERNET but limited to OpenSSL
- Effective Marketing and promotion
- Known not just in Information Security Community but to the world
- In short a lucky draw worth 64KB max of data (data =! information)

Twitter Reactions



Ref : Twitter.com

Reactions

RETWEETED BY

Sergio Hernando @sergiohernando · Apr 10

Heartbleed bug. Let's patch. Wait we can't! We don't have patches for our VPNs, gateways, WAFs, ESX servers. Now what? Ehmmm next question?

17 6

RETWEETED BY

Taylor Hornby @DefuseSec · Apr 8

Fun fact: It costs $24.90 USD to revoke a free certificate from @StartSSL #heartbleed

115 34

RETWEETED BY

Sergio Hernando @sergiohernando · Apr 10

OpenSSL: quite easy to recommend patching, another story is dealing with products that use OpenSSL that we can't patch (vendor dependencies)

RETWEETED BY

Philip @_miw · Apr 9

@troyhunt @bengrubb @anantshri @makash @caseyjohnellis ie: little known fact, Microsoft OCSP takes 24h to mark a revoked cert as revoked.

1

Ref : Twitter.com

DIY

- Server : heartbleed.anantshri.info
  Test Scripts :
- http://heartbleed.anantshri.info/test.txt (Shell)
- http://heartbleed.anantshri.info/hbtest.txt (Python)

- Login Page : https://heartbleed.anantshri.info/login_post.html
- https://heartbleed.anantshri.info/login.html

- Video Demo

Trivia Facts

- First well thought out exploit release where public presentation had prime focus (domain registered 2 days before announcement).
- 3 different sources found same issue within a gap of a week.
- Multiple exploits came out based on initial script which only looked at TLS 1.1 and not of 1.2 and 1.0 hence a lot of the servers were marked safe even when they were not
- Hugely undervalued exploit even by author. Original founder didn't expected the private key disclosure.
- Akamai opensourced its solution for key safety and same was hacked left right center within few hours.

Trivia Facts

- Not a protocol fault rather implementation flaw and hence GNUTLS, Mozilla NSS or Microsoft SSL is not effected.
- 75 of Cisco Products found effected
- Tor among effected products
- OpenSSL 1.0.1 through 1.0.1f
- LibreSSL (stripped down OpenBSD implementation)
- OpenSSL Bugbounty
- According to CloudFlare, GlobalSign's CRL grew from 22KB before Heartbleed to 4.9MB afterward.
- The number of revoked certificates on the CRL increased from 1,492 to 133,243. And that was just GlobalSign's CRL

Reverse Heartbleed : Client Attack

- Script
  - https://github.com/Lekensteyn/pacemaker

So What?

- Administrators
  - Patch meticulously
  - Monitor religiously
  - Co-relate, cross-ref, leverage bigdata identify anomoly and act on it.
- Developers
  - Not just a admin task
  - Start caring about older version of libraries.
  - Do not bundle dependencies or maintain updates
  - OpenSource MORE EYES != LESS SECURITY BUGS

Technical solutions

- Enable TLS 1.1 and 1.2
- Enable forward secrecy
- Change SSL certificate (I know there is a revocation cost)

- Going forward you are secure **till no one finds a flaw in newer** algorithms

Perfect Forward Secrecy

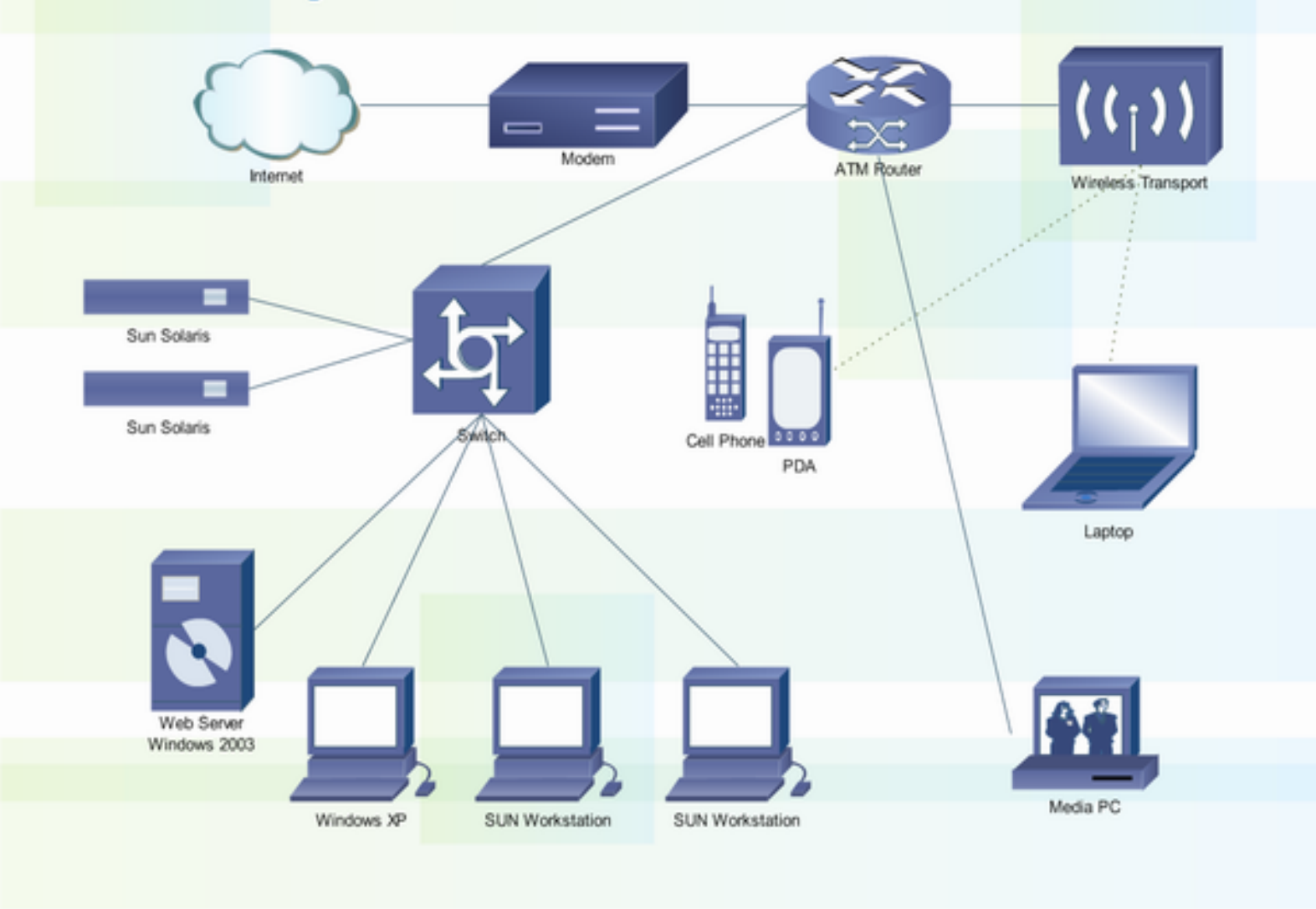
- random public keys per session for the purposes of key agreement with generation using non deterministic algorithm.

- Even if connection is compromised it makes sure compromise affects only one connection.

Policy based solution

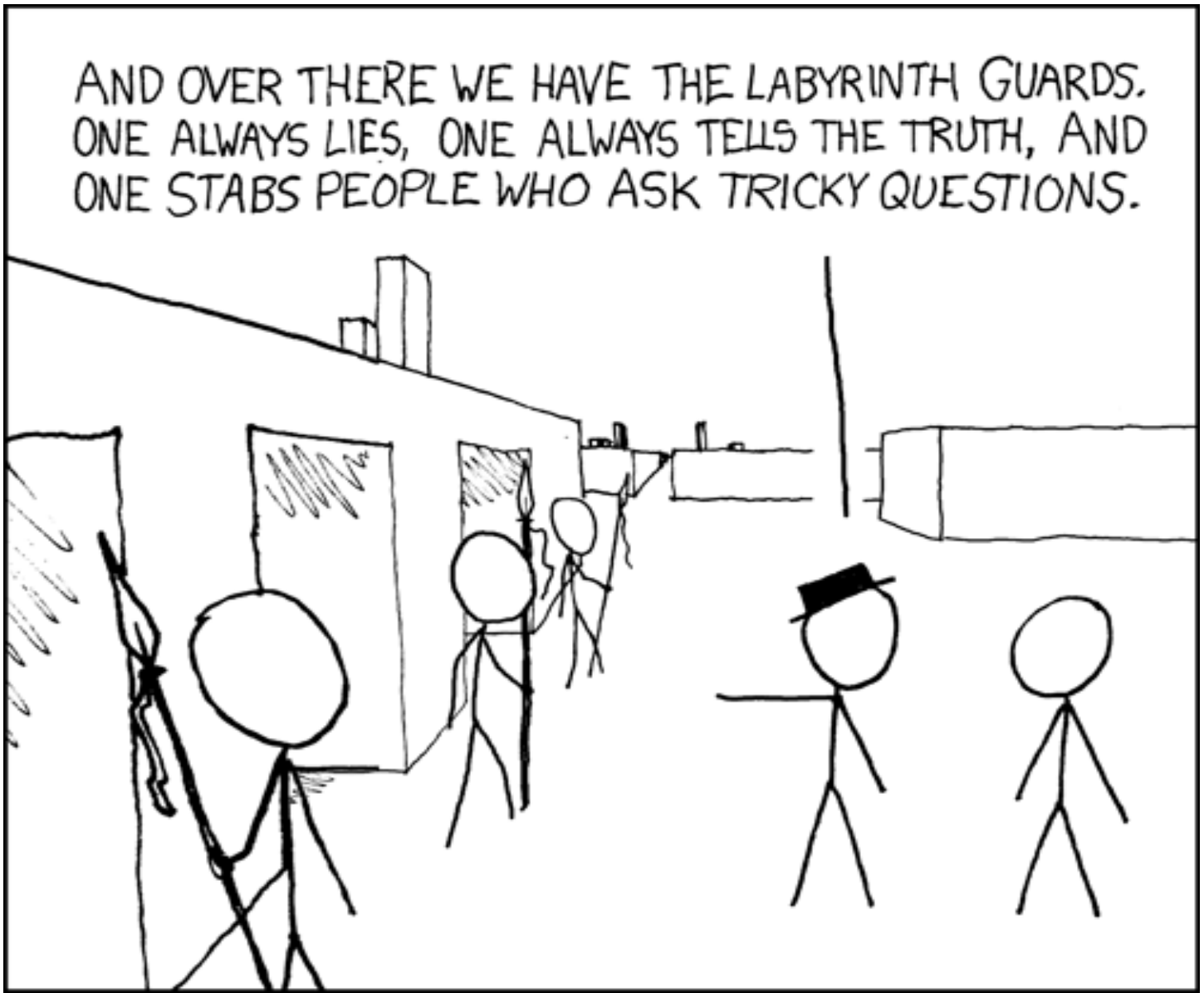
- **Fail hard, Fail early** : Setup exigency process in place :Inform customers if you suspect foul play. Keep them updated. Block login if required.
- **Force password reset** : Don’t inform and ask them to change : force it.
- Don't forget **API Keys and other secrets**
- Keep **hardware** support subscriptions relevant or get lifetime **support** : it helps

Grave scenario



Ref : http://www.edrawsoft.com/images/network/Cisco%20Network%20Diagram_Full.png

Questions?



Ref : XKCD.com

Thanks for Listening

Anant Shrivastava
http://www.anantshri.info
Freelance Consultant / Trainer
RHCE, SANS GWAPT, CEH
Web, Mobile and Linux